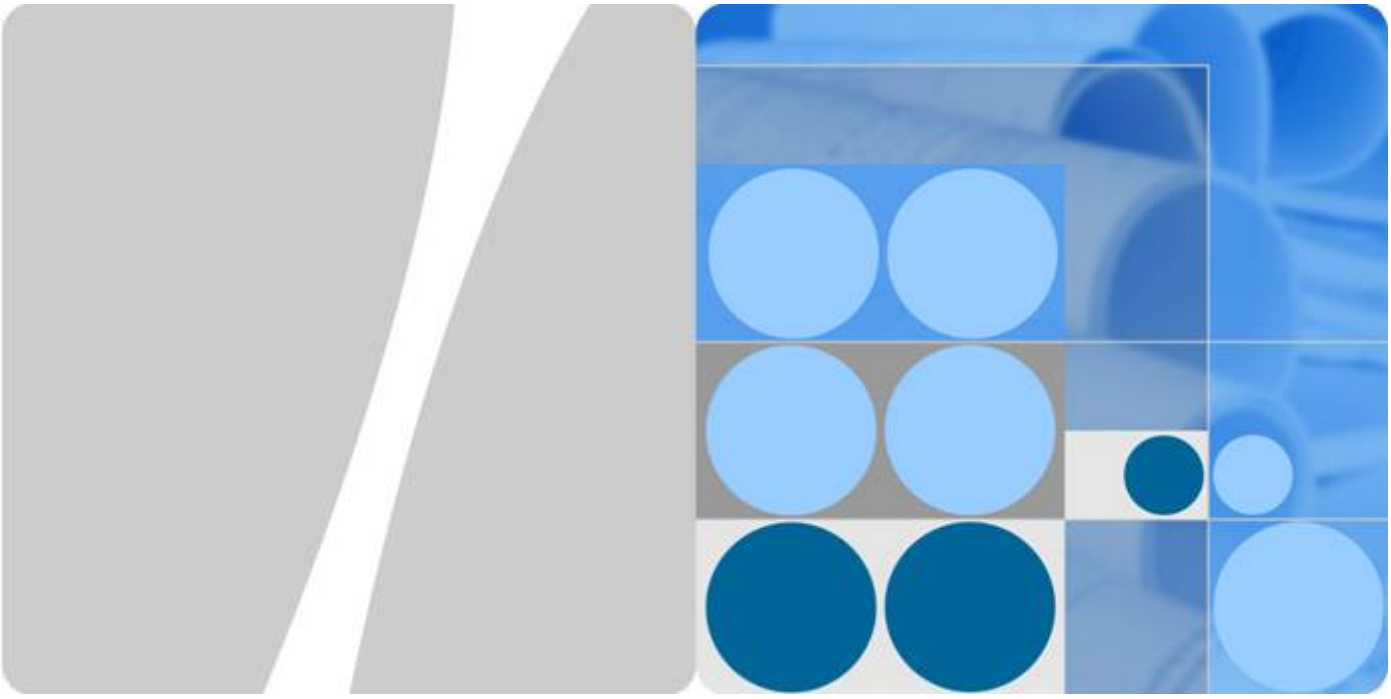
e-DOC 16A8F5D0-e
Proc 13409/2016



S1720&S2700&S5700&S6720 Series Ethernet Switches

V200R009C00

Configuration Guide - Basic Configuration

Issue 03

Date 2016-07-22

HUAWEI TECHNOLOGIES CO., LTD.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Copyright © Huawei Technologies Co., Ltd. 2016. 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: http://www.huawei.com

Email: support@huawei.com

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 describes how to configure the Basic configuration.

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
DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Symbol	Description
NOTE	Calls attention to important information, best practices and tips. 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.

Security Conventions

- Password setting

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

  - To ensure device security, use ciphertext when configuring a password and change the password periodically.
  - The switch considers all passwords starting and ending with %^%#, %#%#, %@%@ or @%@% as ciphertext and decrypts them. If you configure a plaintext password that starts and ends with %^%#, %#%#, %@%@ or @%@%, the switch decrypts it and records it into the configuration file (plaintext passwords are not recorded for the sake of security). Therefore, do not set a password starting and ending with %^%#, %#%#, %@%@ or @%@%.
  - When you configure passwords in ciphertext, different features must use different ciphertext passwords. For example, the ciphertext password set for the AAA feature cannot be used for other features.

- Encryption algorithms

  The switch currently supports the 3DES, AES, RSA, SHA1, SHA2, and MD5 encryption algorithms. 3DES, RSA, and AES are reversible, whereas SHA1, SHA2, and MD5 are irreversible. Using the encryption algorithms DES , 3DES, RSA (RSA-1024 or lower), MD5 (in digital signature scenarios and password encryption), or SHA1 (in digital signature scenarios) is a security risk. If protocols allow, use more secure encryption algorithms, such as AES, RSA (RSA-2048 or higher), SHA2, or HMAC-SHA2.

  An irreversible encryption algorithm must be used for the administrator password. SHA2 is recommended for this purpose.

- Personal data

  Some personal data may be obtained or used during operation and fault location of your purchased products, services, or features. Set up privacy policies and take appropriate measures to protect personal data based on regional privacy laws.

- Mirroring

  The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this document 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.

Disclaimer

This document is designed as a reference for you to configure your devices. Its contents, including web pages, command line input and output, are based on laboratory conditions. It provides instructions for general scenarios, but does not cover all use cases of all product models. The examples given may differ from your use case due to differences in software versions, models, and configuration files. When configuring your advice, alter the configuration depending on your use case.

The specifications provided in this document 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Mappings between Product Software Versions and NMS Versions

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

S1720&S2700&S5700&S6720 Product Software Version	eSight
V200R009C00	V300R006C00

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue 03 (2016-07-22) V200R009C00

This version has the following updates:

Some contents are modified according to updates in the product.

Changes in Issue 02 (2016-03-31) V200R009C00

This version has the following updates:

- **Configuring a Web User and Logging In to the Web System**
- **Clearing the Configuration File**

Changes in Issue 01 (2015-10-23) V200R009C00

Initial commercial release.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Contents

About This Document....ii

1 Basic Features Supported in This Version....1

2 CLI Overview....3

2.1 Entering Command Views....4
2.2 Editing Command Lines....6
2.3 Using Command Line Online Help....7
2.4 Using the undo Command Line....9
2.5 Executing Commands in a Batch....10
2.6 Executing User View Commands in the System View....10
2.7 Using Command Line Shortcut Keys....11
2.8 Displaying Command Line Configurations....12
2.9 Controlling the Display Mode of Commands....13
2.10 Filtering Output Information Based on the Regular Expression....14
2.11 Setting Command Levels....18
2.12 Displaying History Commands....20

3 EasyDeploy Configuration....23

3.1 Introduction to EasyDeploy....24
3.2 EasyDeploy Implementation....25
3.2.1 Concepts....25
3.2.2 Unconfigured Device Deployment Using Option Fields or an Intermediate File....28
3.2.3 Unconfigured Device Deployment Using the Commander....34
3.2.4 Pre-configured Device Deployment Using an Intermediate File....36
3.2.5 Faulty Device Replacement....38
3.2.6 Batch Upgrade....41
3.2.7 Batch Configuration....42
3.3 Configuration Notes....44
3.4 Default Configuration....49
3.5 Deploying Unconfigured Devices Using Option Fields....50
3.5.1 Configuring a File Server....50
3.5.2 Configuring DHCP....51
3.6 Deploying Unconfigured Devices Using an Intermediate File....52
3.6.1 Configuring a File Server....52

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.6.2 Editing an Intermediate File..... 53
3.6.3 Configuring DHCP..... 54
3.7 Deploying Pre-configured Devices Using an Intermediate File..... 55
3.7.1 Configuring a File Server..... 56
3.7.2 Editing an Intermediate File..... 57
3.7.3 Configuring DHCP..... 58
3.7.4 Deploying a Pre-configured Device..... 59
3.8 Deploying Unconfigured Devices Using the Commander..... 60
3.8.1 Configuring a File Server..... 61
3.8.2 Configuring DHCP..... 62
3.8.3 Configuring the Commander..... 63
3.8.4 Checking the Configuration..... 71
3.9 Manually Replacing Faulty Devices Using the Commander..... 72
3.10 Automatically Replacing Faulty Devices Using the Commander..... 73
3.11 Implementing a Batch Upgrade Using the Commander..... 74
3.12 Implementing a Batch Configuration Using the Commander..... 77
3.13 Adding Configured Devices to the Management Domain of the Commander..... 79
3.14 Maintaining EasyDeploy..... 81
3.14.1 Maintaining Client Information..... 81
3.14.2 Checking Power Consumption Information..... 82
3.15 Configuration Examples..... 82
3.15.1 Example for Deploying Unconfigured Devices Using Option Fields..... 83
3.15.2 Example for Deploying Unconfigured Devices Using an Intermediate File..... 85
3.15.3 Example for Deploying Unconfigured Devices Using the Commander (with Network Topology Collection Disabled)..... 89
3.15.4 Example for Deploying Unconfigured Devices Using the Commander (with Network Topology Collection Enabled)..... 94
3.15.5 Example for Manually Replacing Faulty Devices Using the Commander..... 100
3.15.6 Example for Implementing a Batch Upgrade Using the Commander..... 103
3.15.7 Example for Implementing a Batch Configuration Using the Commander..... 108
3.15.8 Example of Adding Configured Devices to the Management Domain of the Commander..... 109
3.15.9 Example for Implementing Topology-based Zero Touch provisioning for the Campus Headquarters..... 112
3.15.10 Example for Implementing MAC/ESN-based Zero Touch Provisioning..... 120
3.16 Reference..... 124
4 USB-based Deployment Configuration..... 125
4.1 USB-based Deployment Overview..... 126
4.2 Principles..... 126
4.3 Configuration Notes..... 131
4.4 Making an Index File..... 134
4.5 Configuring USB-based Deployment..... 144
4.6 Configuration Examples..... 147
4.6.1 Example for Configuring USB-based Deployment (Using a smart_config.ini Index File)..... 147
4.6.2 Example for Configuring USB-based Deployment (Using an Index File usbload_config.txt)..... 149

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

5 Logging In to a Device for the First Time.....151
5.1 First Login Overview.....152
5.2 Logging In to a Device.....152
5.2.1 Logging In to a Device for the First Time Through a Console Port.....152
5.2.2 Logging In to a Device for the First Time Through a Mini USB Port.....155
5.2.3 Logging In to the Device Through the Web System for the First Time (S1720GFR).....159
5.2.4 Logging In to the Device Through the Web System for the First Time (Switches Excluding the S1720GFR).....162
5.3 Basic Configuration on the Device at First Login.....167
5.4 Logging In to a Device for the First Time Configuration Example.....171
5.4.1 Example for Performing Basic Configuration on the Device at First Login Through the Console Port.....171
6 CLI Login Configuration.....174
6.1 CLI Login Method Overview.....175
6.2 User Interface Overview.....177
6.3 Configuring Login Through a Console Port.....180
6.3.1 (Optional) Configuring Attributes for the Console User Interface.....180
6.3.2 Configuring an Authentication Mode for the Console User Interface.....182
6.3.3 Configuring a User Level for the Console User Interface.....184
6.3.4 Logging In to a Device Through the Console Port.....186
6.4 Configuring Login Through the Mini USB Port.....188
6.4.1 (Optional) Configuring Attributes for the Console User Interface.....189
6.4.2 Configuring an Authentication Mode for the Console User Interface.....191
6.4.3 Configuring a User Level for the Console User Interface.....193
6.4.4 Logging In to a Device Through the Mini USB Port.....194
6.5 Configuring Telnet Login.....197
6.5.1 (Optional) Configuring Attributes for a VTY User Interface.....197
6.5.2 Configuring an Authentication Mode for a VTY User Interface.....198
6.5.3 Configuring a User Level for a VTY User Interface.....201
6.5.4 Enabling the Telnet Server Function.....202
6.5.5 Logging In to a Device Through Telnet.....204
6.5.6 (Optional) Using Telnet to Log In to Another Device From the Local Device.....205
6.6 Configuring STelnet Login.....206
6.6.1 (Optional) Configuring Attributes for a VTY User Interface.....206
6.6.2 Configuring an Authentication Mode for a VTY User Interface.....208
6.6.3 Configuring a User Level for a VTY User Interface.....209
6.6.4 Configuring an SSH User.....210
6.6.5 Enabling the SSH Server Function.....213
6.6.6 Logging In to a Device Through STelnet.....215
6.6.7 (Optional) Using STelnet to Log In to Another Device From the Local Device.....217
6.7 Common Operations After Login.....221
6.8 CLI Login Configuration Examples.....223
6.8.1 Example for Configuring Login Through a Console Port.....223
6.8.2 Example for Configuring Telnet Login.....227

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

6.8.3 Example for Configuring a Security Policy to Limit Telnet Login....229
6.8.4 Example for Configuring STelnet Login....231
6.8.5 Example for Configuring the Device as the Telnet Client to Log In to Another Device....234
6.8.6 Example for Configuring the Device as the STelnet Client to Log In to Another Device....236
6.9 CLI Login Common Misconfigurations....241
6.9.1 Failing to Log In Through the Console Port....241
6.9.2 Failing to Log In Through Telnet....242
6.9.3 Failing to Log In Through STelnet....243
6.10 FAQ....244
6.10.1 What Is the Default Login Password?....244
6.10.2 What If I Forget the Password for Console Port Login?....245
6.10.3 What If I Forget the Password for Telnet Login?....246
6.10.4 How Do I Configure Screen Display?....247
7 Web System Login Configuration....248
7.1 Overview....249
7.2 Web System Login Configuration Tasks....250
7.3 Web System Login Default Configuration....251
7.4 Configuring Device Login Through the Web System (Simple Mode)....252
7.4.1 Uploading and Loading a Web Page File....252
7.4.2 Enabling the HTTPS Service....253
7.4.3 Configuring a Web User and Logging In to the Web System....254
7.4.4 Checking the Configuration of Configuring Device Login Through the Web System (Simple Mode)....259
7.5 Configuring Device Login Through the Web System (Secure Mode)....259
7.5.1 Uploading and Loading a Web Page File....259
7.5.2 Configuring an SSL Policy and Loading a Digital Certificate....260
7.5.3 Enabling the HTTPS Service....263
7.5.4 Configuring a Web User and Logging In to the Web System....264
7.5.5 Checking the Configuration of Configuring Device Login Through the Web System (Secure Mode)....269
7.6 Configuring Access Control on Web Users....269
7.7 Web System Login Configuration Examples....271
7.7.1 Example for Configuring Device Login Through the Web System (Secure Mode)....271
7.8 Web System Login Common Misconfigurations....276
7.8.1 Web System Login Failure....276
7.9 FAQ....277
7.9.1 How Do I Obtain the Web Page File?....277
7.9.2 Why Only a Few Options Are Available on the Web System?....278
7.9.3 How Do I Change the Password for Web Login?....278
7.9.4 What Is the Difference Between Web and HTTP?....278
8 File Management....279
8.1 File System Overview....280
8.2 File Management Modes....281
8.3 Local File Management....285

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

8.3.1 Logging In to the Device to Manage Files.... 286
8.3.2 Managing Files When the Device Functions as an FTP Server.... 289
8.3.3 Managing Files When the Device Functions as an SFTP Server.... 296
8.3.4 Managing Files When the Device Functions as an SCP Server.... 307
8.3.5 Managing Files When the Device Functions as an FTPS Server.... 316
8.4 File Management on Other Devices.... 323
8.4.1 Managing Files When the Device Functions as a TFTP Client.... 323
8.4.2 Managing Files When the Device Functions as an FTP Client.... 327
8.4.3 Managing Files When the Device Functions as an SFTP Client.... 332
8.4.4 Managing Files When the Device Functions as an SCP Client.... 339
8.4.5 Managing Files When the Device Functions as an FTPS Client.... 344
8.5 File Management Configuration Examples.... 351
8.5.1 Example of Logging In to the Device to Manage Files.... 351
8.5.2 Example for Configuring the FTP Server.... 352
8.5.3 Example for Configuring the SFTP Server.... 355
8.5.4 Example for Configuring the FTPS Server.... 357
8.5.5 Example for Configuring the TFTP Client.... 359
8.5.6 Example for Configuring an FTP Client.... 361
8.5.7 Example for Configuring an SFTP Client.... 362
8.5.8 Example for Configuring an SCP Client.... 368
8.5.9 Example for Configuring an FTPS Client.... 370
8.6 Common Misconfigurations.... 374
8.6.1 FTP Login Failure.... 374
8.6.2 File Upload Failure.... 376
8.7 FAQ.... 377
8.7.1 How to View the Deleted Files in the System?.... 377
8.7.2 Which SSH Version Does the Device Support?.... 377
8.7.3 Why Local Users Must Be Configured on a Device When SSH Users Configure Remote Authentication?.... 377
8.7.4 How Can I Repair a Storage Device Where an Exception Occurred?.... 378
8.7.5 How to Delete the Files in the Recycle Bin?.... 378
8.7.6 How Do I Upload or Download Files?.... 378
8.7.7 How Do I Limit the FTP Upload or Download Speed?.... 380
8.7.8 How Do I Check Whether an Uploaded File Is Complete?.... 380
8.7.9 What Are the Extensions of Different Types of Files?.... 381
8.7.10 Where Are Log Files Saved?.... 381
8.7.11 How Do I Delete Files?.... 381
8.7.12 How Do I Transfer Files Between Two Switches?.... 382
9 Configuring System Startup.... 383
9.1 System Startup Overview.... 384
9.2 Managing Configuration Files.... 388
9.2.1 Saving the Configuration File.... 388
9.2.2 Comparing Configuration Files.... 390

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

9.2.3 Backing Up the Configuration File ... 391
9.2.4 Recovering the Configuration File ... 393
9.2.5 Executing a Configuration File ... 394
9.2.6 Clearing the Configuration ... 394
9.2.7 Setting Factory Configurations on the S1720GFR ... 396
9.3 Configuring System Startup Files ... 397
9.4 Restarting the Device ... 399
9.5 Configuration Examples ... 400
9.5.1 Example for Backing Up the Configuration File ... 400
9.5.2 Example for Recovering the Configuration File ... 401
9.5.3 Example of Configuring System Startup ... 402
9.6 FAQ ... 404
9.6.1 How Can I Save the Device Configuration? ... 405
9.6.2 How Can I Delete the Device Configuration? ... 405
9.6.3 What Files Will Be Displayed in the Flash Memory in Addition to the Default Startup System Software Package and Configuration File? ... 406

10 BootROM Menu Operation ... 407

10.1 BootROM Menu Overview ... 408
10.2 BootROM Main Menu ... 408
10.3 Serial Port Submenu ... 410
10.4 Startup Configuration Submenu ... 411
10.4.1 Checking the Startup Configuration ... 412
10.4.2 Modifying Startup Configuration Information ... 413
10.5 Ethernet Submenu ... 415
10.5.1 Modifying Parameters on the Ethernet Port ... 416
10.6 File System Submenu ... 419
10.7 Password Submenu ... 420
10.7.1 Submenu for Changing the Password of the BootROM Menu ... 421
10.7.2 Restoring the BootROM Password ... 422
10.8 Deleting the Password for Login Through the Console Port ... 423
10.9 Configuration Example ... 424
10.9.1 Example for Upgrading the System Software Using the BootROM Menu ... 424
10.10 FAQ ... 428
10.10.1 What Is the Default BootROM Password of the Switch? ... 428

11 BootLoad Menu Operation ... 429

11.1 BootLoad Main Menu ... 430
11.2 Startup Configuration Submenu ... 431
11.2.1 Display startup configuration ... 432
11.2.2 Modifying Startup Configuration Information ... 433
11.3 Ethernet Submenu ... 435
11.3.1 Modifying Parameters on the Ethernet Interface ... 436
11.4 File System Submenu ... 438

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

11.5 Password Submenu....440
11.5.1 Submenu for Changing the Password of the BootLoad Menu....441
11.5.2 Restoring the BootLoad Password....442
11.6 Submenu for Deleting the Password for Logging In Using the Serial Port....442
11.7 Configuration Example....443
11.7.1 Upgrading the System Software Using the BootLoad Menu....443
12 Checking Declaration Information of an Open Source Software....449

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

1 Basic Features Supported in This Version

Feature	S1720 S2720 S2750 EI	S5700LI S5700S-LI S5710-X-LI	S5720SI S5720S-SI	S5720EI S5720HI	S6720EI S6720S-EI
EasyDeploy	All device models except S1720 can function only as clients.	Supported only as a client	Supported only as a client	Supported only as a Commander or client	Supported only as a Commander or client
USB-based deployment	Not supported	Supported	Supported	Supported	Supported
Console port login	Supported	Supported	Supported	Supported	Supported
Mini USB port login	Not supported	Only supported by the S5700LI and S5700S-LI	Not supported	Not supported by the S5720-50X-EI-AC, S5720-50X-EI-DC, S5720-50X-EI-46S-DC and S5720-50X-EI-46S-AC	Not supported

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Feature	S1720 S2720 S2750 EI	S5700LI S5700S-LI S5710-X-LI	S5720SI S5720S-SI	S5720EI S5720HI	S6720EI S6720S-EI
Telnet login	Supported	Supported	Supported	Supported	Supported
STelnet login	Supported	Supported	Supported	Supported	Supported
Login through the web platform	Supported	Supported	Supported	Supported	Supported
File management	Supported	Supported	Supported	Supported	Supported
BootROM menu	Supported	Only supported by the S5700LI and S5700S-LI (excluding S5700S-28X-LI-AC and S5700S-52X-LI-AC)	Not supported	Not supported	Not supported
BootLoad menu	Not supported	Only supported by the S5710-X-LI, S5700S-28X-LI-AC and S5700S-52X-LI-AC	Supported	Supported	Supported

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

2 CLI Overview

About This Chapter

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

2.1 Entering Command Views

2.2 Editing Command Lines

2.3 Using Command Line Online Help

2.4 Using the undo Command Line

2.5 Executing Commands in a Batch

2.6 Executing User View Commands in the System View

2.7 Using Command Line Shortcut Keys

2.8 Displaying Command Line Configurations

2.9 Controlling the Display Mode of Commands

2.10 Filtering Output Information Based on the Regular Expression

2.11 Setting Command Levels

2.12 Displaying History Commands

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 switch 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 *S1720&S2700&S5700&S6720 Series Ethernet Switches 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.

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-GigabitEthernetX/Y/Z]`
	X/Y/Z indicates the number of an interface that needs to be specified. It is in the format of stack ID/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.

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

You can enter ! or # followed by a character string in any view. All entered content (including ! and #) is displayed as comments. That is, the corresponding configuration is not generated.

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.
- You can enter ! or # followed by a character string in any view. All the entered content (including ! and #) is displayed as comments and can be properly. That is, no error message is displayed and no the corresponding configuration is not generated.

Exiting Command Views

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

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

```
[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>
```

Intelligent Rollback

Intelligent rollback enables the system to automatically return to the previous view if a command fails to be executed in the current view. The system performs view return attempts until the applicable view of the command is displayed. The system can return to the system view at the maximum extent.

The following provides two application examples for intelligent rollback. The system enters the applicable view of a command after performing one view return attempt in the first example, and performs multiple attempts in the second example.

1. After entering an OSPF area view, the system allows a user to directly enter another OSPF area view, without the need to manually return to the OSPF view.

   ```
   <HUAWEI> system-view
   [HUAWEI] ospf 100
   [HUAWEI-ospf-100] area 1
   [HUAWEI-ospf-100-area-0.0.0.1] area 2
   [HUAWEI-ospf-100-area-0.0.0.2]
   ```

2. After entering an OSPF area view, the system allows a user to directly enter an interface view, without the need to manually return to the system view.

   ```
   <HUAWEI> system-view
   [HUAWEI] ospf 100
   ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] interface gigabitEthernet 0/0/3
[HUAWEI-GigabitEthernet0/0/3]
```

2.2 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 2-1 lists keys that are frequently used for command editing.

Table 2-1 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**. However, you cannot enter **d c** or **dis c** because they do not match unique keywords.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTICE

The maximum length of a command (including the incomplete command) to be entered is 510 characters. If a command in incomplete for m is configured, the system saves it to the configuration file in its complete form, which may exceed the 510-character limit. 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 followed by a space. For example:
  a. Enter an incomplete keyword.
  ```
  [HUAWEI] info-
  ```
  b. Press **Tab**.
  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 loghost
  ```
  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 logbuffer
  ```
  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. This indicates that this keyword does not exist.

2.3 Using Command Line Online Help

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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:
  backup         Backup electronic elabel
  cd             Change current directory
  check          Check information
  clear          Clear information
  clock          Specify the system clock
  compare        Compare function
...
```

- 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, and this authentication mode is recommended
  none      Login without checking
  password  Authentication through the password of a user terminal interface

[HUAWEI-ui-vty0-4] authentication-mode aaa ?
  <cr>

[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, the default value is 30 minutes
[HUAWEI] ftp timeout 35 ?
  <cr>

[HUAWEI] ftp timeout 35
```

  "INTEGER<1-35791>" describes the value range of the parameter. "The value of FTP timeout, the default value is 30 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                                delete
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
  dir                                     display
<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?
  bpdu                                    bridge
  buffer
```

- 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.

NOTE

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

2.4 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
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Succeeded in starting the FTP server.
[HUAWEI] undo ftp server
Info: Succeeded in closing the FTP server.
```

- 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:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 5.
      The current login time is 2012-06-09 04:46:00.
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
<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:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 5.
      The current login time is 2012-06-09 04:52:10.
<HUAWEI>
```

NOTE

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

2.5 Executing Commands in a Batch

Procedure

- Automatic batch command execution

  Assistant tasks help implement automatic batch command execution. You can create a maximum of five assistant tasks on the device and each assistant task is bound with a batch file. After an execution time is configured, the device automatically executes commands in the batch file one by one. Automatic batch command execution is frequently used for periodic system upgrade or configuration.

  A batch file is a collection of executable commands and the file is in the format of ***.bat**. When the batch file is processed, commands in the file are executed one by one. Before configuring automatic batch command execution, edit the batch file on the PC and upload the batch file to the device. If the file name extension is not **.bat**, change it to **.bat** before you upload the batch file to the device. Alternatively, upload the batch file to the device and then run the **rename** command to change the file name extension.

  a. Run the **system-view** command to enter the 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 for performing assistant tasks.
  d. Run the **perform** *priority* **batch-file** *filename* command to bind the batch file with the assistant task.
  e. Run the **display assistant task history** [*task-name*] command to check the operation records of assistant tasks.

----End

2.6 Executing User View Commands in the System View

Context

Some commands need to be executed in the user view. To execute these commands, you need to exit from the system view to the user view and then execute the commands. In order to ease

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

command execution, you can use the **run** command to execute user view commands directly in the system view.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
run command-line
```

The user view command is executed.

The parameter *command-line* is a user view command. You must enter the complete command manually because automatic command line completion is not supported.

----End

2.7 Using Command Line Shortcut Keys

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

System-defined shortcut keys cannot be defined by users and have fixed functions. **Table 2-2** lists the system-defined shortcut keys.

NOTE

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

System-defined Shortcut Keys

Table 2-2 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 current line.
Ctrl+F	Moves the cursor forward one character.
Ctrl+H	Deletes the character on the left side of the cursor.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Key	Function
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+R	Redisplays information about the current line.
Ctrl+T	Stops outgoing connections.
Ctrl+V	Pastes the text of the clipboard.
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.
Esc+N	Moves the cursor downward a line.
Esc+P	Moves the cursor upward a line.

2.8 Displaying Command Line Configurations

After the configurations are complete, you can run the **display** command to check 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 check the current running configurations and configurations in the current view.

- Check the current running configurations:

  display current-configuration

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

This command does not display parameters that use default settings.

- Check configurations in the current view:

  display this

  This command does not display parameters that use default settings.

  To view the default configurations that have not been modified in the current view, run the **display this include-default** command.

2.9 Controlling the Display Mode of Commands

Info and warning messages and command execution results are displayed after you run commands on the device. You can control on the display mode of the command outputs.

- When the display output is more than one page, you can use **<PageUp>** and **<PageDown>** 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 2-3** to control the display mode of command lines.

Table 2-3 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, letter key, and so on) except space and Enter.
Space	Continues to display the next screen of information.
Enter	Continues to display the next line of information.

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.

- You can not only control the display mode of output information but also control the mode in which a command is displayed on the screen.

  The system supports two command output modes: character mode and line mode, which can be configured using the **terminal echo-mode** { **character** | **line** } command. By default, the character mode is used.

  - **character**: The command output mode is the character mode. When you enter a character in the command line, the system displays this character.
  - **line**: The command output mode is the line mode. When you enter a character in the command line, the system displays this character only after you press **Enter**, **Tab** or **?**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

When you operate a device using the NMS, you can change the command output mode to **line** to improve operation efficiency. Common users have a habit of using the **character** mode. Therefore, use the **character** mode for common users to improve operation efficiency.

2.10 Filtering Output Information Based on the Regular Expression

Regular Expressions

When you run the **display** command to check the device configuration and running status information, you can filter out unnecessary information based on the regular expression.

A regular expression is a mode matching tool. You can create a matching mode based on specified rules and then match target objects based on the matching mode. A regular expression consists of 1 to 256 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, underline, 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 a set of symbols with special meanings which are provided to flexibly create matching modes. The special characters are also called metacharacters. Table 2-4 describes special characters and their syntax.

Table 2-4 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Special Characters	Function	Example
+	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. **NOTE** Huawei datacom devices do not support regular expressions with ?. When regular expressions with ? are entered on Huawei datacom devices, helpful information is provided.	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.
[^a-z]	Matches any character beyond the specified range.	[^0-9] matches all non-numeric characters.

A simple regular expression does not contain any special character. For example, you can create a simple regular expression "hello" to match the character string "hello" only. In practice, multiple common and special characters are used together to match a character string with special features.

- Degeneration of special characters

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

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- 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.

Usage of Regular Expressions

There are two modes to filter output information based on the regular expression.

- Specifying a filtering mode in a command: enter the keyword **begin**, **exclude**, or **include**, and a regular expression in the command line to filter command outputs.
- Specifying a filtering mode on a split screen: enter a slash (/), minus (-), or plus (+) symbol, and a regular expression to filter command outputs to be displayed on a split screen. The slash (/), minus (-), and plus (+) symbols have the same functions as the keywords **begin**, **exclude**, and **include**.

Specifying a Filtering Mode in a Command

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

You can specify the filtering mode of output information for some display commands that have large amount of output information.

After the command output is filtered, the displayed information is displayed with its context. Context rules are as follows:

- **before** *before-line-number*: displays lines that match filtering rules and the preceding *before-line-number* lines.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- **after** *after-line-number*: displays lines that match filtering rules and the subsequent *after-line-number* lines.
- **before** *before-line-number* + **after** *after-line-number* or **after** *after-line-number* + **before** *before-line-number*: displays lines that match filtering rules, the preceding *before-line-number* lines, and the subsequent *after-line-number* lines.

  Values of *before-line-number* and *after-line-number* are a string of 1 to 999 characters.

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

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

```
<HUAWEI> display interface brief | exclude Ethernet|NULL|Tunnel
PHY: Physical
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
Eth-Trunk1                  down  down        0%     0%          0          0
Eth-Trunk17                 down  down        0%     0%          0          0
LoopBack1                   up    up(s)       0%     0%          0          0
Vlanif1                     up    down        --     --          0          0
MEth0/0/1                   down  down        0%     0%          0          0
Vlanif2                     down  down        --     --          0          0
Vlanif10                    down  down        --     --          0          0
Vlanif12                    down  down        --     --          0          0
Vlanif13                    down  down        --     --          0          0
Vlanif20                    up    up          --     --          0          0
Vlanif22                    down  down        --     --          0          0
Vlanif222                   down  down        --     --          0          0
Vlanif4094                  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 2 10 101 to 102 800 1000
vlan 2
vlan 10
 port trunk pvid vlan 800
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10 101 800
 undo port hybrid vlan 1
 undo port hybrid vlan 1
 port hybrid untagged vlan 10
 undo port hybrid vlan 1
 undo port hybrid vlan 1
```

NOTE

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

Specifying a Filtering Mode on a Split Screen

When the output of the following commands is displayed screen by screen, you can specify a filtering mode:

- **display current-configuration**

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- **display interface**
- **display arp**

When a lot of information is displayed on a split screen, you can specify a filtering mode in the prompt "---- More ----".

- /*regular-expression*: displays all the lines beginning with the line that matches the regular expression.
- -*regular-expression*: displays all the lines that do not match the regular expression.
- +*regular-expression*: displays all the lines that match the regular expression.

For example, run the **display current-configuration** command to display only VLANIF-related information when the command output is displayed on a split screen.

```
<HUAWEI> display current-configuration
!Software Version V200R009C00
#
sysname HUAWEI
#
vlan batch 10 to 11 100
#
hotkey CTRL_G "display tcp status"
#
lldp enable
#
undo http server enable
undo http secure-server enable
#
dhcp enable
#
dhcp snooping enable
+Vlanif            //Enter the filtering mode.

Filtering...
interface Vlanif10
interface Vlanif100
```

2.11 Setting Command Levels

Context

Each command on the device has a default level. The device administrator can change the command level as required so that users of different levels can execute commands correspondingly.

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 2-5** describes the relationship between command levels and user levels.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 2-5 Relations between command levels and user levels

Command Level	Description	Example	User Level
Visit level (level-0)	Diagnostic commands	● **tracert** ● **ping**	All levels (level-0 to level-15)
	External device access commands	● **telnet** ● **stelnet**	
Monitoring level (level-1)	System maintenance commands	**display** commands **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are level-3 commands.	Not lower than the monitoring level (level-1 to level-15)
Configuration level (level-2)	Service configuration commands	Route configuration commands	Not lower than the configuration level (level-2 to level-15)
Management level (level-3)	Basic system operation commands	● User management ● Setting command levels ● Setting system parameters ● **debugging** commands	Management level (level-3 to level-15)
	Support module commands	● File system ● FTP/TFTP downloading ● Configuration file switching	

For details about command levels, see the *S1720&S2700&S5700&S6720 Series Ethernet Switches Command Reference*.

The default command level setting is appropriate for user operation rights control; therefore, you are advised not to change command levels. If there are special requirements on user operation rights of a specific-level users, you can change the command level of specified commands. For example, if only level-4 and a higher level users are allowed to execute the **stelnet** command, you can upgrade the command level of the **stelnet** command to level-4.

In addition to upgrade a command level, you can also lower a command level.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

Do not change the default level of a command. Otherwise, some users may be unable to use the command. If command levels are changed separately before you upgrade command levels in a batch, the levels of these commands remain unchanged. Therefore, you are advised to upgrade command levels in a batch before you upgrade the level of each command separately.

The execution of some commands depends on some conditions. For example, a command can be configured only when other commands are configured or the command is an upgrade-compatible command. When levels of these commands are adjusted using the **command-privilege level** command, the adjusted commands may not be executed. Level adjustment of a command is irrelevant to execution of the command.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Set the command level.

- Run:

  ```
  command-privilege level level view view-name command-key
  ```

  The command level is set in the specified view.

- Run:

  ```
  command-privilege level rearrange
  ```

  The command levels are upgraded in batches.

  - If command levels are not changed separately, the levels change according to the following rules after a batch command level upgrade command is executed:
    - The visit level and monitoring level remain unchanged.
    - The configuration level is upgraded to level 10, and the management level is upgraded to level 15.
    - There are no commands at levels 2 to 9 and levels 11 to 14. You can set commands to any of these levels separately to implement refined user rights management.
  - If you have run the **command-privilege level** *level* **view** *view-name command-key* command to change a command level before you execute the batch command level upgrade command, the level of this command remains unchanged.

  Before you run the batch command level upgrade command, ensure that your user level is 15. Otherwise, you cannot run the command.

----End

2.12 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 2-6 shows operations on history commands.

Table 2-6 Accessing history commands

Action	Command or Key	Result
Display history commands.	**display history-command** [**all-users**]	● The history commands entered by the current users are displayed when **all-users** is not selected. ● The history commands entered by all users are displayed when **all-users** is selected. (**all-users** can be selected only by users of level 3 or higher.)
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.

NOTE

You cannot access history commands using the Up arrow key ↑ in HyperTerminal Windows 9X. The Up arrow key ↑ has a different function in HyperTerminal Windows 9X and needs to be replaced by the shortcut key **Ctrl+P**.

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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.

- History commands entered by the current user can be deleted using the **reset history-command** command in all view. The deleted history commands cannot be displayed or accessed. To delete history commands entered by all users, run the **reset history-command** [**all-users**] command as a user of level 3 or higher.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3 EasyDeploy Configuration

About This Chapter

This chapter provides an overview of and how to configure EasyDeploy.

3.1 Introduction to EasyDeploy
3.2 EasyDeploy Implementation
3.3 Configuration Notes
3.4 Default Configuration
3.5 Deploying Unconfigured Devices Using Option Fields
3.6 Deploying Unconfigured Devices Using an Intermediate File
3.7 Deploying Pre-configured Devices Using an Intermediate File
3.8 Deploying Unconfigured Devices Using the Commander
3.9 Manually Replacing Faulty Devices Using the Commander
3.10 Automatically Replacing Faulty Devices Using the Commander
3.11 Implementing a Batch Upgrade Using the Commander
3.12 Implementing a Batch Configuration Using the Commander
3.13 Adding Configured Devices to the Management Domain of the Commander
3.14 Maintaining EasyDeploy
3.15 Configuration Examples
3.16 Reference

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.1 Introduction to EasyDeploy

Definition

EasyDeploy is a collection of functions that facilitate device operation and maintenance.

EasyDeploy enables a device to automatically load version files, including system software, patch files, web page files, and configuration files. It simplifies network configuration, implements remote service deployment, and allows centralized device management.

Purpose

EasyDeploy improves efficiency of device deployment, routine maintenance, and faulty device replacement, while reducing labor costs.

EasyDeploy can be used in the following scenarios:

- Unconfigured device deployment

  After new switches are installed and powered on, they start the EasyDeploy process to automatically load configuration files, patch files and other required files.

  EasyDeploy also provides the function and workflow of the Auto-Config feature supported in earlier versions.

  With EasyDeploy, a network administrator does not need to be on site to commission switches. In addition to specifying the configuration files (*.cfg or *.zip files) to be used, network administrators can specify other files to be automatically loaded on the switches.
- Pre-configured device deployment

  Before delivery, a device can load a configuration file that contains commands for specifying file server addresses, name of an intermediate file for site deployment, and a shared key between the device and an SNMP host. After your simple login configuration, the device can automatically obtain and load correct configurations.

  A pre-configured device refers to a switch that has loaded a configuration file before it is delivered.
- Faulty device replacement

  During routine maintenance, EasyDeploy can periodically back up configuration files to a file server. When a faulty switch is replaced by a new one, the new switch downloads the configuration file of the faulty switch according to the backup information and activates the downloaded configuration file. In this scenario, EasyDeploy provides a plug-and-play device replacement solution.
- Batch upgrade

  During routine network maintenance, the network administrator can add devices that all require the same upgrade files and specify upgrade files for the entire group. EasyDeploy allows multiple devices to be upgraded in a batch.
- Batch configuration

  During routine network maintenance, EasyDeploy allows the network administrator to edit a command line script to issue commands to multiple devices, eliminating the need to configure these commands one by one on the devices.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Addition of configured devices to the management domain of the Commander

  If you need to monitor and manage configured devices on a network running EasyDeploy, add the configured devices to the management domain of the Commander.

Related Content

Videos

Huawei Switches EasyDeploy Feature Introduction

3.2 EasyDeploy Implementation

3.2.1 Concepts

The following concepts are important to understand before using EasyDeploy.

Commander

The Commander is a device that manages all other devices on a network. It communicates with clients using User Datagram Protocol (UDP) unicast packets, with the default port number 60000.

The Commander provides the following functions:

- Saves client deployment information in a database.
- Delivers the file server IP address, user name, password, and names of system software packages, configuration files, license files, patch files, web page files, and user-defined files to clients.
- Manages all clients. The network administrator configures and queries device deployment information on the Commander.

Client

A client is a device managed by the Commander. Clients obtain information about required files from the Commander, download the files from the specified file server, and then activate the downloaded files in the configured mode.

NOTE

Unless otherwise specified, clients mentioned in this document refer to devices to be configured using the Commander.

Group

A group is a series of clients that need to download the same files. Defining groups for clients further simplifies configuration. You can configure various groups on the Commander according to network device deployment.

There are two classifications for groups:

- Built-in group

  Clients are grouped based on predefined device types on the Commander. Clients of the same type load the same system software package, patch file, web file, and other files.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Customized group

  The clients are grouped based on MAC addresses, ESNs, IP addresses, types, and models. You can group the clients according to network requirements. Device types used in customized groups are not predefined on the Commander.

File Server

A file server is an SFTP, FTP, or TFTP server that saves the files to be loaded to devices, including system software packages, configuration files, license files, patch files, and web page files.

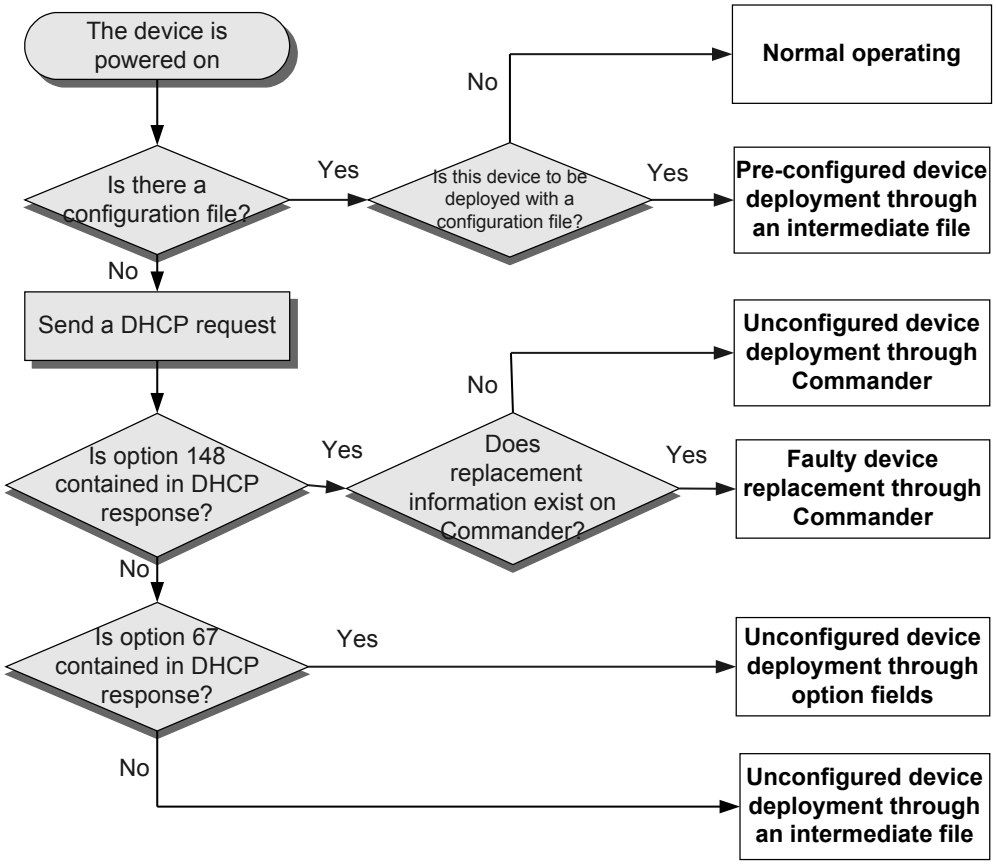
NOTE

A file server must have sufficient space to save files. Before configuring an S series switch as a file server, ensure that its storage space is sufficient for the files.

DHCP Server

A DHCP server allocates IP addresses to devices to be configured in unconfigured device deployment, pre-configured device deployment, and faulty device replacement scenarios. After a new device is powered on, it starts the corresponding EasyDeploy process depending on whether it has a configuration file and whether the DHCP server returns the related option fields. **Figure 3-1** illustrates the EasyDeploy decision process.

Figure 3-1 EasyDeploy decision mechanism



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Intermediate File

An intermediate file is saved on a file server to specify information about files to be downloaded. Each line in an intermediate file specifies the MAC address or ESN of a device and files for the device. Devices to be configured can obtain information about files to be downloaded from the intermediate file and implement automatic configuration.

On the S series switches, the intermediate file name is configurable, and the file name extension is .cfg.

To configure multiple devices, define the configuration information for a device in each line in the intermediate file.

For example, the MAC address of a device is 0018-82C5-AA89 and the device needs to download system software **easy_V200R009C00.cc** of version **V200R009C00SPC100**, path file **easy_V200R009C00.pat**, configuration file **easy_V200R009C00.cfg**, and web page file **easy.web.7z**. The intermediate file content for this device is as follows:

```
mac=0018-82C5-
AA89;vrpfile=easy_V200R009C00.cc;vrpver=V200R009C00SPC100;patchfile=easy_V200R009C
00.pat;cfgfile=easy_V200R009C00.cfg;webfile=easy.web.7z;
```

NDP

The Neighbor Discovery Protocol (NDP) is a Huawei proprietary protocol used to collect information about neighboring devices, such as the interfaces connected to the neighboring devices and system software versions of the neighboring devices.

NDP packets are encapsulated in Ethernet-II frames and periodically transmitted with a multicast destination MAC address. A device creates and maintains an NDP table based on received NDP packets.

The NDP protocol defines two timers for maintaining the NDP table on a device:

- Update timer: When this timer expires, the device immediately sends an Update packet.
- Aging timer: If the device does not receive any NDP packet from a neighbor before this timer expires, the device deletes the NDP entry matching the neighbor.

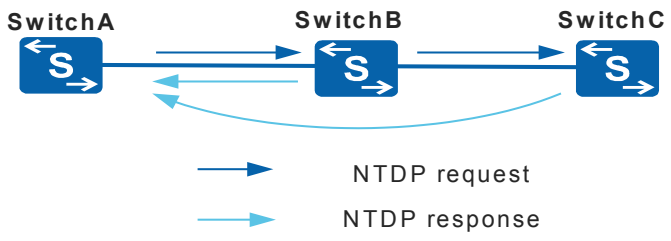
NTDP

The Network Topology Discovery Protocol (NTDP) is a Huawei proprietary protocol used to collect topology information within the configured scope on a network. The collected topology includes NDP entries.

NTDP packets are encapsulated in Ethernet-II frames. NTDP requests are periodically sent with a multicast destination MAC address, and NTDP responses are sent with a unicast destination MAC address.

Figure 3-2 shows an example of a network using NTDP to collect topology information.

Figure 3-2 Topology information collection using NTDP



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

In **Figure 3-2**, SwitchA sends an NTDP request packet to collect topology information. After SwitchB receives the NTDP request packet, it immediately sends a response packet to SwitchA and forwards the request packet to SwitchC. SwitchC then performs the same operations as SwitchB. This process proceeds until all the devices on the network receive the NTDP request packet and send response packets to SwitchA. In this way, SwitchA obtains NDP entries and connection information of all devices and figures out the network topology based on the obtained information.

Network Topology Collection

The network topology collection function is provided by the Commander using the Neighbor Discovery Protocol (NDP) and Network Topology Discovery Protocol (NTDP). When this function is enabled on the Commander to deploy unconfigured devices, users do not need to manually collect such information as device's MAC address or ESN. After unconfigured devices are powered on and started, the Commander automatically collects device information and assigns client IDs to devices to pair device information with devices. The Commander can collect network topology information and specify information of files to be downloaded based on the collected network topology information. The Commander can also automatically replace faulty devices based on network topology information.

3.2.2 Unconfigured Device Deployment Using Option Fields or an Intermediate File

Unconfigured devices can obtain file information from:

- Option fields contained in DHCP packets sent from a DHCP server
- Intermediate file, which can be obtained from a file server

The option fields or intermediate file method only applies to unconfigured device deployment. The Commander method applies to both deployment and maintenance scenarios and therefore is recommended.

On the network shown in **Figure 3-3**, switches in the black frame are newly deployed switches without configuration files.

NOTE

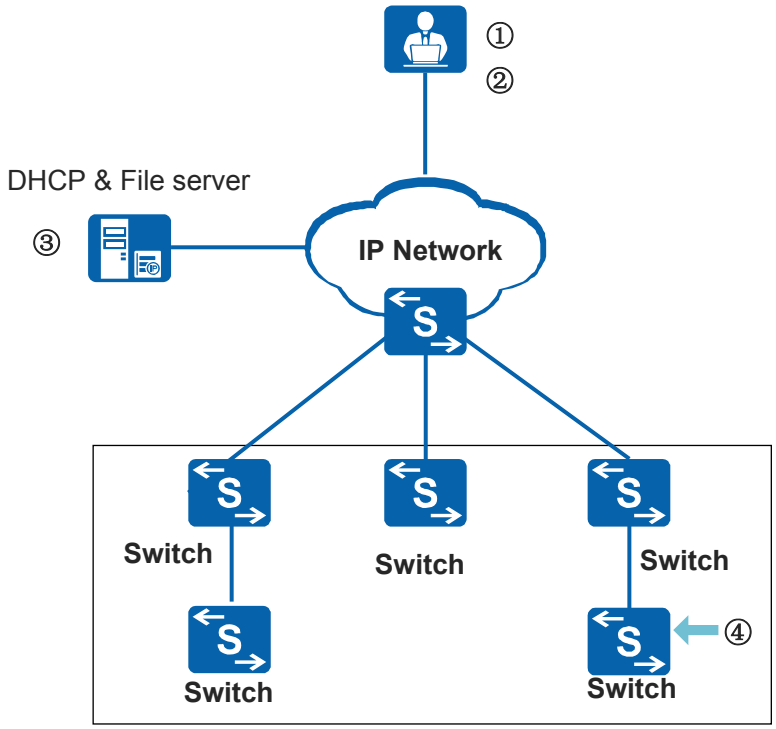
This deployment method is the same as Auto-Config deployment and does not involve the Commander and clients.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-3 Networking for unconfigured device deployment



The following procedure uses one of these switches as an example to describe how unconfigured devices are configured using option fields or an intermediate file.

1. The network administrator plans the physical position, management IP address, management VLAN, and other basic network and service parameters for the switch, and creates a configuration file for the switch.
2. The administrator determines whether to use option fields or an intermediate file to implement device deployment according to network requirements:
   - If only a few devices need to be configured and the devices can use the same configuration file, they can be configured using option fields. When this method is used, the administrator needs to configure option fields on the DHCP server to specify information about the files that the devices need to download.
   - If many devices need to be configured and the devices require different configuration files, they can be configured using an intermediate file. When this method is used, the administrator needs to create an intermediate file offline and specify information about the files that the devices need to download in this intermediate file.
3. The administrator configures the DHCP server (including option fields) and file server, and then saves the configuration file and other files to be downloaded on the file server. If an intermediate file is used, the administrator saves the intermediate file on the file server.

   If the unconfigured switch and the DHCP server are located on different network segments, a DHCP relay agent must be deployed between them.
4. After the administrator completes the configuration, the switch starts the unconfigured device deployment process.

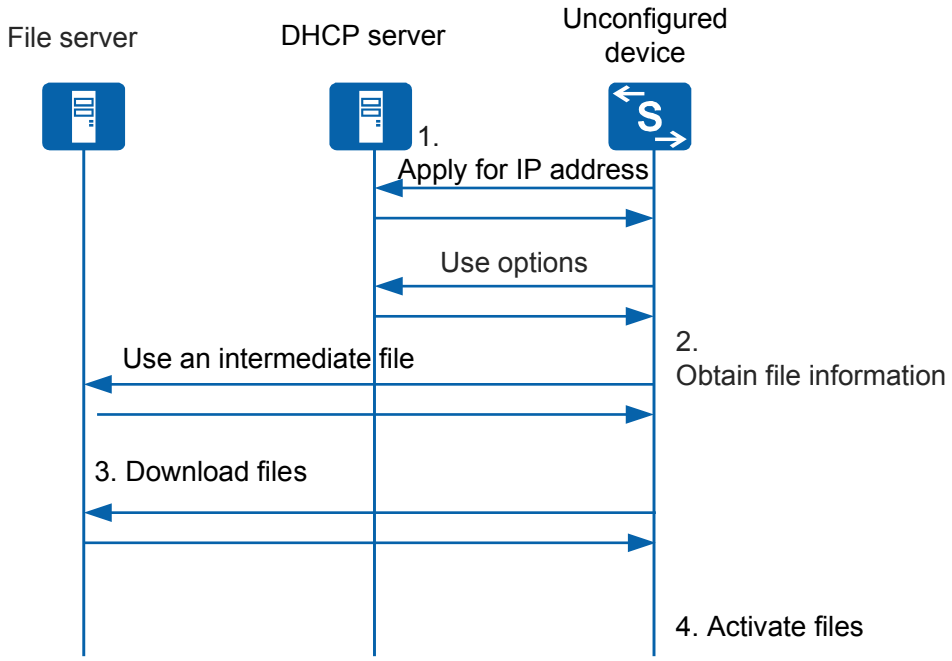
Figure 3-4 shows the interaction between network devices during the unconfigured device deployment process.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-4 Interaction between network devices



Unconfigured device deployment goes through four stages:

1. Apply for an IP address.

   The unconfigured device sends a DHCP request to apply for an IP address. The DHCP server replies with a DHCP response that carries the allocated IP address and file server information.

2. Obtain file information.

   After receiving the DHCP response, the unconfigured device checks the option field values in the DHCP response to determine whether to obtain file information from the option fields or intermediate file.

3. Download files.

   The unconfigured device downloads the required files from the file server according to the obtained file information.

   The unconfigured device downloads required files in the following sequence:

   a. System software package
   b. Patch file
   c. Web page file
   d. Configuration file

4. Activate the configuration file.

   You can specify Option 146 on the DHCP server to configure a configuration file activation policy.

If the unconfigured device is a stacked switch, the downloaded system software package, patch file, and web page file are copied from the master switch to standby and slave switches. After the file copy is complete, the device activates the files and then starts to operate normally.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Options Used for Unconfigured Device Deployment

Options must be configured on the DHCP server before deploying unconfigured devices. **Table 3-1** describes the options used in this scenario.

Table 3-1 Option fields

Option	Description	Remarks
Option 67	Indicates the name and path of the configuration file allocated to a DHCP client. The file path and name cannot contain spaces and the total length cannot exceed 69 characters. For example, this field can be set to **easy/vrpcfg.cfg**, where **easy** is a file path.	Optional ● If this field is specified, the unconfigured devices are configured using option fields. ● If this field is not specified, the unconfigured devices are configured using an intermediate file.
Option 141	Indicates the SFTP/FTP user name assigned to DHCP clients.	Mandatory (At least one file server is required.) ● Options 141, 142, and 143 enable unconfigured devices to obtain the FTP user name, FTP password, and FTP server IP address. ● Options 141, 142, and 149 enable unconfigured devices to obtain the SFTP user name, SFTP password, and SFTP server IP address and port number. ● Option 150 enables unconfigured devices to obtain the TFTP server IP address. If multiple types of file servers are specified by option fields on the DHCP server, the file servers are selected in the following sequence: 1. SFTP server 2. TFTP server 3. FTP server
Option 142	Indicates the SFTP/FTP password assigned to DHCP clients. An SFTP/FTP password can be configured using either of the following commands: ● **option 142 ascii** *password* ● **option 142 cipher** *password* A password in ASCII format is saved in plain text. A password in cipher format is saved in cipher text. When the two commands are executed in turn for multiple times, only the latest configuration takes effect. For better password security, you should configure the password in cipher format.	
Option 143	Indicates the FTP server IP address assigned to DHCP clients.	

Option 149	Indicates the 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 the port number is 22 (default), option 149 can be set in either of the following formats:
	option 149 ascii ipaddr=10.10.10.1;
	option 149 ascii ipaddr=10.10.10.1;port=22;	

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Option	Description	Remarks
Option 150	Indicates the TFTP server IP address assigned to DHCP clients.	The file server user account obtained by an unconfigured device is only used for EasyDeploy. The device does not store the file server user name and password.

Option 145	Indicates information about files other than the configuration file.
	If this field contains a file path, ensure that the total length of the file path and file name does not exceed 69 characters.
	To specify the system software name, software version, web page file name, and path file name, set option 145 as follows:
	`vrpfile=VRPFILENAME;vrpver=VRPVERSION;patchfile=PATCHFILENAME;webfile=WEBFILE;`
	For example:
	`vrpfile=easy_V200R009C00SPC100.cc;vrpver=V200R009C00SPC100;patchfile=easy_V200R009C00.pat;webfile=easy_V200R009C00.web.7z;`
		● This field is optional if Option 67 is used.
		● You do not need to configure this field if Option 67 is not used.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Option	Description	Remarks
Option 146	Indicates the operation performed by unconfigured devices. It contains the following subfields: ● opervalue This indicates whether to delete the system software from the file system if the storage space is insufficient. The value 0 indicates that the system software will not be deleted. The value 1 indicates that the system software will be deleted. The default value of this subfield is 0. ● delaytime This indicates the delay time before making a downloaded file take effect. The delay time is expressed in seconds. The default value of this subfield is 0. ● netfile This indicates the intermediate file name The intermediate file name contains a maximum of 64 bytes, consisting of digits (0 to 9), lowercase letters (a to z), uppercase letters (A to Z), hyphens (-), and underscores (_). The file name extension must be .cfg. If the file name is invalid, the default file is **lswnet.cfg**. ● intime This indicates the file activation time, ranging from 00:00 to 23:59. ● actmode This indicates how a file is activated. The value 0 indicates that the file is activated in default mode. – If the configuration file and patch file are downloaded, the files can be automatically activated, eliminating the need to reset the device. – If the downloaded files include a version file, the files need to be activated after the device is reset.	● This field is optional. ● When unconfigured devices are deployed through an intermediate file and the intermediate file name needs to be specified, the **netfile** subfield in Option 146 needs to be configured.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

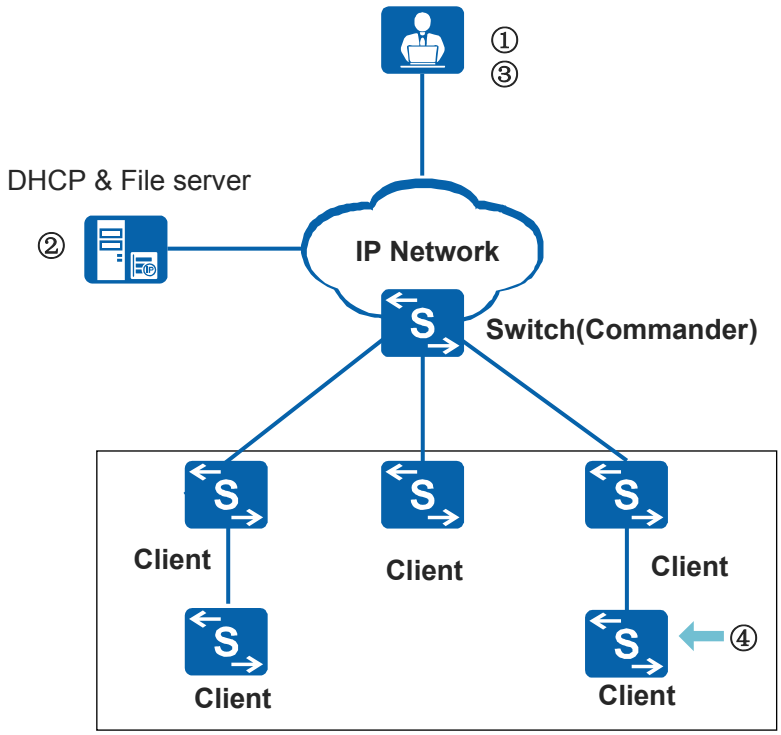
Option	Description	Remarks
	The value 1 indicates that the downloaded files can be activated after the device is reset. The default value of this subfield is 0. **NOTE** ● The maximum delay time before restarting a device is one day (86400 seconds). A delay longer than one day is counted as one day. ● If both **delaytime** and **intime** are configured, **delaytime** takes effect.	
Option 147	Indicates the authentication information. The value must be AutoConfig.	Optional

3.2.3 Unconfigured Device Deployment Using the Commander

Unconfigured devices can obtain file information from the Commander for deployment.

On the network shown in **Figure 3-5**, the clients are newly deployed switches without configuration files. The following uses one of these clients as an example to describe how the unconfigured devices are configured through the Commander.

Figure 3-5 Networking for unconfigured device deployment



The following procedure uses one of these clients as an example to describe how unconfigured devices are configured using the Commander.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

1. The network administrator selects a device as the Commander, plans the physical location, management IP address, management VLAN, and service parameters for the client, and makes a configuration file for the client.

   NOTE

   Record the Commander IP address in the configuration file to facilitate client management and maintenance after the unconfigured device deployment is complete.

2. The administrator configures the file server and DHCP server (only Option 148 is required), and saves the files required by the client to the working directory of the file server.

   If the client and the DHCP server are located on different network segments, a DHCP relay agent must be deployed between them.

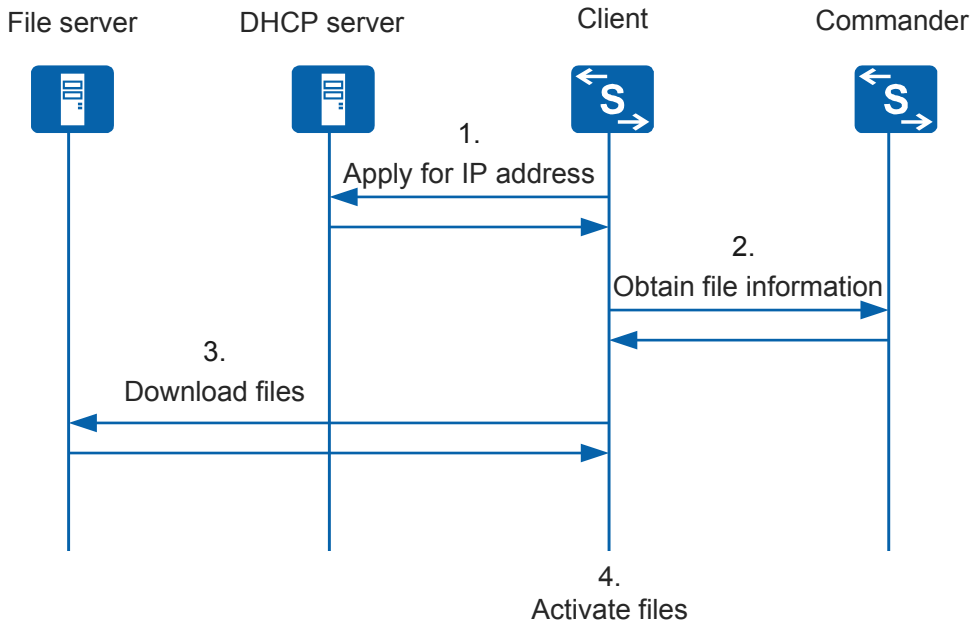
3. The administrator configures the file server IP address, user name, and password on the Commander and specifies files to be downloaded to the client based on the client MAC address or ESN reported by the hardware installation engineer.

   If the network topology collection function is enabled on the Commander, the Commander can collect topology information automatically and specify information of files to be downloaded based on the collected topology information. Therefore, the network administrator does not need to obtain client MAC addresses or ESNs from the hardware installation engineer.

4. After the administrator completes the configuration, the client starts the unconfigured device deployment process.

Figure 3-6 shows the interaction between network devices during the unconfigured device deployment process.

Figure 3-6 Interaction between the network devices



The unconfigured device deployment process goes through four stages:

1. Apply for an IP address.

   The client sends a DHCP request to apply for an IP address. The DHCP server replies with a DHCP response that carries the allocated IP address and Commander IP address.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

2. Obtain file information.

   The client obtains file information from the Commander.

3. Download files.

   The client downloads the required files from the file server according to the obtained information.

   The client downloads required files in the following sequence:

   a. System software package
   b. Patch file
   c. Web page file
   d. Configuration file
   e. User-defined file

   License files cannot be downloaded in the unconfigured device deployment scenario.

4. Activate files.

   The client activates the downloaded files according to the configured file activation policy.

   If the client is a stack, the downloaded files are copied from the master switch to slave switches when the file activation time is reached. After the file copy is complete, the client activates the files and then starts to operate normally.

During the unconfigured device deployment process, if an unconfigured device cannot obtain an IP address, the device remains in the IP address application stage and periodically sends requests to apply for an IP address. The IP address application stage continues until the device obtains an IP address or the deployment process is stopped manually.

If an error occurs (for example, the server information is incorrect) after the device obtains an IP address, the device changes to the initial state and restarts the deployment process. If an error occurs again, the device returns to the initial state. This process repeats until it is stopped manually.

If the device fails to download a file in the file downloading stage, it tries again 1 minute later. If the download still fails after five retries, the device changes to the initial state 5 minutes later and restarts the DHCP process to obtain the file information and download the file again.

3.2.4 Pre-configured Device Deployment Using an Intermediate File

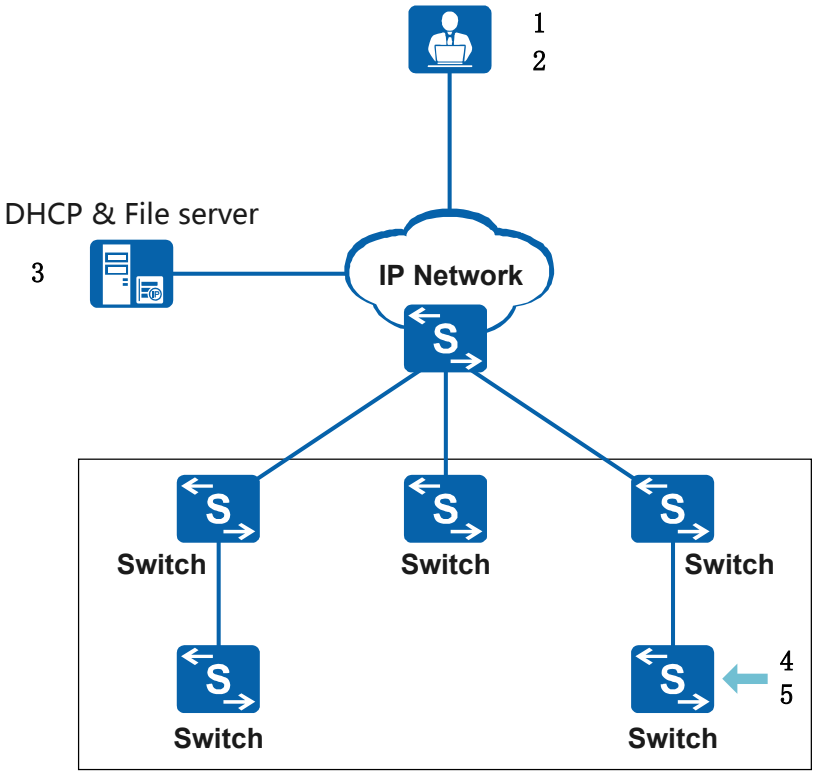
On the network shown in **Figure 3-7**, switches in the dotted box are newly deployed switches with configuration files. The following uses one of these switches as an example to describe how the pre-configured devices are configured using an intermediate file.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-7 Networking for pre-configured device deployment



1. The network administrator plans the physical position, management IP address, management VLAN, and other basic network and service parameters for the switch, and creates a configuration file for the switch.
2. The network administrator obtains the SNMP host's address and names of files to be downloaded from the intermediate file that has been created offline.
3. The administrator configures the DHCP server and file server, and then saves the configuration file, the intermediate file, and other files to be downloaded on the file server.

   If the switch to be deployed and the DHCP server are located on different network segments, a DHCP relay agent must be deployed between them.
4. The device to be delivered has loaded a configuration file that contains commands for specifying file server addresses, name of an intermediate file for site deployment, and a shared key between the device and an SNMP host.
5. The administrator starts deploying the pre-configured device.

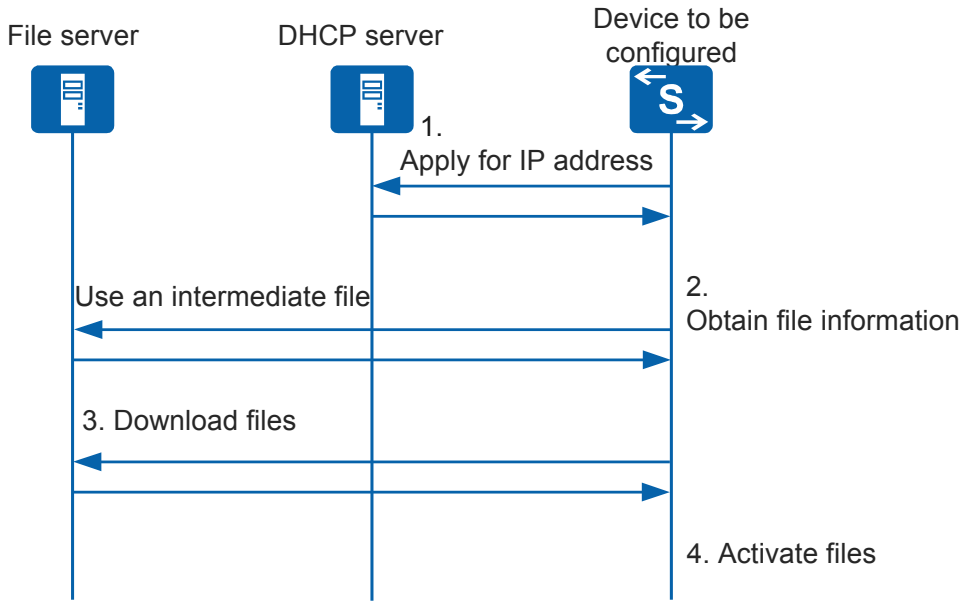
Figure 3-8 shows the interaction between network devices during the pre-configured device deployment process.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-8 Interaction between network devices



Pre-configured device deployment goes through four stages:

1. Apply for an IP address.

   The device to be deployed sends a DHCP request to apply for an IP address. The DHCP server replies with a DHCP response that carries the allocated IP address information.

2. Obtain file information.

   After receiving the DHCP response, the device to be deployed checks the option field values in the DHCP response to determine whether to obtain file information from the intermediate file.

3. Download files.

   The device to be deployed downloads the required files from the file server according to the obtained file information in the following sequence:

   a. system software package
   b. patch file
   c. web page file
   d. configuration file

4. Activate the configuration file.

   Reset the device to activate the file.

If the device to be deployed is a stacked switch, the downloaded system software package, patch file, and web page file are copied from the master switch to standby and slave switches. After the file copy is complete, the device activates the files and then starts to operate normally.

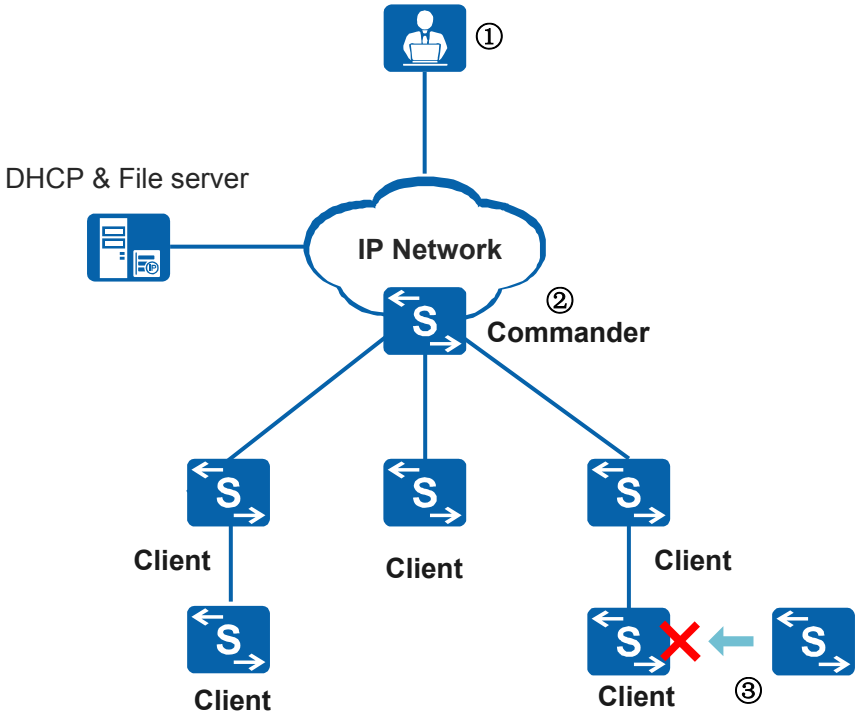
3.2.5 Faulty Device Replacement

On a network supporting EasyDeploy shown in **Figure 3-9**, a client cannot start due to a hardware failure. This section describes the faulty device replacement process.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Figure 3-9 Networking for faulty device replacement



1. The network administrator identifies the faulty client. The hardware installation engineers replace the faulty client and report the MAC address or ESN of the new device to the network administrator.
2. The administrator obtains the MAC address or ESN of the new client and configures a mapping between the new client and the faulty client on the Commander.

   If all the devices on the network support topology discovery and the new client only needs to restore the configuration file of the faulty client, the network administrator does not need to perform any configuration. The Commander can automatically discover the mapping between the new client and the faulty one.

   If the new client needs to load other files besides the configuration file, the administrator must save these files to the file server and specify the file names on the Commander.
3. After the administrator completes the configuration, the new client starts the faulty device replacement process and downloads the configuration file of the faulty client from the file server to restore the configuration.

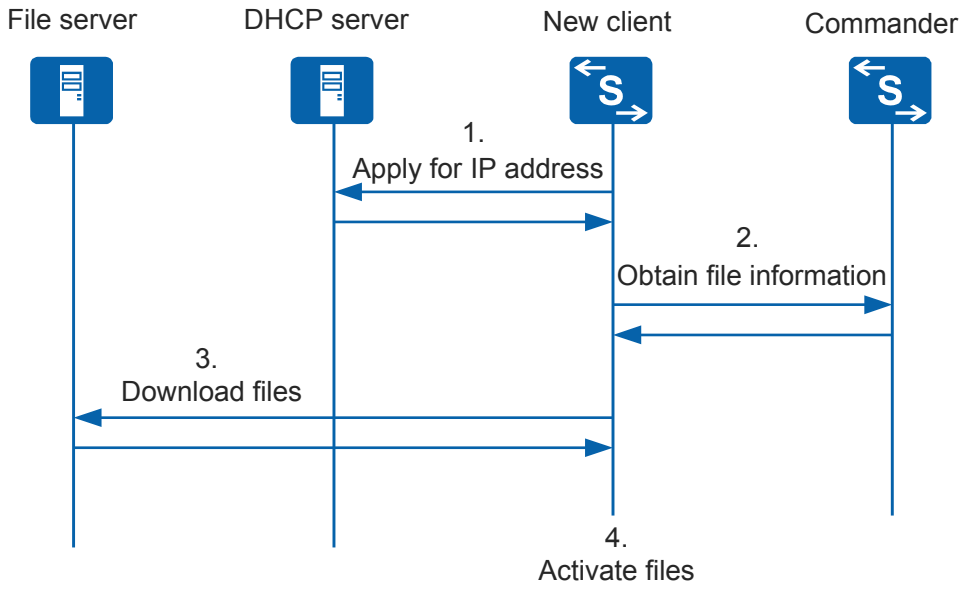
Figure 3-10 shows the interaction between the network devices during a faulty device replacement process.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-10 Interaction between the network devices



The faulty device replacement process goes through four stages:

1. Apply for an IP address.

   The new client sends a DHCP request to apply for an IP address. The DHCP server replies with a DHCP response that carries the allocated IP address and Commander IP address.

2. Obtain file information.

   The new client obtains information about the backup configuration file and other required files from the Commander according to the client replacement information.

3. Download files.

   The new client downloads other required files and then the backup configuration file from the file server.

   The client downloads required files in the following sequence:

   a. System software package
   b. Patch file
   c. Web page file
   d. User-defined file
   e. Configuration file

   License files cannot be downloaded in the faulty device replacement scenario.

4. Activate files.

   After downloading the files, the new client activates the downloaded files according to the file activation policy and starts to operate.

During the faulty device replacement process, if an unconfigured new device cannot obtain an IP address, the device remains in the IP address application stage and periodically sends requests to apply for an IP address. The IP address application stage continues until the device obtains an IP address or the replacement process is stopped manually.

If an error occurs (for example, the server information is incorrect) after the device obtains an IP address, the device changes to the initial state and restarts the replacement process. If an

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

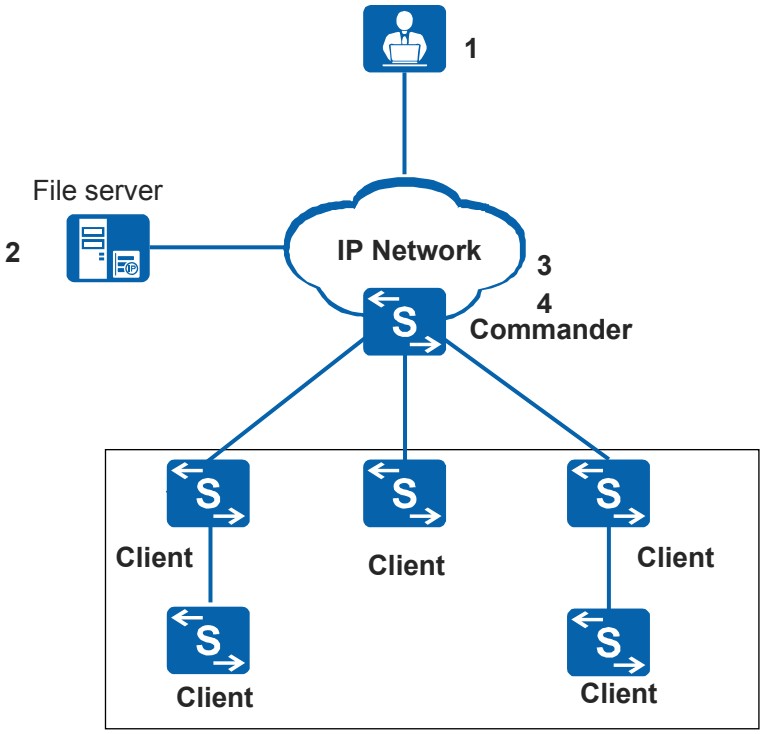
error occurs again, the device returns to the initial state. This process repeats until it is stopped manually.

If the device fails to download a file in the file downloading stage, it tries again 1 minute later. If the download still fails after five retries, the device changes to the initial state 5 minutes later and restarts the DHCP process to obtain the file information and download the file again.

3.2.6 Batch Upgrade

On a network supporting EasyDeploy shown in **Figure 3-11**, the clients need to be upgraded. This section describes how to perform a batch upgrade.

Figure 3-11 Networking for a batch upgrade



1. The network administrator decides which devices are to be upgraded, prepares upgrade files, and makes an upgrade policy.
2. The network administrator saves the upgrade files to the file server.
3. The network administrator specifies the file server IP address, user name, password, and upgrade file information on the Commander.
4. The Commander issues an upgrade instruction to the clients according to the upgrade policy, and the clients start the upgrade process.

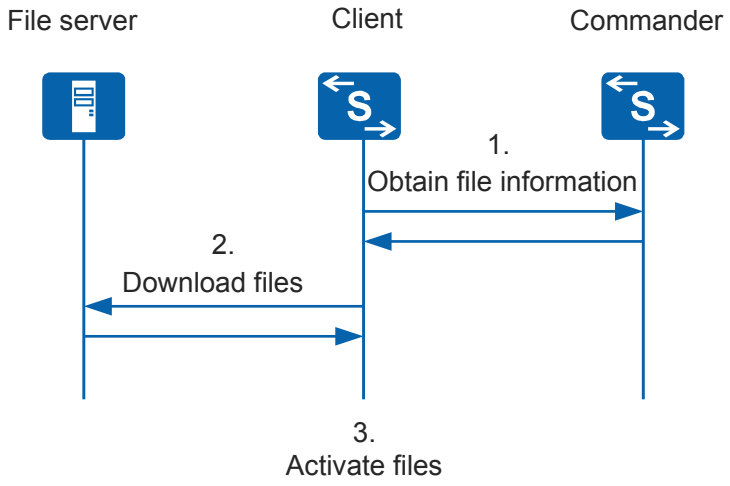
Figure 3-12 shows the interaction between network devices during a batch upgrade.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-12 Interaction between the network devices



The batch upgrade process goes through three stages:

1. Obtain file information.

   The clients obtain file information from the Commander.

2. Download files.

   The clients download the required files from the file server according to the obtained information.

   A client downloads files in the following sequence:

   a. System software
   b. Patch file
   c. License file
   d. Web page file
   e. Configuration file
   f. User-defined file

3. Activate files.

   The client activates the downloaded files according to the configured file activation policy.

   If the client is a stack, the downloaded files are copied from the master switch to slave switches when the file activation time is reached. After the file copy is complete, the client activates the files and then starts to operate normally.

During the batch upgrade process, if an error occurs (for example, the file server information is incorrect or a specified file does not exist), the clients stop the batch upgrade process and restore to the original running status. The downloaded files are retained on the clients. After a client fails to download a file, it tries again 1 minute later. If the download still fails after five retries, the client stops the upgrade process.

3.2.7 Batch Configuration

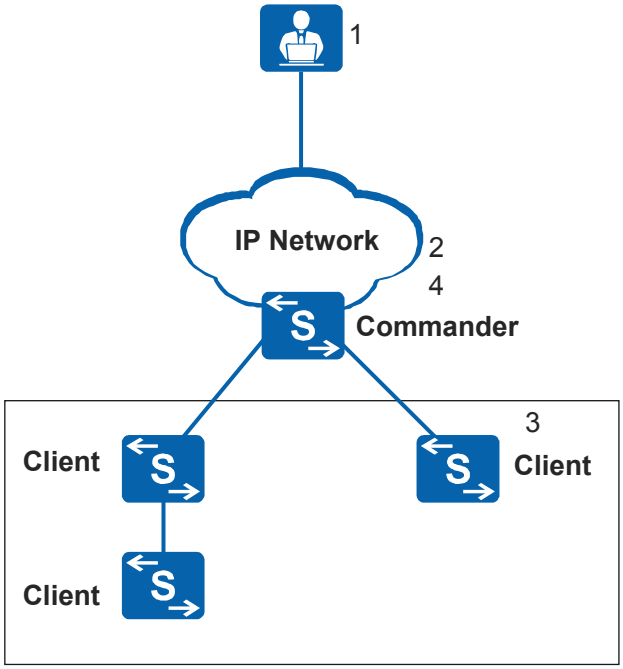
On a network supporting EasyDeploy shown in **Figure 3-13**, all the clients require the same configurations. This section describes the batch configuration process.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-13 Networking for batch configuration



1. The network administrator makes a command line script locally and uploads the script to the Command, or edits a command line script on the Commander directly.
2. The network administrator specifies on the Commander the clients or groups to which commands need to be issued and executes the command line script.
3. After the clients receive the commands from the Commander, they execute the commands and saves the command execution results.
4. The network administrator can check the command execution results on the Commander.

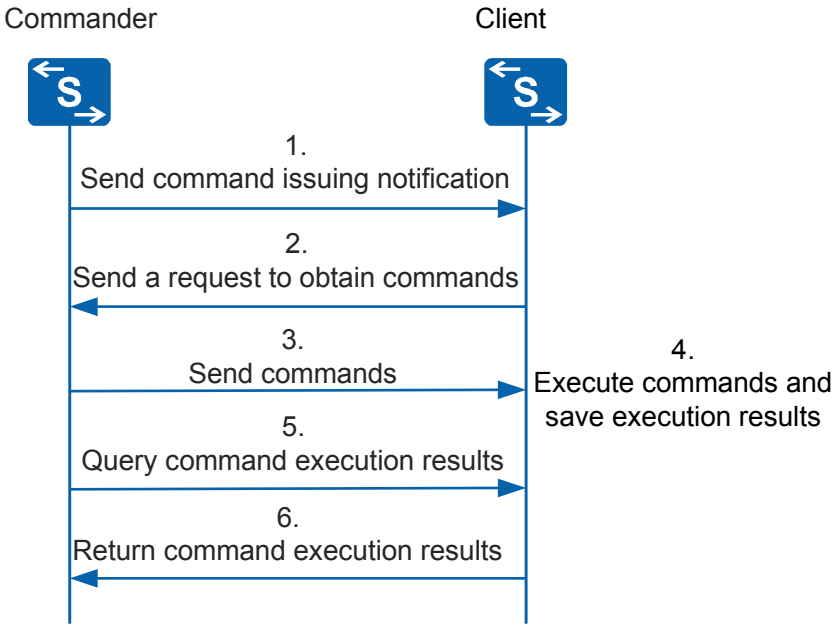
Figure 3-14 shows the interaction between the Commander and a client after the administrator executes the command line script.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-14 Interaction between the Commander and a client



1. The Commander sends a command issuing notification to the client.
2. After the client receives the notification, it sends a request to the Commander to obtain command lines.
3. After the Commander receives the request, it sends the commands to the client.
4. The client executes the commands and saves the command execution results.
5. The Commander sends a request to the client to query the command execution results.
6. The client responds with the command execution results.

3.3 Configuration Notes

Involved Network Elements

EasyDeploy networking involves the following components:

- DHCP server
- File server
- Commander and client

License Support

EasyDeploy is not under license control.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Version Support

Table 3-2 Products and minimum version supporting EasyDeploy

Series	Product	Minimum Version Required
S1700	S1720GFR	Not supported
S2700	S2700SI/S2700EI	Not supported
	S2710SI	Not supported
	S2720EI	V200R006 (The S2720EI is unavailable in V200R007 and V200R008 versions.)
	S2750EI	V200R003
S3700	S3700SI/S3700EI	Not supported
	S3700HI	Not supported
S5700	S5700LI/S5700S-LI	V200R003
	S5710-C-LI	Not supported
	S5710-X-LI	V200R008
	S5700EI/S5700SI	V200R003 (The S5700SI and S5700EI are unavailable in V200R006 and later versions.)
	S5710EI	V200R003 (The S5710EI is unavailable in V200R006 and later versions.)
	S5720EI	V200R007
	S5720SI/S5720S-SI	V200R008
	S5700HI	V200R003 (The S5700HI is unavailable in V200R006 and later versions.)
	S5710HI	V200R003 (The S5710HI is unavailable in V200R006 and later versions.)
	S5720HI	V200R006

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Series	Product	Minimum Version Required
	S6700	S6700EI

V200R003(TheS6700EIisunavailableinV200R006andlate

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Series	Product	Minimum Version Required
S6720EI		V200R008
S6720S-EI		V200R009

r v e r s i o n s .)

Feature Dependencies and Limitations

When configuring EasyDeploy, note the following points:

- The EasyDeploy feature cannot be applied on an IPv6 or VPN network.
- In the unconfigured device deployment or faulty device replacement scenarios, if you log in to a device to be configured through its console interface, the device stops the EasyDeploy process and starts to operate.
- In the unconfigured device deployment and faulty device replacement scenarios, EasyDeploy can only run on the service interfaces in the default VLAN.
- The option fields or intermediate file method only applies to unconfigured device deployment. The Commander method applies to both deployment and maintenance scenarios and therefore is recommended.
- The Commander can be located anywhere on a network, as long as reachable routes exist between the Commander and clients. If a client does not have the configuration file, the client must already obtain an IP address.
- EasyDeploy is mutually exclusive with USB-based deployment, SVF, and web initial login mode.
- EasyDeploy allows a stack system to act as a client. In this case, the client MAC address is the system MAC address of the stack system, and the client ESN is the ESN of the stack master switch.
- When the EasyDeploy topology collection function is enabled, the Commander that initiates topology collection will receive a large number of protocol packets if the Network Topology Discovery Protocol (NTDP) needs to collect the topology of more than 200 devices. If the rate of NTDP packets exceeds the default committed access rate (CAR), NTDP packets will be dropped. To prevent packet loss from affecting topology collection, you can run the **car (attack defense policy view)** command to increase the central processor CAR (CPCAR) of NTDP packets.

Specifications

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 3-3 lists the product models that support the EasyDeploy feature and specifications of this feature.

Table 3-3 EasyDeploy feature specifications

EasyDeploy Implementation	Role	Product Model	Version	Maximum Number of Managed Clients	Description
Through the Commander	Commander	S5700HI, S5710HI, S6700EI	V200R003C00 to V200R005C00	128	● If the clients are modular switches, EasyDeploy can only be applied to the batch upgrade and batch configuration scenarios. ● If the clients are fixed switches, EasyDeploy applies to the batch upgrade, batch configuration, unconfigured device deployment, and faulty device replacement scenarios.
		S5700EI and S5710EI		64	
		S5720HI	V200R006C00 and later	128	
		S5720EI	V200R007C00 and later	128	
		S6720EI	V200R008C00 and later	128	
		S6720S-EI	V200R009C00 and later	128	
	Client	All fixed switch models except S1720GFR All modular switch models	V200R003C00 and later	-	

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

EasyDeploy Implementation	Role	Product Model	Version	Maximum Number of Managed Clients	Description
Through option fields or an intermediate file	All the devices to be configured can be fixed switches.				

Table 3-4 lists the types of files that can be loaded through EasyDeploy in various scenarios.

Table 3-4 File types supported by EasyDeploy

Usage Scenario	File Type
Unconfigured device deployment	System software, patch file, web page file, configuration file (mandatory), and user-defined file
Faulty device replacement	System software, patch file, web page file, configuration file (automatically backed up), and user-defined file
Batch upgrade	System software, patch file, web page file, configuration file, license file (supported when the clients are modular switches), and user-defined file
Batch configuration	Command script

NOTE

Each device can download a maximum of three user-defined files, including batch file and login headline file. Devices cannot download user-defined files when unconfigured device deployment is implemented using option fields or an intermediate file.

3.4 Default Configuration

Table 3-5 Default EasyDeploy configuration

Parameter	Default Setting
Commander	Disabled
Client	Enabled

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.5 Deploying Unconfigured Devices Using Option Fields

Pre-configuration Tasks

Before configuring DHCP options to implement EasyDeploy, complete the following tasks:

- Configure routing to ensure that the DHCP server, file server, and unconfigured devices (have obtained IP addresses) have reachable routes to each other.
- Collect each unconfigured device's MAC address or ESN by viewing the barcode label on the device.

Procedure

Perform the following operations in sequence.

3.5.1 Configuring a File Server

Context

A file server saves the files to be downloaded to unconfigured devices. You can use a switch or server as the file server. Supported file servers include FTP, TFTP, and SFTP servers. Using an SFTP server is recommended.

NOTE

The following procedure configures a Huawei switch as an SFTP server. If a third-party server is used, configure it according to the server manual.

Procedure

Step 1 Enable SFTP.

For details, see **8.3 Local File Management** > **8.3.3 Managing Files When the Device Functions as an SFTP Server** > **Set SFTP server parameters** in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - File Management*.

Step 2 Configure the Secure Shell (SSH) user login interface, user name, authentication method, service type, and SFTP working directory.

For details, see **Configure the VTY user interface for SSH users to log in to the device** and **Configure SSH user information** under **8.3 Local File Management** > **8.3.3 Managing Files When the Device Functions as an SFTP Server** in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - File Management*.

----End

Follow-up Procedure

After configuring the file server, upload the files required by the unconfigured devices to the working directory of the file server. When uploading files, ensure the working directory of the file server has sufficient space to save the files.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

If many devices need to download files from the file server, set the maximum number of concurrent connections on the file server to a large value. If the value is not set to an appropriate number, some devices have to wait until other devices complete downloading, delaying the deployment.

To ensure security of the file server, configure a unique user name for the file server. After the EasyDeploy process is complete, disable the file server function.

3.5.2 Configuring DHCP

Context

Before configuring option fields to implement the EasyDeploy function, deploy a DHCP server from which the unconfigured devices can obtain information about files to be downloaded according to the option configuration.

If the unconfigured devices and the DHCP server are located on the same network segment, you only need to configure the DHCP server. If they are located on different network segments, deploy a DHCP relay agent between the DHCP server and the unconfigured devices.

The DHCP server must support the options required for device deployment. This section provides basic configurations of the DHCP server. For more information about DHCP configuration, see DHCP Configuration in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - IP Services*.

The following procedure configures a Huawei switch as the DHCP server. To use a third-party device as the DHCP server, configure it according to its manual.

Procedure

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

Step 2 Run the **dhcp enable** command to enable DHCP.

Step 3 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 4 (Optional) On an Ethernet interface, run:

```
undo portswitch
```

The interface is switched to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

NOTE

Only the S5720HI, S5720EI, S6720EI, and S6720S-EI support switching between Layer 2 and Layer 3 modes.

Step 5 Run the **dhcp select global** command to configure the interface to use the global IP address pool.

Step 6 Run the **quit** command to return to the system view.

Step 7 Run the **ip pool** *ip-pool-name* command to create a global DHCP address pool and enter its view.

Step 8 Run the **network** *ip-address* [**mask** { *mask* | *mask-length* }] command to specify the range of IP addresses in the global address pool.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- To prevent IP address conflicts, ensure that the configured IP address range does not include the IP addresses specified in the configuration files to be loaded to the unconfigured devices.
- The DHCP server must have sufficient IP addresses to assign to unconfigured devices.

Step 9 Run the **gateway-list** *ip-address* &<1-8> command to set a gateway address for DHCP clients.

Step 10 Run the **option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command to configure DHCP options.

- If devices need to obtain file information according to option fields, configure Option 67.
- Configure at least one file server. For details about DHCP options specifying file server information and other related options, see **Table 3-1** in **3.2.2 Unconfigured Device Deployment Using Option Fields or an Intermediate File**.

----End

3.6 Deploying Unconfigured Devices Using an Intermediate File

Pre-configuration Tasks

Before deploying unconfigured devices using an intermediate file, complete the following tasks:

- Configure routing to ensure that the DHCP server, file server, and devices to be configured (have obtained IP addresses) have reachable routes to each other.
- Collect each unconfigured device's MAC address or ESN by viewing the barcode label on the device.

Procedure

Perform the following operations in sequence.

3.6.1 Configuring a File Server

Context

A file server saves the files to be downloaded to unconfigured devices. You can use a switch or server as the file server. Supported file servers include FTP, TFTP, and SFTP servers. Using an SFTP server is recommended.

NOTE

The following procedure configures a Huawei switch as an SFTP server. If a third-party server is used, configure it according to the server manual.

Procedure

Step 1 Enable SFTP.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

For details, see **8.3 Local File Management** > **8.3.3 Managing Files When the Device Functions as an SFTP Server** > **Set SFTP server parameters** in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - File Management*.

Step 2 Configure the Secure Shell (SSH) user login interface, user name, authentication method, service type, and SFTP working directory.

For details, see **Configure the VTY user interface for SSH users to log in to the device** and **Configure SSH user information** under **8.3 Local File Management** > **8.3.3 Managing Files When the Device Functions as an SFTP Server** in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - File Management*.

----End

Follow-up Procedure

After configuring the file server, upload the files required by the unconfigured devices to the working directory of the file server. When uploading files, ensure the working directory of the file server has sufficient space to save the files.

If many devices need to download files from the file server, set the maximum number of concurrent connections on the file server to a large value. If the value is not set to an appropriate number, some devices have to wait until other devices complete downloading, delaying the deployment.

To ensure security of the file server, configure a unique user name for the file server. After the EasyDeploy process is complete, disable the file server function.

3.6.2 Editing an Intermediate File

Context

If neither Option 148 nor Option 67 (configuration file information) is configured on the DHCP server, EasyDeploy is implemented using an intermediate file.

An intermediate file is saved on a file server to specify information about files to be downloaded. Each line in an intermediate file specifies the MAC address or ESN of a device and files for the device. After an unconfigured device obtains the IP address of the file server, the device downloads the intermediate file from the file server. After the device finds the system software name, system software version, patch file name, web page file name, and configuration file name that match its MAC address or ESN, it downloads the files from the file server.

You can edit an intermediate file by writing MAC addresses or ESNs of the devices to be configured and names of the matching system software packages, patch files, web page files, and configuration files in the intermediate file.

Procedure

1. Create a text file and name it **lswnet.cfg**.
2. Edit the file.

   When editing a line for a device, enter the device's MAC address, ESN, or both. The configuration file is mandatory. The system software, web page file, and patch file are optional and can be written in any sequence.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

If the intermediate file contains the software version, the system software package name must be specified in the intermediate file, and the version of the specified system software must be the same as the software version specified in the intermediate file.

For example, assume that a device's MAC address is 0018-82C5-AA89 and ESN is 9300070123456789 and the device needs to download the software package **auto_V200R009C00SPC200.cc** (version V200R009C00SPC200), patch file **auto_V200R009C00.pat**, configuration file **auto_V200R009C00.cfg**, and web page file **auto_V200R009C00.web.7z**, write the following content in the intermediate file (fields in the intermediate file must be in lowercase):

```
mac=0018-82C5-
AA89;vrpfile=auto_V200R009C00SPC200.cc;vrpver=V200R009C00SPC200;patchfile=auto
_V200R009C00.pat;cfgfile=auto_V200R009C00.cfg;webfile=auto_V200R009C00.web.7z;
```

You can also specify the paths of the system software, patch file, web page file, and configuration file in the intermediate file. In the following file, **auto** is the folder that saves the files on the file server.

```
mac=0018-82C5-AA89;vrpfile=auto/
auto_V200R009C00SPC200.cc;vrpver=V200R009C00SPC200;patchfile=auto/
auto_V200R009C00.pat;cfgfile=auto/auto_V200R009C00.cfg;webfile=auto/
auto_V200R009C00.web.7z;
```

NOTE

- If multiple devices need to be configured, each line in the intermediate file records file information for a device. The size of the intermediate file cannot exceed 1 MB.
- The file path specified in the intermediate file contains a maximum of 48 characters.

3.6.3 Configuring DHCP

Context

Before deploying unconfigured devices using an intermediate file, you must configure a DHCP server to allow the unconfigured devices to obtain IP addresses, file server addresses, and intermediate file names from the DHCP server.

If the devices to be configured and the DHCP server are located on the same network segment, you only need to configure the DHCP server. If they are located on different network segments, deploy a DHCP relay agent between the DHCP server and the devices to be configured.

The DHCP server must support the options required for device deployment. This section provides basic configurations of the DHCP server. For more information about DHCP configuration, see DHCP Configuration in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - IP Services*.

In the following operations, the DHCP server is Huawei switch. If a third-party device is used, configure them according to the manual of the device.

Procedure

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

Step 2 Run the **dhcp enable** command to enable DHCP.

Step 3 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 4 (Optional) On an Ethernet interface, run:

```
undo portswitch
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

The interface is switched to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

NOTE

Only the S5720HI, S5720EI, S6720EI, and S6720S-EI support switching between Layer 2 and Layer 3 modes.

Step 5 Run the **dhcp select global** command to configure the interface to use the global IP address pool.

Step 6 Run the **quit** command to return to the system view.

Step 7 Run the **ip pool** *ip-pool-name* command to create a DHCP address pool and enter its view.

Step 8 Run the **network** *ip-address* [**mask** { *mask* | *mask-length* }] command to specify the range of IP addresses in the global address pool.

- To prevent IP address conflicts, ensure that the IP address range does not include the IP addresses specified in the configuration file to be loaded to the unconfigured devices.
- The DHCP server must have sufficient IP addresses to assign.

Step 9 Run the **gateway-list** *ip-address* &<1-8> command to set a gateway address for DHCP clients.

Step 10 Run the **option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command to configure DHCP option fields.

- If devices obtain file information using an intermediate file, do not configure Option 67. Instead, configure Option 146 and set the netfile field to the name of the intermediate file.
- Configure at least one file server. For details about DHCP options specifying file server information and other related options, see **Table 3-1** in **3.2.2 Unconfigured Device Deployment Using Option Fields or an Intermediate File**.

----End

3.7 Deploying Pre-configured Devices Using an Intermediate File

NOTE

Pre-configured commands are contained in the configuration file delivered together with the device. This configuration file can be customized as required. When the device is running properly, these commands cannot be manually executed.

When the device is running properly, to start the pre-configured device deployment process, specify the configuration file for the next startup again and restart the device. The configuration file for the next startup must contain pre-configured device deployment commands.

Pre-configuration Tasks

Before deploying unconfigured devices using an intermediate file, complete the following tasks:

- Configure routing to ensure that the DHCP server, file server, and devices to be configured (have obtained IP addresses) have reachable routes to each other.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

- Collect each unconfigured device's MAC address or ESN by viewing the barcode label on the device.

Procedure

Perform the following operations in sequence.

3.7.1 Configuring a File Server

Context

A file server saves the files to be downloaded to unconfigured devices. You can use a switch or server as the file server. Supported file servers include FTP, TFTP, and SFTP servers. Using an SFTP server is recommended.

NOTE

The following procedure configures a Huawei switch as an SFTP server. If a third-party server is used, configure it according to the server manual.

Procedure

Step 1 Enable SFTP.

For details, see **8.3 Local File Management** > **8.3.3 Managing Files When the Device Functions as an SFTP Server** > **Set SFTP server parameters** in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - File Management*.

Step 2 Configure the Secure Shell (SSH) user login interface, user name, authentication method, service type, and SFTP working directory.

For details, see **Configure the VTY user interface for SSH users to log in to the device** and **Configure SSH user information** under **8.3 Local File Management** > **8.3.3 Managing Files When the Device Functions as an SFTP Server** in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - File Management*.

----End

Follow-up Procedure

After configuring the file server, upload the files required by the unconfigured devices to the working directory of the file server. When uploading files, ensure the working directory of the file server has sufficient space to save the files.

If many devices need to download files from the file server, set the maximum number of concurrent connections on the file server to a large value. If the value is not set to an appropriate number, some devices have to wait until other devices complete downloading, delaying the deployment.

To ensure security of the file server, configure a unique user name for the file server. After the EasyDeploy process is complete, disable the file server function.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.7.2 Editing an Intermediate File

Context

An intermediate file is saved on a file server to specify information about an SNMP host's IP address and files to be downloaded. Each line in the intermediate file specifies the MAC address or ESN of a device and files for the device. After a device to be deployed obtains the IP address of the file server, the device downloads the intermediate file from the file server. After the device finds the system software name, system software version, patch file name, web page file name, and configuration file name that match its MAC address or ESN, it downloads the files from the file server. Alarms generated by a pre-configured device can be sent to an SNMP host with a specified address.

Procedure

You can edit an intermediate file by writing MAC addresses or ESNs of the devices to be configured and names of the matching system software packages, patch files, web page files, and configuration files in the intermediate file. Perform the following steps to edit an intermediate file:

1. Create a text file with a name extension **.cfg**.
2. Edit the file.

   When editing a line for a device, enter the device's MAC address, ESN, or both. The configuration file is mandatory. The system software, web page file, and patch file are optional and can be written in any sequence.

   If the intermediate file contains the software version, the system software package name must be specified in the intermediate file, and the version of the specified system software must be the same as the software version specified in the intermediate file.

   For example, assume that a device's MAC address is 0018-82C5-AA89 and ESN is 9300070123456789, and the device needs to download the software package **auto_V200R009C00SPC200.cc** (version V200R009C00SPC200), patch file **auto_V200R009C00.pat**, configuration file **auto_V200R009C00.cfg**, and web page file **auto_V200R009C00.web.7z**. The SNMP host's IP address is 192.168.1.1. Write the following content in the intermediate file (fields in the intermediate file must be in lowercase):

   ```
   snmphostv4=192.168.1.1;
   mac=0018-82C5-
   AA89;vrpfile=auto_V200R009C00SPC200.cc;vrpver=V200R009C00SPC200;patchfile=auto
   _V200R009C00.pat;cfgfile=auto_V200R009C00.cfg;webfile=auto_V200R009C00.web.7z;
   ```

   You can also specify the paths of the system software, patch file, web page file, and configuration file in the intermediate file. In the following file, **auto** is the folder that saves the files on the file server.

   ```
   snmphostv4=192.168.1.1;
   mac=0018-82C5-
   AA89;vrpfile=auto_V200R009C00SPC200.cc;vrpver=V200R009C00SPC200;patchfile=auto
   _V200R009C00.pat;cfgfile=auto_V200R009C00.cfg;webfile=auto_V200R009C00.web.7z;
   ```

   NOTE

   - If multiple devices need to be configured, each line in the intermediate file records file information for a device. The size of the intermediate file cannot exceed 1 MB.
   - The file path specified in the intermediate file contains a maximum of 48 characters.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.7.3 Configuring DHCP

Context

Before deploying devices to be deployed using an intermediate file, you must configure a DHCP server to allow the devices to obtain IP addresses, file server addresses, and intermediate file names from the DHCP server.

If the devices to be configured and the DHCP server are located on the same network segment, you only need to configure the DHCP server. If they are located on different network segments, deploy a DHCP relay agent between the DHCP server and the devices to be configured.

In the following operations, the DHCP server is Huawei switch. If a third-party device is used, configure them according to the manual of the device.

NOTE

The DHCP server must support the options required for device deployment. This section provides basic configurations of the DHCP server. For more information about DHCP configuration, see DHCP Configuration in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - IP Services*.

Procedure

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

Step 2 Run the **dhcp enable** command to enable DHCP.

Step 3 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 4 (Optional) On an Ethernet interface, run:

```
undo portswitch
```

The interface is switched to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

NOTE

Only the S5720HI, S5720EI, S6720EI, and S6720S-EI support switching between Layer 2 and Layer 3 modes.

Step 5 Run the **dhcp select global** command to configure the interface to use the global IP address pool.

Step 6 Run the **quit** command to return to the system view.

Step 7 Run the **ip pool** *ip-pool-name* command to create a DHCP address pool and enter its view.

Step 8 Run the **network** *ip-address* [**mask** { *mask* | *mask-length* }] command to specify the range of IP addresses in the global address pool.

- To prevent IP address conflicts, ensure that the IP address range does not include the IP addresses specified in the configuration file to be loaded to the devices to be deployed.
- The DHCP server must have sufficient IP addresses to assign.

Step 9 Run the **gateway-list** *ip-address* &<1-8> command to set a gateway address for DHCP clients.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.7.4 Deploying a Pre-configured Device

Context

Before delivery, a device can load a configuration file that contains commands for specifying file server addresses, name of an intermediate file for site deployment, and a shared key between the device and an SNMP host. After your simple login configuration, the device can automatically obtain and load correct configurations, reducing the manual operation cost.

NOTE

Pre-configured devices stay in the Busy state when being deployed. You can execute only display commands, not configuration commands.

Pre-configured device deployment commands are contained in the configuration file delivered together with the device. When the device is running properly, these commands cannot be manually executed.

When the device is running properly, to start the pre-configured device deployment process, specify the configuration file for the next startup again and restart the device. The configuration file for the next startup must contain pre-configured device deployment commands.

If you do not need the pre-configured device deployment function, run undo commands to delete these configurations to prevent them from affecting other functions.

Related Commands

Table 3-6 lists the pre-configured commands in a device's configuration file.

Table 3-6 Pre-configured commands

Function	Command	Remarks
Enable pre-configured device deployment.	**easy-operation client ztp-with-cfg enable**	By default, pre-configured device deployment is disabled.
(Optional) Specify an intermediate file for pre-configured device deployment.	**easy-operation client netfile** *filename*	By default, devices use the intermediate file **lswnet.cfg** for pre-configured device deployment.
Configure file servers.	**Specifying IP addresses:** ● **easy-operation client ftp-server** *ipaddress* &<1-4> [**username** *username* [**password** *password*]] ● **easy-operation client sftp-server** *ipaddress* &<1-4> [**username** *username* [**password** *password*]] ● **easy-operation client ftp-server ip-address** *ipaddress* &<1-4>	● Only one type of file server can be specified. ● A file server can be specified using either an IP address or URL. ● If a user name and a password have been set on an SFTP or FTP server, the device must have the same user name and password configured. ● FTP and TFTP have security risks. Using an

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Function	Command	Remarks
	Specifying URLs: ● **easy-operation client ftp-server-url** *ipaddress* [**username** *username* [**password** *password*]] ● **easy-operation client sftp-server-url** *ipaddress* [**username** *username* [**password** *password*]] ● **easy-operation client ftp-server-url ip-address** *ipaddress*	SFTP file server is recommended.
Configure a shared key between the device and an SNMP host.	**easy-operation client snmp securityname cipher** *password*	-

Configuration File Example

A batch of pre-configured Huawei switches needs to be deployed. The intermediate file **ztpwithcfg.cfg** and version files have been uploaded to the SFTP file server with IP address 10.1.1.1, user name **test**, and password **easyoperation**. The shared key between the switches and SNMP host is **huawei123**.

The configuration files of the switches contain the following configurations:

```
#
easy-operation client ztp-with-cfg enable
easy-operation client netfile ztpwithcfg.cfg
easy-operation client sftp-server ip-address 10.1.1.1 username test password
easyoperation
easy-operation client snmp securityname cipher huawei123
#
return
```

3.8 Deploying Unconfigured Devices Using the Commander

There are two methods for deploying unconfigured devices using the Commander, depending on whether the network topology collection function is enabled on the Commander.

When the network topology collection function is enabled, users do not need to manually collect such information as device's MAC address or ESN; the Commander automatically collects device information and assigns client IDs to devices to bind device information with devices.

When the network topology collection function is disabled, users need to manually collect each device's MAC address or ESN and specify the binding relationship between client ID and device.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Pre-configuration Tasks

Before deploying unconfigured devices using the Commander, complete the following tasks:

- If the network topology collection function is disabled:
  - Ensure that reachable routes exist between the DHCP server, file server, Commander, and clients with IP addresses assigned.
  - Collect each unconfigured device's MAC address or ESN by viewing the barcode label on the device.
- If the network topology collection function is enabled:
  - Ensure that reachable routes exist between the DHCP server, file server, Commander, and clients with IP addresses assigned.
  - Power on and start the clients.

Procedure

Perform the following operations in sequence.

3.8.1 Configuring a File Server

Context

A file server stores the files to be downloaded by clients. The Commander can function as a file server. Before configuring the Commander as a file server, ensure that there is sufficient storage space for the files. Generally, a third-party server is used as the file server on an EasyDeploy network.

Supported file servers include FTP, TFTP, and SFTP servers. Using an SFTP server is recommended.

NOTE

In the following operations, a Huawei switch is used as the SFTP server. If a third-party server is used, configure it according to the server manual.

Procedure

Step 1 Enable SFTP.

For details, see **8.3 Local File Management** > **8.3.3 Managing Files When the Device Functions as an SFTP Server** > **Set SFTP server parameters** in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - Configuration Guide - Basic Configuration- File Management*.

Step 2 Configure the user login page, user name, authentication mode, service mode, and SFTP service authorized directory for the SSH user.

For details, see **8.3 Local File Management** > **8.3.3 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 the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - Configuration Guide - Basic Configuration- File Management*.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Follow-up Procedure

After configuring the file server, save the files to be downloaded in the working directory of the file server.

If many devices need to download files from the file server, set the maximum number of concurrent connections on the file server to a large value. If the value is not set to an appropriate number, some devices have to wait until other devices complete downloading, delaying the deployment.

To ensure security of the file server, configure a unique user name for the file server. After the EasyDeploy process is complete, disable the file server function.

3.8.2 Configuring DHCP

Context

Before deploying unconfigured devices, you must configure the DHCP functions to allow the DHCP clients to obtain an IP address and Commander's address from the DHCP server. The clients then can communicate with the Commander to obtain information about the files they need to download.

If the clients and server are located on the same network segment, you only need to configure the DHCP server. If they are located on different network segments, deploy a DHCP relay agent between the server and clients.

You can configure the Commander, another Huawei switch, or a third-party device on the network as the DHCP server or DHCP relay agent. In the following operations, another Huawei switch is configured as the DHCP server. If a third-party device is used, configure them according to the manual of the device.

The DHCP server must support the options required for device deployment. This section provides basic configurations of the DHCP server. For more information about DHCP configuration, see DHCP Configuration in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - IP Services*.

Procedure

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

Step 2 Run the **dhcp enable** command to enable DHCP.

Step 3 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 4 (Optional) On an Ethernet interface, run:

```
undo portswitch
```

The interface is switched to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

NOTE

Only the S5720HI, S5720EI, S6720EI, and S6720S-EI support switching between Layer 2 and Layer 3 modes.

Step 5 Run the **dhcp select global** command to configure the interface to use the global IP address pool.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 6 Run the **quit** command to return to the system view.

Step 7 Run the **ip pool** *ip-pool-name* command to create a DHCP address pool and enter its view.

Step 8 Run the **network** *ip-address* [**mask** { *mask* | *mask-length* }] command to specify the range of IP addresses in the global address pool.

- To prevent IP address conflicts, ensure that the configured IP address range does not include the IP addresses specified in the configuration files.
- The DHCP server must have sufficient IP addresses to assign.

Step 9 Run the **gateway-list** *ip-address* &<1-8> command to set a gateway address for DHCP clients.

Step 10 Run the **option 148 ascii** *ascii-string* command to configure DHCP option fields.

- The **option 148** parameter must be specified first, indicating the Commander's IP address. After this parameter is specified, the clients implement EasyDeploy using the Commander.
- The *ascii-string* parameter is set in the format of "ipaddr=*ip-address*;port=*udp-port*;". For example, if the IP address and port number of the Commander are 10.10.10.1 and 60000, respectively, the *ascii-string* parameter is expressed as **ipaddr=10.10.10.1;port=60000;** or **ipaddr=10.10.10.1;** (the default port number 60000 is omitted).

----End

3.8.3 Configuring the Commander

Configuring Basic Commander Functions

Context

To implement EasyDeploy using the Commander, you must configure a device on a network as the Commander.

NOTE

For unified device management, specify only one device as the Commander on a networking running EasyDeploy.

Procedure

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

Step 2 Run the **easy-operation commander ip-address** *ip-address* [**udp-port** *udp-port*] command to configure the Commander IP address.

The specified IP address must exist on the network.

Step 3 Run the **easy-operation commander enable** command to enable the Commander function.

By default, the Commander function is disabled.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuring File Server Information

Context

File server information includes the IP address of the file server from which clients obtain files, user names, and passwords.

The files clients need to download are saved on the file server. After obtaining information about files to be downloaded, clients download specific files from the file server specified by the Commander based on the obtained file information.

Procedure

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

Step 2 Run the **easy-operation** command to enter the Easy-Operation view.

Step 3 Perform any of the following steps based on the file server type:

- Run the **tftp-server** *ip-address* command to assign an IP address to the TFTP server.
- Run the **ftp-server** *ip-address* [**username** *username* [**password** *password*]] command to assign an IP address to the FTP server and configure a user name and password.
- Run the **sftp-server** *ip-address* [**username** *username* [**password** *password*]] command to assign an IP address to the SFTP server and configure a user name and password.

  If the file server is an SFTP or FTP server and has a user name and password configured, configure the user name and password on the Commander.

  Only information about one file server can be configured. If you run this command multiple times, only the latest configuration takes effect.

  NOTE

  Using an SFTP server is recommended. FTP and TFTP protocols are less secure than SFTP.

----End

(Optional) Configuring Network Topology Collection

Context

Network topology collection is provided by the Commander using the Neighbor Discovery Protocol (**NDP**) and Network Topology Discovery Protocol (**NTDP**). When this function is enabled on the Commander to deploy unconfigured devices, users do not need to manually collect such information as device's MAC address or ESN. After unconfigured devices are powered on and started, the Commander automatically collects device information and assigns client IDs to devices to bind device information with devices.

Procedure

1. Enable NDP.
   a. Run the **system-view** command to enter the system view.
   b. Run the **ndp enable** command to enable NDP globally.

      By default, NDP is enabled globally.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

c. (Optional) Run the **ndp enable interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10> command to enable NDP on interfaces.

   By default, NDP is enabled on an interface.

d. (Optional) Run the **ndp timer aging** *aging-time* command to configure an aging time for NDP packets.

   By default, the aging time of the NDP packets on the receiving switch is 180 seconds. The aging time of the NDP packets must be larger than the interval for sending NDP packets.

e. (Optional) Run the **ndp timer hello** *interval* command to set the interval for sending NDP packets.

   By default, the interval for sending NDP packets is 60 seconds. The interval for sending NDP packets must be smaller than the aging time of the NDP packets.

f. (Optional) Run the **ndp trunk-member enable** command to enable trunk member interface-based NDP.

   By default, trunk member interface-based NDP is disabled.

   If links are established between devices through trunk interfaces, the system discovers neighbors and displays NTDP topology information based on the trunk interfaces. To obtain link information about trunk member interfaces, run this command to enable trunk member interface-based NDP for the system to discover neighbors and query topology information about the trunk member interfaces from the NMS.

2. Enable NTDP.

   a. Run the **ntdp enable** command to enable NTDP globally.

      By default, NTDP is enabled globally.

   b. (Optional) Enable NTDP on an interface.

      i. Run the **interface range** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> command to enter the interface group view.

      ii. Run the **ntdp enable** command to enable NTDP on an interface.

      By default, NTDP is enabled on an interface.

      iii. Run the **quit** command to return to the system view.

   c. (Optional) Run the **ntdp hop** *max-hop-value* command to set the maximum number of hops for collecting topology information using NTDP.

      By default, the maximum number of hops for collecting topology information using NTDP is 8. When the maximum number of hops is set to a large value, large memory space is occupied on the topology collection device.

   d. (Optional) Run the **ntdp timer hop-delay** *hop-delay-time* command to set the delay for the first interface to forward NTDP topology request packets.

      By default, the delay for the first interface to forward NTDP topology request packets is 200 milliseconds.

   e. (Optional) Run the **ntdp timer port-delay** *port-delay-time* command to set the delay for the other interfaces to forward NTDP topology request packets.

      By default, the delay for other interfaces to forward NTDP topology request packets is 20 milliseconds.

   f. Run the **ntdp timer** *interval* command to set the interval for collecting topology information.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

By default, the interval for collecting topology information using NTDP is 0, which indicates that topology information is not periodically collected.

NOTE

The Commander collects network topology information at an interval of 5 minutes; therefore, you are advised to set the interval for collecting topology information using NTDP to less than 5 minutes.

g. (Optional) Run the **ntdp explore** command in the user view to collect topology information manually.

You can run this command to collect network topology information at any time.

3. Configure a cluster management VLAN.
   a. Run the **system-view** command to enter the system view.
   b. Run the **cluster enable** command to enable the cluster function.

      By default, the cluster function is disabled.
   c. Run the **cluster** command to enter the cluster view.
   d. Run the **mngvlanid** *vlanid* command to configure a cluster management VLAN.

      By default, the cluster management VLAN is VLAN 1. However, VLAN 1 is not recommended as the cluster management VLAN. You are advised to change the cluster management VLAN to a different VLAN.

      NOTE

      The cluster management VLAN must be the same as the VLAN to which the Commander's interfaces connected to clients.
4. Configure Commander topology collection.
   a. Run the **system-view** command to enter the system view.
   b. Run the **easy-operation** command to enter the Easy-Operation view.
   c. Run the **topology enable** command to enable the Commander to collect network topology information.

      By default, the Commander cannot collect network topology information.
   d. (Optional) Run the **topology save** command to save the currently collected network topology information.
   e. (Optional) Run the **client auto-join enable** command to enable clients to automatically join the management domain of the Commander.

      By default, clients do not automatically join the management domain of the Commander.

      After a client automatically joins the management domain of the Commander, the Commander automatically learns client information and assigns the minimum ID not in use to the client. If the auto-join function is not enabled, the Commander does not assign IDs to clients, and you must run the **client** [*client-id*] { **mac-address** *mac-address* | **esn** *esn* } command to assign IDs to clients.

Example

Run the **display easy-operation topology** command to view network topology information collected by the Commander after clients are enabled to automatically join the management domain of the Commander.

```
<HUAWEI> display easy-operation topology
<-->:normal device          <??>:lost device
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
Total topology node number: 3
------------------------------------------------------------------------------
[HUAWEI: 4CB1-6C8F-0447](Commander)
|-(GE0/0/8)<-->(GE0/0/38)[HUAWEI: 0200-2326-1007](Client 1)
| |-(GE0/0/16)<-->(GE0/0/16)[HUAWEI: 0200-0000-0001](Client 2)
```

The command output shows that IDs are assigned to clients within the management domain of the Commander. If the auto-join function is not enabled, client IDs are not displayed.

Configuring Information About Files to Be Downloaded

Context

Information about files to be downloaded by clients includes the configuration file name (mandatory), system software package name and version number, and patch file name.

When deploying unconfigured devices, you can specify file information for each device or specify the same file information for a group of devices with the same attribute. The system preferentially matches the rule of a single client. If no matching rule is found, the system then matches the rule of a group. If still no matching rule is found or a rule is matched but no file information is specified in the rule, the system uses the default file information.

Procedure

Perform the following steps based on the network planning.

Configure file information for a client.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. In the following two situations, you need to manually bind device information with devices. In other situations, go to the next step.
   - Unconfigured devices are deployed without using the network topology collection function:

     Run the **client** [*client-id*] { **mac-address** *mac-address* | **esn** *esn* } command to define a matching rule for the client. The client can be uniquely identified by a MAC address or an ESN.

     If *client-id* is not specified, the system assigns the smallest unused ID to the client.
   - Unconfigured devices are deployed using the network topology collection function, but client auto-join is disabled:

     Run the **client** [*client-id*] **mac-address** *mac-address* command to define a matching rule based on the client's MAC address.
4. Run the **client** *client-id* { **system-software** *file-name* [*version*] | **patch** *file-name* | **configuration-file** *file-name* | **web-file** *file-name* | { **custom-file** *file-name* } &<1-3> }* command to configure information about files to be downloaded.

Configure file information for a client group.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Perform either of the following steps based on the group type:
   - Configure a matching rule for a built-in group.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

i. Run the **group build-in** *device-type* command to create a built-in group and enter the group view.

- Configure a matching rule for a customized group.

  i. Run the **group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name* command to create a customized group and enter the group view.

  ii. Run the **match** { **mac-address** *mac-address* [*mac-mask* | *mac-mask-length*] | **esn** *esn* | **ip-address** *ip-address* [*ip-mask* | *ip-mask-length*] | **model** *model* | **device-type** *device-type* } command to define the matching rule for the customized group.

NOTE

- A maximum of 256 groups can be created and a maximum of 256 matching rules can be defined for the groups on the Commander. For groups created based on MAC addresses, IP addresses, or ESNs, multiple matching rules can be defined. For groups created based on device types and models, only one matching rule can be defined for each group.
- If multiple types of groups are configured, the clients match the groups in the following sequence: MAC address > ESN > IP address > device model > device type in the customized group > device type in the built-in group.
- If a client matches multiple groups of the same type, the groups are selected in alphabetical order of their names.

4. Perform the following steps based on your requirements to specify the files to be downloaded:
   - Run the **system-software** *file-name version* command to specify the system software package name and version number.
   - Run the **patch** *file-name* command to specify the patch file name.
   - Run the **configuration-file** *file-name* command to specify the configuration file name.
   - Run the **web-file** *file-name* command to specify the web page file name.
   - Run the { **custom-file** *file-name* } &<1-3> command to specify the user-defined file name. A maximum of three user-defined files can be specified.

Configure default file information.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Perform the following steps based on your requirements to specify the files to be downloaded:
   - Run the **system-software** *file-name version* command to specify the system software package name and version number.
   - Run the **patch** *file-name* command to specify the patch file name.
   - Run the **configuration-file** *file-name* command to specify the configuration file name.
   - Run the **web-file** *file-name* command to specify the web page file name.
   - Run the { **custom-file** *file-name* } &<1-3> command to specify the user-defined file name. A maximum of three user-defined files can be specified.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuring an Activation Policy for Downloaded Files

Context

When configuring an activation policy, you can configure a file activation time and a file activation mode.

- Configuring a file activation time involves two values:
  - Specific time to activate files

    Clients will activate files at a specified time.
  - Delay time before activating files

    Clients activate downloaded files after a certain delay. The maximum delay can be 24 hours.
- Configuring a file activation mode involves choosing between two modes:
  - Non-reset mode

    By default, a client activates downloaded files without resetting. However, if a system software package (*.cc) is downloaded, the client resets to activate downloaded files regardless of whether the reset mode is configured. If no system software package is downloaded, the client activates the downloaded files as follows:
    - The patch file is automatically activated.
    - The configuration file is reversely compiled, and commands are saved in the client one by one. The client will use the configuration for next startup. If any command configuration fails during configuration recovery, the client resets to activate the configuration file.
    - The web page file must be activated manually.
  - Reset mode

    A client will use the downloaded system software package, patch file, and configuration file for the next startup. The web page file must be activated manually after the client resets.
    - If a hot patch needs to be downloaded, you can use the default file activation mode (non-reset). If a cold patch needs to be downloaded, set the file activation mode to reset.
    - If the client uses the non-reset mode to activate a configuration file but some commands in the configuration file cannot be restored, the client automatically uses the reset mode to activate the configuration file.
    - If some clients have downstream clients attached in cascading networking, it is recommended that you configure the global file activation delay time on the Commander. If an upstream client restarts or updates the configuration immediately after downloading required files, the downstream clients connected to this client are disconnected from the Commander or file server. As a result, the EasyDeploy process fails on the downstream clients. The file activation delay time avoids this problem.

      Set an appropriate delay time based on the size of files to be downloaded, to ensure that all the downstream clients can complete file downloading within this delay time.

Clients select an appropriate activation policy based on the downloaded file information.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- If you configure a group for clients when configuring the file information, the file activation mode and time configured in the group take effect for the matching clients. If no file activation mode or time is configured in the group, the global file activation mode and time configured on the Commander take effect. If no global file activation mode or time is configured on the Commander, the default file activation mode and time are used.
- If you specify a specific client when configuring the file information or retain the default file information, the global file activation mode and time configured on the Commander take effect. If no global file activation mode or time is configured, the default file activation mode and time are used.

Procedure

Configure a file activation policy in the group view.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Run either of the following commands depending on your situation:

   To enter the built-in group view, run the **group build-in** *device-type* command.

   To enter the customized group view, run the **group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name* command.
4. Run the **activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } } * command to configure an activation policy for the group.

Configure a global file activation policy.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Run the **activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }* command to configure a global activation policy.

(Optional) Enabling Clients to Automatically Clear Storage Space

Context

If storage space on a client is insufficient, the client cannot download system software. If this function is enabled, the client automatically deletes non-startup files if the storage space is insufficient.

NOTE

Startup system software, including the running system software and the system software specified for next startup, will not be deleted when a client clears storage space.

This function is invalid for some types of file servers. If the file server is a TFTP server, this function does not take effect because the TFTP server does not return file size to clients. If an FTP or SFTP server does not support the function of returning file size, this function does not take effect. When an S switch serves as an FTP or a TFTP file server, the switch does not support the function of returning file size.

Procedure

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

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 2 Run the **easy-operation** command to enter the Easy-Operation view.

Step 3 Run the **client auto-clear enable** command to enable the client to automatically clear storage space.

By default, a client does not automatically clear storage space.

----End

(Optional) Enabling Automatic Configuration File Backup

Context

After automatic configuration file backup is enabled, the configuration file of a client is automatically backed up to the file server for use in a faulty device replacement scenario. After a faulty client is replaced by a new client, the new client needs to obtain the latest configuration file of the faulty client to minimize impact on service.

Procedure

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

Step 2 Run the **easy-operation** command to enter the Easy-Operation view.

Step 3 Run the **backup configuration interval** *interval* [**duplicate**] command to set the interval and mode of automatic configuration file backup.

By default, the configuration file is not backed up automatically.

----End

3.8.4 Checking 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 have assigned to clients.
- Run the **display easy-operation configuration** command to check the configuration on the Commander.
- Run the **display easy-operation client** [*client-id* | **mac-address** *mac-address* | **esn** *esn* | **verbose**] command to check the client on the Commander.
- Run the **display easy-operation group** [**build-in** [*device-type*] | **custom** [*groupname*]] command to check group configuration on the Commander.
- Run the **display easy-operation download-status** [**client** *client-id* | **verbose**] command to check file download status on a client.
- (With network topology collection enabled) Run the **display ndp** command to check the NDP configuration.
- (With network topology collection enabled) Run the **display ndp interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10> command to check neighbor information discovered through NDP on a specified interface.
- (With network topology collection enabled) Run the **display ntdp** command to check the global NTDP configuration.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- (With network topology collection enabled) Run the **display ntdp device-list** [**verbose**] command to check device information collected using NTDP.
- (With network topology collection enabled) Run the **display easy-operation topology** command to check network topology information collected by the Commander.

----End

3.9 Manually Replacing Faulty Devices Using the Commander

Context

When a client on a network supporting EasyDeploy fails, you can configure replacement information on the Commander so that the new client can quickly obtain the configuration file of the faulty one. This minimizes impact of client failures on the network.

This faulty device replacement function can only be implemented on a network that already has EasyDeploy configured.

In addition, automatic configuration file backup must be enabled on the Commander using the **backup configuration interval** *interval* [**duplicate**] command. If the new client fails to obtain backup configuration file information after you start the unconfigured device deployment process, it attempts to obtain configuration file information from the client database. If the new client still fails to obtain configuration file information, it uses default configuration file information. The default configuration of the new client may differ from the configuration of the faulty client.

Pre-configuration Tasks

Before manually replacing faulty devices using the Commander, complete the following tasks:

- Configure a routing protocol to ensure that the DHCP server, file server, Commander, and new client (has obtained an IP address) have reachable routes to each other.
- **Configure a file server**, **configure the DHCP service**, and **configure the Commander**.
- Ensure that the new client has no configuration file.
- Obtain the MAC address or ESN of each device to be configured by viewing the barcode label on the device.
- Ensure that upgrade files or files to be downloaded have been uploaded to the working directory of the file server.

Procedure

Configure client replacement information.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Run one of the following commands as required:
   - If the new client only needs to restore the configuration of the faulty client, run the **client** *client-id* **replace** { **mac-address** *mac-address* | **esn** *esn* } command to map the *client-id* to the MAC address or ESN of the new client.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- If the new client needs to be upgraded or download other files, run the **client** *client-id* **replace** { { **mac-address** *mac-address* | **esn** *esn* } | **system-software** *file-name* [*version*] | **patch** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> }* command to specify replacement information. The preceding configurations can be completed using the command once or multiple times. You must specify the faulty client ID and the MAC address or ESN of the new client in the command.

Configure an activation policy for downloaded files.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Run the **activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }* command to configure an activation policy for downloaded files.

Replace the faulty device.

Remove the faulty device and connect the new device to the network.

Checking the Configuration

- Run the **display easy-operation client replace** [**verbose**] or **display easy-operation client** *client-id* **replace** command to check client replacement information on the Commander.

3.10 Automatically Replacing Faulty Devices Using the Commander

Context

This faulty device replacement function can only be implemented on a network that already has EasyDeploy configured, network topology information collection has been configured on the Commander, and clients are enabled to join the management domain of the Commander. If a client becomes faulty, a new client can automatically download the backup configuration file to restore the configuration of the faulty client. You do not need to perform any configuration on the new client.

In addition, automatic configuration file backup must be enabled on the Commander using the **backup configuration interval** *interval* [**duplicate**] command. If the new client fails to obtain backup configuration file information after you start the unconfigured device deployment process, it attempts to obtain configuration file information from the client database. If the new client still fails to obtain configuration file information, it uses default configuration file information. The default configuration of the new client may differ from the configuration of the faulty client.

Pre-configuration Tasks

Before automatically replacing faulty devices using the Commander, complete the following tasks:

- Configure a routing protocol to ensure that the DHCP server, file server, Commander, and new client (has obtained an IP address) have reachable routes to each other.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- **Configure a file server**, **configure DHCP**, and **configure the Commander**.
- Ensure that the new client has no configuration file.
- Ensure that upgrade files or files to be downloaded have been uploaded to the working directory of the file server.

Procedure

If the new client needs to be upgraded or download other files besides the configuration file, perform the following steps:

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Run the **client** *client-id* **replace** { { **mac-address** *mac-address* | **esn** *esn* } | **system-software** *file-name* [*version*] | **patch** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> }* command to specify replacement information. The preceding configurations can be completed using the command once or multiple times. You may not specify the MAC address or ESN of the new client.

NOTE

If the new device only needs to obtain the configuration file of the faulty device, you only need to deploy the new device in the same position as the faulty one and do not need to perform the preceding configuration. The new device can automatically download the configuration file.

Configure an activation policy for downloaded files.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Run the **activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }* command to configure an activation policy for downloaded files.

Replace the faulty device.

Remove the faulty device and connect the new device to the network.

Checking the Configuration

- Run the **display easy-operation client replace** [**verbose**] or **display easy-operation client** *client-id* **replace** command to check client replacement information on the Commander.

3.11 Implementing a Batch Upgrade Using the Commander

Context

To upgrade devices that are running properly on a network supporting EasyDeploy, classify devices using the same upgrade file into one group. The network administrator only needs to specify the upgrade file for the group to implement a batch upgrade.

Generally, you need to upgrade system software or patch files of devices. You are advised to create a group based on the following rules:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Create a built-in group if clients are the same model and use the same upgrade files.
- Create a built-in group if clients are different models, but they have the same device type and use the same upgrade files.
- Create a customized group based on client IP addresses if the clients are different models and use different upgrade files.

If no matching rule is found or a rule is matched but no file information is specified in the rule, the system uses the default file information.

Pre-configuration Tasks

Before implementing a batch upgrade using the Commander, complete the following tasks:

- Ensure that reachable routes exist between the file server, Commander and clients.
- **Configure a file server**, **configure basic Commander functions**, and **configure file server information**.
- **Add configured devices to the management domain of the Commander**.
- Ensure that clients operate properly.
- Ensure that upgrade files have been uploaded to the working directory of the file server.

  NOTE

  To enhance security for communication between the Commander and clients and prevent a bogus Commander from controlling clients, run the **easy-operation shared-key** command in the system views of the Commander and clients to configure the same shared key.

Procedure

1. Configure information about files to be downloaded.
   - Configure file information for a client group.
     i. Run the **system-view** command to enter the system view.
     ii. Run the **easy-operation** command to enter the Easy-Operation view.
     iii. Perform either of the following steps based on the group type:
     - Configure a matching rule for a built-in group.
       1) Run the **group build-in** *device-type* command to create a built-in group and enter the group view.
     - Configure a matching rule for a customized group.
       1) Run the **group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name* command to create a customized group and enter the group view.
       2) Run the **match** { **mac-address** *mac-address* [*mac-mask* | *mac-mask-length*] | **esn** *esn* | **ip-address** *ip-address* [*ip-mask* | *ip-mask-length*] | **model** *model* | **device-type** *device-type* } command to define the matching rule for the customized group.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

- A maximum of 256 groups can be created and a maximum of 256 matching rules can be defined for the groups on the Commander. For groups created based on MAC addresses, IP addresses, or ESNs, multiple matching rules can be defined. For groups created based on device types and models, only one matching rule can be defined for each group.
- If multiple types of groups are configured, the clients match the groups in the following sequence: MAC address > ESN > IP address > device model > device type in the customized group > device type in the built-in group.
- If a client matches multiple groups of the same type, the groups are selected in alphabetical order of their names.

iv. Perform the following steps to specify the files to be downloaded:

- Run the **system-software** *file-name* [*version*] command to specify the system software package name and version number.
- Run the **patch** *file-name* command to specify the patch file name.
- Run the **configuration-file** *file-name* command to specify the configuration file name.
- Run the **web-file** *file-name* command to specify the web page file name.
- Run the **license** *file-name* command to specify the license file name.
- Run the { **custom-file** *file-name* } &<1-3> command to specify the user-defined file name. A maximum of three user-defined files can be specified.

– Configure default file information.

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

ii. Run the **easy-operation** command to enter the Easy-Operation view.

iii. Perform the following steps to specify the files to be downloaded:

- Run the **system-software** *file-name* [*version*] command to specify the system software package name and version number.
- Run the **patch** *file-name* command to specify the patch file name.
- Run the **configuration-file** *file-name* command to specify the configuration file name.
- Run the **web-file** *file-name* command to specify the web page file name.
- Run the **license** *file-name* command to specify the license file name.
- Run the { **custom-file** *file-name* } &<1-3> command to specify the user-defined file name. A maximum of three user-defined files can be specified.

2. Configure an activation policy for downloaded files.

If no file activation mode or time is configured in the group, the global file activation mode and time configured on the Commander take effect. If no global file activation mode or time is configured on the Commander, the default file activation mode and time are used.

By default, if downloaded files include the system software or configuration file, the devices activate all files by resetting. If the downloaded files do not include the system software and configuration file, the devices do not reset.

– Configure a file activation policy in the group view.

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

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

ii. Run the **easy-operation** command to enter the Easy-Operation view.

iii. Run either of the following commands depending on your situation:

To enter the built-in group view, run the **group build-in** *device-type* command.

To enter the customized group view, run the **group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name* command.

iv. Run the **activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } } * command to configure an activation policy for the group.

- Configure a global file activation policy.

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

ii. Run the **easy-operation** command to enter the Easy-Operation view.

iii. Run the **activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }* command to configure a global activation policy.

3. Start batch upgrade.

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

b. Run the **easy-operation** command to enter the Easy-Operation view.

c. Run the **upgrade group** [*group-name*] &<1-15> command to start batch upgrade.

Checking the Configuration

- Run the **display easy-operation group** [**build-in** [*device-type*] | **custom** [*groupname*]] command to check the group database on the Commander.
- Run the **display easy-operation download-status** [**client** *client-id* | **verbose**] command to check file download status on a client.

3.12 Implementing a Batch Configuration Using the Commander

Context

To implement a batch configuration of clients on a network supporting EasyDeploy, edit commands to be executed, save them as a script, and deliver the edited commands to clients using the Commander.

You can make scripts in online or offline mode. If a script contains many commands, the offline mode is recommended. If you want to use the online mode, ensure that your inputs are correct. The commands entered in online mode cannot be modified or queried. If an error occurs in online mode, you need to exit from the editing mode and then enter the editing mode to enter all the commands once again.

Pre-configuration Tasks

Before implementing a batch configuration using the Commander, complete the following tasks:

- Ensure that reachable routes exist between the Commander and clients.
- **Configure basic Commander functions**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- **Add configured devices to the management domain of the Commander**.
- Ensure that clients operate properly.

  NOTE

  Run the **easy-operation shared-key** command in the system views of the Commander and clients to configure the same shared key to enhance security for communication between the Commander and clients and prevent a bogus Commander from controlling clients.

Procedure

Step 1 Create a group if you want to deliver commands to a group.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Perform either of the following steps based on the group type:
   - Configure a matching rule for a built-in group.
     i. Run the **group build-in** *device-type* command to create a built-in group and enter the group view.
   - Configure a matching rule for a customized group.
     i. Run the **group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name* command to create a customized group and enter the group view.
     ii. Run the **match** { **mac-address** *mac-address* [*mac-mask* | *mac-mask-length*] | **esn** *esn* | **ip-address** *ip-address* [*ip-mask* | *ip-mask-length*] | **model** *model* | **device-type** *device-type* } command to define the matching rule for the customized group.

Step 2 Edit commands and save them as a script.

- Make a script online.
  a. Run the **system-view** command to enter the system view.
  b. Run the **easy-operation** command to enter the Easy-Operation view.
  c. Run the **batch-cmd begin** command to enter the batch command editing mode.
     - Only one network administrator is allowed to edit commands online at one time.
     - If no operation is performed in the batch command editing mode within 30 seconds, the system automatically exits from the editing mode displays the Easy-Operation view. The complied commands are saved in the script.
  d. Edit commands in the script.
     - The maximum length of a command (including the incomplete command) to be entered is 510 characters. If the command contains more than 510 characters, it cannot be saved in the script.
     - A script can contain a maximum of 200 commands.
     - After you enter a command, press **Enter** to confirm the input. After that, you cannot modify the inputted command.
  e. Press **Ctrl+C** to exit the batch command editing mode.
- Make a script offline.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

To make a script offline, add commands to be executed to a batch processing file one by one. The batch processing file can be edited in .txt mode. Save it in the *.txt or *.bat format and upload the script file to the root directory of the Commander.

The format of the offline script must be the same as the format of a script made online. Scripts cannot contain Chinese characters. To ensure security, scripts made offline should not contain password information.

Step 3 Deliver commands.

- Run the **execute** [*script-file*] **to client** { *client-id1* [**to** *client-id2*] }&<1 - 10> command to deliver commands to a specified client.
- Run the **execute** [*script-file*] **to client all** command to deliver commands to all clients.
- Run the **execute** [*script-file*] **to group** { **name** *group-name* }&<1 - 10> command to deliver commands to a specified group.
- Run the **execute** [*script-file*] **to group all** command to deliver commands to all groups.

If *script-file* is not specified, the Commander delivers a script made online. If *script-file* is specified, the Commander delivers a specific script made offline.

Command execution results are saved in the memory of clients. If the script contains commands used to clear the client memory, such as the **reboot** command, you cannot run the **display easy-operation batch-cmd result** command to check the command execution result after the commands are delivered to clients.

----End

Checking the Configuration

- Run the **display easy-operation batch-cmd result** command to check the command execution results.

3.13 Adding Configured Devices to the Management Domain of the Commander

Context

If you need to monitor and manage configured devices on a network running EasyDeploy, add the configured devices to the management domain of the Commander.

After you add configured devices to the management domain of the Commander on a network running EasyDeploy, the Commander automatically learns basic information about the configured devices, including each device's MAC address, ESN, IP address, device type, device model, and system software.

You can also implement a batch upgrade, batch configuration, and faulty device replacement on these devices.

Pre-configuration Tasks

Before adding configured devices to the management domain of the Commander, complete the following tasks:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Ensure that the configured devices operate properly.
- Ensure that the configured devices have reachable routes to the Commander.
- Ensure that the configured devices have reachable routes to a DHCP server and configure the DHCP server correctly if the configured devices need to obtain information from the DHCP server. The DHCP server configuration in this scenario is the same as the DHCP server configuration in the unconfigured device deployment scenario. For details, see **3.8 Deploying Unconfigured Devices Using the Commander-3.8.2 Configuring DHCP**.

  NOTE

  To enhance security for communication between the Commander and clients and prevent a bogus Commander from controlling clients, run the **easy-operation shared-key** command in the system views of the Commander and clients to configure the same shared key.

Procedure

Step 1 Specify the Commander IP addresses on the clients using either of the following methods:

- Use commands.
  a. Run the **system-view** command to enter the system view.
  b. Run the **easy-operation commander ip-address** *ip-address* [**udp-port** *udp-port*] command to specify the Commander IP address.
- Obtain the Commander IP address from the DHCP server.
  - Enable the DHCP client on the configured devices so that they can obtain IP addresses from the DHCP server. For details about the configuration, see Configuration Guide - IP Service-DHCP Configuration-Configuring a DHCP Client-Enabling the DHCP Client Function.

    The clients can obtain the Commander IP address from the DHCP server only after they are configured to obtain their IP addresses from the DHCP server. The DHCP server sends the Commander IP address to the clients using the Option 148 field in DHCP response messages. Therefore, you must configure the Option 148 field on the DHCP server.

NOTE

- If the configuration files of the clients contain the required configuration, you do not need to configure related functions on the clients again.
- If both methods are available for a client to obtain a Commander IP address, the Commander IP address configured using the command takes effect. If the configured Commander IP address is deleted, the client uses the Commander IP address obtained from the DHCP server. If the client obtains multiple Commander IP addresses from the DHCP server, the client uses the first Commander IP address that it can correctly parse.

Step 2 Perform the following steps on the Commander:

- Manually add configured devices to the management domain of the Commander.
  a. Run the **system-view** command to enter the system view.
  b. Run the **easy-operation** command to enter the Easy-Operation view.
  c. Run the **client** [*client-id*] { **mac-address** *mac-address* | **esn** *esn* } command to define a matching rule for the client. The client can be uniquely identified by a MAC address or an ESN.
- Enable the client auto-join function.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

a. Run the **system-view** command to enter the system view.
b. Run the **easy-operation** command to enter the Easy-Operation view.
c. Run the **client auto-join enable** command to enable clients to automatically join the management domain of the Commander.

   After this function is enabled, the Commander automatically learns basic information about clients.

   By default, clients do not join the management domain of the Commander automatically.

----End

Checking the Configuration

- Run the **display easy-operation client** [*client-id* | **mac-address** *mac-address* | **esn** *esn* | **verbose**] command to check the client database on the Commander.

3.14 Maintaining EasyDeploy

3.14.1 Maintaining Client Information

Context

Client information saved on the Commander includes the global parameter settings, group information, and client information. Based on client information, the Commander determines what files each client needs to load and tracks the client status in real time.

The maximum number of clients managed by the Commander depends on the device specifications. If the number of clients exceeds the upper limit, information about new clients cannot be configured on the Commander. To prevent clients in lost state from occupying the database resources for a long time, enable the function of aging lost state clients. When the aging time expires, lost state clients are deleted. If some clients in lost state occupy the database resources for a long time, delete these clients.

Procedure

Age lost state clients.

1. Run the **system-view** command to enter the system view.
2. Run the **easy-operation** command to enter the Easy-Operation view.
3. Run the **client aging-time** *aging-time* command to age clients in lost state and specify the aging time.

   By default, clients in lost state are not aged.
   - Automatically learnt clients are deleted after their aging time expires.
   - Manually configured clients are not deleted but their status changes to unknown.

Delete lost state clients.

Run the **reset easy-operation client-offline** command in the user view to delete lost state clients.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- If clients are automatically learnt, they can be deleted.
- If clients are configured manually, they cannot be deleted but their status changes to unknown.

Clear the client database.

NOTICE

If you clear the client database, information about configured clients is lost. Exercise caution when you clear the client database.

Run the **reset easy-operation client-database** command in the user view to delete the client database.

After you clear the client database, information about manually configured and automatically learnt clients is deleted. If the client auto-join function is enabled on the Commander, it continues adding learned client information to the client database.

3.14.2 Checking Power Consumption Information

Context

You can view power consumption data on both clients and the Commander to obtain power consumption information on the entire network.

Procedure

Step 1 Run the **display easy-operation power** [**client** *client-id* | **commander**] command to check power consumption information about the Commander and clients.

The parameters specified in commands used to check power consumption information differ between the Commander and clients:

- On the Commander
  - If no parameter is specified, you can check power consumption information about the Commander and all the clients in initial, upgrade, and normal operating states.
  - If **client** *client-id* is specified, you can check power consumption information about the specified client.
  - If **commander** is specified, you can check power consumption information about the Commander.
- On the client

  The parameters **client** *client-id* and **commander** are not supported. You can only check power consumption information about the current client.

----End

3.15 Configuration Examples

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

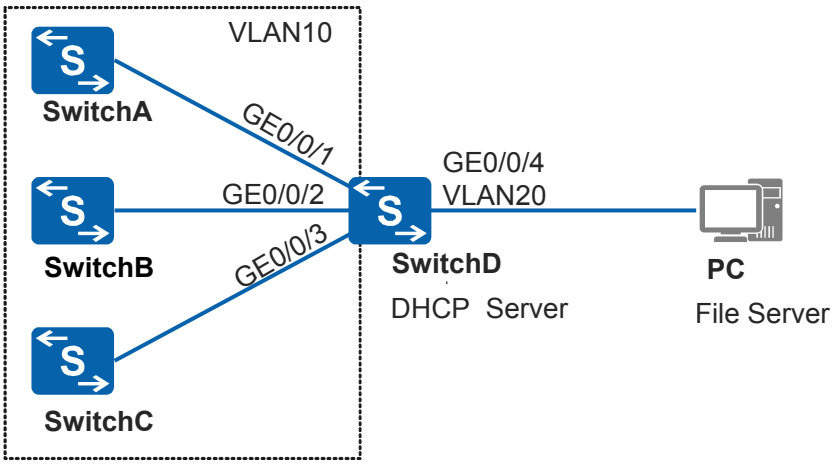
3.15.1 Example for Deploying Unconfigured Devices Using Option Fields

Networking Requirements

Figure 3-15 shows the network of a residential community. SwitchD is an aggregation switch and connects to all devices newly deployed in the community. SwitchA, SwitchB, and SwitchC are three of the new devices and are used as an example here.

All the new devices in the community need to load the same system software, patch file, and configuration file. Since many new devices need to be configured, the customer requires batch configuration of all the new devices to reduce labor costs and device deployment time.

Figure 3-15 Networking diagram for unconfigured device deployment using option fields



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a file server on the PC directly connected to SwitchD. Save the system software, patch file, and configuration file to the working directory of the file server, so that the new devices can obtain these files.
2. Configure SwitchD as a DHCP server to assign network configuration information to new devices. All the new devices require the same system software, patch file, and configuration file; therefore, configure Option 67 and Option 145 on the DHCP server to specify information about the files to be downloaded.
3. Power on SwitchA, SwitchB, and SwitchC. They can automatically start the EasyDeploy process to load the system software, patch file, and configuration file.

Procedure

Step 1 Configure the file server.

Configure the file server according to the server manual.

After completing the configuration, save the required files on the file server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 2 Configure the DHCP server.

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP_Server
[DHCP_Server] dhcp enable
[DHCP_Server] vlan batch 10 20
[DHCP_Server] interface gigabitethernet 0/0/1
[DHCP_Server-GigabitEthernet0/0/1] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[DHCP_Server-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[DHCP_Server-GigabitEthernet0/0/1] quit
[DHCP_Server] interface gigabitethernet 0/0/2
[DHCP_Server-GigabitEthernet0/0/2] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[DHCP_Server-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[DHCP_Server-GigabitEthernet0/0/2] quit
[DHCP_Server] interface gigabitethernet 0/0/3
[DHCP_Server-GigabitEthernet0/0/3] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[DHCP_Server-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[DHCP_Server-GigabitEthernet0/0/3] quit
[DHCP_Server] interface gigabitethernet 0/0/4
[DHCP_Server-GigabitEthernet0/0/4] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/4] port hybrid pvid vlan 20
[DHCP_Server-GigabitEthernet0/0/4] port hybrid untagged vlan 20
[DHCP_Server-GigabitEthernet0/0/4] 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] interface vlanif 20
[DHCP_Server-Vlanif20] ip address 192.168.1.1 255.255.255.0
[DHCP_Server-Vlanif20] 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 s_V200R009C00.cfg
[DHCP_Server-ip-pool-auto-config] option 141 ascii user
[DHCP_Server-ip-pool-auto-config] option 142 cipher huawei123
[DHCP_Server-ip-pool-auto-config] option 143 ip-address 192.168.1.6
[DHCP_Server-ip-pool-auto-config] option 145 ascii
vrpfile=s_V200R009C00.cc;vrpver=V200R009C00SPC200;patchfile=s_V200R009C00.pat;
[DHCP_Server-ip-pool-auto-config] quit
```

Step 3 Power on SwitchA, SwitchB, and SwitchC to start the EasyDeploy process.

Step 4 Verify the configuration.

After the EasyDeploy process ends, log in to the new devices and run the **display startup** command to check the startup system software, configuration file, and patch file. The command output on SwitchA is used as an example.

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:        flash:/s_V200R009C00.cc
  Startup system software:                   flash:/s_V200R009C00.cc
  Next startup system software:              flash:/s_V200R009C00.cc
  Startup saved-configuration file:          flash:/s_V200R009C00.cfg
  Next startup saved-configuration file:     flash:/s_V200R009C00.cfg
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     flash:/s_V200R009C00.pat
  Next startup patch package:                flash:/s_V200R009C00.pat
```

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuration Files

DHCP server configuration file

```
#
sysname DHCP_Server
#
vlan batch 10 20
#
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 s_V200R009C00.cfg
 option 141 ascii user
 option 142 cipher %^%#%AC[/dp2*'%0FWN7]p{SWrB`$}i[:7VBPZQj5@)%%^%#
 option 143 ip-address 192.168.1.6
 option 145 ascii
vrpfile=s_V200R009C00.cc;vrpver=V200R009C00SPC200;patchfile=s_V200R009C00.pat;
#
interface Vlanif10
 ip address 192.168.2.6 255.255.255.0
 dhcp select global
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/4
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

3.15.2 Example for Deploying Unconfigured Devices Using an Intermediate File

Networking Requirements

As shown in **Figure 3-16**, newly delivered devices SwitchA, SwitchB, and SwitchC are deployed in a branch and connect to GE0/0/1, GE0/0/2, and GE0/0/3 of SwitchD, respectively. SwitchD is the egress gateway of the branch and connects to the headquarters network across a Layer 3 network.

SwitchA, SwitchB, and SwitchC are different device models and need to load different system software packages, patch files, and configuration files. The enterprise wants the new devices to automatically download required version files to save labor costs of onsite configuration.

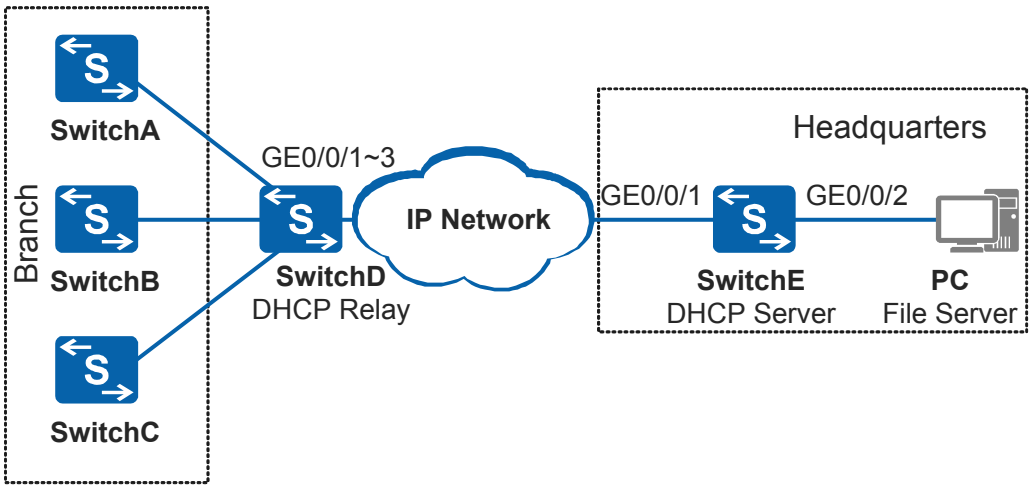
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

The following lists MAC addresses of SwitchA, SwitchB, and SwitchC and the files that the switches need to load:

- SwitchA: Its MAC address is 0025-9e1e-773b and it needs to load the system software package **s57li_easy_V200R009C00.cc** (version V200R009C00SPC100), patch file **s57li_easy_V200R009C00.pat**, and configuration file **s57li_easy_V200R009C00.cfg**.
- SwitchB: Its MAC address is 0025-9e1e-773c and it needs to load the system software package **s2750ei_easy_V200R009C00.cc** (version V200R009C00SPC100), patch file **s2750ei_easy_V200R009C00.pat**, and configuration file **s2750ei_easy_V200R009C00.cfg**.
- SwitchC: Its MAC address is 0025-9e1e-773d and it needs to load the system software package **s57li_easy_V200R009C00.cc** (version V200R009C00SPC100), patch file **s57li_easy_V200R009C00.pat**, and configuration file **s57li_easy_V200R009C00.cfg**.

Figure 3-16 Networking diagram for unconfigured device deployment using an intermediate file across a Layer 3 network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a file server on the PC directly connected to SwitchE.
2. Edit an intermediate file to enable SwitchA, SwitchB, and SwitchC to obtain their system software packages, configuration files, and patch files according to the intermediate file.
3. Save the intermediate file, system software packages, patch files, and configuration files in the working directory of the file server, so that the new devices can obtain these files.
4. Configure DHCP relay on the egress gateway (SwitchD) of the branch, and configure the DHCP server on SwitchE. Then the DHCP server can deliver network configuration to the unconfigured devices across the Layer 3 network.
5. Power on SwitchA, SwitchB, and SwitchC. They can automatically start the EasyDeploy process to load their system software, patch files, and configuration files.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Edit the intermediate file **lswnet.cfg**.

Create a file and name it **lswnet.cfg**. Write the following content in the file:

```
mac=0025-9e1e-773b;vrpfile=s57li_easy_V200R009C00.cc;vrpver=V200R009C00SPC100;patc
hfile=s57li_easy_V200R009C00.pat;cfgfile=s57li_easy_V200R009C00.cfg;
mac=0025-9e1e-773c;vrpfile=s2750ei_easy_V200R009C00.cc;vrpver=V200R009C00SPC100;pa
tchfile=s2750ei_easy_V200R009C00.pat;cfgfile=s2750ei_easy_V200R009C00.cfg;
mac=0025-9e1e-773d;vrpfile=s57li_easy_V200R009C00.cc;vrpver=V200R009C00SPC100;patc
hfile=s57li_easy_V200R009C00.pat;cfgfile=s57li_easy_V200R009C00.cfg;
```

Step 2 Configure the file server.

Configure the file server according to the server manual.

After completing the configuration, save the required files on the file server.

Step 3 Configure SwitchD.

Configure DHCP relay.

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP_Relay
[DHCP_Relay] dhcp enable
[DHCP_Relay] vlan 10
[DHCP_Relay-vlan10] quit
[DHCP_Relay] interface gigabitethernet 0/0/1
[DHCP_Relay-GigabitEthernet0/0/1] port link-type hybrid
[DHCP_Relay-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[DHCP_Relay-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[DHCP_Relay-GigabitEthernet0/0/1] quit
[DHCP_Relay] interface gigabitethernet 0/0/2
[DHCP_Relay-GigabitEthernet0/0/2] port link-type hybrid
[DHCP_Relay-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[DHCP_Relay-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[DHCP_Relay-GigabitEthernet0/0/2] quit
[DHCP_Relay] interface gigabitethernet 0/0/3
[DHCP_Relay-GigabitEthernet0/0/3] port link-type hybrid
[DHCP_Relay-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[DHCP_Relay-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[DHCP_Relay-GigabitEthernet0/0/3] quit
[DHCP_Relay] interface vlanif 10
[DHCP_Relay-Vlanif10] ip address 192.168.1.6 255.255.255.0
[DHCP_Relay-Vlanif10] dhcp select relay
[DHCP_Relay-Vlanif10] dhcp relay server-ip 192.168.2.6
[DHCP_Relay-Vlanif10] quit
```

Configure a static route. Set the destination IP address of the route to the PC's IP address, and the next hop to the IP address of the interface on the Layer 3 network directly connected to SwitchD.

Step 4 Configure SwitchE.

Configure the DHCP server.

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP_Server
[DHCP_Server] dhcp enable
[DHCP_Server] vlan batch 20 30
[DHCP_Server] interface gigabitethernet 0/0/1
[DHCP_Server-GigabitEthernet0/0/1] port link-type trunk
[DHCP_Server-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[DHCP_Server-GigabitEthernet0/0/1] quit
[DHCP_Server] interface gigabitethernet 0/0/2
[DHCP_Server-GigabitEthernet0/0/2] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/2] port hybrid pvid vlan 30
[DHCP_Server-GigabitEthernet0/0/2] port hybrid untagged vlan 30
[DHCP_Server-GigabitEthernet0/0/2] quit
[DHCP_Server] interface vlanif 20
[DHCP_Server-Vlanif20] ip address 192.168.2.6 255.255.255.0
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[DHCP_Server-Vlanif20] dhcp select global
[DHCP_Server-Vlanif20] quit
[DHCP_Server] interface vlanif 30
[DHCP_Server-Vlanif30] ip address 192.168.4.1 255.255.255.0
[DHCP_Server-Vlanif30] quit
[DHCP_Server] ip pool easy-operation
[DHCP_Server-ip-pool-easy-operation] network 192.168.1.0 mask 255.255.255.0
[DHCP_Server-ip-pool-easy-operation] gateway-list 192.168.1.6
[DHCP_Server-ip-pool-easy-operation] option 141 ascii user
[DHCP_Server-ip-pool-easy-operation] option 142 cipher huawei
[DHCP_Server-ip-pool-easy-operation] option 143 ip-address 192.168.4.6
[DHCP_Server-ip-pool-easy-operation] option 146 ascii
opervalue=1;delaytime=0;netfile=lswnet.cfg;
[DHCP_Server-ip-pool-easy-operation] quit
```

Configure a static route. Set the destination IP address of the route to the network segment in the IP address pool configured on SwitchD, and the next hop to the IP address of the interface on the Layer 3 network directly connected to SwitchE.

Step 5 Power on SwitchA, SwitchB, and SwitchC to start the EasyDeploy process.

Step 6 Verify the configuration.

After the EasyDeploy process ends, log in to the new devices and run the **display startup** command to check the startup system software, configuration file, and patch file. The command output on SwitchB is used as an example.

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:        flash:/s2750ei_easy_V200R009C00.cc
  Startup system software:                   flash:/s2750ei_easy_V200R009C00.cc
  Next startup system software:              flash:/s2750ei_easy_V200R009C00.cc
  Startup saved-configuration file:          flash:/s2750ei_easy_V200R009C00.cfg
  Next startup saved-configuration file:     flash:/s2750ei_easy_V200R009C00.cfg
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     flash:/s2750ei_easy_V200R009C00.pat
  Next startup patch package:                flash:/s2750ei_easy_V200R009C00.pat
```

----End

Configuration Files

- DHCP relay agent configuration file

```
#
sysname DHCP_Relay
#
vlan batch 10
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.2.6
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- DHCP server configuration file

```
#
sysname DHCP_Server
#
vlan batch 20 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 141 ascii user
 option 142 cipher %^%#2RC4@B`rZ/{##$1x03%Eh&S.)l7zcQUDl6MLPS"$%^%#
 option 143 ip-address 192.168.4.6
 option 146 ascii opervalue=1;delaytime=0;netfile=lswnet.cfg;
#
interface Vlanif20
 ip address 192.168.2.6 255.255.255.0
 dhcp select global
#
interface Vlanif30
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
return
```

3.15.3 Example for Deploying Unconfigured Devices Using the Commander (with Network Topology Collection Disabled)

Networking Requirements

Figure 3-17 shows a network of an enterprise on which the file server, DHCP server, and SwitchA have reachable routes to each other. New devices Client1, Client2, and Client3 need to be deployed on the enterprise network. The new devices are located on a different network segment from the DHCP server. To reduce labor costs and save time on device deployment, the enterprise wants to realize automatic batch configuration and maintenance of the new devices.

The address of VLANIF 20 on SwitchA is 192.168.4.2/24 and its peer address is 192.168.4.1/24.

The address of VLANIF 30 on SwitchB is 192.168.3.2/24 and its peer address is 192.168.3.1/24.

Table 3-7 lists information about the new devices to be configured.

Copyright © Huawei Technologies Co., Ltd.

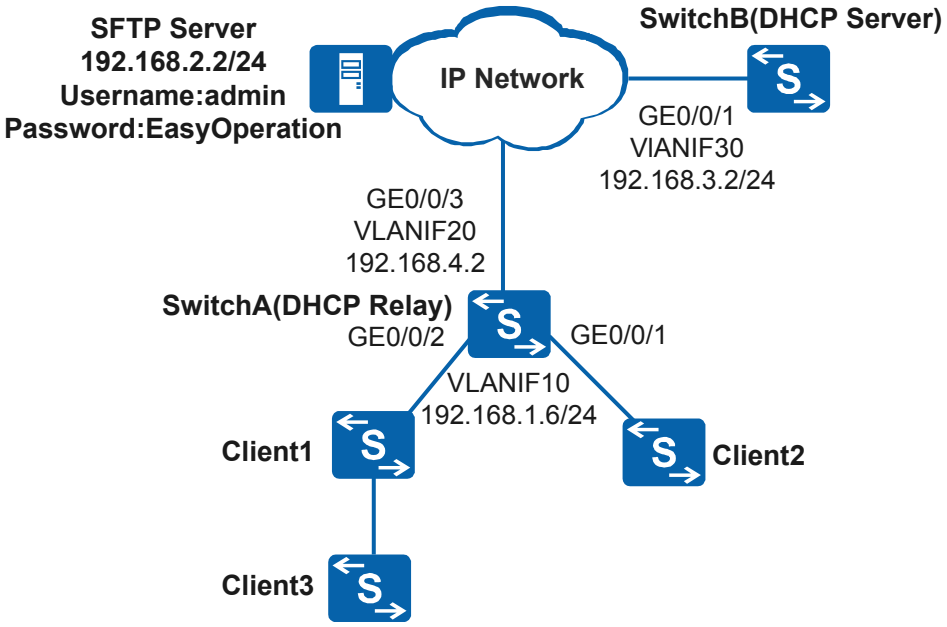
Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 3-7 Device information

New Device	Device Model	Files to Be Loaded
Client1	S5700-HI	s5700-hi.cfg User-defined file header1.txt
Client2	S5700-HI	s5700-hi.cfg User-defined file header1.txt
Client3	S5700-X-LI	s5700-x-li.cfg User-defined file header2.txt

Figure 3-17 Networking diagram for unconfigured device deployment using the commander



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the file server and save the files to be loaded on the file server.
2. Configure the DHCP server function based on the global address pool on SwitchB and configure DHCP relay on SwitchA, so that the new devices can obtain IP addresses of their own and the Commander.
3. Configure the Commander on SwitchA so that the new devices can be configured using the Commander.
   - Enable automatic configuration backup on the Commander to facilitate replacement of faulty devices in future maintenance.
   - Client1 and Client2 are devices of the same type and need to load the same configuration file. Therefore, you can configure a built-in group for them. Client3

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

needs to load a different configuration file. You can specify the file information exclusively for Client3.

- Client3 is connected to Client1 in cascading networking. Therefore, an appropriate global file activation delay time needs to be configured on the Commander to ensure that Client3 has enough time to download the required files.

Procedure

Step 1 Configure the file server.

Configure the file server according to the server manual.

After completing the configuration, save the required files on the file server.

Step 2 Configure the DHCP service.

Configure a DHCP server based on the global address pool.

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] dhcp enable
[SwitchB] vlan batch 30
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] ip address 192.168.3.2 24
[SwitchB-Vlanif30] dhcp select global
[SwitchB-Vlanif30] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type hybrid
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 30
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 30
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] ip pool easy-operation
[SwitchB-ip-pool-easy-operation] network 192.168.1.0 mask 255.255.255.0
[SwitchB-ip-pool-easy-operation] gateway-list 192.168.1.6
[SwitchB-ip-pool-easy-operation] option 148 ascii ipaddr=192.168.1.6;
[SwitchB-ip-pool-easy-operation] quit
```

Configure a default route on SwitchB.

```
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
```

Configure DHCP relay on SwitchA (Commander).

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 20
[SwitchA] dhcp enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 192.168.1.6 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 192.168.4.2 24
[SwitchA-Vlanif20] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type hybrid
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type hybrid
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type hybrid
[SwitchA-GigabitEthernet0/0/3] port hybrid pvid vlan 20
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[SwitchA-GigabitEthernet0/0/3] port hybrid untagged vlan 20
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] dhcp select relay
[SwitchA-Vlanif10] dhcp relay server-ip 192.168.3.2
[SwitchA-Vlanif10] quit
```

Configure a default route on SwitchA.

```
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

Step 3 Configure basic functions for the Commander.

```
[SwitchA] easy-operation commander ip-address 192.168.1.6
[SwitchA] easy-operation commander enable
```

Step 4 Configure file server information.

```
[SwitchA] easy-operation
[SwitchA-easyoperation] sftp-server 192.168.2.2 username admin password
EasyOperation
[SwitchA-easyoperation] backup configuration interval 2
```

Step 5 Configure information about files to be downloaded.

On the Commander, configure a built-in group based on the device type of Client1 and Client2, and specify information about the files to be downloaded in the group.

```
[SwitchA-easyoperation] group build-in S5700-HI
[SwitchA-easyoperation-group-build-in-S5700-HI] configuration-file s5700-hi.cfg
[SwitchA-easyoperation-group-build-in-S5700-HI] custom-file header1.txt
[SwitchA-easyoperation-group-build-in-S5700-HI] quit
```

Specify information about the files to be downloaded to Client3.

```
[SwitchA-easyoperation] client 3 mac-address 5489-9875-edff
[SwitchA-easyoperation] client 3 configuration-file s5700-x-li.cfg custom-file
header2.txt
```

In the Easy-Operation view of the Commander, set the file activation delay time to 15 minutes (900 seconds) based on the size of files that Client3 needs to download.

```
[SwitchA-easyoperation] activate-file delay 900
[SwitchA-easyoperation] quit
```

Step 6 Verify the configuration.

Check global configuration of the Commander.

```
[SwitchA] display easy-operation configuration
------------------------------------------------------------------------------
 Role                            : Commander
 Commander IP address            : 192.168.1.6
 Commander UDP port              : 60000
 IP address of file server       : 192.168.2.2
 Type of file server             : SFTP
 Username of file server         : admin
 Default system-software file    : -
 Default system-software version : -
 Default configuration file      : -
 Default patch file              : -
 Default WEB file                : -
 Default license file            : -
 Default custom file 1           : -
 Default custom file 2           : -
 Default custom file 3           : -
 Auto clear up                   : Disable
 Auto join in                    : Disable
 Topology collection             : Disable
 Activating file time            : Delay 900s
 Activating file method          : Default
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
 Aging time of lost client(hours): -
 Backup configuration file mode  : Default
 Backup configuration file interval(hours): 2
--------------------------------------------------------------------------------
```

Check the file downloading progress on each client after the unconfigured device deployment process starts.

```
[SwitchA] display easy-operation download-status
The total number of client in downloading files is : 3

--------------------------------------------------------------------------------
  ID     Mac address    IP address      Method      Phase         Status
--------------------------------------------------------------------------------
  1      00E0-FC12-A34B 192.168.1.254   Zero-touch  Config-file  Upgrading
  2      00E0-FC34-3190 192.168.1.253   Zero-touch  Config-file  Upgrading
  3      5489-9875-edff 192.168.1.252   Zero-touch  Config-file  Upgrading
```

----End

Configuration Files

SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 10 20
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.3.2
#
interface Vlanif20
 ip address 192.168.4.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 sftp-server 192.168.2.2 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 2
 activate-file delay 900
 client 3 mac-address 5489-9875-EDFF
 client 3 configuration-file s5700-x-li.cfg
 client 3 custom-file header2.txt
 group build-in S5700-HI
  configuration-file s5700-hi.cfg
  custom-file header1.txt
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
#
return
```

SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
#
return
```

3.15.4 Example for Deploying Unconfigured Devices Using the Commander (with Network Topology Collection Enabled)

Networking Requirements

Figure 3-18 shows a network of an enterprise on which the file server, DHCP server, and SwitchA have reachable routes to each other. New devices SwitchC, SwitchD, and SwitchE need to be deployed on the enterprise network. The new devices are located on a different network segment from the DHCP server. To reduce labor costs and save time on device deployment, the enterprise wants to realize automatic batch configuration and maintenance of the new devices. Network topology information collection is configured because the client MAC addresses or ESNs are not reported by the hardware installation engineer.

The address of VLANIF 20 on SwitchA is 192.168.4.2/24 and its peer address is 192.168.4.1/24.

The address of VLANIF 30 on SwitchB is 192.168.3.2/24 and its peer address is 192.168.3.1/24.

Table 3-8 lists information about the new devices to be configured.

Table 3-8 Device information

New Device	Device Model	Files to Be Loaded
SwitchC	S5700-HI	s5700-hi.cfg User-defined file header1.txt
SwitchD	S5700-HI	s5700-hi.cfg User-defined file header1.txt

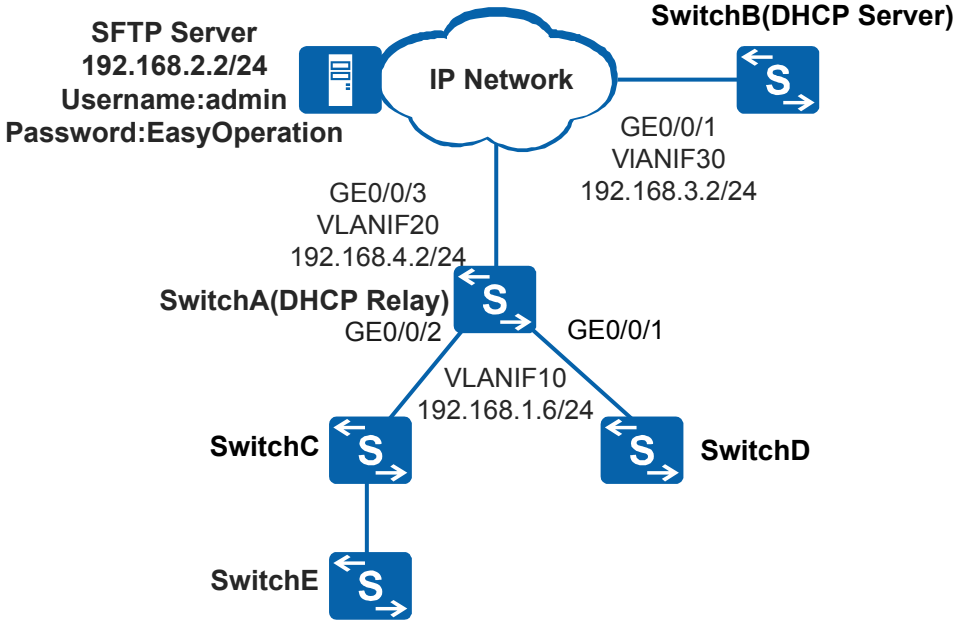
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

New Device	Device Model	Files to Be Loaded
SwitchE	S5700-X-LI	s5700-x-li.cfg User-defined file header2.txt

Figure 3-18 Networking diagram for unconfigured device deployment using the commander



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the file server and save the files to be loaded on the file server.
2. Configure the DHCP server function based on the global address pool on SwitchB and configure DHCP relay on SwitchA, so that the new devices can obtain IP addresses of their own and the Commander.
3. Configure the Commander on SwitchA so that the new devices can be configured using the Commander.
   - Enable automatic configuration backup on the Commander to facilitate replacement of faulty devices in future maintenance.
   - Configure information about files to be downloaded for each client based on the network topology.
   - SwitchE is connected to SwitchC in cascading networking. Therefore, an appropriate global file activation delay time needs to be configured on the Commander to ensure that SwitchE has enough time to download the required files.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Configure the file server according to the server manual.

After completing the configuration, save the required files on the file server.

Step 2 Configure the DHCP service.

Configure a DHCP server based on the global address pool.

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] dhcp enable
[SwitchB] vlan batch 30
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] ip address 192.168.3.2 24
[SwitchB-Vlanif30] dhcp select global
[SwitchB-Vlanif30] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type hybrid
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 30
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 30
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] ip pool easy-operation
[SwitchB-ip-pool-easy-operation] network 192.168.1.0 mask 255.255.255.0
[SwitchB-ip-pool-easy-operation] gateway-list 192.168.1.6
[SwitchB-ip-pool-easy-operation] option 148 ascii ipaddr=192.168.1.6;
[SwitchB-ip-pool-easy-operation] quit
```

Configure a default route on SwitchB.

```
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
```

Configure DHCP relay on SwitchA (Commander).

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 20
[SwitchA] dhcp enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 192.168.1.6 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 192.168.4.2 24
[SwitchA-Vlanif20] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type hybrid
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type hybrid
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type hybrid
[SwitchA-GigabitEthernet0/0/3] port hybrid pvid vlan 20
[SwitchA-GigabitEthernet0/0/3] port hybrid untagged vlan 20
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] dhcp select relay
[SwitchA-Vlanif10] dhcp relay server-ip 192.168.3.2
[SwitchA-Vlanif10] quit
```

Configure a default route on SwitchA.

```
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 3 Configure basic functions for the Commander.

```
[SwitchA] easy-operation commander ip-address 192.168.1.6
[SwitchA] easy-operation commander enable
```

Step 4 Configure file server information.

```
[SwitchA] easy-operation
[SwitchA-easyoperation] sftp-server 192.168.2.2 username admin password
EasyOperation
[SwitchA-easyoperation] quit
```

Step 5 Configure network topology collection.

```
[SwitchA] ndp enable
[SwitchA] ntdp enable
[SwitchA] ntdp timer 5
[SwitchA] easy-operation
[SwitchA-easyoperation] topology enable
[SwitchA-easyoperation] client auto-join enable
[SwitchA-easyoperation] quit
```

Step 6 Enable the cluster function and configure a cluster management VLAN.

```
[SwitchA] cluster enable
[SwitchA] cluster
[SwitchA-cluster] mngvlanid 10
[SwitchA-cluster] quit
```

Step 7 Configure information about files to be downloaded.

Check network topology information collected on the Commander.

```
[SwitchA] display easy-operation topology
<-->:normal device          <??>:lost device
Total topology node number: 3
------------------------------------------------------------------------------
[SwitchA: 4CB1-6C8F-0447](Commander)
|-(GE0/0/1)<-->(GE0/0/1)[HUAWEI: 00E0-FC34-3190](Client 1)
|-(GE0/0/2)<-->(GE0/0/1)[HUAWEI: 00E0-FC12-A34B](Client 2)
| |-(GE0/0/2)<-->(GE0/0/1)[HUAWEI: 5489-9875-edff] (Client 3)
```

Based on the network planning and topology information, you can see that **SwitchD**, **SwitchC**, and **SwitchE** are **Client1**, **Client2**, and **Client3** respectively.

Specify information about the files to be downloaded to Client1.

```
[SwitchA] easy-operation
[SwitchA-easyoperation] client 1 configuration-file s5700-hi.cfg custom-file
header1.txt
```

Specify information about the files to be downloaded to Client2.

```
[SwitchA-easyoperation] client 2 configuration-file s5700-hi.cfg custom-file
header1.txt
```

Specify information about the files to be downloaded to Client3.

```
[SwitchA-easyoperation] client 3 configuration-file s5700-x-li.cfg custom-file
header2.txt
```

In the Easy-Operation view of the Commander, set the file activation delay time to 15 minutes (900 seconds) based on the size of files that Client3 needs to download.

```
[SwitchA-easyoperation] activate-file delay 900
```

Step 8 Configure SwitchA to automatically back up configuration files.

```
[SwitchA-easyoperation] backup configuration interval 2
[SwitchA-easyoperation] quit
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 9 Verify the configuration.

Check global configuration of the Commander.

```
[SwitchA] display easy-operation configuration
-------------------------------------------------------------------------------
 Role                             : Commander
 Commander IP address             : 192.168.1.6
 Commander UDP port               : 60000
 IP address of file server        : 192.168.2.2
 Type of file server              : SFTP
 Username of file server          : admin
 Default system-software file     : -
 Default system-software version  : -
 Default configuration file       : -
 Default patch file               : -
 Default WEB file                 : -
 Default license file             : -
 Default custom file 1            : -
 Default custom file 2            : -
 Default custom file 3            : -
 Auto clear up                    : Disable
 Auto join in                     : Enable
 Topology collection              : Enable
 Activating file time             : Delay 900s
 Activating file method           : Default
 Aging time of lost client(hours): -
 Backup configuration file mode   : Default
 Backup configuration file interval(hours): 2
-------------------------------------------------------------------------------
```

Check the file downloading progress on each client after the unconfigured device deployment process starts.

```
[SwitchA] display easy-operation download-status
The total number of client in downloading files is : 3

-------------------------------------------------------------------------------
  ID     Mac address    IP address      Method      Phase          Status
-------------------------------------------------------------------------------
  1      00E0-FC12-A34B 192.168.1.254   Zero-touch  Config-file  Upgrading
  2      00E0-FC34-3190 192.168.1.253   Zero-touch  Config-file  Upgrading
  3      5489-9875-edff 192.168.1.252   Zero-touch  Config-file  Upgrading
```

----End

Configuration Files

SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 10 20
#
cluster enable
#
ntdp timer 5
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.3.2
#
interface Vlanif20
 ip address 192.168.4.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
cluster
 mngvlanid 10
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 client auto-join enable
 topology enable
 sftp-server 192.168.2.2 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 2
 activate-file delay 900
 client 1 configuration-file s5700-hi.cfg
 client 1 custom-file header1.txt
 client 2 configuration-file s5700-hi.cfg
 client 2 custom-file header1.txt
 client 3 configuration-file s5700-x-li.cfg
 client 3 custom-file header2.txt
#
return
```

SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
#
return
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.15.5 Example for Manually Replacing Faulty Devices Using the Commander

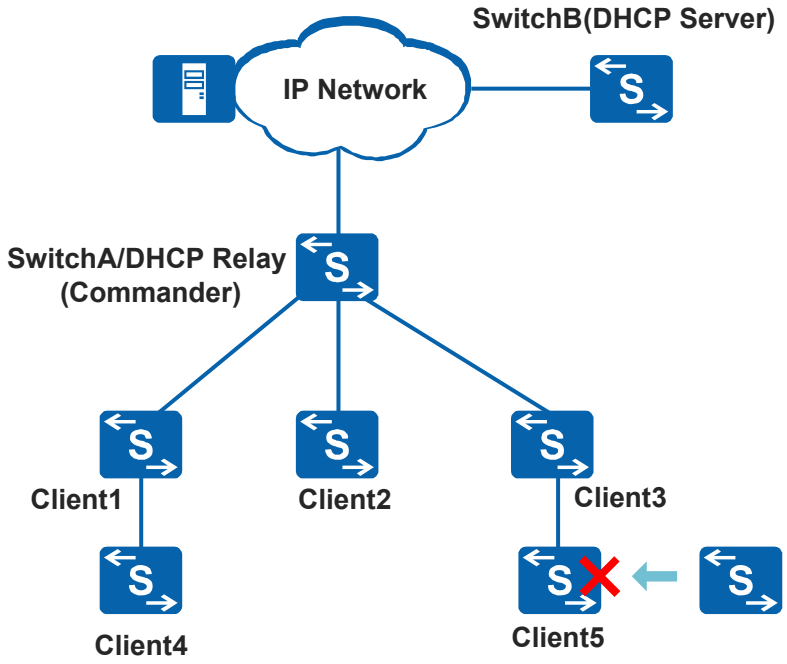
Networking Requirements

The enterprise network shown in **Figure 3-19** supports the EasyDeploy function. SwitchA functions as a DHCP relay agent and Commander. SwitchA, DHCP server, and the file server have reachable routes to each other.

Client5 on the network fails, and services of users connected to Client5 are interrupted. To resume services for users, Client5 must be replaced by a new client. The new client needs to take over services of Client5 quickly to minimize impact of the fault.

The MAC address of the new client is 0200-0000-0000, and the new client needs to download the web page file **web_1.web.7z**.

Figure 3-19 Networking diagram for faulty device replacement using the Commander



Configuration Roadmap

The configuration roadmap is as follows:

1. Save web_1.web.7z to be loaded on the file server.
2. Specify client replacement information on SwitchA to enable the new client to obtain the backup configuration file of the faulty client.

NOTE

Faulty device replacement can be implemented on a network where EasyDeploy has been deployed, and the file server, DHCP server, and Commander have been configured.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Configure automatic configuration backup to enable the new client to obtain the configuration file of the faulty client.

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] easy-operation
[SwitchA-easyoperation] backup configuration interval 72
```

Step 2 Specify client replacement information on SwitchA.

```
[SwitchA-easyoperation] client 5 replace mac-address 0200-0000-0000
[SwitchA-easyoperation] client 5 replace web-file web_1.web.7z
```

Step 3 Verify the configuration.

Check client replacement information.

```
[SwitchA-easyoperation] display easy-operation client replace
The total number of replacement information is :  1

-------------------------------------------------------------
  ID      Replaced Mac       Replaced Esn
-------------------------------------------------------------
  5       0200-0000-0000   -
-------------------------------------------------------------
```

After the faulty device replacement process starts, run the **display easy-operation client 5** command to check the status of the new client.

```
[SwitchA-easyoperation] display easy-operation client 5
------------------------------------------------------------------------------
 Client ID                    : 5
 Host name                    : HUAWEI
 Mac address                  : 0200-0000-0000
 ESN                          : 210235182810C3001039
 IP address                   : 192.168.1.254
 Model                        : S5701-28X-LI-AC
 Device Type                  : S5700-X-LI
 System-software file         : flash:/S5700XLI.cc
 System-software version      : V200R005C00
 Configuration file           : -
 Patch file                   : -
 WEB file                     : -
 License file                 : -
 System CPU usage             : 55%
 System Memory usage          : 44%
 Backup configuration file    : vrpcfg-0300-0000-0000.zip
 Backup result                : Successful
 Last operation result        : -
 Last operation time          : 0000-00-00  00:00:00
 State                        : UPGRADING
 Aging time left (hours)      : -
------------------------------------------------------------------------------
```

You can also run the **display easy-operation download-status** command to check the file downloading progress of the new client.

```
[SwitchA-easyoperation] display easy-operation download-status
The total number of client in downloading files is : 1

-------------------------------------------------------------------------------
 ID  Mac address      IP address           Method       Phase        Status
-------------------------------------------------------------------------------
 5   0200-0000-0000   192.168.1.254        Zero-touch   Web-file     Upgrading
```

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuration Files

SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 10 20
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.3.2
#
interface Vlanif20
 ip address 192.168.4.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/4
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 sftp-server 192.168.2.2 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 72
 client 5 mac-address 0300-0000-0000
#
return
```

SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
 dhcp select global
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
#
return
```

3.15.6 Example for Implementing a Batch Upgrade Using the Commander

Networking Requirements

On the enterprise network shown in **Figure 3-20**, clients 1 through 6 in office buildings have reachable routes to the switch and file server. The IP address of the switch is 172.31.20.10/24, and the IP address of the file server is 172.31.1.90. To reduce labor costs and facilitate later upgrade and maintenance, the enterprise wants the clients to automatically obtain required files for batch upgrades.

Table 3-9 lists information about clients 1 through 6 and files that they need to load.

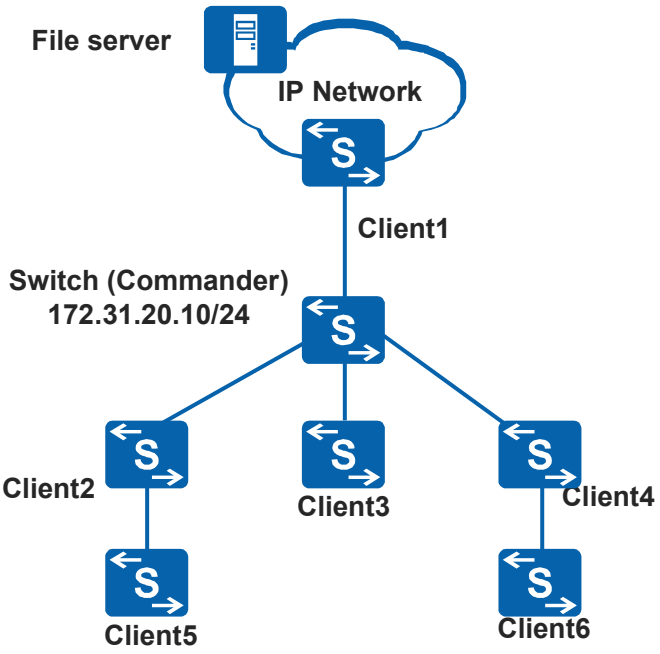
Table 3-9 Client information and files to be loaded

Client	Device Type	MAC Address	IP Address	Files to Be Loaded
Client1	S7700	-	172.31.20.100/24	s7700.cc license.dat header1.txt
Client2	S5700-HI	-	-	s5700-hi.cc
Client3	S5700-HI	-	-	s5700-hi.cc
Client4	S5700-X-LI	-	172.31.10.10/24	s5700-x-li.cc
Client5	S5700-HI	-	-	s5700-hi.cc
Client6	S5700-SI	5489-9875-ea12	-	web_1.web.7z header.txt

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Figure 3-20 Networking diagram for a batch upgrade using the Commander



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the file server and save the files to be loaded on the file server.
2. Specify the Commander IP address on the clients.
3. Configure the Commander function on the switch to implement a batch upgrade using the Commander.
   - Configure basic functions for the Commander.
   - Configure groups for the clients and specify files to be loaded in the groups.
   - Enable automatic configuration backup on the Commander to facilitate replacement of faulty devices in future maintenance.
   - Some clients are connected in cascading networking. To ensure that downstream Client5 and Client6 can download required files successfully, configure a specific file activation time on the Commander. To minimize the impact of the upgrade on services, configure the clients to active downloaded files at 2:00 a.m.
4. Start the batch upgrade process.

Procedure

Step 1 Configure the file server.

Configure the file server according to the server manual.

After completing the configuration, save the required files on the file server.

Step 2 Specify the Commander IP address on the clients.

Specify the Commander IP address on Client1.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
<HUAWEI> system-view
[HUAWEI] easy-operation commander ip-address 172.31.20.10
```

Specify the Commander IP address on Client2 to Client6 in the same way.

Step 3 Configure basic functions for the Commander.

```
<HUAWEI> system-view
[HUAWEI] sysname Commander
[Commander] easy-operation commander ip-address 172.31.20.10
[Commander] easy-operation commander enable
[Commander] easy-operation
[Commander-easyoperation] sftp-server 172.31.1.90 username admin password
EasyOperation
[Commander-easyoperation] backup configuration interval 2
```

Step 4 Enable the client auto-join function on the Commander.

```
[Commander-easyoperation] client auto-join enable
```

After the auto-join function is enabled, you can run the **display easy-operation client** command to check information about the clients and files that the clients have downloaded from the Commander.

Step 5 Specify file information and file activation mode on the Commander.

Configure a group based on the IP address of Client1, and specify information about the files to be loaded.

```
[Commander-easyoperation] group custom ip-address g1
[Commander-easyoperation-group-custom-g1] match ip-address 172.31.20.100 24
[Commander-easyoperation-group-custom-g1] system-software s7700.cc
[Commander-easyoperation-group-custom-g1] license license.dat
[Commander-easyoperation-group-custom-g1] custom-file header1.txt
[Commander-easyoperation-group-custom-g1] quit
```

On the Commander, configure a built-in group based on the device type of Client2, Client3 and Client5, and specify information about the files to be downloaded in the group.

```
[Commander-easyoperation] group build-in s5700-hi
[Commander-easyoperation-group-build-in-S5700-HI] system-software s5700-hi.cc
[Commander-easyoperation-group-build-in-S5700-HI] quit
```

Configure a group based on the IP address of Client4, and specify information about the files to be loaded.

```
[Commander-easyoperation] group custom ip-address g2
[Commander-easyoperation-group-custom-g2] match ip-address 172.31.10.10 24
[Commander-easyoperation-group-custom-g2] system-software s5700-x-li.cc
[Commander-easyoperation-group-custom-g2] quit
```

Configure a group based on the MAC address of Client6, and specify information about the files to be loaded.

```
[Commander-easyoperation] group custom mac-address g3
[Commander-easyoperation-group-custom-g3] match mac-address 5489-9875-ea12
[Commander-easyoperation-group-custom-g3] web-file web_1.web.7z
[Commander-easyoperation-group-custom-g3] custom-file header.txt
[Commander-easyoperation-group-custom-g3] quit
```

In the Easy-Operation view of the Commander, set the file activation mode and time.

```
[Commander-easyoperation] activate-file in 2:00 reload
[Commander-easyoperation] quit
```

Step 6 Verify the configuration.

Check global configuration of the Commander.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[Commander] display easy-operation configuration
-------------------------------------------------------------------------------
 Role                            : Commander
 Commander IP address            : 172.31.20.10
 Commander UDP port              : 60000
 IP address of file server       : 172.31.1.90
 Type of file server             : SFTP
 Username of file server         : admin
 Default system-software file    : -
 Default system-software version : -
 Default configuration file      : -
 Default patch file              : -
 Default WEB file                : -
 Default license file            : -
 Default custom file 1           : -
 Default custom file 2           : -
 Default custom file 3           :
-
 Auto clear up                   : Disable
 Auto join in                    : Enable
 Topology collection             : Disable
 Activating file time            : In 02:00
 Activating file method          : Reload
 Aging time of lost client(hours): -
 Backup configuration file mode  : Default
 Backup configuration file interval(hours): 2
-------------------------------------------------------------------------------
```

Check group configuration on the Commander.

```
[Commander] display easy-operation group
The total number of group configured is : 4
The number of build-in group is         : 1
The number of custom group is           : 3

-----------------------------------------------------
 Groupname                      Type     MatchType
-----------------------------------------------------
 S5700-HI                       build-in device-type
 g1                             custom   ip-address
 g2                             custom   ip-address
 g3                             custom   mac-address
-----------------------------------------------------
```

Check configuration of the group **g1** on the Commander.

```
[Commander] display easy-operation group custom g1
-------------------------------------------------------------------------------
 Group name               : g1
 Configuration file       : -
 System-software file     : s7700.cc
 Patch file               : -
 WEB file                 : -
 License file             : license.dat
 Customs file 1           : header1.txt
 Customs file 2           : -
 Customs file 3           : -
 Activating file time     :
Immediately
 Activating file method   : Default
 Ip-address list          :
  Ip-address        Ip-mask
  172.31.20.100      255.255.255.0
-------------------------------------------------------------------------------
```

Step 7 Start the batch upgrade process.

```
[Commander] easy-operation
[Commander-easyoperation] upgrade group
Warning: This command will start the upgrade process of all groups and clients i
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
n these groups may reboot. Ensure that configurations of the clients have been s
aved. Continue?[Y/N]:y
```

You can run the **display easy-operation download-status** command to check the file downloading progress on each client.

```
[Commander-easyoperation] display easy-operation download-status
The total number of client in downloading files is : 6

--------------------------------------------------------------------------------
  ID     Mac address    IP address      Method      Phase         Status
--------------------------------------------------------------------------------
  1      0011-2233-4455 172.31.20.100   Upgrade     Sys-file      Upgrading
  2      00E0-FC34-3190 172.31.10.15    Upgrade     Sys-file      Upgrading
  3      0011-2233-4457 172.31.10.20    Upgrade     Sys-file      Upgrading
  4      70F3-950B-1A52 172.31.10.10    Upgrade     Sys-file      Upgrading
  5      0011-2233-4459 172.31.10.18    Upgrade     Sys-file      Upgrading
  6      5489-9875-ea12 172.31.10.11    Upgrade     Web-file      Upgrading
```

----End

Configuration Files

Commander configuration file

```
#
sysname Commander
#
easy-operation commander ip-address 172.31.20.10
easy-operation commander enable
#
easy-operation
 client auto-join enable
 sftp-server 172.31.1.90 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 2
 activate-file reload
 activate-file in 02:00
 group build-in S5700-HI
  system-software s5700-hi.cc
 group custom ip-address g1
  system-software s7700.cc
  license license.dat
  custom-file header1.txt
  match ip-address 172.31.20.100 255.255.255.0
 group custom ip-address g2
  system-software s5700-x-li.cc
  match ip-address 172.31.10.10 255.255.255.0
 group custom mac-address g3
  web-file web_1.web.7z
  custom-file header.txt
  match mac-address 5489-9875-EA12 FFFF-FFFF-FFFF
#
return
```

clients 1 to 6 configuration file

```
#
easy-operation commander ip-address 172.31.20.10
#
return
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.15.7 Example for Implementing a Batch Configuration Using the Commander

Networking Requirements

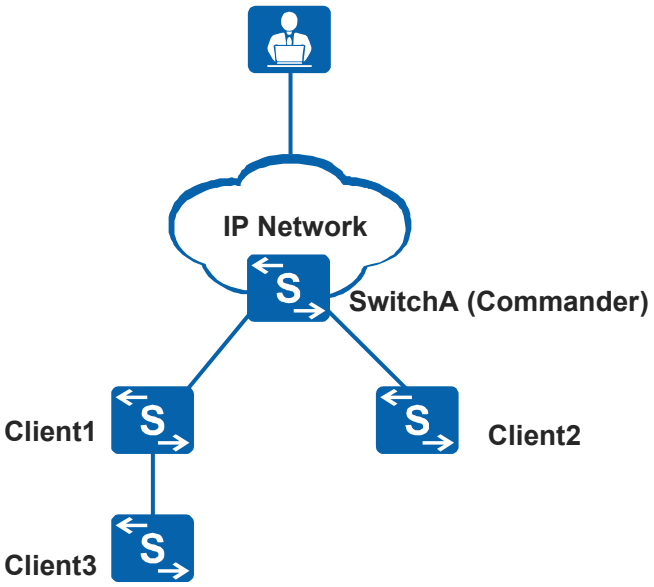
The enterprise network shown in **Figure 3-21** supports the EasyDeploy function. Clients 1 to 3 in office buildings have reachable routes to SwitchA and the file server. The enterprise wants to implement a batch configuration on the clients using the Commander.

Table 3-10 lists information about clients 1 to 3.

Table 3-10 Device information

New Device	Device Model	Command Script
Client1	S2750-EI	cfg1.bat
Client2	S5700-X-LI	cfg2.bat
Client3	S5700-X-LI	cfg2.bat

Figure 3-21 Networking diagram for a batch configuration using the Commander



Configuration Roadmap

The configuration roadmap is as follows:

1. Load scripts that are made offline to SwitchA.
2. Deliver commands.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Make scripts offline.

Create a .txt file and edit commands to be delivered in the file. Then, save the file and change the file name extension from .txt to .bat.

After making the scripts, load them to the Commander.

Step 2 Deliver commands.

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] easy-operation
[SwitchA-easyoperation] execute cfg1.bat to client 1
Warning: This operation will start the batch command executing process to the cl
ients. Continue?[Y/N]:y
Info: This operation will take some seconds, please wait..
[SwitchA-easyoperation] execute cfg2.bat to client 2 to 3
Warning: This operation will start the batch command executing process to the cl
ients. Continue?[Y/N]:y
Info: This operation will take some seconds, please wait..
```

Step 3 Verify the configuration.

Check the execution result of batch configuration.

```
[SwitchA-easyoperation] display easy-operation batch-cmd result
This operation will take some seconds, please
wait..
-------------------------------------------------------------
  ID   Total  Successful     Failed    Time
-------------------------------------------------------------
  1     50    50             0         2013-09-04  21:45:29
  2     30    30             0         2013-09-04  21:55:29
  3     30    30             0         2013-09-04  21:55:29
-------------------------------------------------------------
```

----End

3.15.8 Example of Adding Configured Devices to the Management Domain of the Commander

Networking Requirements

The enterprise network shown in **Figure 3-22** supports the EasyDeploy function. SwitchA functions as a DHCP relay agent and Commander. SwitchA, DHCP server, and the file server have reachable routes to each other.

A configured device Client6 on the network needs to be added to the management domain of the Commander for monitoring and management.

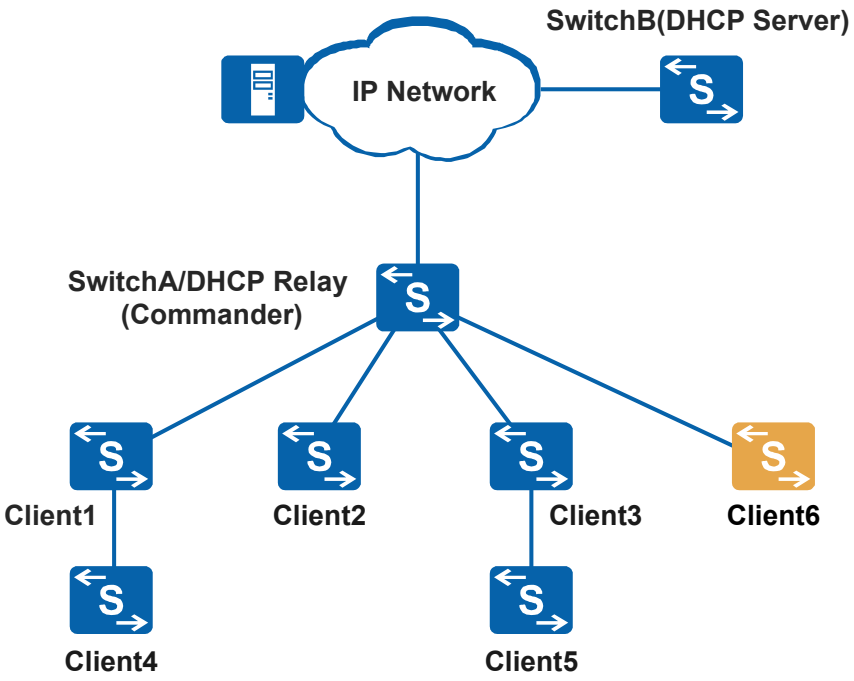
The IP address of the Commander is 192.168.1.6/24, and the MAC address of Client6 is 0200-0000-0000.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 3-22 Adding configured devices to the management domain of the Commander



Configuration Roadmap

The configuration roadmap is as follows:

1. Ensure that Client6 has reachable routes to the Commander.
2. Configure the Commander IP address on Client6.
3. Configure a client matching rule on the Commander so that the Commander can identify new devices.

NOTE

Adding configured devices to the management domain of the Commander can be implemented on a network where the EasyDeploy function has been deployed, and the file server, DHCP server, and Commander have been configured.

Procedure

Step 1 Configure the Commander IP address on Client6.

```
<HUAWEI> system-view
[HUAWEI] sysname Client6
[Client6] easy-operation commander ip-address 192.168.1.6
```

Step 2 Configure information about Client6 on SwitchA.

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] easy-operation
[SwitchA-easyoperation] client 6 mac-address 0200-0000-0000
[SwitchA-easyoperation] quit
```

NOTE

If many devices need to be added to the management domain of the Commander, enabling the client auto join function on the Commander is recommended.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 3 Verify the configuration.

Check client database information.

```
[SwitchA] display easy-operation client
The total number of client is : 6

-------------------------------------------------------------------------------
 ID   Mac address    ESN                                 IP address       State
-------------------------------------------------------------------------------
 1    0025-9EF4-ABCD 2102113089P0BA000390                192.168.1.208    RUNNING
 2    0000-C102-0701 -                                   -                INITIAL
 3    -              210235182810C3001041                192.168.1.210    INITIAL
 4    0011-0010-0200 2102351263187A600121                192.168.1.167    RUNNING
 5    0102-0301-ABCD 210235345120B3810104                192.168.1.105    RUNNING
 6    0200-0000-0000 2102352763107C800132                192.168.1.254    RUNNING
-------------------------------------------------------------------------------
```

Check detailed information about the new client with MAC address 0200-0000-0000.

```
[SwitchA] display easy-operation client mac-address 0200-0000-0000
-------------------------------------------------------------------------
 Client ID                   : 6
 Host name                   : HUAWEI
 Mac address                 : 0200-0000-0000
 ESN                         : 2102352763107C800132
 IP address                  : 192.168.1.254
 Model                       : S5720C-EI
 Device Type                 : S5720-EI
 System-software file        : flash:/s5720-ei-v200r009c00.cc
 System-software version     : V200R009C00
 Configuration file          : flash:/254.cfg
 Patch file                  : -
 WEB file                    : -
 License file                : -
 System CPU usage            : 6%
 System Memory usage         : 55%
 Backup configuration file   : -
 Backup result               : -
 Last operation result       : -
 Last operation time         : 0000-00-00  00:00:00
 State                       : RUNNING
 Aging time left (hours)     : -
-------------------------------------------------------------------------
```

----End

Configuration Files

SwitchA configuration file

```
#
sysname SwitchA
#
easy-operation
 client 6 mac-address 0200-0000-0000
#
return
```

Client6 configuration file

```
#
sysname SwitchA
#
easy-operation commander ip-address 192.168.1.6
#
return
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3.15.9 Example for Implementing Topology-based Zero Touch provisioning for the Campus Headquarters

Prerequisites

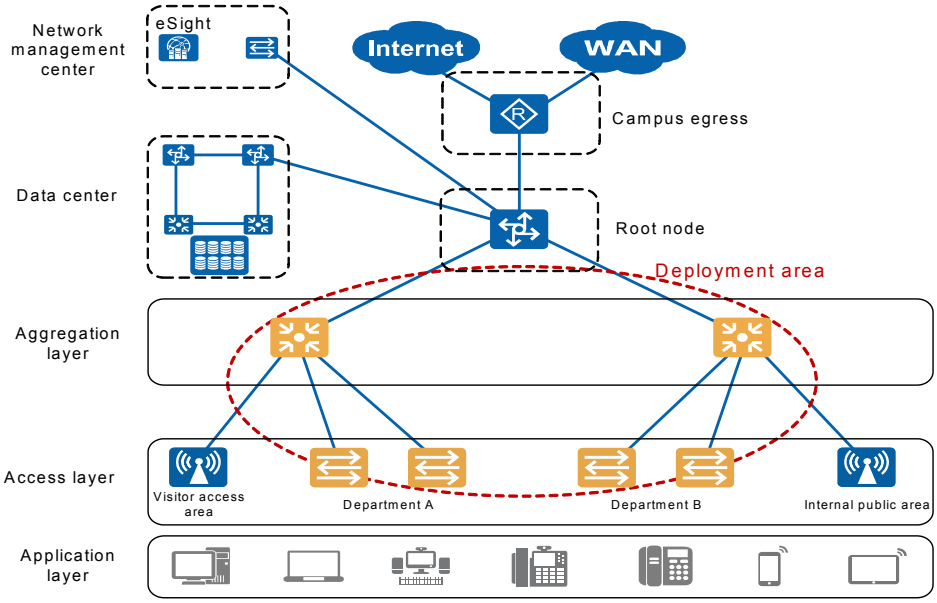
- The root device and devices to be deployed support zero touch provisioning. For details about device types, see *eSight Release Notes*.
- A root device has been added to eSight for management and can communicate normally with eSight through SNMP and Telnet.
- A DHCP server has been configured and uses the root device as a gateway.
- Input or output is not allowed on console interfaces during zero touch provisioning.
- The device software package, license file, and patch file have been prepared and uploaded to eSight. If not, choose **Configuration** > **Configuration Management** > **Device Software Management** to upload the files.

Networking Requirements

On the wired campus network of company M, there are lots of devices at the aggregation and access layers. Traditionally, the network design, and software/hardware installation and commissioning are performed by different personnel. Each device to be deployed needs to be manually associated with provisioning files through a USB flash drive. The configuration is complex and has low efficiency. Jack, the network administrator of the company, requires that eSight implement unified zero touch provisioning for aggregation and access devices to reduce management cost.

In the following figure, the red circle specifies the devices to be deployed.

Figure 3-23 Implementing topology-based zero touch provisioning for the campus headquarters



Configuration Roadmap

The configuration roadmap is as follows:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

1. Select a root device and configure VLAN 1 as a pass VLAN on the root device.
2. Configure the root device as a DHCP server.
3. Plan the network topology on the **Topo Plan-based Provisioning** page.
4. Prepare configuration files for devices to be deployed.
5. Configure mappings between the configuration files and devices.
6. Install and power on devices according to the planned topology (performed by the hardware commissioning personnel).
7. Check whether the actual physical topology is consistent with the planned topology on eSight (performed by the software commissioning personnel).
8. Trigger provisioning if the topologies are consistent (performed by the software commissioning personnel). The devices to be deployed then download corresponding files.

Data Plan

Table 3-11 Root device

Device Type	Device IP Address	Downstream Port 1	Downstream Port 2
S5720 - 56C-PWR-HI-AC	10.137.58.61	GE0/0/1	GE0/0/2

Table 3-12 Devices at the aggregation layer

Device Type	IP Address	Upstream Port	Downstream Port 1	Downstream Port 2
S5720 - 32C-HI-24S-AC	10.137.58.1	GE0/0/1	GE0/0/2	GE0/0/3
S5720 - 32C-HI-24S-AC	10.137.58.2	GE0/0/1	GE0/0/2	GE0/0/3

Table 3-13 Devices at the access layer

Device Type	IP Address	Upstream Port
S2750 - 28TP-EI-AC	10.137.58.3	GE0/0/1
S2750 - 28TP-EI-AC	10.137.58.4	GE0/0/1
S2750 - 28TP-EI-AC	10.137.58.5	GE0/0/1
S2750 - 28TP-EI-AC	10.137.58.6	GE0/0/1

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

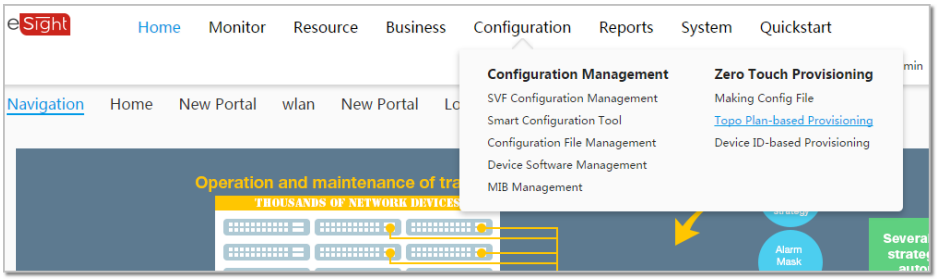
Procedure

Step 1 Specify VLAN 1 as a pass VLAN on the root device (the configuration is not provided here).

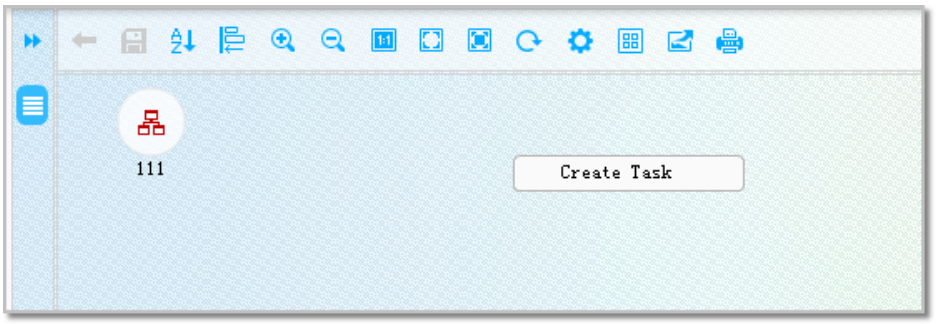
Step 2 Configure the root device as a DHCP server. For details, see **Configuring a DHCP Server**.

Step 3 Plan the network topology on the **Topo Plan-based Provisioning** page.

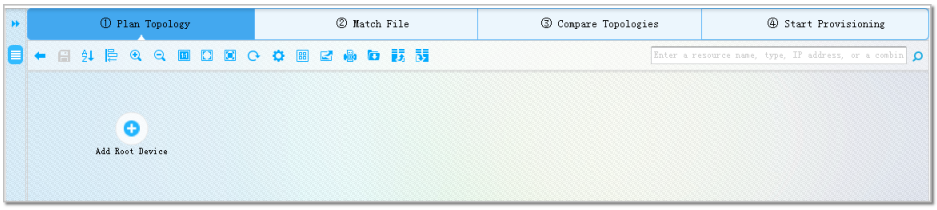
1. Choose **Configuration** > **Zero Touch Provisioning** > **Topo Plan-based Provisioning**.



2. Right-click a blank area in the main topology and select **Create Task**.



3. In the **Create Provisioning Task** dialog box that is displayed, set **Task name** to **Task for Department AB**. A provisioning task view is added in the main topology.
4. Double-click **Task for Department AB**. The subview page of the task is displayed.



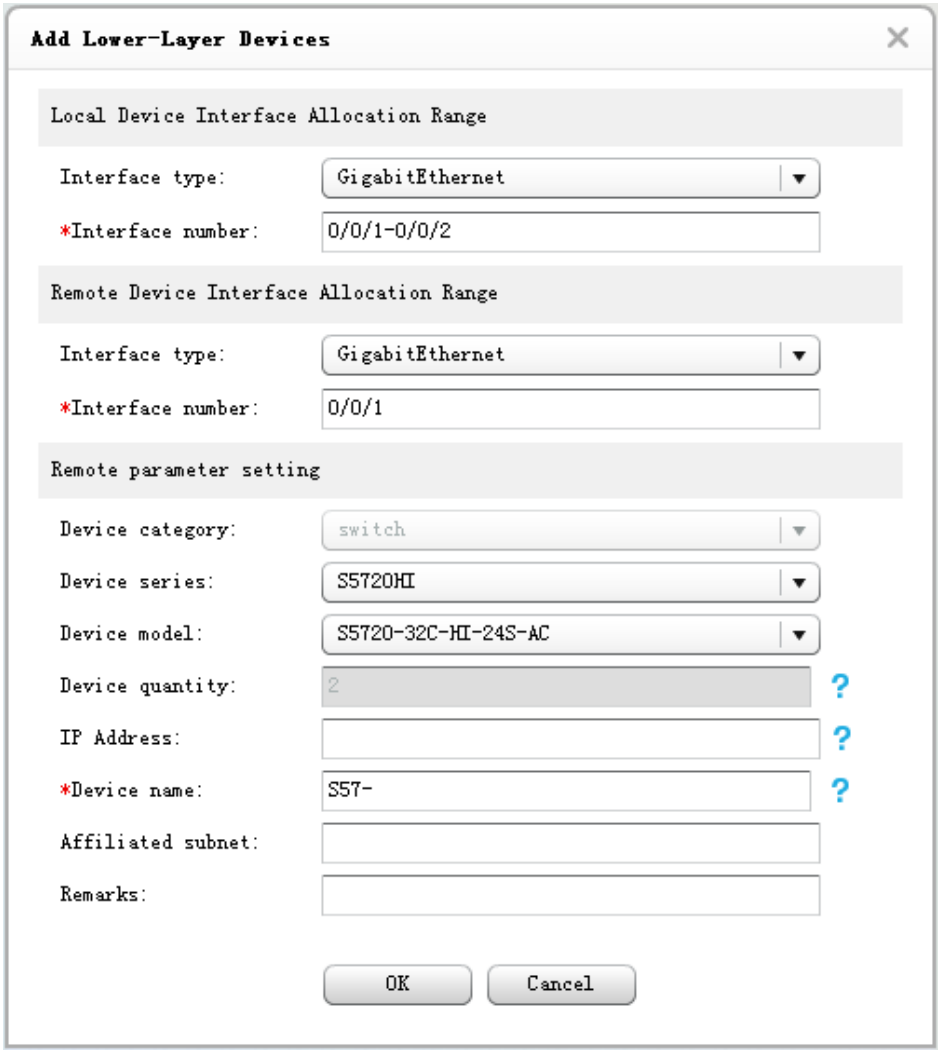
5. Click the **Add Root Device** icon. In the **Add Root Device** dialog box that is displayed, select a root device based on the subnet and click **OK**. The page displays the added root device.

   If you have a planning form, you can use the template to import the device to generate a topology.
6. Add an aggregation device: On the **Plan Topology** page, right-click the root device icon and choose **Add Remote Device** > **Switches**. In the **Add Lower-Layer Devices** dialog box that is displayed, enter the following parameters and click **OK**.

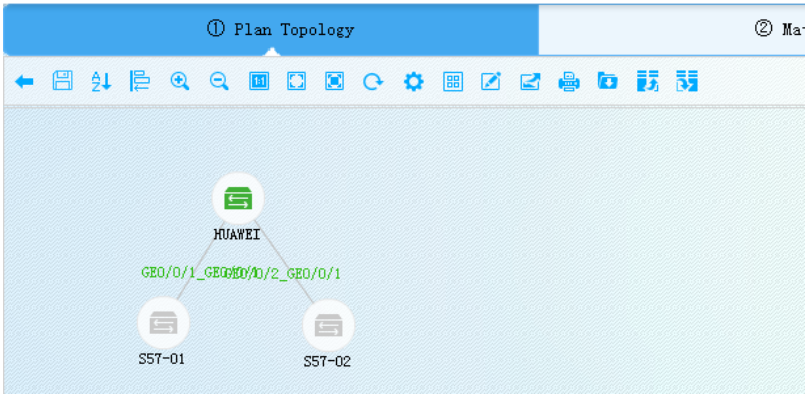
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016



7. The page displays the aggregation devices that have been created. Click on the toolbar and select **From Top to Bottom**. The page displays the root device and aggregation devices in the sorted order.

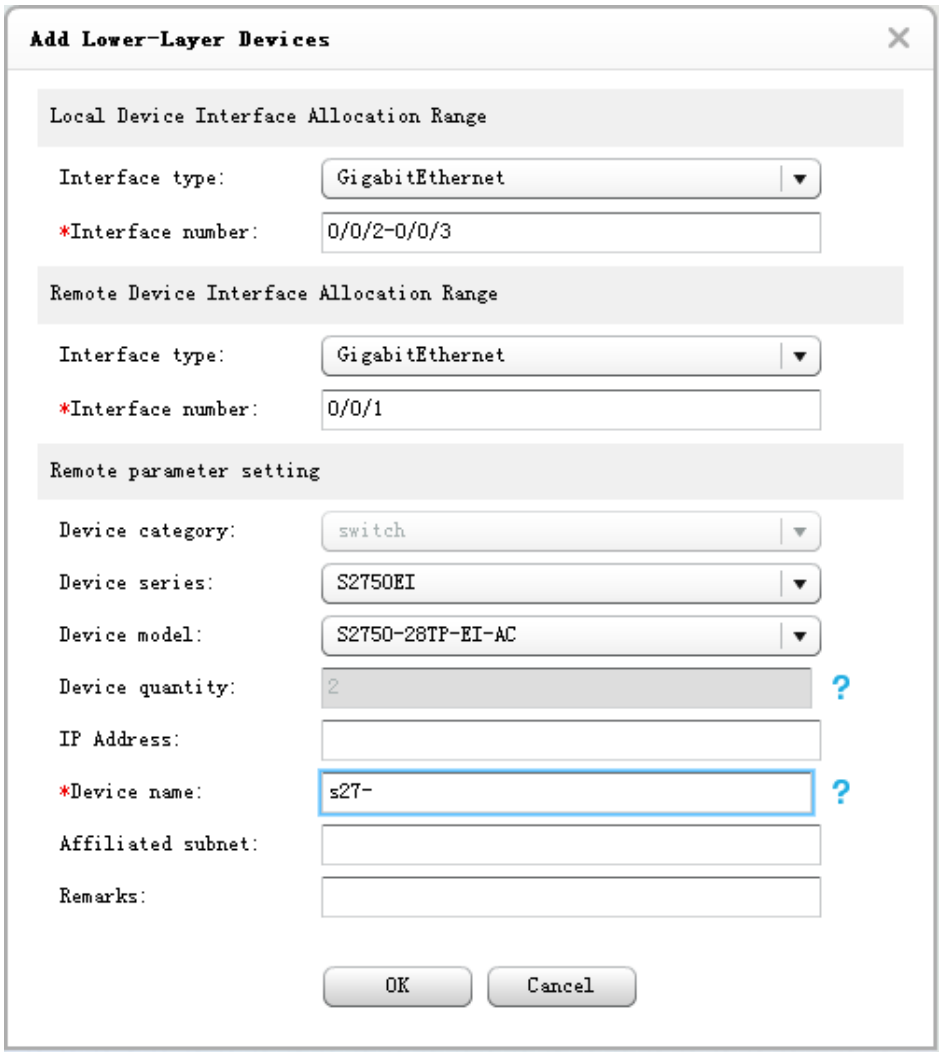


8. Right-click the **S57－00** icon and choose **Add Remote Device** > **Switches**. In the **Add Lower-Layer Devices** dialog box that is displayed, enter the following parameters and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

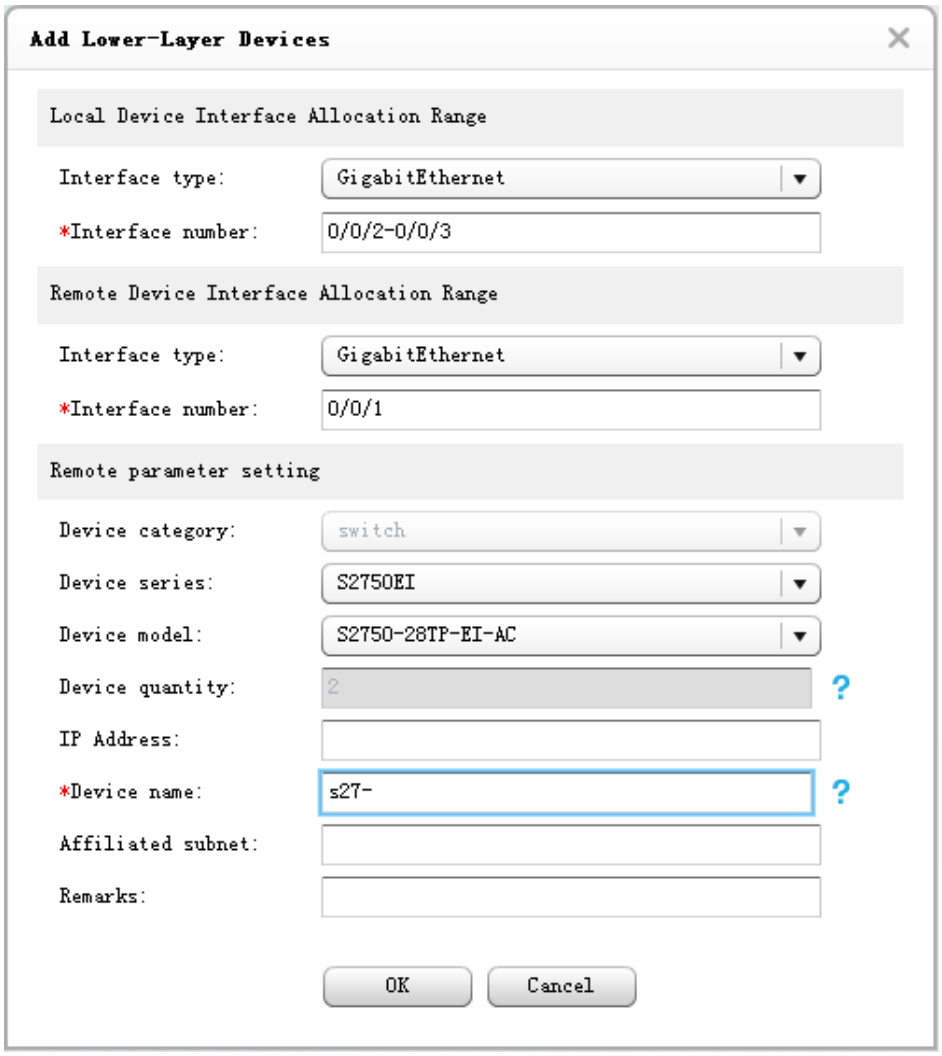


9. Right-click the **S2750－01** icon and choose **Add Remote Device** > **Switches**. In the **Add Lower-Layer Devices** dialog box that is displayed, enter the following parameters and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

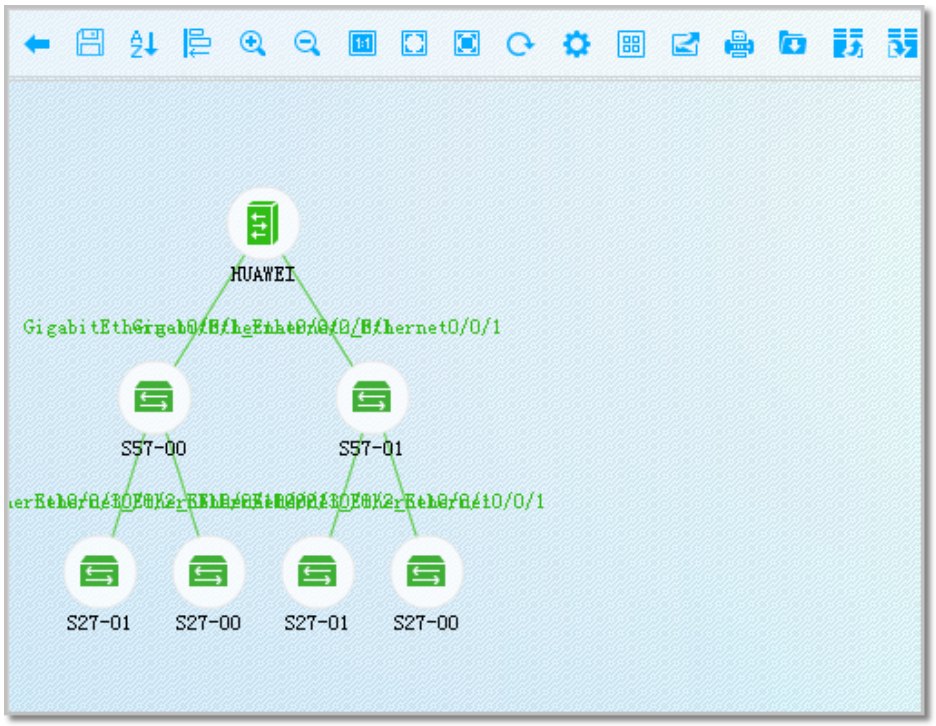
e-DOC 16A8F5D0-e
Proc 13409/2016



10. Click on the toolbar and select **From Top to Bottom**. The page displays the root device, aggregation devices, and access devices in the sorted order.

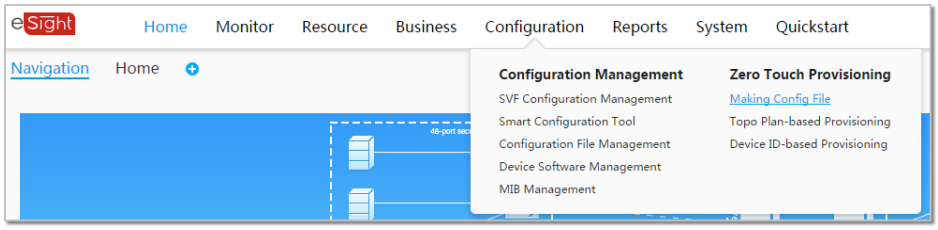
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

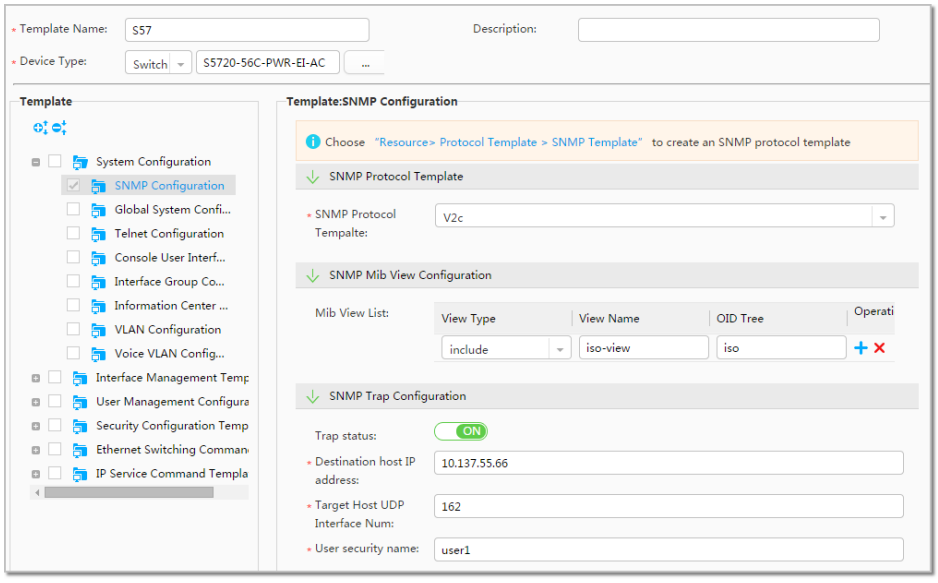


Step 4 Prepare configuration files for devices to be deployed.

1. Choose **Configuration** > **Zero Touch Provisioning** > **Making Config File**.



2. Click **Create**, enter the following parameters, and click **Next**. Click **OK**. The configuration file is created for the aggregation devices.



3. Repeat the preceding step to create a configuration file for the access devices.

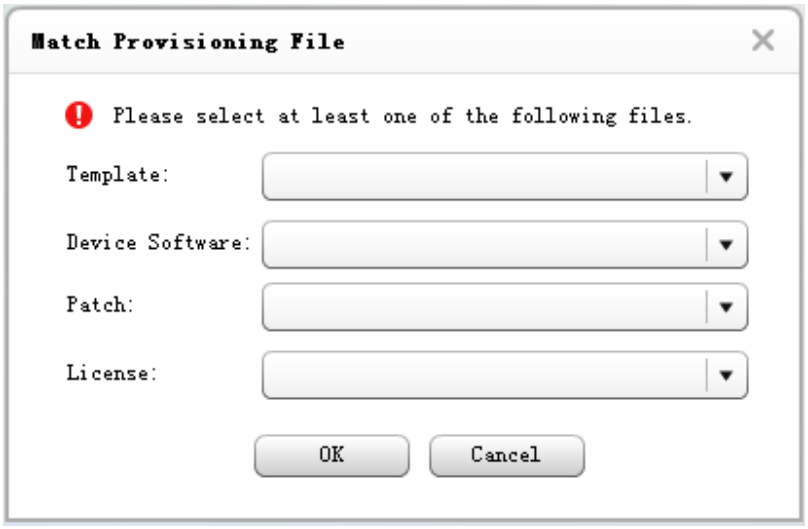
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 5 Configure mappings between the configuration file, software package, and license file and device.

1. Switch to the **Match File** page.
2. Drag to select the two aggregation devices, right-click the aggregation device icon, and select **Match Provisioning File**. Select the correct provisioning files and click **OK**.
3. Drag to select the four access devices, right-click the access device icon, and select **Match Provisioning File**. Select the correct provisioning files and click **OK**.



Step 6 Install and power on devices according to the planned topology (performed by the hardware commissioning personnel).

Step 7 Check whether the actual physical topology is consistent with the planned topology on eSight (performed by the software commissioning personnel). After topology collection is enabled, eSight collects the network topology of the provisioning area from the root node, maps the collected topology with the planned topology, and shows the differences for users to correct.

1. Switch to the **Compare Topologies** page. The page displays the topology comparison result at the bottom.

Step 8 Trigger provisioning if the topologies are consistent (performed by the software commissioning personnel). The devices then download corresponding files.

1. Switch to the **Start Provisioning** page. Drag to select devices to be deployed, and right-click and select **Start to Deploy**.
2. The page displays the provisioning delivery result. Drag to select all devices to be deployed, and right-click and select **Active**. The devices restart and load the new configuration file. The provisioning delivery is complete.

----End

Result

After the provisioning is complete, choose **Monitor** > **Topology** > **Topology Management**. All deployed devices can be displayed, and alarm messages of the devices can be reported to eSight.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

3.15.10 Example for Implementing MAC/ESN-based Zero Touch Provisioning

Prerequisites

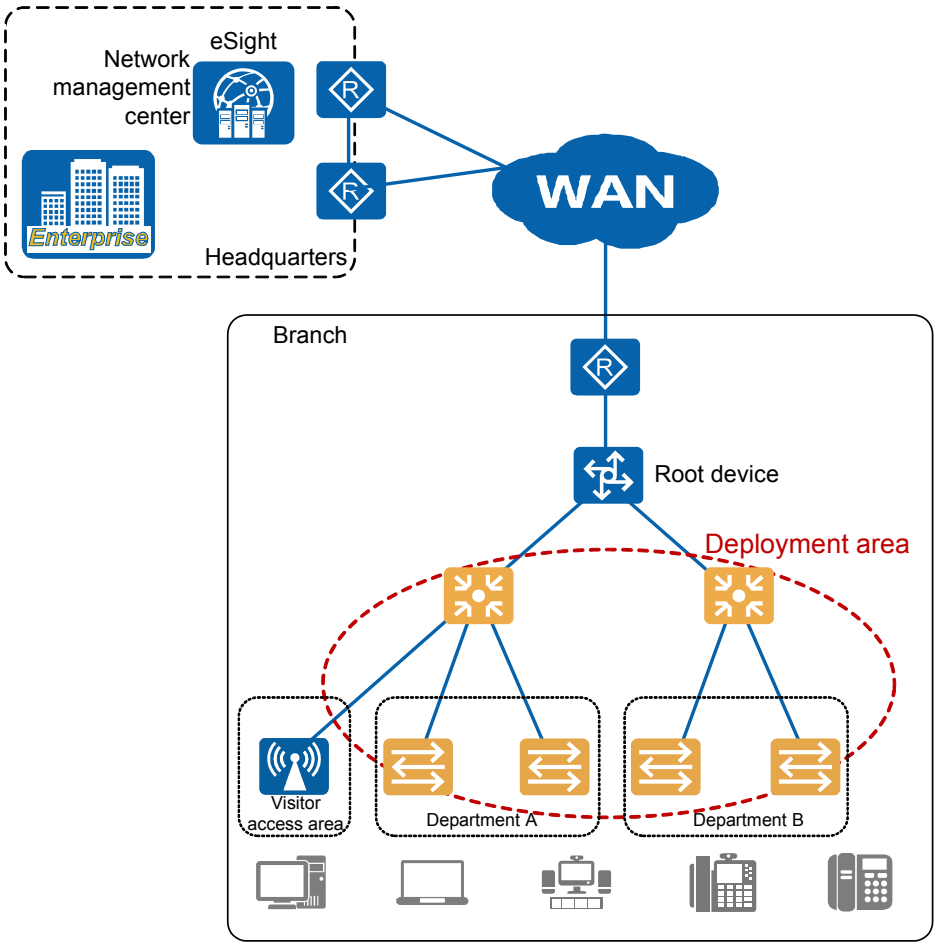
- A root device has been added to eSight for management and can communicate normally with eSight through SNMP and Telnet.
- A DHCP server has been configured and uses the root device as a gateway.
- Input or output is not allowed on console interfaces during zero touch provisioning.
- The device software package, license file, and patch file have been prepared and uploaded to eSight. If not, choose **Configuration** > **Configuration Management** > **Device Software Management** to upload the files.

Networking Requirements

On the wired campus network of company M, there are lots of devices at the aggregation and access layers. The configuration is complex. Jack, the network administrator of the company, requires that eSight implement unified MAC/ESN-based Zero Touch Provisioning for aggregation and access devices to reduce management cost.

In the following figure, the red circle specifies the devices to be deployed.

Figure 3-24 Implementing MAC/ESN-based zero touch provisioning



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuration Roadmap

The configuration roadmap is as follows:

1. Select a root device and configure VLAN 1 as a pass VLAN on the root device.
2. Configure the root device as a DHCP server.
3. Plan provisioning files for devices.
4. Power on the devices and manually record MAC addresses/ESNs of the devices.
5. Match the MAC addresses/ESNs with provisioning files.
6. Trigger provisioning. After the devices upload the provisioning files, the provisioning is complete.

Data Plan

Table 3-14 Root device

Device Type	Device IP Address	Downstream Port 1	Downstream Port 2
S5720 - 56C-PWR-HI-AC	10.137.58.61	GE0/0/1	GE0/0/2

Table 3-15 Devices at the aggregation layer

Device Type	IP Address	Upstream Port	Downstream Port 1	Downstream Port 2
S5720 - 32C-HI-24S-AC	10.137.58.1	GE0/0/1	GE0/0/2	GE0/0/3
S5720 - 32C-HI-24S-AC	10.137.58.2	GE0/0/1	GE0/0/2	GE0/0/3

Table 3-16 Devices at the access layer

Device Type	IP Address	Port
S2750 - 28TP-EI-AC	10.137.58.3	GE0/0/1
S2750 - 28TP-EI-AC	10.137.58.4	GE0/0/1
S2750 - 28TP-EI-AC	10.137.58.5	GE0/0/1
S2750 - 28TP-EI-AC	10.137.58.62	GE0/0/1

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 3-17 Device MAC/ESN

Location	IP Address	ESN	Device Type	Device Model	Configuration File	Other Files
Aggregation 1	00E0-FC12-AA4B	—	S5700	S5700-28C-HI	N1.zip	S5700.cc
Aggregation 2	00E0-FC12-AA5B	—	S5700	S5700-28C-HI	N2.zip	S5700.cc
Access 1	—	AAC1223431	S2700	S2750-28TP-EI-AC	N3.zip	S2700.cc
Access 2	—	AAC1223432	S2700	S2750-28TP-EI-AC	N4.zip	S2700.cc
Access 3	—	BAC1223433	S2700	S2750-28TP-EI-AC	N5.zip	S2700.cc
Access 4	—	BAC1223436	S2700	S2750-28TP-EI-AC	N6.zip	S2700.cc

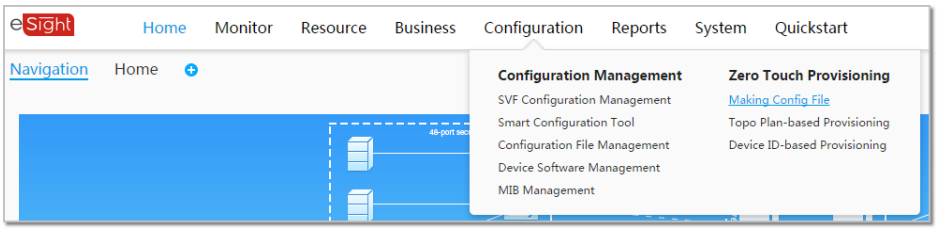
Procedure

Step 1 Specify VLAN 1 as a pass VLAN on the root device (the configuration is not provided here).

Step 2 Configure the root device as a DHCP server. For details, see **Configuring a DHCP Server**.

Step 3 Prepare configuration files for devices to be deployed.

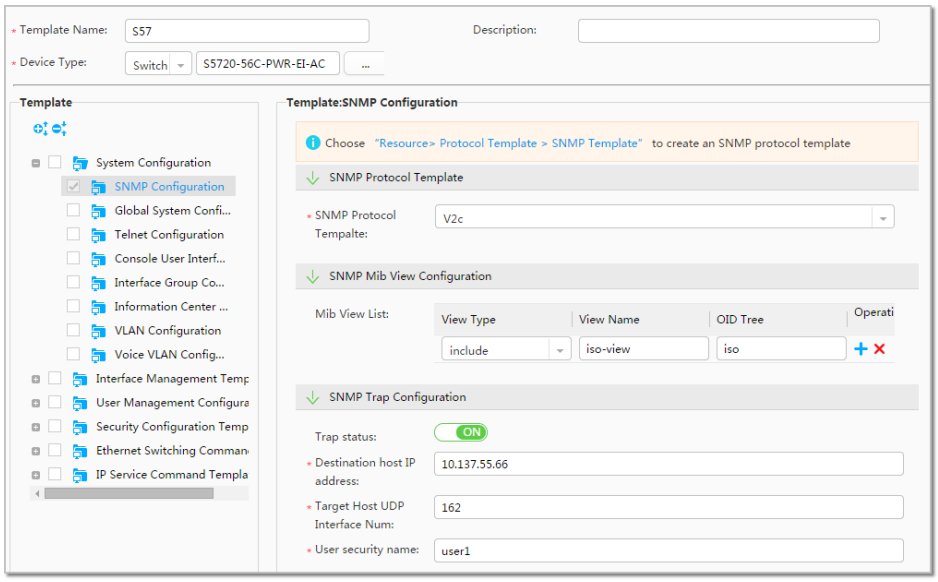
1. Choose **Configuration** > **Zero Touch Provisioning** > **Making Config File**.



2. Click **Create**, enter the following parameters, and click **Next**. Click **OK**. The configuration file is created for the aggregation devices.

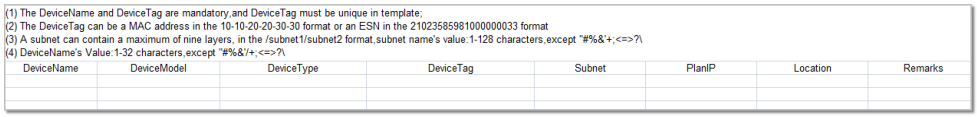
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0



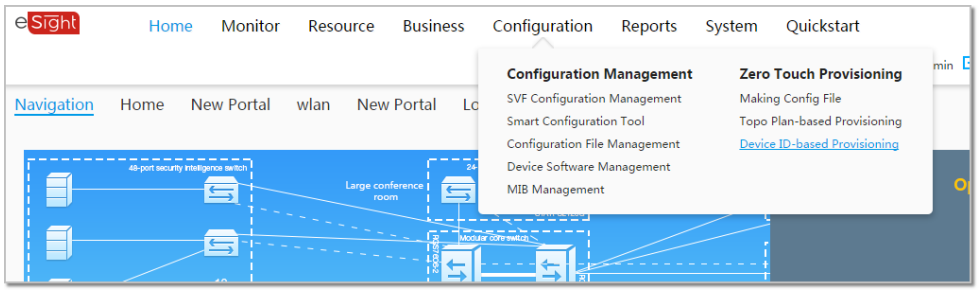
3. Repeat the preceding step to create a configuration file for the access devices.

Step 4 Connect cables of devices to be deployed and power on them. Manually record MAC addresses/ESNs, locations, and models of the devices into an excel file.

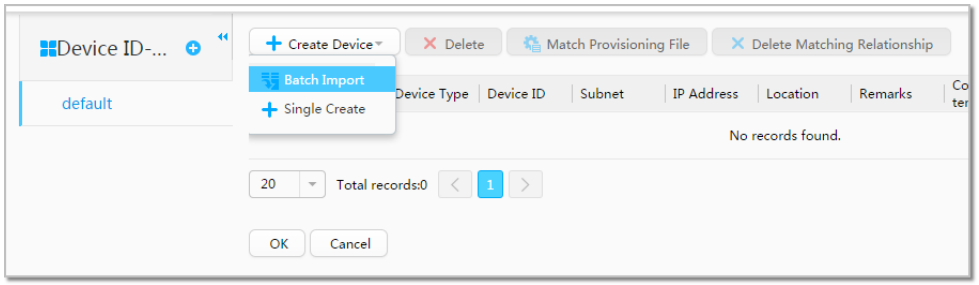


Step 5 Match the configuration file, software package, patch file, and license file with the devices to be deployed.

1. Choose **Configuration** > **Zero Touch Provisioning** > **Device ID-based Provisioning**.



2. Click **Create** and then choose **Create Device** > **Batch Import**.



3. In the **Batch Import** dialog box that is displayed, upload the excel file created in step 2 and click **OK**. The provisioning task is created.
4. Select the provisioning task, click **Match Provisioning File**, and select the correct configuration file, software package, patch file, and license file.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

5. Click **OK**. The provisioning file matching task is complete.

Step 6 Trigger provisioning and restart the switches after they download corresponding files.

1. Select the created manual provisioning task and click **Start**.
2. Click **Active**. The devices are restarted and download the latest provisioning files. After that, the entire provisioning task delivery is complete.

----End

Result

After the provisioning is complete, choose **Monitor** > **Topology** > **Topology Management**. All deployed devices can be displayed, and alarm messages of the devices can be reported to eSight.

3.16 Reference

The following table lists the references for this document.

Document	Description	Remarks
RFC1534	Interoperation Between DHCP and BOOTP	-
RFC2131	Dynamic Host Configuration Protocol	-
RFC2132	DHCP Options and BOOTP Vendor Extensions	-
RFC3046	DHCP Relay Agent Information Option	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

4 USB-based Deployment Configuration

About This Chapter

This chapter describes how to configure USB-based deployment to simplify the deployment process, reduce the deployment costs, and relieve users from software commissioning.

4.1 USB-based Deployment Overview

4.2 Principles

4.3 Configuration Notes

4.4 Making an Index File

4.5 Configuring USB-based Deployment

4.6 Configuration Examples

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

4.1 USB-based Deployment Overview

Definition

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

4.2 Principles

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.

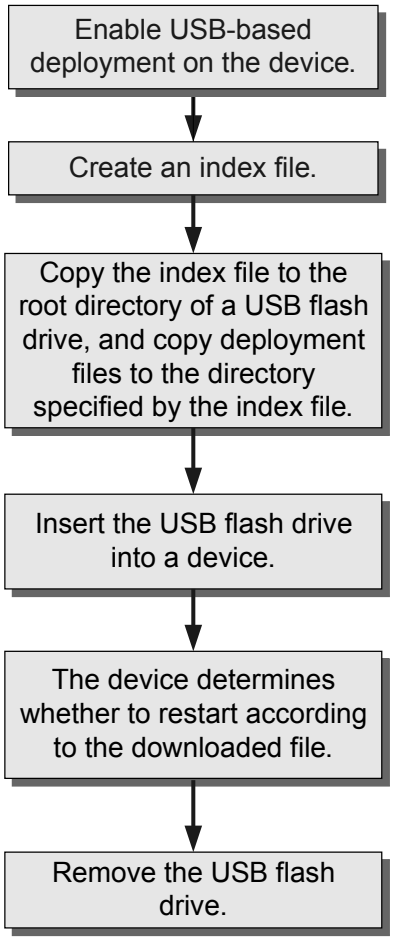
Figure 4-1 shows the USB-based deployment flowchart.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 **usbload_config.txt** or **smart_config.ini**.
- **Optional files**
  - System software: The file name extension is .cc.
  - Configuration file: The file name extension is .cfg or .zip.
  - Patch file: The file name extension is .pat.
  - Web file: The file name extension is .web.7z.
  - User-defined file: It can be specified only in the **smart_config.ini** file.
  - Script file: The file name extension is .bat.

    A script file can import stack configurations to a device during a USB-based deployment.

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

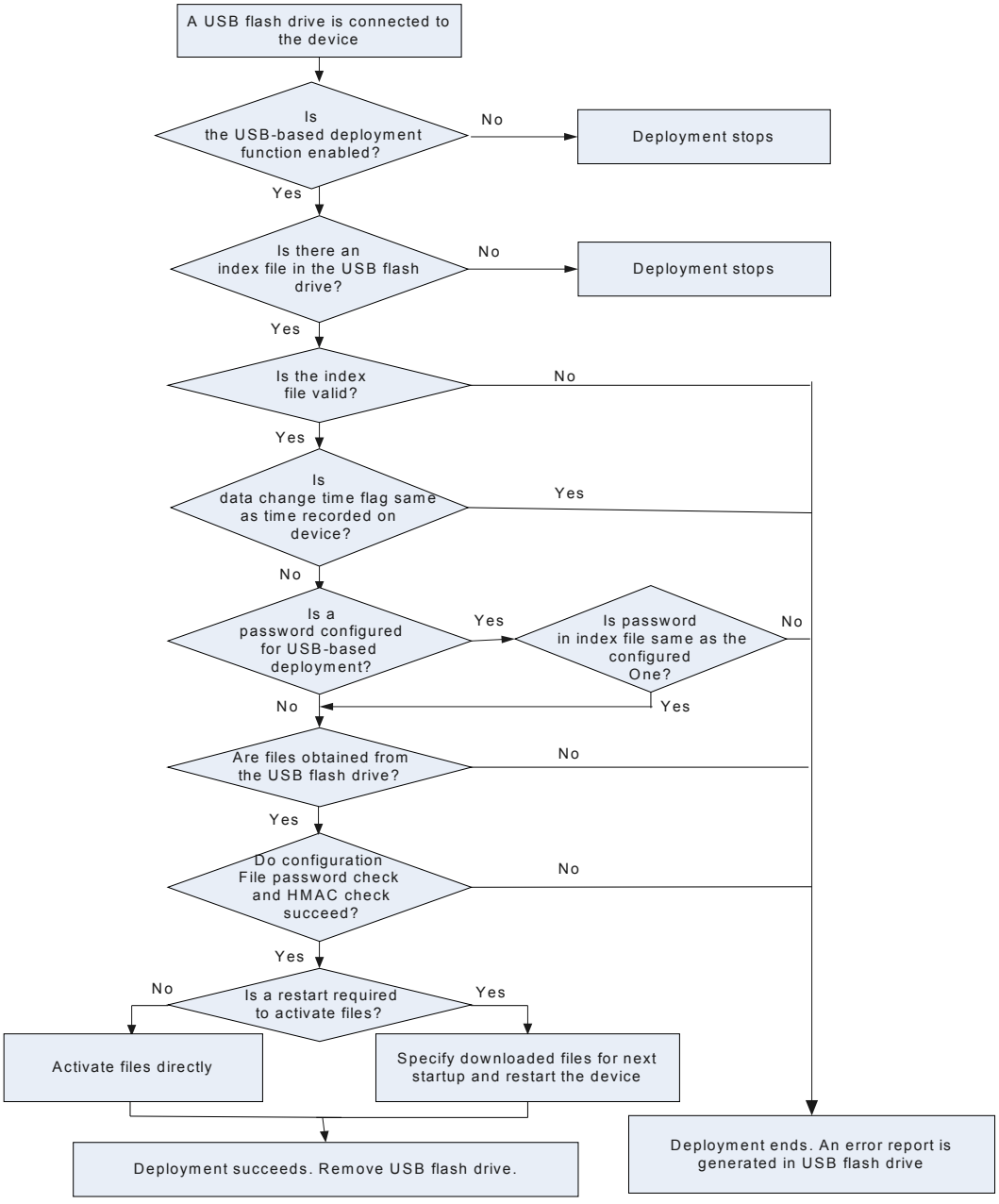
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Device Running Process

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

Figure 4-2 Device running flowchart



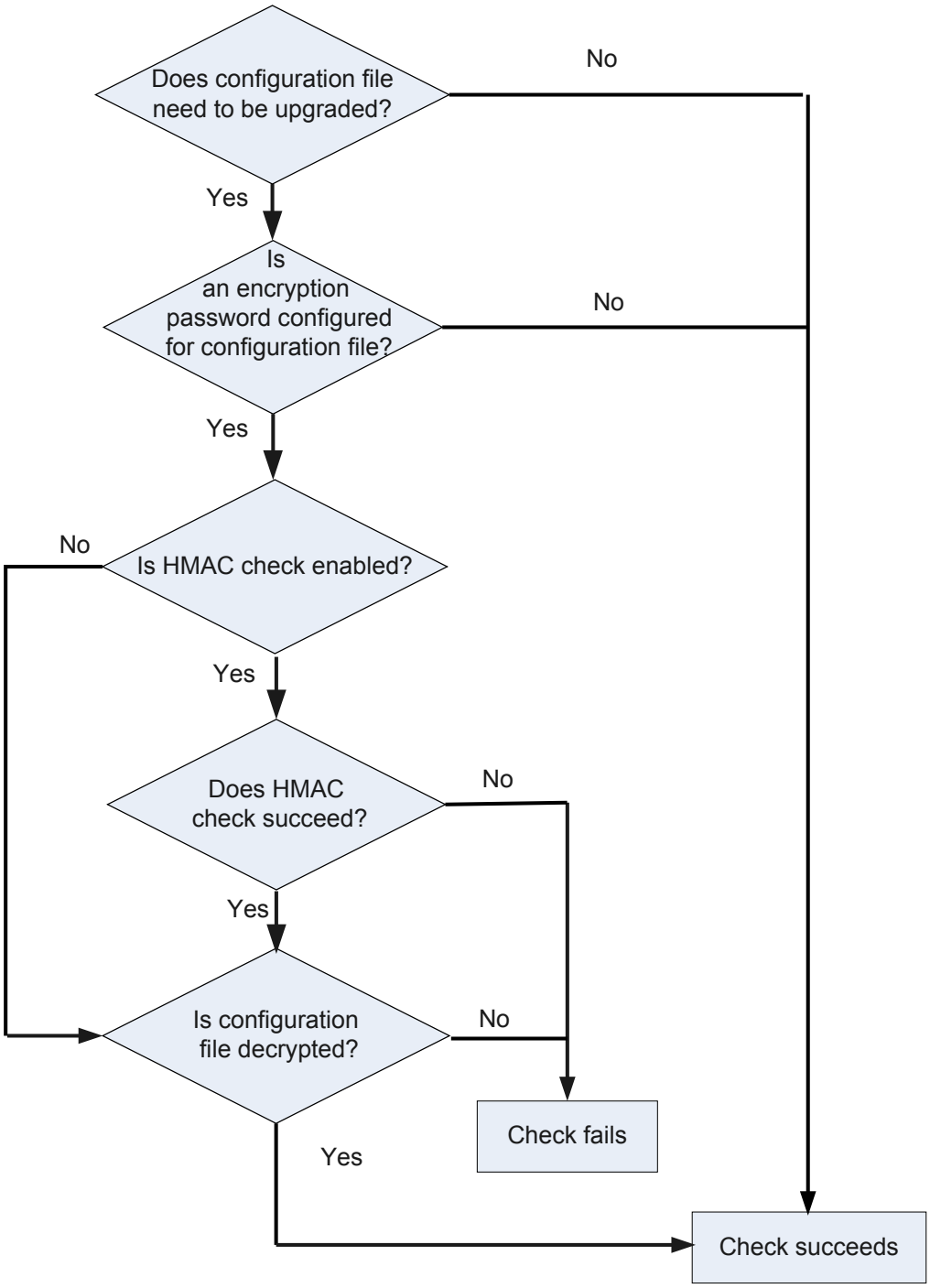
Password check and HMAC check for the configuration file are performed only when a **smart_config.ini** index file is used. The check processes are shown in **Figure 4-3**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 4-3 Password check and HMAC check for the configuration file during USB-based deployment



1. A user connects a USB flash drive to a device, the system detects the USB flash drive.
2. The process proceeds depending on whether the USB-based deployment function is enabled:
   - If the device has no configuration file, the USB-based deployment function is always enabled. In this case, the deployment process starts from step 3.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- If the device has a configuration file and the USB-based deployment function has been enabled, the deployment process starts from step 3.
- If the device has a configuration file but the USB-based deployment function is disabled, USB-based deployment cannot be performed.

3. The system checks whether an index file exists in the USB flash drive.
   - If an index file exists, the process goes to step 4.
   - If no index file exists, the process ends.
4. The system checks whether the index file is valid.
   - If the index file is valid, the process goes to step 5.
   - If the index file is invalid, the USB-based deployment fails and the system creates an error report in the USB flash drive. The process ends.
5. The device compares the data change time in the index file with the time of last USB-based deployment recorded in the system.
   - If the data change time is different from the time of last USB-based deployment, the process goes to step 6.
   - If the data change time is the same as the time of last USB-based deployment, the USB-based deployment fails and the system creates an error report in the USB flash drive. The process ends.
6. The device checks whether a password is configured for USB-based deployment.
   - If a password is configured, the device checks whether the password in the index file is the same as the configured password. If they are the same, the process goes to step 7. If they are different, the USB-based deployment fails and the system creates an error report in the USB flash drive. The process ends.

     NOTE

     From V200R007, the authentication password for USB-based deployment cannot be manually configured. If an authentication password has been configured before the upgrade, the password is saved as pre-upgrade configuration after the software version is upgraded to V200R007 or later. It is recommended that you run the **undo set device usb-deployment password** command to delete the configured password after the upgrade is complete.

     The S5720EI, S5720SI, S5720S-SI, S6720EI, S6720S-EI, S5710-X-LIand S5700S-LI do not support the configuration of the authentication password for USB-based deployment.
   - If no password is configured, the process goes to step 7.
7. The device obtains the required files from the USB flash drive according description in the index file.
   - If the required files are obtained successfully, the process goes to step 8.
   - If files fail to be obtained, the USB-based deployment fails and the system creates an error report in the USB flash drive.
8. The device checks the password and HMAC of the configuration file. (This step can be performed only when a **smart_config.ini** index file is used.)
   - If the upgrade files do not include the configuration file, the process goes to step 9.
   - If the upgrade files include the configuration file but no encryption password is configured, the process goes to step 9.
   - If the upgrade files include the configuration file, an encryption password is configured but HMAC check is not enabled, the device decrypts the configuration file using the configured password. If the decryption succeeds, the process goes to step 9. If the decryption fails, the UBS-based deployment fails and the process ends. An error report is created in the USB flash drive.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- If the upgrade files include the configuration file, an encryption password is configured and HMAC check is enabled, the device performs HMAC check and then decrypts the configuration file. If HMAC check and file decryption succeed, the process goes to step 9. Otherwise, the process ends, and an error report is created in the USB flash drive.

9. The device determines whether to restart to activate the obtained files based on the file types or the file activation mode configured in the system.
   - If the device does not need to restart, it activates the files directly. The process ends.
   - If the device needs to restart, it specifies the obtained files for next startup and restarts. After the device restarts, the process ends.
10. The USB-based deployment succeeds, and the process ends. The user removes the USB flash drive from the device.

NOTE

During a USB-based deployment, the system creates an error report **usbload_error.txt** if an error occurs in any step. You can view this report to analyze the cause of the deployment failure. If the deployment succeeds, the system creates a deployment success report **usbload_verify.txt**.

4.3 Configuration Notes

Involved Network Elements

Other network elements are not required.

License Support

USB-based deployment is not under license control.

Version Support

Table 4-1 Products and minimum version supporting USB-based deployment

Series	Product	Minimum Version Required
S1700	S1720	Not supported
S2700	S2700SI/S2700EI	Not supported
	S2710SI	Not supported
	S2720EI	Not supported
	S2750EI	Not supported
S3700	S3700SI/S3700EI	Not supported
	S3700HI	Not supported
S5700	S5700LI	V200R003
	S5700S-LI	V200R008

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Series	Product	Minimum Version Required
	S5710-C-LI	V200R001 (The S5710-C-LI is unavailable in V200R002 and later versions.)
	S5710-X-LI	V200R008
	S5700SI	V100R005 (The S5700SI is unavailable in V200R006 and later versions.)
	S5700EI	Not supported
	S5710EI	V200R001 (The S5710EI is unavailable in V200R006 and later versions.)
	S5720EI	V200R007
	S5700HI	V100R006 (The S5700HI is unavailable in V200R006 and later versions.)
	S5710HI	V200R003 (The S5710HI is unavailable in V200R006 and later versions.)
	S5720HI	V200R006
	S5720SI/S5720S-SI	V200R008
S6700	S6700EI	V100R006 (The S6700EI is unavailable in V200R006 and later versions.)
	S6720EI	V200R008
	S6720S-EI	V200R009

Feature Dependencies and Limitations

In the S5700LI series, only the S5700-52X-LI-48CS-AC, S5701-28X-LI-24S-AC, S5701-28X-LI-AC, S5700-28X-LI-24S-DC, and S5700-28X-LI-24S-AC support USB-based deployment.

In the S5700S-LI series, only the S5700S-28X-LI-AC and S5700S-52X-LI-AC support USB-based deployment.

Constraints on USB-based deployment

- The file system format of the USB flash drive must be FAT32, and standard for the USB interface is USB2.0 (USB1.1 interface on the S5700LI). To ensure compatibility between

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

USB flash drives and devices, use Huawei-certified USB flash drives to configure the Huawei devices. **Table 4-2** lists the USB flash drives applicable to a switch.

Table 4-2 USB flash drives applicable to a switch

Capacity	Vendor	Model	Remarks
4 GB	Netac	U208	You can buy Netac USB 4 GB flash drives from Huawei or other vendors.
	SanDisk	Cruzer Blade	Huawei does not offer this USB flash drive, and you need to buy it from other vendors.
	Hewlett-Packard	v218G	Huawei does not offer this USB flash drive, and you need to buy it from other vendors.
	PNY	M1	Huawei does not offer this USB flash drive, and you need to buy it from other vendors.
8 GB	Netac	U208	Huawei does not offer this USB flash drive, and you need to buy it from other vendors.
	Hewlett-Packard	v225w	Huawei does not offer this USB flash drive, and you need to buy it from other vendors.
	STEC	SLUFD8GU2TUI	Huawei does not offer this USB flash drive, and you need to buy it from other vendors.

- Only one USB flash drive can be connected to a device.
- In V200R005C00 and later versions, USB-based deployment using a **smart_config.ini** index file is supported, and this deployment mode is supported in a stack. The USB flash drive must be connected to the master switch of the stack. If it is connected to the standby switch or a slave switch, the USB-based deployment process will not start.
- USB-based deployment using the **usbload_config.txt** index file can only be performed in a single switch, not a stack of multiple switches. In a stack of multiple switches, if the USB flash drive is connected to the standby switch or a slave switch, the USB-based deployment process will not start. If the USB flash drive is connected to the master switch, the USB indicator blinks red fast, indicating that the USB-based deployment fails. In this case, the switch records an error report including the following information: The usbload_config.txt index file cannot be used for USB deployment of a multi-member stack.
- The S5710-X-LI, S5720SI, S5720S-SI, S6720EI, S6720S-EI, S5720EI and S5720HI series switches support only the **smart_config.ini** format.
- The S5700S-28X-LI-AC, S5700S-52X-LI-AC, and S5700S-28P-PWR-LI-AC in the S5700S-LI series support only the **smart_config.ini** format.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Fields in an index file are restricted by the current system version. For example, if some fields in the index file are not supported by the current system version, these fields are invalid for an upgrade to a later version.
- USB-based deployment is mutually exclusive with the SVF, web initial login mode and EasyDeploy functions.
- In USB-based deployment scenarios, the devices (S5720HI switches) may be upgraded to V200R008C00 or a later version after restart. In this case, the devices check whether the configuration file for next startup contains WLAN configuration that conflicts with the software package for next startup. If so, the devices cannot restart and the USB-based deployment fails. The error report file **usbload_error.txt** is generated in the root directory of the USB flash drive, recording the failure causes. To solve this problem, you need to use **eDesk** to convert the configuration file and then set it as the next startup configuration file.

Precautions for USB-based deployment

- Devices to be deployed are unconfigured devices and do not have security measures configured. Therefore, when onsite non-professionals perform deployment task, ensure that they do not perform any unauthorized operations on the devices, USB flash drive, and deployment files.
- Before saving files to a USB flash drive, disable the write-protection function of the USB flash drive.
- Do not use a partitioned USB flash drive to deploy the S5720EI, S5720HI, S5720SI, S5720S-SI, S6720EI, or S6720S-EI switches. Otherwise, the switches may fail to find the files saved on the USB flash drive, resulting in a failed USB-based deployment.
- Before using a USB flash drive to upgrade a device, ensure that the device can start successfully and has sufficient space to store the required files.
- Do not power off the device during a USB-based deployment process. Otherwise, the upgrade fails or the device cannot start.
- Do not remove the USB flash drive before the USB-based deployment process is complete. Otherwise, data in the USB flash drive may be corrupted.
- A **smart_config.ini** index file supports encryption and HMAC check for a configuration file, whereas a **usbload_config.txt** index file does not. Therefore, if upgrade files include a configuration file, you are advised to make a **smart_config.ini** index file, configure an encryption password for the configuration file, and enable HMAC check to enhance security.
- The S5700LI supports two index file formats: **smart_config.ini** and **usbload_config.txt**. If both types of index files are saved in a USB flash drive, the **smart_config.ini** file is preferred. During USB-based deployment, it is not recommended to save the two types of index files in the USB flash drive. When rolling back a device to V200R003 or earlier using a USB flash drive, it is recommended to use the **usbload_config.txt** index file because V200R003 and earlier versions do not support the **smart_cfg.ini** index file.

4.4 Making an Index File

Background

In V200R005C00 and later versions, two index file formats can be used in USB-based deployment: smart_config.ini and usbload_config.txt. The S5700LI series switches support

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

both the two formats, and you can make an index file in either format. If both two types of index files are saved in a USB flash drive, the smart_config.ini file is preferred. Switches of other series support only the smart_config.ini format.

Procedure for Making an Index File

To edit an index file on a PC, perform the following operations:

1. Create a text file.
2. Edit the file in a specific format.
3. Save the file as **smart_config.ini** or **usbload_config.txt**.
4. Copy the **smart_config.ini** or **usbload_config.txt** file to the root directory of the USB flash drive.

Index File Formats

NOTE

- In a smart_config.ini index file, each line can contain no more than 512 characters. Otherwise, the index file is invalid.
- The field names in the **smart_config.ini** index file are case insensitive, and the field names in the **usbload_config.txt** index file must be in lowercase. All field values except passwords are case insensitive.
- In the index file, fields related to file loading are all optional, but you must specify at least one file type field. The system software name, configuration file name, and path file name are at most 48 bytes long, and names of other files are at most 64 bytes long.

Format of the smart_config.ini index file

```
BEGIN LSW
[GLOBAL CONFIG]
TIMESN=
AUTODELFILE=
ACTIVEMODE=
USB-DEPLOYMENT PASSWORD=
[DEVICEn DESCRIPTION]
OPTION=
ESN=
MAC=
AUTODELFILE=
ACTIVEMODE=
DEVICETYPE=
HMAC=
DIRECTORY=
SYSTEM-SOFTWARE=
SYSTEM-CONFIG=
SYSTEM-PAT=
SYSTEM-WEB=
SYSTEM-SCRIPT=
SYSTEM-USERDEF1=
SYSTEM-USERDEF2=
SYSTEM-USERDEF3=
END LSW
```

The **smart_config.ini** index file can contain comments. A comment starts with a semicolon (;). You can add a comment after a field in the same line (separate the field and comment with a space) or the next line.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 4-3 Fields in the smart_config.ini index file

Field	Description
BEGIN LSW	Mandatory. It is the start flag of the index file and cannot be modified.
GLOBAL CONFIG	Mandatory. It is the start flag of the global configuration and cannot be modified.
TIMESN	Mandatory. It indicates when the data was changed. The value is a string of 1 to 16 characters without spaces. The recommended format is yyyymmdd.hhmmss. For example, if the index file was edited at 08:09:10 on June 28, 2011, you can set this field to TIMESN=20110628.080910. Each device to be upgraded has a TIMESN field. In a USB-based upgrade, a device sets the TIMESN field before it restarts (or after the upgrade is complete if the device does not need to restart). This TIMESN field cannot be used in the next upgrade. If the upgrade fails after the device restarts, you must change the TIMESN value before starting a USB-based upgrade again.
AUTODELFILE	Optional. It specifies whether to delete the old system software after a successful upgrade. ● AUTODELFILE=YES: The original system software will be deleted after a successful upgrade. ● AUTODELFILE=NO: The original system software will not be deleted after a successful upgrade. The default value of the AUTODELFILE field is NO. If this field does not exist, is empty, or has an invalid value, the default value is used. The AUTODELFILE field can be used in the global configuration or the configuration for a single device. ● The AUTODELFILE field in the [GLOBAL CONFIG] section applies globally, and the AUTODELFILE field in the [DEVICE*n* DESCRIPTION] section applies only to the specific device. ● If the AUTODELFILE field is set to **YES** or **NO** for a device, the configuration takes effect for this device. If the AUTODELFILE field is not set or kept empty for a device, the global configuration takes effect for the device.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Field	Description
ACTIVEMODE	Optional. It specifies the mode in which the downloaded files are activated. ● DEFAULT: uses the respective default activation modes of the downloaded files. The default activation modes for different files are as follows: – System software and configuration file: activated after a restart. – Patch file: activated without a need to restart the device. – Web page file and user-defined file: do not need to be activated. The USB-based deployment ends when these files are downloaded. ● RELOAD: activates the downloaded files by restarting the device. The default value of the ACTIVEMODE field is DEFAULT. If this field does not exist, is empty, or has an invalid value, the default value is used. The ACTIVEMODE field can be used in the global configuration or the configuration for a single device. ● The ACTIVEMODE field in the [GLOBAL CONFIG] section applies globally, and the ACTIVEMODE field in the [DEVICE*n* DESCRIPTION] section applies only to the specific device. ● If the ACTIVEMODE field is set to **DEFAULT** or **RELOAD** for a device, the configuration takes effect for this device. If the ACTIVEMODE field is not set or kept empty for a device, the global configuration takes effect for the device.
USB-DEPLOYMENT PASSWORD	Optional. It specifies the authentication password for USB-based deployment. If an authentication password has been configured on the device to be upgraded, fill this field with the configured password. If no password is configured on the device, keep this field blank or delete it. Only one authentication password can be specified in an index file. If an index file is used to upgrade multiple devices, configure the same authentication password on these devices. **NOTE** From V200R007, the authentication password for USB-based deployment cannot be manually configured. If an authentication password has been configured before the upgrade, the password is saved as pre-upgrade configuration after the software version is upgraded to V200R007 or later. It is recommended that you run the **undo set device usb-deployment password** command to delete the configured password after the upgrade is complete. The S5720EI, S5720SI, S5720S-SI, S6720EI, S6720S-EI, S5710-X-LI and S5700S-LI do not support the configuration of the authentication password for USB-based deployment.
DEVICE*n* DESCRIPTION	Mandatory. It is the start flag of the file description, where *n* is a device number. The device number starts at 0 and ends at 65535. **NOTE** ● Each field in the DEVICE*n* DESCRIPTION section can be used only once. If a field is used repeatedly, no device will match DEVICE*n*. ● The system matches the DEVICE fields from top to bottom in the file and stops the matching when it finds a matching device description.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>OPTION</td><td colspan="2">Optional. It specifies whether the file information for a device is valid.
● OPTION=OK: The file information is valid.
● OPTION=NOK: The file information is invalid and the system does not check the file information for this device.
The default value of this field is OK. If this field does not exist, is empty, or has an invalid value, the default value is used.</td></tr>
<tr><td>ESN</td><td>Optional. It specifies the equipment serial number of a device. If this field is set to DEFAULT, the ESN of the device is not checked. If this field is set to another value, the ESN of the device must be the same as the configured value.
The default value of this field is DEFAULT. If this field does not exist or is empty, the default value is used.</td><td rowspan="3">The system matches the devices to be upgraded with device description from top to bottom in the index file. The matching priority of the fields is MAC > ESN > DEVICETYPE > DEFAULT (descending order). Once a device matches DEVICEn, files specified in DEVICEn are loaded to the device. When an error occurs during file loading, the system does not match this device with other device description and only generates an error report.</td></tr>
<tr><td>MAC</td><td>Optional. It specifies the MAC address of a device, in the XXXX-XXXX-XXXX format. X is a hexadecimal number. If this field is set to DEFAULT, the device MAC address is not checked. If this field is set to another value, the device MAC address must be the same as the configured value.
The default value of this field is DEFAULT. If this field does not exist or is empty, the default value is used.</td></tr>
<tr><td>DEVICETYPE</td><td>Optional. It specifies a device type, for example, S5700-X-LI. If this field is set to DEFAULT, the device type is not checked. If this field is set to another value, the device type must be the same as the configured value.
The default value of this field is DEFAULT. If this field does not exist or is empty, the default value is used.</td></tr>
</table>

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Field	Description
HMAC=	Optional. It specifies the hashed message authentication code (HMAC) used to verify the configuration file to be loaded. The HMAC is a string of 64 characters, which is calculated for the configuration file saved in the USB flash drive by an HMAC-SHA256 calculation tool. The key used to calculate the HMAC must be the same as the password configured by the **set device usb-deployment config-file password** command. By default, the configuration file to be loaded is not verified. **NOTE** The HMAC can be generated for a configuration file using an HMAC-SHA256 calculation tool (such as OpenSSL or HashCalc). If upgrade files include a configuration file, it is recommended that you run the **set device usb-deployment config-file password** command to configure an encryption password for the configuration file, compress the configuration file using the configured password before saving it in the USB flash drive, and run the **set device usb-deployment hmac** command to enable HMAC check on the device to be upgraded. This configuration improves security.
DIRECTORY	Optional. It specifies the directory where files are saved in the USB flash drive. ● If this field is empty or does not exist, files are saved in the root directory of the USB flash drive. ● DIRECTORY=/abc: Files are saved in the **abc** directory. By default, this field is empty. The directory name specified in the index file must be in the same format as required by the file system. ● The directory depth must be smaller than or equal to 4 levels. The full path must start with a slash (/), and subdirectories are separated by a slash. The directory cannot end with a slash. For example, abc/test is a valid directory, whereas /abc/test/ is an invalid directory. ● Each subdirectory can contain 1 to 15 characters. ● The directory name is case insensitive and cannot contain spaces and the following special characters: ~ * / \ : ' " < > | ? [ ] %.
SYSTEM-SOFTWARE	Optional. It specifies a system software name, with an extension .cc. If this field is set, the device compares the specified system software version with the running system software version. If they are the same, the device does not copy the system software from the USB flash drive and stops the upgrade.
SYSTEM-CONFIG	Optional. It specifies a configuration file name, with an extension .cfg or .zip.
SYSTEM-PAT	Optional. It specifies a patch file name, with an extension .pat.
SYSTEM-WEB	Optional. It specifies a web page file name, with an extension .web.7z.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Field	Description

SYSTEM-SCRIPT	Optional. It specifies a script file name.
	When this field is specified, the stack configuration will be imported to the device during USB-based deployment. After the device restarts, the stack configuration takes effective.
	A script file uses .bat as the file name extension. The file name consists of 5-64 characters. The file content format is the same as the format of a configuration file. The exclamation mark (!) indicates a comment. An example of a script file is as follows:
	`#`
	`stack slot 0 renumber 2`
	`! Modify the stack ID`
	`#`
	`interface stack-port 0/1`
	`port interface xgigabitethernet 0/0/27 enable`
	`#`
	`interface stack-port 0/2`
	`port interface xgigabitethernet 0/0/28 enable`
	NOTE
	● The script file edited in the UNIX or Linux system is not supported because the device cannot identify the content of such a file.
	● If a script file contains a command that is not supported by stack and that will be saved to the configuration file, the command will be lost after the device restarts.
	● If the slot ID in the stack commands in the script file is different from the slot ID of the device, the script file cannot be executed. If the **stack slot** *slot-id* **renumber** *new-slot-id* command is included in the script file, the slot ID in other stack commands must be the same as *slot-id* in this command. The following is an example of an incorrect script file. The current slot ID of the device is 0, and 2 is the new slot ID used after a restart. Other stack commands should use the current slot ID 0, but not 2.
	`#`
	`stack slot 0 renumber 2`
	`#`
	`interface stack-port 2/1`
	`port interface XGigabitEthernet 2/0/1 enable`
	● The stack cables can be connected before or after the USB-based deployment is complete. If a switch connected by a stack cable becomes a non-master switch after the script file is imported, the switch does not generate a USB-based deployment success report.

SYSTEM-USERDEF1 SYSTEM-USERDEF2 SYSTEM-USERDEF3	Optional. It specifies a user-defined file name.
END LSW	Mandatory. It is the end flag of the index file.

Format of the usbload_config.txt index file

A usbload_config.txt index file can be edited in any of the following formats:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Format 1:

  To upgrade the system software, configuration file, web file, and patch file on multiple devices to the same version, use the following index file format:

```
<time-sn=;/>
<usb-deployment password=;/>
<boardtype=; vrpfile=; cfgfile=; webfile=; patchfile=; delfile=; system-
script=;/>
```

- Format 2:

  To upgrade a specific device, use the following index file format:

```
<time-sn=;/>
<usb-deployment password=;/>
<mac=; vrpfile=; cfgfile=; webfile=; patchfile=; delfile=; system-script=;/>
```

- Format 3:

  To upgrade a specific model of device, use the following index file format:

```
<time-sn=;/>
<usb-deployment password=;/>
<esn=; vrpfile=; cfgfile=; webfile=; patchfile=; delfile=; system-script=;/>
```

NOTE

The three index file formats use the boardtype, mac, and esn fields to match devices respectively. The three fields can be used together to upgrade multiple devices using a USB flash drive. If the fields match the same device, the mac field has the highest priority, and the boardtype field has the lowest priority. The following is an example:

```
<time-sn=201305091219;/>
<usb-deployment password=;/>
<boardtype=; vrpfile=S5700-V200R009C00.CC; cfgfile=; webfile=; patchfile=;
delfile=; system-script=;/>
<mac=0018-8200-0001; vrpfile=; cfgfile=vrpcfg.cfg; webfile=; patchfile=;
delfile=0; system-script=;/>
<esn=21023518231098000028; vrpfile=; cfgfile=; webfile=; patchfile=patch.pat;
delfile=1; system-script=;/>
```

Table 4-4 Fields in the usbload_config.txt index file

Field	Description
time-sn	Mandatory. It specifies the time when the configuration data is changed, in the format of yyyymmdd.hh.mm.hh. The value must be a string of 12 digits. For example, the value **201105091219** indicates that the configuration data was changed at 12:19 on May 9, 2011. Each device to be upgraded has a time-sn field. In a USB-based upgrade, a device sets the time-sn field before it restarts (or after the upgrade is complete if the device does not need to restart). This time-sn field cannot be used in the next upgrade. If the upgrade fails after the device restarts, you must change the time-sn value before starting a USB-based upgrade again.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Field	Description
usb-deployment password	Optional. It specifies the authentication password for USB-based deployment. If an authentication password has been configured on the device to be upgraded, fill this field with the configured password. If no password is configured on the device, keep this field blank or delete it. Only one authentication password can be specified in an index file. If an index file is used to upgrade multiple devices, configure the same authentication password on these devices. **NOTE** From V200R007, the authentication password for USB-based deployment cannot be manually configured. If an authentication password has been configured before the upgrade, the password is saved as pre-upgrade configuration after the software version is upgraded to V200R007 or later. It is recommended that you run the **undo set device usb-deployment password** command to delete the configured password after the upgrade is complete. The S5720EI, S5720SI, S5720S-SI, S6720EI, S6720S-EI, S5710-X-LI and S5700S-LI do not support the configuration of the authentication password for USB-based deployment.
boardtype	Optional. It specifies the model of the device to be upgraded using a USB flash drive. The displayed device model must be the same as the actual model of the device, for example, S5700-52X-LI-48CS-AC.
vrpfile	Optional. It specifies the system software name, with an extension .cc. If this field is set, the device compares the specified system software version with the running system software version. If they are the same, the device does not copy the system software from the USB flash drive and stops the upgrade.
cfgfile	Optional. It specifies a configuration file name, with an extension .cfg or .zip.
webfile	Optional. It specifies a web file name, with an extension .web.7z.
patchfile	Optional. It specifies a patch file name, with an extension .pat.
mac	Optional. It specifies the MAC address of a device, in the XXXX-XXXX-XXXX format. X is a hexadecimal number. If this field is set to **default**, the device MAC address is not checked. If this field is set to another value, the device MAC address must be the same as the configured value. The default value of this field is **default**. If this field does not exist or is empty, the default value is used.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Field	Description
esn	Optional. It specifies the equipment serial number of a device. If this field is set to **default**, the ESN of the device is not checked. If this field is set to another value, the ESN of the device must be the same as the configured value. The default value of this field is **default**. If this field does not exist or is empty, the default value is used.
delfile	Optional. It specifies whether to delete the old system software after a successful upgrade. The value 1 indicates that the old software will be deleted, and the value 0 indicates that the old system software will not be deleted. If the index file does not contain this field or the field is set to an invalid value (not 0 or 1), the old system software will not be deleted after a successful upgrade.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Field	Description

system-script	Optional. It specifies a script file name.
	When this field is specified, the stack configuration will be imported to the device during USB-based deployment. After the device restarts, the stack configuration takes effective.
	A script file uses .bat as the file name extension. The file name consists of 5-64 characters. The file content format is the same as the format of a configuration file. The exclamation mark (!) indicates a comment. An example of a script file is as follows:
	`#`
	`stack slot 0 renumber 2`
	`! Modify the stack ID`
	`#`
	`interface stack-port 0/1`
	`port interface xgigabitethernet 0/0/27 enable`
	`#`
	`interface stack-port 0/2`
	`port interface xgigabitethernet 0/0/28 enable`
	NOTE
	● The script file edited in the UNIX or Linux system is not supported because the device cannot identify the content of such a file.
	● If a script file contains a command that is not supported by stack and that will be saved to the configuration file, the command will be lost after the device restarts.
	● If the slot ID in the stack commands in the script file is different from the slot ID of the device, the script file cannot be executed. If the **stack slot** *slot-id* **renumber** *new-slot-id* command is included in the script file, the slot ID in other stack commands must be the same as *slot-id* in this command. The following is an example of an incorrect script file. The current slot ID of the device is 0, and 2 is the new slot ID used after a restart. Other stack commands should use the current slot ID 0, but not 2.
	`#`
	`stack slot 0 renumber 2`
	`#`
	`interface stack-port 2/1`
	`port interface XGigabitEthernet 2/0/1 enable`
	● The stack cables can be connected before or after the USB-based deployment is complete. If a switch connected by a stack cable becomes a non-master switch after the script file is imported, the switch does not generate a USB-based deployment success report.

NOTE

- When editing an index file, press **Enter** when a line is finished. After editing the file, save it.
- If a field is not found, the system considers that the field is left blank.

4.5 Configuring USB-based Deployment

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Pre-configuration Tasks

Start the device.

Procedure

Before using a USB flash drive to upgrade a device, make an index file and save the index file and files to be loaded to the USB flash drive. Then connect the USB flash drive to the device to start the upgrade.

1. Run the **system-view** command to enter the system view.
2. Run the **undo set device usb-deployment disable** command to enable the USB-based deployment function.

   The USB-based deployment function is disabled by default. It is recommended that you disable this function after a USB-based deployment is complete. If a device has no configuration file, the USB-based deployment function is always enabled on the device.
3. (Optional) Run the **set device usb-deployment config-file password** *password* command to configure an encryption password for the configuration file.

   NOTE

   If upgrade files include a configuration file, it is recommended that you run this command to configure an encryption password for the configuration file and compress the configuration file using the configured password before saving it in the USB flash drive. This configuration improves security. This step is mandatory if HMAC check is required for the configuration file.

   Configuration file encryption is supported only when a **smart_config.ini** index file is used.
4. (Optional) Run the **set device usb-deployment hmac** command to enable HMAC check for configuration files.

   NOTE

   HMAC check can be performed for a configuration file only when a **smart_config.ini** file is used.

   If upgrade files include a configuration file, you can enable HMAC check to ensure validity of the configuration file to be loaded.

   During USB-based deployment, if HMAC check is enabled on a device, the device uses the password configured by the **set device usb-deployment config-file password** command to calculate the HMAC for the configuration file, and compares the calculated value with the HMAC field value in the index file. If the two values are the same, the configuration file is considered valid and loaded to the device. If not, the configuration file is considered invalid and cannot be loaded.
5. Make an index file.

   For details, see **4.4 Making an Index File**.
6. Save the index file in the root directory of the USB flash drive. If you make a **smart_config.ini** index file, save the upgrade files specified in the index file to the specified directory of the USB flash drive (root directory by default). If you make a **usbload_config.txt** file, save the upgrade files specified in the index file to the root directory of the USB flash drive.
7. Connect the USB flash drive to the device and start the upgrade process.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTICE

Devices to be deployed are unconfigured devices and do not have security measures configured. Therefore, when onsite non-professionals perform deployment task, ensure that they do not perform any unauthorized operations on the devices, USB flash drive, and deployment files.

- During the upgrade, the system obtains the upgrade files according to the description in the **usbload_config.txt** or **smart_config.ini** file and saves the files in the default storage medium. In a stack, the master switch copies the upgrade files to all the member switches.
- If the **smart_config.ini** index file is used, the system activates the upgrade files using the method specified in the ACTIVEMODE field.

  If the **usbload_config.txt** index file is used and the index file specifies a system software, configuration file, or script file, the device sets the system software or configuration file as the next-startup file, and then restarts to complete the upgrade and make the script file take effect. By default, the device activates patch files without restarting and does not activate web page files.
- If an upgrade requires the device to restart, the device waits 10 seconds before a restart. In this period, the USB indicator is steady yellow.

Observing the Indicator to Check the USB-based Deployment Progress

Observe the SYS indicator on the S5700LI or S6720S-EI to determine the progress of USB-based deployment:

- Slow blinking yellow (once every 2s): The USB-based deployment has succeeded.
- Fast blinking green (four times every 1s): The system is reading data from the USB flash drive.
- Fast blinking red (four times every 1s): USB-based deployment has failed.

Observe the USB indicator on the S5710-X-LI, S5700S-LI, S5720SI, S5720S-SI, S6720EI, S5720HI or S5720EI to determine the progress of USB-based deployment:

- Steady green: The USB-based deployment has succeeded.
- Fast blinking green (four times every 1s): The system is reading data from the USB flash drive.
- Fast blinking red (four times every 1s): USB-based deployment has failed.
- Steady yellow: The system will restart.
- Off: An error occurred. For example, no index file is saved in the USB flash drive, no USB flash drive is installed, the USB port is damaged, the ACT indicator is damaged, the USB flash drive contains no file for device deployment, or the switch is restarting.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

- If the USB-based deployment succeeds, the system creates a deployment success report **usbload_verify.txt** in the root directory of the USB flash drive. You can remove the USB flash drive now.
- If the USB-based deployment fails, the system creates an error report **usbload_error.txt** in the root directory of the USB flash drive. View the report to analyze cause of the deployment failure.
- It is recommended that you run the **set device usb-deployment disable** command to disable the USB-based deployment function after completing a deployment. Otherwise, an unnecessary upgrade will be triggered if a USB flash drive is connected to the device by mistake, causing service interruption.

4.6 Configuration Examples

4.6.1 Example for Configuring USB-based Deployment (Using a smart_config.ini Index File)

Networking Requirements

To reduce labor costs and save time in device deployment, two new devices need to be automatically upgraded and configured. Requirements for the deployment are as follows:

- The devices need to be upgraded at 02:09 a.m. on July 28, 2013.
- The first device S5700-X-LI needs to be upgraded from V200R009C00 to a later version, and its MAC address is 0018-0303-1234. This device needs to load the new system software package **S5700LI-new.CC** and a user-defined file **userfile.txt**. After the upgrade, the old system software package needs to be deleted.
- The second device S5720HI needs to be upgraded from V200R009C00 to a later version, and its ESN is 020TEA10A9000016. This device needs to load the new system software package **S5720HI-new.CC**, configuration file **vrpcfgnew.zip**, and path file **patch.pat**.

  NOTE

  A configuration file is used for USB-based deployment in this example. To ensure security of the configuration file, the configuration file needs to be encrypted using a password and verified using HMAC check. Therefore, the **vrpcfgnew.zip** file is the encrypted configuration file.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable USB-based deployment. Configure an encryption password for the configuration file and enable HMAC check. (If the device has no configuration file, USB-based deployment does not need to be enabled.)
2. Make an index file **smart_config.ini**.
3. Save the **smart_config.ini** file and upgrade files to the root directory of the USB flash drive.
4. Connect the USB flash drive to a USB port of each device to complete automatic software upgrade.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Enable USB-based deployment. Configure an encryption password for the configuration file and enable HMAC check.

```
<HUAWEI> system-view
[HUAWEI] undo set device usb-deployment disable
[HUAWEI] set device usb-deployment config-file password psw@huawei
[HUAWEI] set device usb-deployment hmac
```

After HMAC check is enabled, the calculated HMAC for the configuration file is **6c4ab0d87142a9e29080d6dfe9e13818a3f6f3cc852a272460394a8d0a4c8649**, which needs to be added to the HMAC field in the index file.

Step 2 Make an index file.

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

```
BEGIN LSW
[GLOBAL CONFIG]
TIMESN=20130728.020900
[DEVICE0 DESCRIPTION]
MAC=0018-0303-1234
AUTODELFILE=YES
DEVICETYPE=S5700-X-LI
SYSTEM-SOFTWARE=S5700LI-new.CC
SYSTEM-USERDEF1=userfile.txt
[DEVICE1 DESCRIPTION]
ESN=020TEA10A9000016
DEVICETYPE=S5720-HI
HMAC=6c4ab0d87142a9e29080d6dfe9e13818a3f6f3cc852a272460394a8d0a4c8649
SYSTEM-SOFTWARE=S5720HI-new.CC
SYSTEM-CONFIG=vrpcfgnew.zip
SYSTEM-PAT=patch.pat
END LSW
```

Step 3 Save the **smart_config.ini** file and upgrade files to the root directory of the USB flash drive.

Step 4 Connect the USB flash drive to the S5700-X-LI to start the deployment process. Observe the SYS indicator on the switch to monitor the deployment state.

After the switch restarts, the system checks the deployment state. If the SYS indicator blinks yellow slowly (once every 2s), the USB-based deployment has succeeded. If the SYS indicator blinks red, the USB-based deployment has failed. View the **usbload_error.txt** file in the root directory of the USB flash drive to analyze why the deployment fails.

If the USB-based deployment succeeds, remove the USB flash drive and connect it to the other device.

Step 5 Connect the USB flash drive to the S5720-HI to start the deployment process. Observe the USB indicator on the switch to monitor the deployment state.

After the switch restarts, the system checks the deployment state. If the USB indicator blinks yellow slowly (once every 2s), the USB-based deployment has succeeded. If the USB indicator blinks red fast (twice every 1s), the USB-based deployment has failed. View the **usbload_error.txt** file in the root directory of the USB flash drive to analyze why the deployment fails.

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

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

4.6.2 Example for Configuring USB-based Deployment (Using an Index File usbload_config.txt)

Networking Requirements

To reduce labor costs and save time in device deployment, two new devices need to be automatically upgraded and configured. The requirements for the upgrade are as follows:

- The devices need to be upgraded at 02:09 a.m. on June 28, 2013.
- The first device S5700-X-LI needs to be upgraded from V200R009C00 to a later version and does not need to load a configuration file, patch file, or any other files. The device MAC address is 0018-0303-1234, and the new system software package is **S5700LI-new.CC**.
- The second device S5700-X-LI needs to be upgraded from V200R009C00 to a later version. Its ESN is 020TEA10A9000016 and the new system software package is **S5700LI-new.CC**. This device needs to load the configuration file **vrpcfg.cfg** and path file **patch.pat**.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable USB-based deployment. (If the device has no configuration file, USB-based deployment does not need to be enabled.)
2. Make an index file **usbload_config.txt** for USB-based deployment. Ensure that all fields in the index file are supported by the current system version of the devices.
3. Save the index file and upgrade files to the root directory of the USB flash drive.
4. Connect the USB flash drive to a USB interface of each device to complete automatic software upgrade.

Procedure

Step 1 Enable USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] undo set device usb-deployment disable
```

Step 2 Make an index file.

Create an index file and name it **usbload_config.txt**. Add the following content in the index file.

```
<time-sn=201306280209;/>
<mac=0018-0303-1234; vrpfile=S5700LI-new.CC;/>
<esn=020TEA10A9000016; vrpfile=S5700LI-new.CC; cfgfile=vrpcfg.cfg;
patchfile=patch.pat;/>
```

Step 3 Save the **usbload_config.txt** file and upgrade files to the root directory of the USB flash drive.

Step 4 Connect the USB flash drive to the first S5700-X-LI to start the deployment process. Observe the SYS indicator on the switch to monitor the deployment state.

After the switch restarts, the system checks the deployment state. If the SYS indicator blinks yellow slowly (once every 2s), the USB-based deployment has succeeded. If the SYS indicator blinks red, the USB-based deployment has failed. View the **usbload_error.txt** file in the root directory of the USB flash drive to analyze why the deployment fails.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

If the USB-based deployment succeeds, remove the USB flash drive and connect it to the other device.

Step 5 Connect the USB flash drive to the second S5700-X-LI to start the deployment process. Observe the SYS indicator on the switch to monitor the deployment state.

After the switch restarts, the system checks the deployment state. If the SYS indicator blinks yellow slowly (once every 2s), the USB-based deployment has succeeded. If the SYS indicator blinks red, the USB-based deployment has failed. View the **usbload_error.txt** file in the root directory of the USB flash drive to analyze why the deployment fails.

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

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

5 Logging In to a Device for the First Time

About This Chapter

To perform basic configuration on the CLI of a new device for the first time, you must log in to the device through a console port, mini USB port, or web system.

NOTE

Only the S5700LI, S5700S-LI, S5720HI, and S5720EI (excluding S5720-50X-EI-AC, S5720-50X-EI-DC, S5720-50X-EI-46S-DC and S5720-50X-EI-46S-AC) support login through the mini USB port.

5.1 First Login Overview

5.2 Logging In to a Device

5.3 Basic Configuration on the Device at First Login

5.4 Logging In to a Device for the First Time Configuration Example

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

5.1 First Login Overview

This section describes first login modes supported by the device and the corresponding basic configuration.

Before configuring a new device, you must log in to the device locally. The device supports first login through the console port, mini USB port, or web system.

After login, configure the system time, device name, management IP address, and user level and authentication mode for Telnet users to facilitate subsequent configuration.

NOTE

- Before logging in to the device using the mini USB port, install the mini USB port driver on the user terminal.
- 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.
- Before you log in to the device for the first time through the web system, the device must be in factory settings.

5.2 Logging In to a Device

5.2.1 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:

- Powering on the device properly
- Preparing the console cable (delivered with the device)
- Installing the terminal emulation software on the PC

  You can use the self-contained terminal emulation software of the operating system (such as HyperTerminal in Windows 2000) on your PC. If the operating system does not provide terminal emulation software, use third-party terminal emulation software. For details on how to use specific terminal emulation software, see the related software user guide or online help. This section uses the third-party software SecureCRT as an example.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Default Configuration

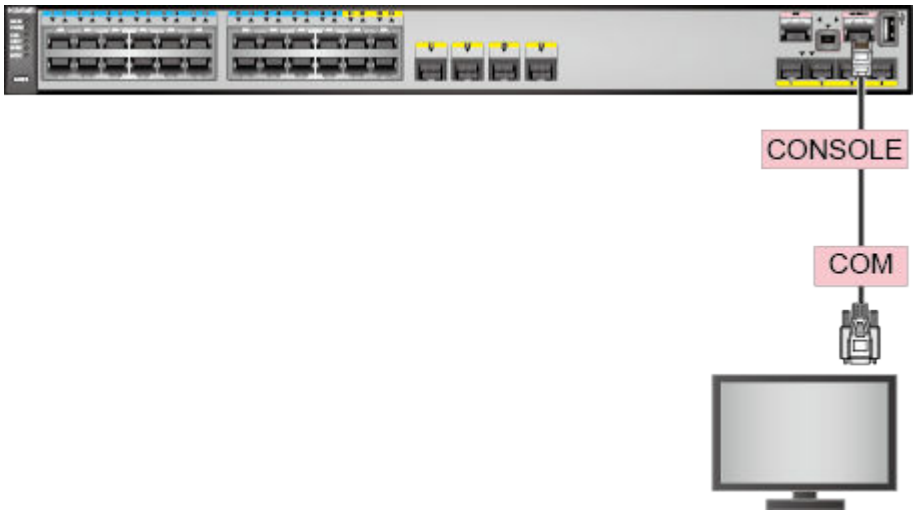
Table 5-1 Default configuration of the console port

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 5-1**.

Figure 5-1 Connecting to the device through the console port



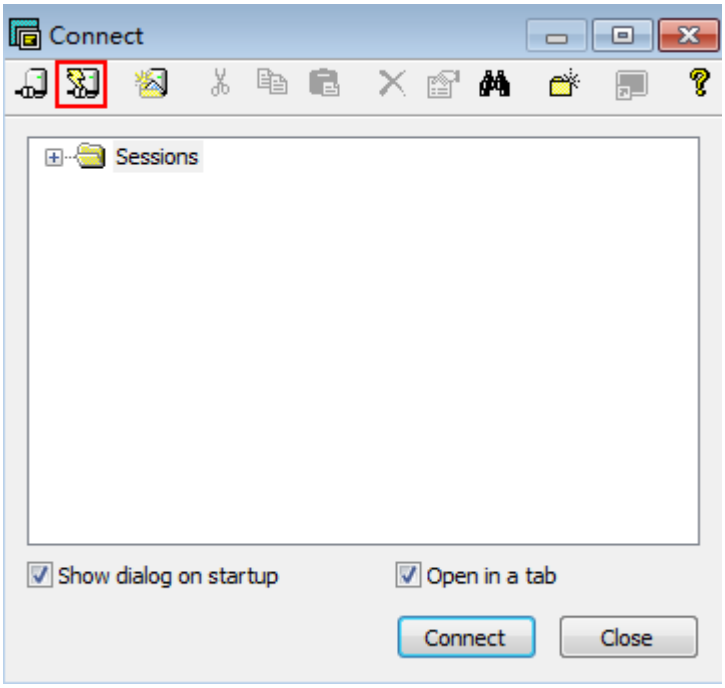
Step 2 Start the terminal emulation software on the PC. Create a connection, select the port for connection, and set communication parameters. (This section uses the third-party software SecureCRT as an example.)

1. Click to establish a connection, as shown in **Figure 5-2**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Figure 5-2 Establishing a connection



2. Set the port for connection and communication parameters, as shown in **Figure 5-3**.

   Select the port for connection. For example, you can view port information in **Device Manager** in the Windows operating system, and select the port for connection.

   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

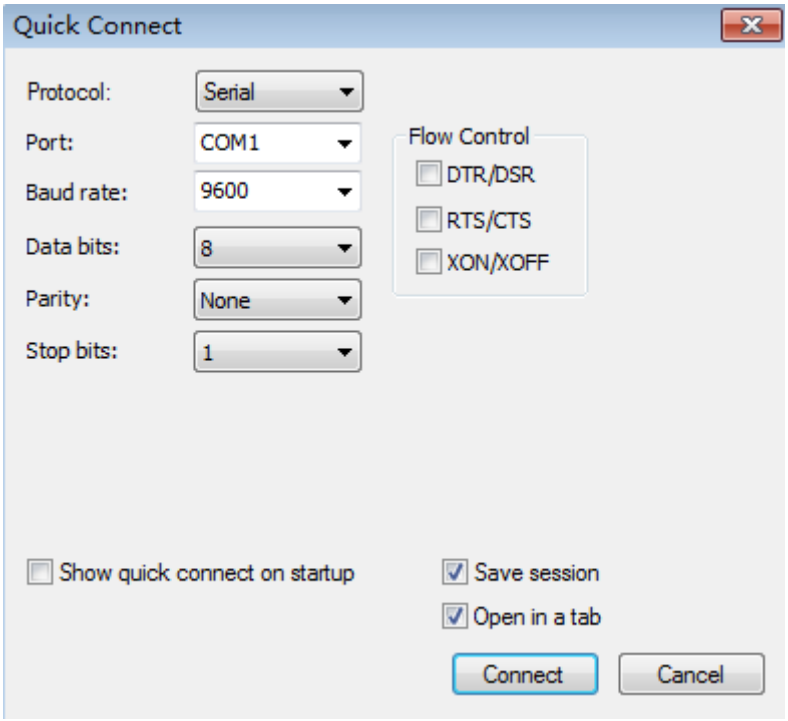
   By default, no flow control mode is configured on the device. Because RTS/CTS is selected in the software by default, you need to deselect RTS/CTS; otherwise, you cannot enter commands.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 5-3 Setting the port for connection and communication parameters



Step 3 Click **Connect**. Infomration similar to the following is displayed, prompting you to set a password. Enter the password and confirm the password, as no default password is available. (The following information is only for reference.)

```
An initial password is required for the first login via the console.
Continue to set it? [Y/N]: y
Set a password and keep it safe. Otherwise you will not be able to login via the
console.

Please configure the login password (8-16)
Enter Password:
Confirm Password:
<HUAWEI>
```

- The value is a string of 8 to 16 case-sensitive characters,containing at least two types of the following: upper-case and lower-case letters, digits, and special characters excluding spaces and question marks (?).
- The password entered in interactive mode is not displayed on the screen.
- When you log in to the device again in password authentication mode, enter the password set during the initial login if you have not modified the authentication mode and password.

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

----End

5.2.2 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Context

NOTE

Only the S5700LI, S5700S-LI, S5720HI, and S5720EI (excluding S5720-50X-EI-AC, S5720-50X-EI-DC, S5720-50X-EI-46S-DC and S5720-50X-EI-46S-AC) support login through the mini USB port.

Pre-configuration Tasks

Before logging in to a device through the mini USB port, complete the following tasks:

- Powering on the device
- Preparing a mini USB cable (You can use type-B mini USB cable, which is not delivered with the device.)
- Obtaining the mini USB driver that is compatible with the PC's operating system

  NOTE

  To obtain the mini USB driver, visit **http://support.huawei.com/enterprise** and download **Switch-MiniUSB-driver.00X.zip** for the required version of the device. The mini USB driver supports only Windows Vista and Windows 7 operating systems.
- Installing the terminal emulation software on the PC

  You can use the self-contained terminal emulation software of the operating system (such as HyperTerminal in Windows 2000) on your PC. If the operating system does not provide terminal emulation software, use third-party terminal emulation software. For details on how to use specific terminal emulation software, see the related software user guide or online help. This section uses the third-party software SecureCRT as an example.

Default Configuration

Table 5-2 Default configuration of 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 Install the mini USB driver on the PC.

For details on how to install a mini USB driver, see *Installation and Uninstallation Guide* in the driver file package.

The driver file **Switch-MiniUSB-driver.00X.zip** contains two drivers: **3410-VersX.X.X.X.zip** and **1410-VersX.X.X.X.zip**, applicable to different devices. (*X* represents

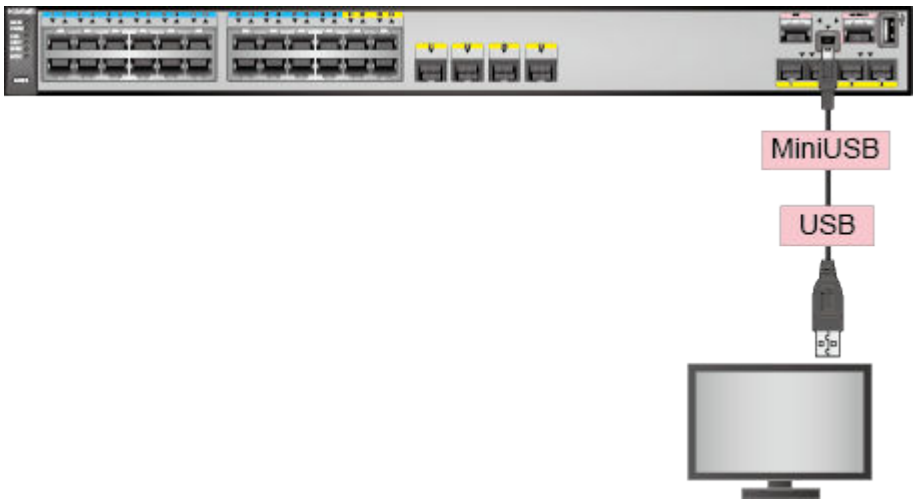
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

the version number, and a larger value indicates a later version.) Select a proper driver based on the device model before installation.

Step 2 Use a mini USB cable to connect the USB port on the PC to the mini USB port on the device, as shown in **Figure 5-4**.

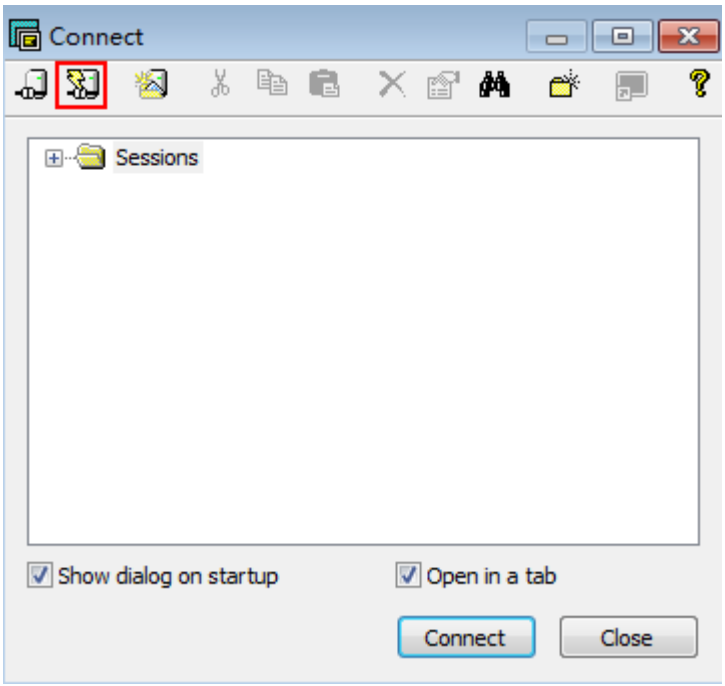
Figure 5-4 Connecting to the device through the mini USB port



Step 3 Start the terminal emulation software on the PC. Create a connection, select the port for connection, and set communication parameters. (This section uses the third-party software SecureCRT as an example.)

1. Click to establish a connection, as shown in **Figure 5-5**.

Figure 5-5 Establishing a connection



2. Set the port for connection and communication parameters, as shown in **Figure 5-6**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

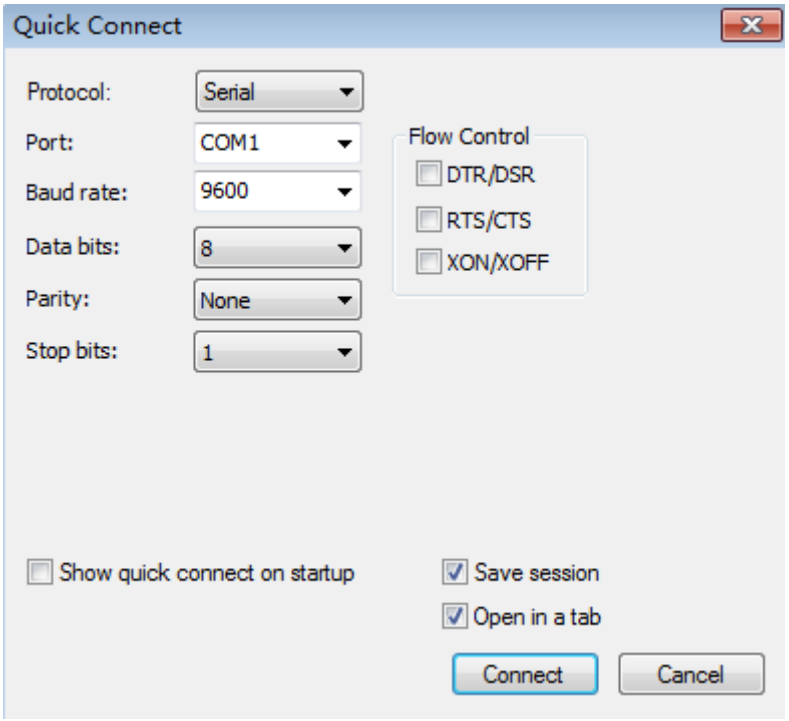
Select the port for connection. For example, you can view port information in **Device Manager** in the Windows operating system, and select the port for connection.

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.

Figure 5-6 Setting the port for connection and communication parameters



Step 4 Click **Connect**. Infomration similar to the following is displayed, prompting you to set a password. Enter the password and confirm the password, as no default password is available. (The following information is only for reference.)

```
An initial password is required for the first login via the console.
Continue to set it? [Y/N]: y
Set a password and keep it safe. Otherwise you will not be able to login via the
console.

Please configure the login password (8-16)
Enter Password:
Confirm Password:
<HUAWEI>
```

- The value is a string of 8 to 16 case-sensitive characters,containing at least two types of the following: upper-case and lower-case letters, digits, and special characters excluding spaces and question marks (?).
- The password entered in interactive mode is not displayed on the screen.
- When you log in to the device again in password authentication mode, enter the password set during the initial login if you have not modified the authentication mode and password.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

----End

5.2.3 Logging In to the Device Through the Web System for the First Time (S1720GFR)

When logging in to the S1720GFR with the factory settings for the first time, users can log in only through the Web system on the PC.

Context

To facilitate device maintenance and use, S1720GFR switches allow for the first login using the Web system.

Pre-configuration Tasks

Before logging in to a device through the Web system, complete the following tasks:

- Power on the device.
- Ensure that the device has only the factory settings.

Default Configuration

Table 5-3 Default configuration of the device

Parameter	Default Setting
User name	admin
Password	admin@huawei.com
User level	15
Login IP address	192.168.1.253 **NOTE** With the factory settings on an S1720GFR, the default IP address of VLANIF 1 is 192.168.1.253. To prevent IP address conflict on the local network, users are advised to change the IP address of VLANIF 1 on the S1720GFR before constructing the network.

Procedure

Step 1 Connect the PC to the device.

Connect the PC to any Ethernet interface on the device.

Step 2 Configure an IP address for the PC.

To ensure that the PC and device have reachable routes to each other, configure an IP address on the same network segment with the device IP address for the PC.

Copyright © Huawei Technologies Co., Ltd.

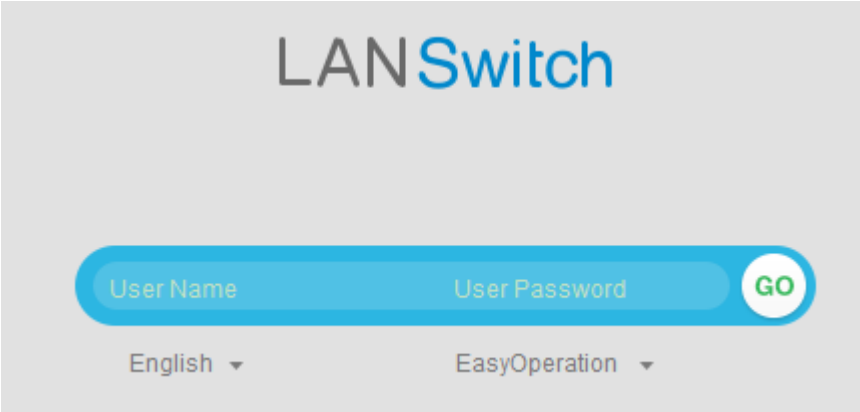
Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 3 Log in to the device through Web system.

Open the browser on the PC and access https://192.168.1.253. On the displayed Web system login page shown in **Figure 5-7**, enter the default user name **admin** and default password **admin@huawei.com**.

Figure 5-7 First login page in the Web system



NOTE

The login to the device through the Web system requires that the browser on the PC must be Internet Explorer 10.0 – 11.0, Firefox35.0 – 43.0, and Google Chrome 34.0 – 48.0. If the browser version is early, the display may be incorrect.

Step 4 Access the password change page of the web system.

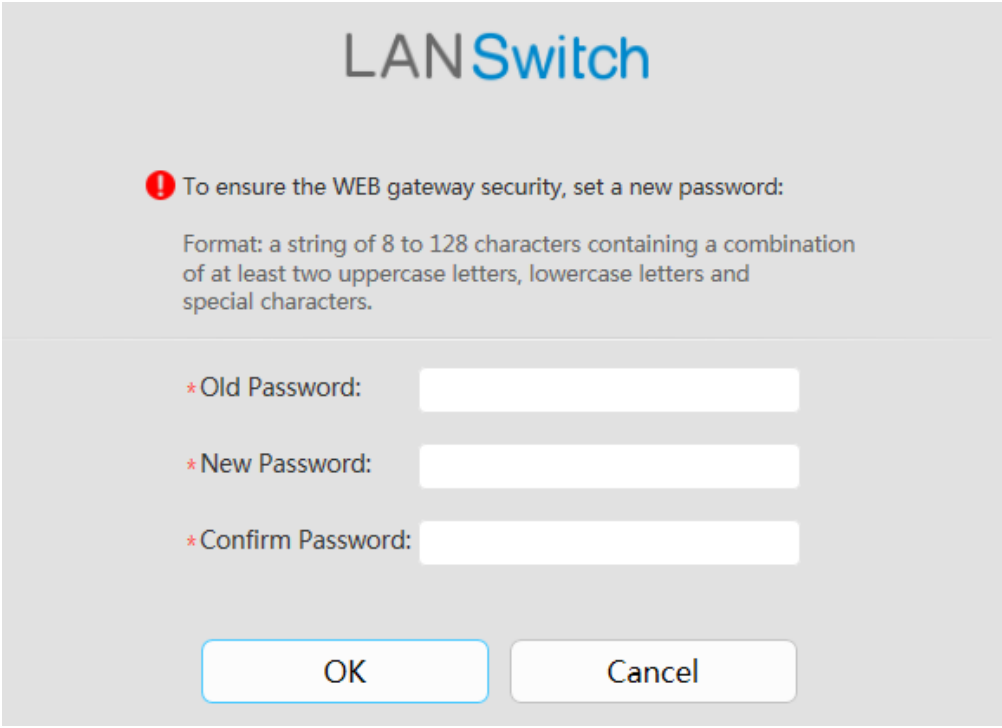
On the web system login page, click **GO** or press **Enter** to access the password change page, as shown in **Figure 5-8**. Change the password and re-log in to the web system as prompted. You can manage and maintain the device after logging in to the web system.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 5-8 Password change page of the web system



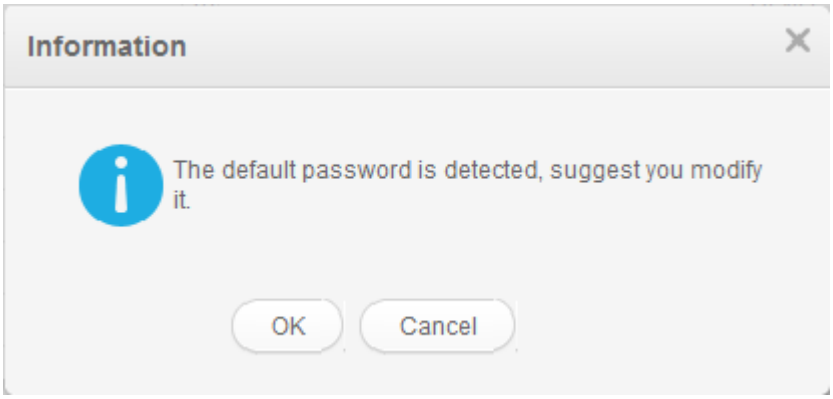
NOTE

- The password change page is displayed during the login process only the first time you log in to the web system.
- The password change page is also displayed if your password will expire or has expired. To access the web system main page, you must change the password.
- To improve security, a password must contain at least two types of the following: lowercase letters, uppercase letters, digits, and special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').

Step 5 (Optional) Changing the Web login password.

If the default password is used to log in to the device, a message is displayed prompting users to change the password, as shown in **Figure 5-9**. Click **Confirm**. Change the login password on the **User Management** page. To ensure security, users are advised to change the Web login password upon the first login to the device.

Figure 5-9 Page prompting users to change the login password



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

A secure password should contain at least two types of the following: lowercase letters, uppercase letters, numerals, special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').

After accessing the user management page, you can change the default user level. Only level 3 users and higher are administrators with management rights. Level 2 users and below are monitoring users. Administrator users have all operation rights of a web page, and monitoring users can only perform ping and tracert operations.

----End

5.2.4 Logging In to the Device Through the Web System for the First Time (Switches Excluding the S1720GFR)

When logging in to the device with the factory settings for the first time, users can log in only through the Web system on the PC and then configure the login mode (Web system, Telnet, or STelnet).

Context

When a PC has no available serial interface or does not carry any console cable, users can log in to the device with the factory settings using the Web system for the first time. After the login, users can conveniently configure the login mode (Web system, Telnet, or STelnet). After the login mode is configured, users can log in to the device using the Web system, Telnet, or STelnet for device maintenance.

NOTE

Devices without the **MODE** button do not support first login through the Web system.

First login through the Web system, SVF, USB-based deployment, and EasyDeploy cannot be used together.

Pre-configuration Tasks

Before logging in to a device through the Web system, complete the following tasks:

- Powering on the device
- Ensuring that the device has only the factory settings

Default Configuration

Table 5-4 Default configuration of the device

Parameter	Default Setting
User name	admin
Password	admin@huawei.com
User level	15
Login IP address	192.168.1.253

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Connect the PC to the device.

For a device that provides only optical interfaces, connect the PC to the management interface on the device. For a device that supports first login through the Web system, connect the PC to any Ethernet interface (except the management interface) on the device.

NOTE

Users can log in to a device for the first time using the Web system only when the device is in factory default state. In this case, do not log in to the device through the console interface, because any operation on the console interface leads to the failure of the first login using the Web system.

Step 2 Enter the initial configuration state.

Press and hold down the **MODE** button for 6 seconds or longer. When all indicators are steady green, the device enters the initial configuration state.

The system sets the switch IP address to 192.168.1.253/24 and the user level to 15 by default.

NOTE

If the device has been configured when users press and hold down the **MODE** button for 6 seconds or longer, all indicators blink green fast. In this case, the device is restored to the normal state after 10 seconds, without impact on existing configuration.

If the device in the factory settings has just started or has been configured through the console interface when users press and hold down the **MODE** button for 6 seconds, the device may fail to enter the initial configuration state. When all indicators blink fast for 10s, the device restores to the factory default state.

The device automatically exits the initial configuration state and restores the factory settings if users have not saved the settings after 10 minutes.

Step 3 Configure an IP address for the PC.

To ensure that the PC and device have reachable routes to each other, configure an IP address on the same network segment with the device IP address for the PC.

Step 4 Log in to the device through Web system.

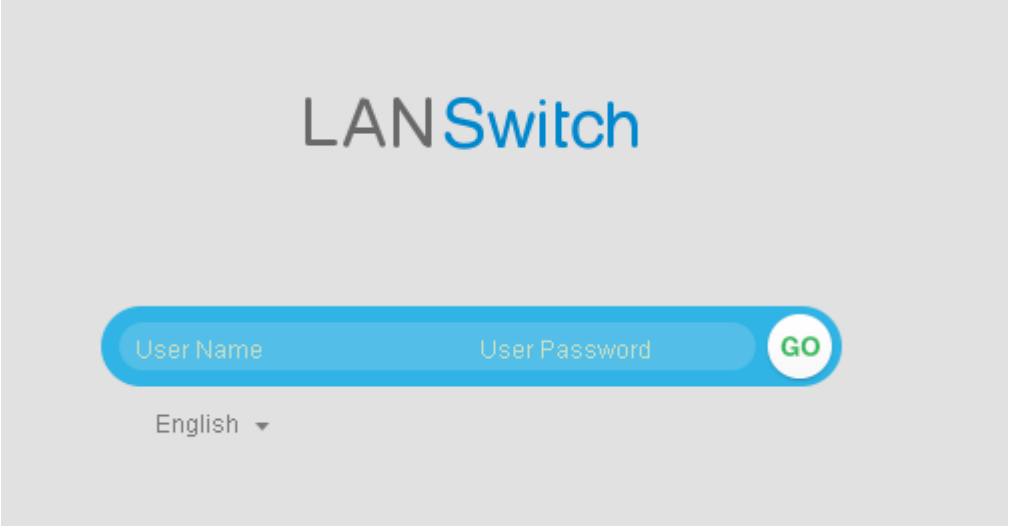
Open the browser on the PC and access https://192.168.1.253. On the displayed Web system login page shown in **Figure 5-10**, enter the default user name **admin** and default password **admin@huawei.com**, and select the system language. Click **GO** or press **Enter**. The Web system configuration page is displayed.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 5-10 First login page in the Web system



NOTE

The login to the device through the Web system requires that the browser on the PC must be Internet Explorer 10.0 – 11.0, Firefox35.0 – 43.0, and Google Chrome 34.0 – 48.0. If the browser version is early, the display may be incorrect.

Step 5 Configure the device.

As shown in **Figure 5-11**, the Web system configuration page allows users to perform the basic and optional configurations. **Table 5-5** describes parameters for the basic configuration. After the basic configuration is complete, users can log in to the device through the Web system. **Table 5-6** describes parameters for the optional configuration. After the optional configuration is complete, users can log in to the device through Telnet or STelnet.

A login user can create users for logging in to the device through Telnet or STelnet. The parameter **Create User** is valid only when **Telnet Server** or **Stelnet Server** is **On**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 5-11 Web system configuration page

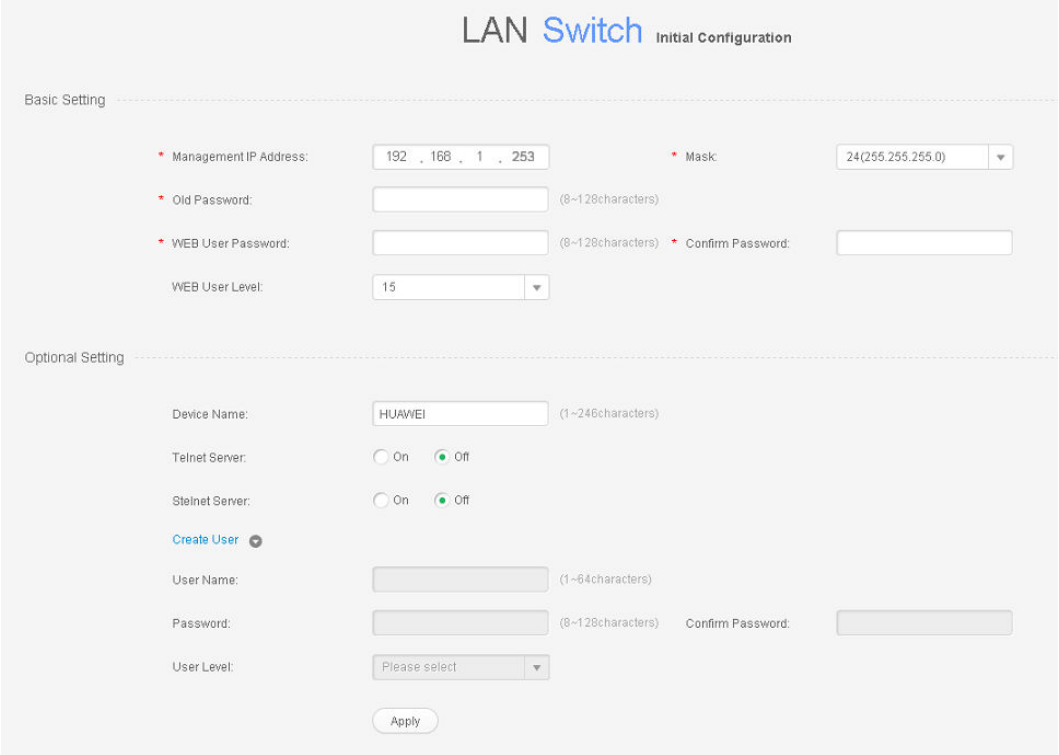


Table 5-5 Basic configuration

Item	Description
Management IP Address	Indicates the management IP address of the device. The value is in dotted decimal notation.
Mask	Indicates the mask of the IP address. Select a subnet mask from the drop-down list box.
Old Password	Indicates the default Web login password. This parameter is mandatory.
WEB User Password	Indicates the new Web login password. This parameter is mandatory. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, numerals, special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').
Confirm Password	Confirms the new Web login password. This parameter is mandatory. The format is the same as that of **WEB User Password**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
WEB User Level	Indicates the Web user level. Select a user level from the drop-down list box. This parameter is optional. Only level 3 users and higher are administrators with management rights. Level 2 users and below are monitoring users. Administrator users have all operation rights of a web page, and monitoring users can only perform ping and tracert operations.

Table 5-6 Optional configuration

Item	Description
Device Name	Specifies the device name. The device name cannot contain question marks (?) and cannot start with spaces.
Telnet Server	Configures the Telnet function. ● On: enables Telnet. ● Off: disables Telnet.
Stelnet Server	Configures the STelnet function. ● On: enables STelnet. ● Off: disables STelnet.
User Name	Specifies the Telnet or STelnet login user name. The user name cannot contain / : * ? " < > | ' or %, and cannot start with @.
Password	Specifies the password. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, numerals, special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').
Confirm Password	Confirms the password. The format is the same as that of **Password**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
User Level	Indicates the Telnet or STelnet user level. Select a user level from the drop-down list box. Only level 3 users and higher are administrators with management rights. Level 2 users and below are monitoring users. Administrator users have all operation rights of a web page, and monitoring users can only perform ping and tracert operations.

Step 6 Save configuration.

Click **Apply**. The configuration is saved. When logging out of the Web system for the first time, the following situations may occur based on the configured management IP address:

- When the management IP address is on the same network segment as 192.168.1.253/24, the Web system login page is displayed.
- When the management IP address is not on the same network segment as 192.168.1.253/24, users cannot log in to device through the Web system. In this case, configure an IP address on the same network segment as the management IP address for the PC so that the PC and device have reachable routes to each other.

Users can log in to the device through the Web system, Telnet, or STelnet for device maintenance.

----End

5.3 Basic Configuration on the Device at First Login

Context

This section describes how to configure the time and date, 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:
   ```
   system-view
   ```
   The system view is displayed.
2. Run:
   ```
   clock timezone time-zone-name { add | minus } offset
   ```
   The time zone is set.

   By default, the system uses the Coordinated Universal Time (UTC) time zone.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- **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*.

3. Run:

```
quit
```

Quit the system view.

4. 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.

5. Run:

```
system-view
```

The system view is displayed.

6. Run:

```
clock daylight-saving-time time-zone-name one-year start-time start-date end-time end-date offset
```

Or

```
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 ] ]
```

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 Set the device name and management IP address.

1. Run:

```
sysname host-name
```

The device name is set.

By default, the device name is HUAWEI.

When the network management tool needs to obtain the network element (NE) name of a device, you can run the **sys-netid** command to set an NE name for the device.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

2. 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 a Layer 3 interface such as a VLANIF interface on the device.

3. Run:

```
ip address ip-address { mask | mask-length }
```

The management IP address is assigned.

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.

4. Run:

```
quit
```

Return to the system view.

Step 3 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 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. An authentication mode must be configured for the VTY user interface; otherwise, users cannot log in to the device.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

The system provides three authentication modes: AAA authentication, password authentication, and non-authentication. AAA authentication requires both the user name and password, and is therefore more secure than password authentication. Non-authentication mode is not recommended because it cannot ensure system security. This section describes how to configure AAA authentication. For details on configuring 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 Telnet—based login 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 simple password may cause a potential security risk. To enhance the security strength, a plain-text password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters excluding spaces and question marks (?). In addition, the password cannot be the same as the user name or the mirror user name.

8. Run:

```
local-user user-name service-type telnet
```

The login mode is set to Telnet.

Step 4 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 **9.2.1 Saving the Configuration File**.

----End

Checking 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Run the **display local-user** command to check the local user list.

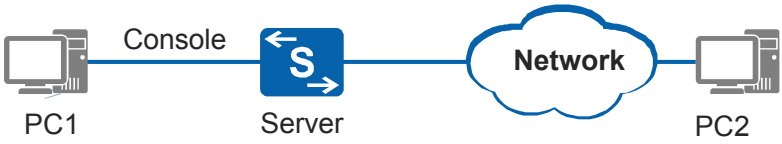
5.4 Logging In to a Device for the First Time Configuration Example

5.4.1 Example for Performing Basic Configuration on the Device at First Login Through the Console Port

Networking Requirements

After logging in to the device for the first time through the console port, perform basic configuration, and set the user level to 15 and authentication mode to AAA for users 0-4 who perform remote login through Telnet. Ensure that there is a reachable route between PC2 and the device.

Figure 5-12 Networking diagram for performing basic configuration on the device through the console port



Configuration Roadmap

1. Log in to the device through the console port.
2. Perform basic configuration on 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 Perform basic configuration on the device.

Set the system date, time, and time zone.

```
<HUAWEI> clock timezone BJ add 08:00:00
<HUAWEI> clock datetime 20:10:00 2012-07-26
```

NOTE

Before setting the current date and time, run the **clock timezone** command to set the time zone. If the time zone is not set first, the **clock datetime** command configures the UTC time.

Set the device name and management IP address.

```
<HUAWEI> system-view
[HUAWEI] sysname Server
[Server] vlan 10
[Server-vlan10] quit
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[Server] interface vlanif 10
[Server-Vlanif10] ip address 10.137.217.177 24
[Server-Vlanif10] quit
[Server] interface gigabitethernet 0/0/10
[Server-GigabitEthernet0/0/10] port link-type access
[Server-GigabitEthernet0/0/10] port default vlan 10
[Server-GigabitEthernet0/0/10] quit
```

Configure a default route for the device, assuming that the device gateway address is 10.137.217.1.

```
[Server] ip route-static 0.0.0.0 0 10.137.217.1
```

Set the user level and authentication mode for Telnet users.

```
[Server] telnet server enable
[Server] user-interface vty 0 4
[Server-ui-vty0-4] protocol inbound telnet
[Server-ui-vty0-4] authentication-mode aaa
[Server-ui-vty0-4] user privilege level 15
[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.

After the configuration is complete, you can log in to the device through Telnet from PC2.

Access the Windows CLI and log in to the device through Telnet by running the following command.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

Press **Enter**. On the displayed login interface, enter the user name and password. If the authentication succeeds, the CLI for the user view is displayed. (The following information is only for reference.)

```
Login authentication


Username:admin1234
Password:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2012-07-26 20:10:05+08:00.
<Server>
```

----End

Configuration Files

Switch configuration file

```
#
sysname Server
#
telnet server enable
#
clock timezone BJ add 08:00:00
#
aaa
 local-user admin1234 password irreversible-cipher %^%#aVW8S=aP=B<OWi1Bu'^R[=_!
~oR*85r_nNY+kA(I}[TiLiVGR-i/'DFGAI-O%^%#
 local-user admin1234 privilege level 15
 local-user admin1234 service-type telnet
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
#
interface Vlanif10
 ip address 10.137.217.177 255.255.255.0
#
interface GigabitEthernet0/0/10
 port link-type access
 port default vlan 10
#
ip route-static 0.0.0.0 0.0.0.0 10.137.217.1
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
 protocol inbound telnet
#
return
```

Related Content

Videos

Log In to a Switch Through the Console Port.

Log In to a Switch Through the MiniUSB Port.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

6 CLI Login Configuration

About This Chapter

This chapter describes how to log in to a device through its console port or mini USB port, or using Telnet or STelnet to manage and maintain the device.

6.1 CLI Login Method Overview
6.2 User Interface Overview
6.3 Configuring Login Through a Console Port
6.4 Configuring Login Through the Mini USB Port
6.5 Configuring Telnet Login
6.6 Configuring STelnet Login
6.7 Common Operations After Login
6.8 CLI Login Configuration Examples
6.9 CLI Login Common Misconfigurations
6.10 FAQ

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

6.1 CLI Login Method Overview

You can manage a device through the CLI or web system.

- CLI

  After logging in to a device through its console port or mini USB port, or using Telnet or STelnet, you can run commands to configure and manage the device. In this mode, you must configure a user interface for each login method.

- Web system

  When a device functions as a server, you can use the web system to log in to the device. The internal web server of the device provides a GUI, on which you can easily manage and maintain the device after login. The web system provides only basic maintenance and management functions. You still need to use the CLI to implement fine-grained management.

  For details about web system configuration, see **Web System Login Configuration**.

You can log in to a device using one of the CLI methods described in **Table 6-1** to configure and manage the device.

Table 6-1 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Login Method	Advantages	Disadvantages	Applicable Scenario	Description
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.
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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

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. **NOTE** SSH in this document refers to SSH 2.0 unless otherwise stated.	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.

6.2 User Interface Overview

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 are restricted by these parameters. Through the parameter configuration, uniform management of various user sessions can be implemented.

The device supports two 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.
- 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. Currently, a device supports concurrent access of a maximum of 15 VTY users.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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.

NOTE

If the device does not respond to commands on a VTY user interface for two consecutive times, the VTY user interface is locked. In this case, users can log in through another VTY user interface. The locked VTY user interface will become unlocked after the device is restarted.

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.
  - 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.

  Each switch supports only one console user interface and 20 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 6-2 lists the default absolute numbers of the console and VTY user interfaces.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 6-2 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
VTY user interface	Manages and controls users who log in using Telnet or STelnet.	34 to 48, 50 to 54. Number 49 is reserved. Numbers 50 to 54 are reserved for the network management system.	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 34 to 48 map relative numbers VTY 0 to VTY 14, respectively. ● Absolute numbers 50 to 54 map relative numbers VTY 16 to VTY 20, respectively. Number 15 is reserved. Numbers 16 to 20 are reserved for the network management system. VTY 16 to VTY 20 can be used only when VTY 0 to VTY 14 are occupied and AAA authentication is configured.

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.

Three authentication modes are available: Authentication, Authorization, and Accounting (AAA) authentication, password authentication, and none 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.
- None authentication: Users can directly log in without entering any information.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTICE

To ensure high security, do not use the None authentication.

Regardless of the authentication mode, the system starts the delayed login mechanism in the case of a device login failure. If the first login fails, the user can log in again 5 seconds later. The delay time is increased by 5 seconds every time a login failure occurs. The second login is delayed to 10 seconds, and the third login is delayed to 15 seconds.

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 or none 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.

6.3 Configuring Login Through a Console Port

6.3.1 (Optional) Configuring Attributes 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 | software }
```

The flow control mode is set.

The default flow control mode is set to none, indicating that the flow control function is not performed.

3. Run:

```
databits { 5 | 6 | 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 | mark | none | odd | space }
```

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 10 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:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
screen-length screen-length [ temporary ]
```

The number of rows displayed on a terminal screen is set.

temporary specifies the number of rows temporarily displayed on a terminal screen. If you specify this parameter, the configured value does not take effect on the next login.

The default number of rows displayed on a terminal screen is 24.

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.

NOTE

This command is valid only for information displayed by the **display interface description** command.

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

6.3.2 Configuring an Authentication Mode for the Console User Interface

Context

The system provides three authentication modes for the console user interface: AAA authentication, password authentication, and none 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.
- None authentication: Users can directly log in without entering any information.

NOTICE

To ensure high security, do not use the None authentication.

Regardless of the authentication mode, the system starts the delayed login mechanism in the case of a device login failure. If the first login fails, the user can log in again 5 seconds later. The delay time is increased by 5 seconds every time a login failure occurs. The second login is delayed to 10 seconds, and the third login is delayed to 15 seconds.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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. Run:
  ```
  quit
  ```
  Exit the console user interface view.
  e. Run:
  ```
  aaa
  ```
  The AAA view is displayed.
  f. Run:
  ```
  local-user user-name password irreversible-cipher password
  ```
  A local user account is created and a password is configured.
  g. Run:
  ```
  local-user user-name service-type terminal
  ```
  The access type of the local user is set to **Console**.
  h. Run:
  ```
  quit
  ```
  Exit the AAA view.

  NOTE

  If multiple switches set up a stack and an active/standby switchover is being performed, you may fail to log in to a switch. You can log in to the switch after the active/standby switchover is complete.
- 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:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
set authentication password [ cipher password ]
```

An authentication password is set.

If you do not specify **cipher** *password*, you can enter a plain text password in interactive mode. The password entered in interactive mode is not displayed on the screen. If you specify **cipher** *password*, you can enter a plain text password or cipher text password. Both types of passwords are saved to the configuration file in cipher text. Plain text passwords have potential security risks. It is recommended that you enter a password in interactive mode.

By default, the system checks the complexity of the entered password. The password takes effect only if it meets the complexity requirement. To disable the password complexity check function, run the **user-interface password complexity-check disable** command. However, keeping the password complexity check function enabled is recommended, which improves system security.

NOTE

By default, the minimum length of plain text passwords allowed by a device is 8 characters. You can set a longer password to increase password complexity and improve device security. Run the **set password min-length** *length* command to set the minimum length of plain text passwords allowed by the device.

- Configure none 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 none
  ```
  The authentication mode is set to none authentication.

----End

6.3.3 Configuring 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 6-3** describes mappings between user levels and command levels.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 6-3 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 *S1720&S2700&S5700&S6720 Series Ethernet Switches 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.

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 or none 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- 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

6.3.4 Logging In to a Device Through the Console Port

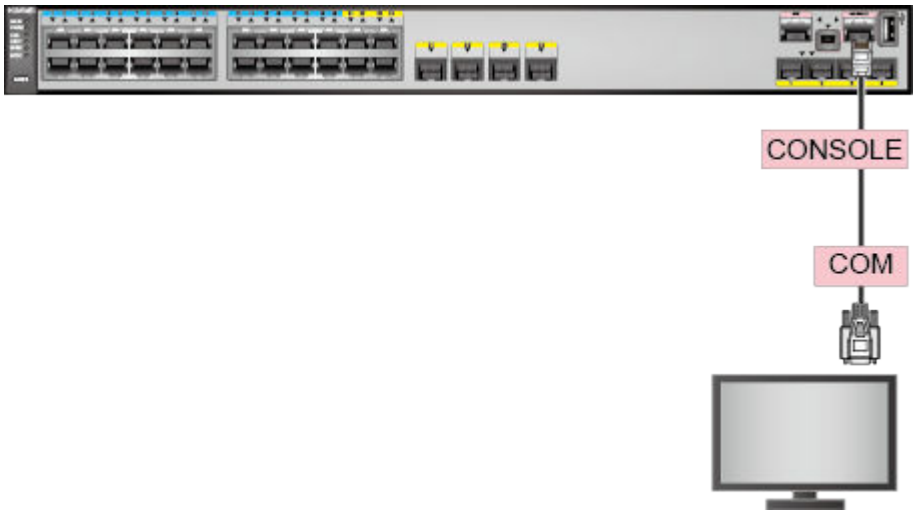
Context

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 switch.

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 6-1**.

Figure 6-1 Connecting to the device through the console port



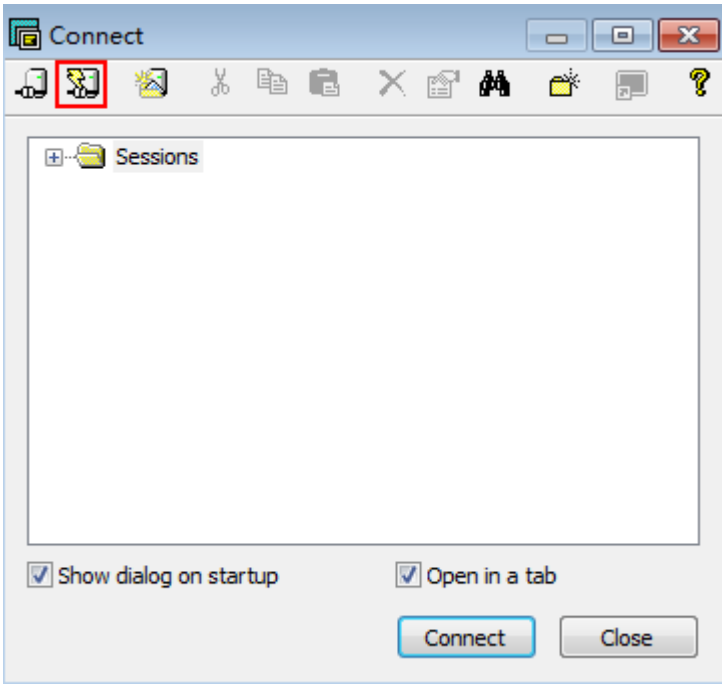
Step 2 Start the terminal emulation software on the PC. Create a connection, select the port for connection, and set communication parameters. (This section uses the third-party software SecureCRT as an example.)

1. Click to establish a connection, as shown in **Figure 6-2**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Figure 6-2 Establishing a connection



2. Set the port for connection and communication parameters, as shown in **Figure 6-3**.

   Select the port for connection. For example, you can view port information in **Device Manager** in the Windows operating system, and select the port for connection.

   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

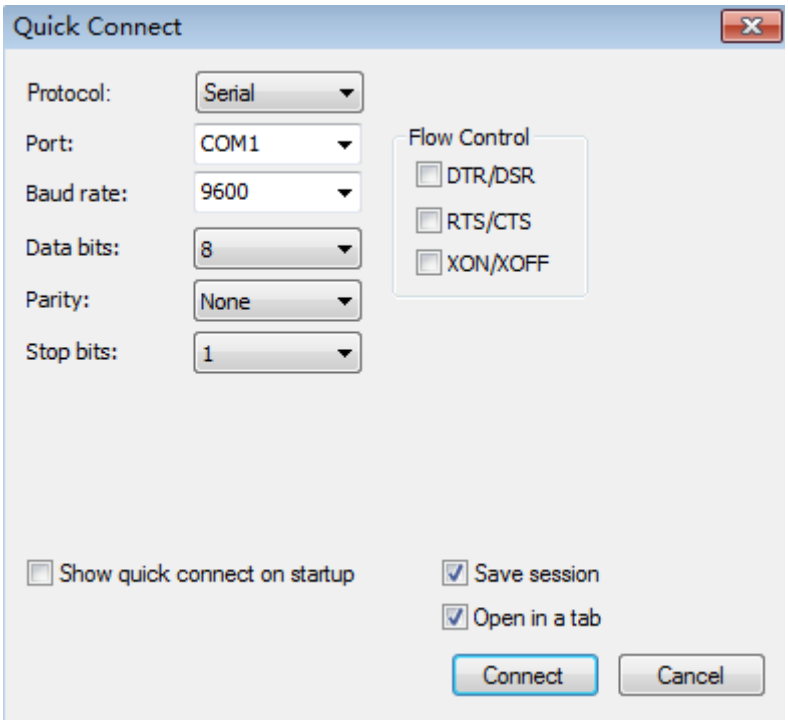
   By default, no flow control mode is configured on the device. Because RTS/CTS is selected in the software by default, you need to deselect RTS/CTS; otherwise, you cannot enter commands.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 6-3 Setting the port for connection and communication parameters



Step 3 Click **Connect**. The following information is displayed, prompting you to enter a password. The system does not provide a default password. You need to enter the configured 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

Checking 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.

6.4 Configuring Login Through the Mini USB Port

NOTE

Only the S5700LI, S5700S-LI, S5720HI, and S5720EI (excluding S5720-50X-EI-AC, S5720-50X-EI-DC, S5720-50X-EI-46S-DC and S5720-50X-EI-46S-AC) support login through the mini USB port.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

6.4.1 (Optional) Configuring Attributes 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 | software }
   ```

   The flow control mode is set.

   The default flow control mode is set to none, indicating that the flow control function is not performed.

3. Run:

   ```
   databits { 5 | 6 | 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 | mark | none | odd | space }
   ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 10 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 [ temporary ]
```

The number of rows displayed on a terminal screen is set.

temporary specifies the number of rows temporarily displayed on a terminal screen. If you specify this parameter, the configured value does not take effect on the next login.

The default number of rows displayed on a terminal screen is 24.

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.

NOTE

This command is valid only for information displayed by the **display interface description** command.

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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

6.4.2 Configuring an Authentication Mode for the Console User Interface

Context

The system provides three authentication modes for the console user interface: AAA authentication, password authentication, and none 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.
- None authentication: Users can directly log in without entering any information.

NOTICE

To ensure high security, do not use the None authentication.

Regardless of the authentication mode, the system starts the delayed login mechanism in the case of a device login failure. If the first login fails, the user can log in again 5 seconds later. The delay time is increased by 5 seconds every time a login failure occurs. The second login is delayed to 10 seconds, and the third login is delayed to 15 seconds.

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. Run:
  ```
  quit
  ```
  Exit the console user interface view.
  e. Run:
  ```
  aaa
  ```
  The AAA view is displayed.
  f. Run:
  ```
  local-user user-name password irreversible-cipher password
  ```
  A local user account is created and a password is configured.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

g. Run:

```
local-user user-name service-type terminal
```

The access type of the local user is set to **Console**.

h. Run:

```
quit
```

Exit the AAA view.

NOTE

If multiple switches set up a stack and an active/standby switchover is being performed, you may fail to log in to a switch. You can log in to the switch after the active/standby switchover is complete.

- 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 password ]
```

An authentication password is set.

If you do not specify **cipher** *password*, you can enter a plain text password in interactive mode. The password entered in interactive mode is not displayed on the screen. If you specify **cipher** *password*, you can enter a plain text password or cipher text password. Both types of passwords are saved to the configuration file in cipher text. Plain text passwords have potential security risks. It is recommended that you enter a password in interactive mode.

By default, the system checks the complexity of the entered password. The password takes effect only if it meets the complexity requirement. To disable the password complexity check function, run the **user-interface password complexity-check disable** command. However, keeping the password complexity check function enabled is recommended, which improves system security.

NOTE

By default, the minimum length of plain text passwords allowed by a device is 8 characters. You can set a longer password to increase password complexity and improve device security. Run the **set password min-length** *length* command to set the minimum length of plain text passwords allowed by the device.

- Configure none authentication.

a. Run:

```
system-view
```

The system view is displayed.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

b. Run:

```
user-interface console 0
```

The console user interface view is displayed.

c. Run:

```
authentication-mode none
```

The authentication mode is set to none authentication.

----End

6.4.3 Configuring 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 6-4** describes mappings between user levels and command levels.

Table 6-4 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 *S1720&S2700&S5700&S6720 Series Ethernet Switches 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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 or none 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

6.4.4 Logging In to a Device Through the Mini USB Port

Context

After completing console user interface configurations on a device, you can log in through the mini USB port. If the console user interface uses the default attribute settings and password authentication, perform the following steps to log in to the device.

Procedure

Step 1 Install the mini USB driver on the PC.

For details on how to install a mini USB driver, see *Installation and Uninstallation Guide* in the driver file package.

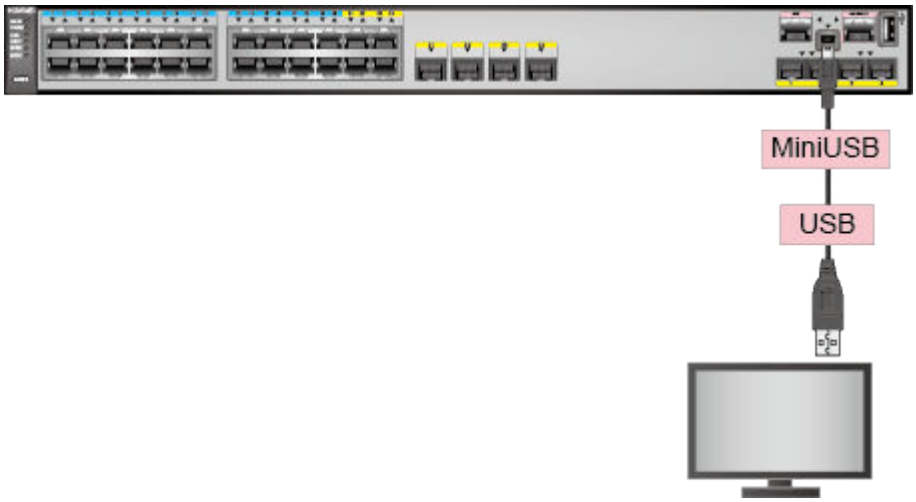
The driver file **Switch-MiniUSB-driver.00X.zip** contains two drivers: **3410-VersX.X.X.X.zip** and **1410-VersX.X.X.X.zip**, applicable to different devices. (*X* represents the version number, and a larger value indicates a later version.) Select a proper driver based on the device model before installation.

Step 2 Use a mini USB cable to connect the USB port on the PC to the mini USB port on the device, as shown in **Figure 6-4**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

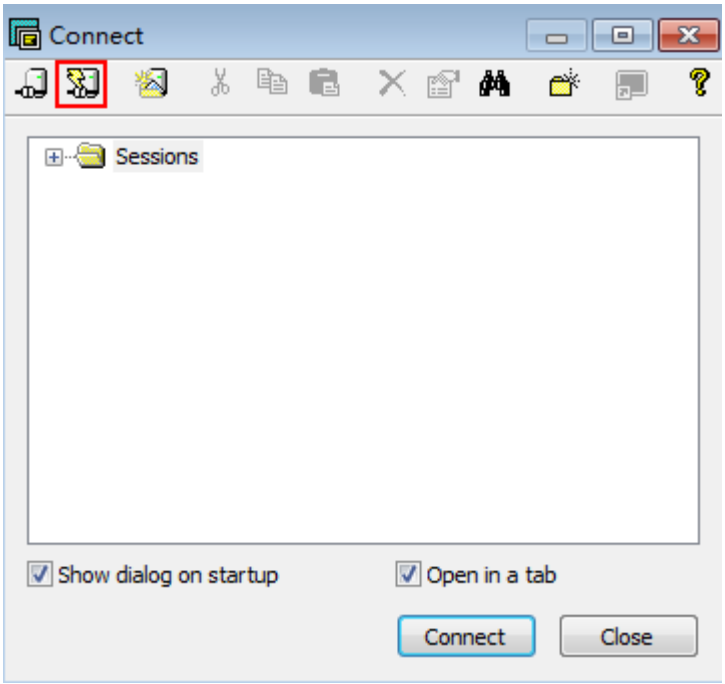
Figure 6-4 Connecting to the device through the mini USB port



Step 3 Start the terminal emulation software on the PC. Create a connection, select the port for connection, and set communication parameters. (This section uses the third-party software SecureCRT as an example.)

1. Click to establish a connection, as shown in **Figure 6-5**.

Figure 6-5 Establishing a connection



2. Set the port for connection and communication parameters, as shown in **Figure 6-6**.

   Select the port for connection. For example, you can view port information in **Device Manager** in the Windows operating system, and select the port for connection.

   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.

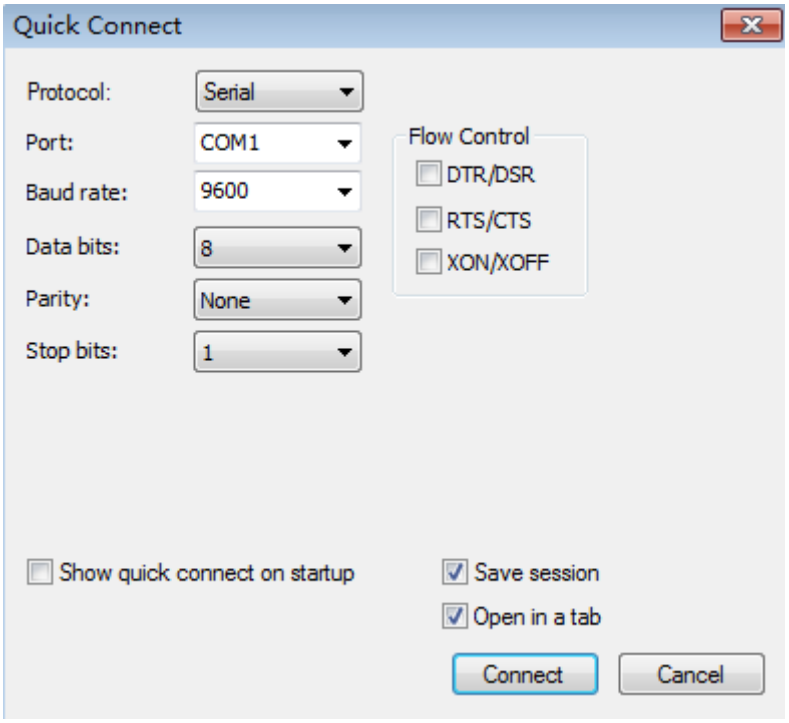
Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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.

Figure 6-6 Setting the port for connection and communication parameters



Step 4 Click **Connect**. The following information is displayed, prompting you to enter a password. The system does not provide a default password. You need to enter the configured 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

Checking 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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

6.5 Configuring Telnet Login

NOTICE

The Telnet protocol has security vulnerabilities. It is recommended that you log in to the device using STelnet V2.

6.5.1 (Optional) Configuring 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 forces users who do not pass the authentication and occupy the VTY channel for longer than 15 seconds to log out. New users can log in to the device through the VTY user interface.
- 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 10 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.

NOTE

This command is valid only for information displayed by the **display interface description** command.

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

6.5.2 Configuring an Authentication Mode for a VTY User Interface

Context

The system provides three authentication modes for a VTY user interface: AAA authentication, password authentication, and none 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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- 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.
- None authentication: Users can directly log in without entering any information.

NOTICE

To ensure high security, do not use the None authentication.

Regardless of the authentication mode, the system starts the delayed login mechanism in the case of a device login failure. If the first login fails, the user can log in again 5 seconds later. The delay time is increased by 5 seconds every time a login failure occurs. The second login is delayed to 10 seconds, and the third login is delayed to 15 seconds.

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 protocol.
  d. Run:
  ```
  authentication-mode aaa
  ```
  The authentication mode is set to AAA authentication.
  e. Run:
  ```
  quit
  ```
  Exit the VTY user interface view.
  f. Run:
  ```
  aaa
  ```
  The AAA view is displayed.
  g. Run:
  ```
  local-user user-name password { cipher | irreversible-cipher } password
  ```
  A local user account is created and a password is configured.
  h. Run:
  ```
  local-user user-name service-type telnet
  ```
  The access type of the local user is set to **Telnet**.
  i. Run:
  ```
  quit
  ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Exit the AAA view.

- Configure password 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 protocol.
  d. Run:
  ```
  authentication-mode password
  ```
  The authentication mode is set to password authentication.
  e. Run:
  ```
  set authentication password [ cipher password ]
  ```
  An authentication password is set.

  If you do not specify **cipher** *password*, you can enter a plain text password in interactive mode. The password entered in interactive mode is not displayed on the screen. If you specify **cipher** *password*, you can enter a plain text password or cipher text password. Both types of passwords are saved to the configuration file in cipher text. Plain text passwords have potential security risks. It is recommended that you enter a password in interactive mode.

  By default, the system checks the complexity of the entered password. The password takes effect only if it meets the complexity requirement. To disable the password complexity check function, run the **user-interface password complexity-check disable** command. However, keeping the password complexity check function enabled is recommended, which improves system security.

  NOTE

  By default, the minimum length of plain text passwords allowed by a device is 8 characters. You can set a longer password to increase password complexity and improve device security. Run the **set password min-length** *length* command to set the minimum length of plain text passwords allowed by the device.

- Configure none 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 }
  ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

The VTY user interface is configured to support the Telnet protocol.

By default, a VTY user interface supports the SSH protocol.

d. Run:

```
authentication-mode none
```

The authentication mode is set to none authentication.

----End

6.5.3 Configuring 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 6-5** describes mappings between user levels and command levels.

Table 6-5 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 *S1720&S2700&S5700&S6720 Series Ethernet Switches 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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 or none 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

6.5.4 Enabling the Telnet Server Function

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.

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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-source -i loopback interface-number
```

The source interface is specified for the Telnet server.

By default, the source interface of a Telnet server is not specified.

Configuring a source interface for a Telnet server prevents exposure of the management IP address of the device, which ensures device security.

NOTE

Before specifying a loopback interface as the source interface for a Telnet server, ensure that the loopback interface has been created and the route between the client and the loopback interface is reachable; otherwise, the configuration cannot be correctly executed.

Step 5 (Optional) Configure ACL-based Telnet access control.

- Control access to the local device.
  - Method 1:
    i. 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.
    ii. 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.
    iii. Run:
    ```
    quit
    ```
    Exit the ACL view.
    iv. Run:
    ```
    telnet [ ipv6 ] server acl acl-number
    ```
    The ACL is configured to control devices that can access the local device using Telnet.
  - Method 2:
    i. 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.
    ii. 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.
    iii. Run:
    ```
    quit
    ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Exit the ACL view.

iv. Run:

```
user-interface vty first-ui-number [ last-ui-number ]
```

The VTY user interface view is displayed.

v. Run:

```
acl [ ipv6 ] { acl-number | acl-name } inbound
```

The ACL-based Telnet access control is configured for the VTY user interface.

- 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 | acl-name } inbound
```

The ACL-based Telnet access control is configured for the VTY user interface.

----End

6.5.5 Logging In to a Device Through 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.)

```
Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
Login authentication


Username:admin1234
Password:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2013-12-16 16:46:42+08:00.
<HUAWEI>
```

----End

Checking the Configuration

- Run the **display users** [**all**] command to check the user interface connections.
- Run the **display tcp status** command to check all TCP connections.
- Run the **display telnet server status** command to check current Telnet server connections.

6.5.6 (Optional) Using Telnet to Log In to Another Device From the Local Device

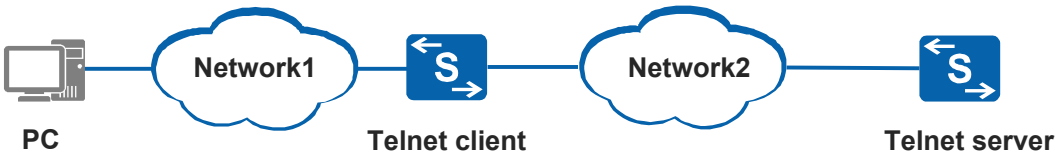
Context

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 and specify a VPN instance to implement remote Telnet login across private networks.

As shown in **Figure 6-7**, 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 6-7 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:

- Logging in to the device from a terminal
- Configuring a reachable route between the device and Telnet server
- Enabling the Telnet server function on the Telnet server

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Obtaining the Telnet user name, password, and port number configured on the Telnet server

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** [**vpn-instance** *vpn-instance-name*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *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*] [**vpn6-instance** *vpn6-instance-name*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*] command to log in to another device as a Telnet IPv6 client.

NOTE

Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support **vpn-instance** *vpn-instance-name* and **vpn6-instance** *vpn6-instance-name*.

----End

6.6 Configuring STelnet Login

NOTE

The STelnet V1 protocol has security vulnerabilities. It is recommended that you log in to the device using STelnet V2.

6.6.1 (Optional) Configuring 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 forces users who do not pass the authentication and occupy the VTY channel for longer than 15 seconds to log out. New users can log in to the device through the VTY user interface.
- 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 10 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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.

NOTE

This command is valid only for information displayed by the **display interface description** command.

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

6.6.2 Configuring an Authentication Mode for a VTY User Interface

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.

NOTICE

The system starts the delayed login mechanism in the case of a device login failure. If the first login fails, the user can log in again 5 seconds later. The delay time is increased by 5 seconds every time a login failure occurs. For example, the second login is delayed to 10 seconds, and the third login is delayed to 15 seconds.

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 4 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 protocol.

----End

6.6.3 Configuring 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 6-6** describes mappings between user levels and command levels.

Table 6-6 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 *S1720&S2700&S5700&S6720 Series Ethernet Switches 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.

Procedure

- If a user uses password authentication mode, the user level is configured in the AAA view.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 DSA 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 DSA 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

6.6.4 Configuring an SSH User

Context

SSH users can be authenticated in six modes: password, Revest-Shamir-Adleman Algorithm (RSA), Digital Signature Algorithm (DSA), password--RSA, password--DSA, 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.
- Revest-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 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Digital Signature Algorithm (DSA) authentication: is similar to RSA authentication. DSA uses the digital signature algorithm to encrypt data.
- 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-DSA authentication: The SSH server implements both password and DSA authentication on login users. The users must pass both authentication modes to log in.
- All authentication: The SSH server implements public key 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 Run:

```
ssh user user-name
```

An SSH user is created.

Step 3 Run:

```
ssh user user-name authentication-type { password | rsa | password-rsa | all | dsa | password-dsa }
```

An authentication mode is set for the SSH user.

By default, an SSH user does not support any authentication mode.

NOTE

- If password authentication is selected, the user priority is the same as that specified on the AAA module.
- If RSA/DSA authentication is selected, the user priority depends on the priority of the VTY window used during user access.
- If all authentication is selected and an AAA user with the same name as the SSH user exists, user priorities may be different in password authentication and RSA/DSA authentication modes. Set relevant parameters as needed.
- You can run the **ssh authentication-type default password** command to set the default authentication mode of an SSH user to password authentication. When multiple SSH users need to be authenticated in password authentication mode, such configuration simplifies configurations and improves configuration efficiency because you do not need to repeatedly configure password authentication for each SSH user.

- If password authentication is used, create a local user with the same name as the SSH user in the AAA view.

  a. Run:

  ```
  aaa
  ```

  The AAA view is displayed.

  b. Run:

  ```
  local-user user-name password { cipher | irreversible-cipher } password
  ```

  A local user with the same name as the SSH user is created and a password is configured.

  c. Run:

  ```
  local-user user-name service-type ssh
  ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

A service type is set for the local user.

d. Run:

```
local-user user-name privilege level level
```

A user level is set for the local user.

e. Run:

```
quit
```

Return to the system view.

- If RSA or DSA 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.

  a. Run:

  ```
  rsa peer-public-key key-name [ encoding-type { der | openssh | pem } ]
  or dsa peer-public-key key-name encoding-type { der | openssh | pem }
  ```

  The RSA or DSA 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 | dsa-key } key-name
  ```

  An RSA or a DSA 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-DSA authentication is used, configure AAA user information and enter the public key generated on the client. Both operations are mandatory.
- If all authentication is used, configure AAA user information or enter the public key generated on the client or perform the two operations together.

Step 4 Run:

```
ssh user user-name service-type { stelnet | all }
```

By default, no service type is configured for an SSH user.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

6.6.5 Enabling the SSH Server Function

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 key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 |
dh_group1_sha1 } *
```

A key exchange algorithm list is configured for the SSH server.

By default, an SSH client supports all key exchange algorithms.

NOTE

Do not add dh_group14_sha1 or dh_group1_sha1 to the list because they provide the lowest security among the supported key exchange algorithms.

Step 4 (Optional) Run:

```
ssh server cipher { 3des_cbc | aes128_cbc | aes128_ctr | aes256_cbc | aes256_ctr
| des_cbc } *
```

An encryption algorithm list is configured for the SSH server.

By default, an SSH server supports five encryption algorithms: 3DES_CBC, AES128_CBC, AES256_CBC, AES128_CTR, and AES256_CTR.

NOTE

Do not add des_cbc or 3des_cbc to the list because they provide the lowest security among the supported encryption algorithms.

Step 5 (Optional) Run:

```
ssh server hmac { md5 | md5_96 | sha1 | sha1_96 | sha2_256 | sha2_256_96 } *
```

An HMAC algorithm list is configured for the SSH server.

By default, an SSH server supports all HMC algorithms.

NOTE

Do not add md5, sha1, md5_96, sha1_96, or sha2_256_96 to the HMAC algorithm list because they provide the lowest security among the supported HMAC algorithms.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 6 Run:

```
rsa local-key-pair create or dsa local-key-pair create
```

A local RSA or DSA key pair is generated.

NOTE

Run either of the commands based on the key pair type you desire. 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.

This command takes effect only for SSH1.X. However, SSH1.X ensures poor security and is not recommended.

Step 9 (Optional) Run:

```
ssh server timeout seconds
```

The timeout period is set for SSH authentication.

The default timeout period is 60 seconds.

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

If the SSH server is enabled to be compatible with earlier SSH versions, the system prompts a security risk.

Step 12 (Optional) Run:

```
ssh server-source -i loopback interface-number
```

The source interface is specified for the SSH server.

By default, the source interface of an SSH server is not specified.

Configuring a source interface for an SSH server prevents exposure of the device's management IP address, which ensures device security.

NOTE

Before specifying a loopback interface as the source interface for an SSH server, ensure that the loopback interface has been created and the route between the client and the loopback interface is reachable; otherwise, the configuration cannot be correctly executed.

----End

6.6.6 Logging In to a Device Through 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 device is 10.137.217.203. The third-party software, PuTTY, is used as an example to illustrate the STelnet login process.

Procedure

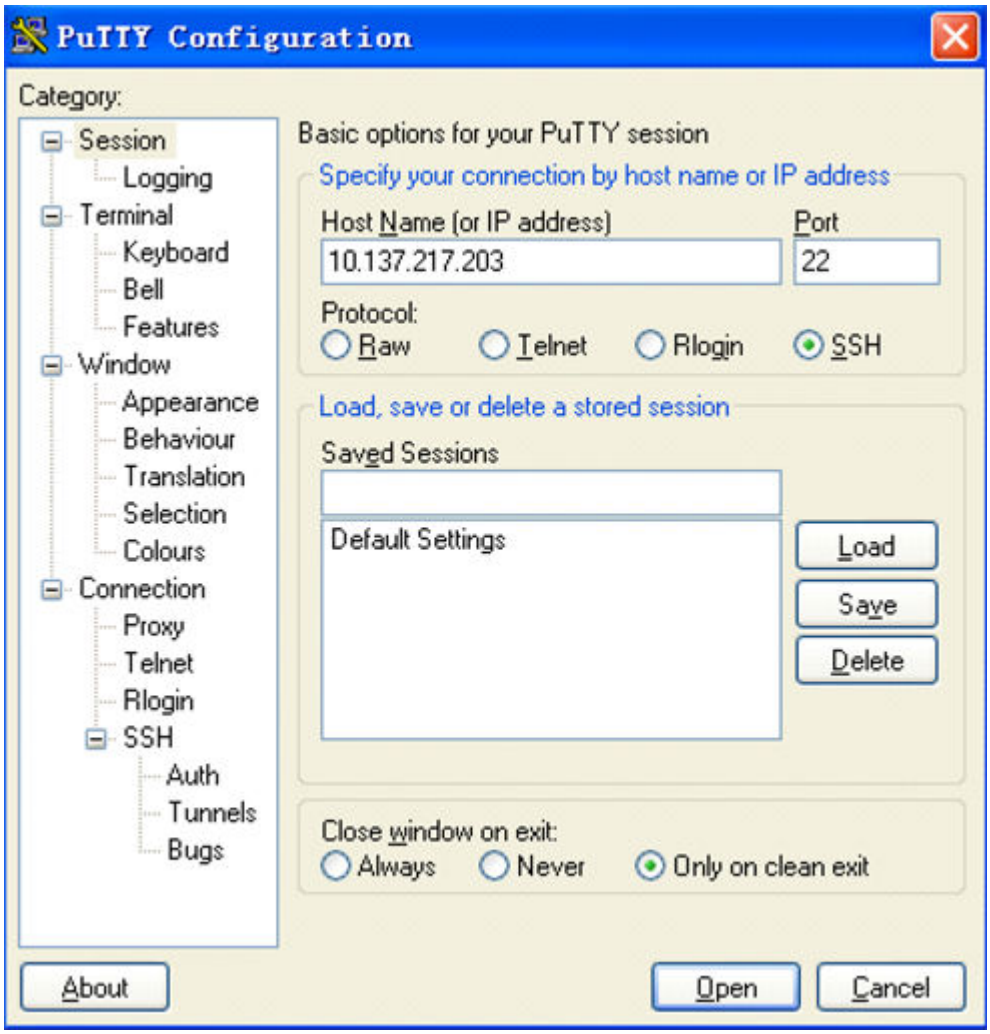
Step 1 Start the PuTTY software, enter the device's IP address, and select the SSH protocol.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 6-8 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.

Info: The max number of VTY users is 21, and the number
      of current VTY users on line is 5.
      The current login time is 2012-08-06 09:35:28+00:00.
<HUAWEI>
```

----End

Checking 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- 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.

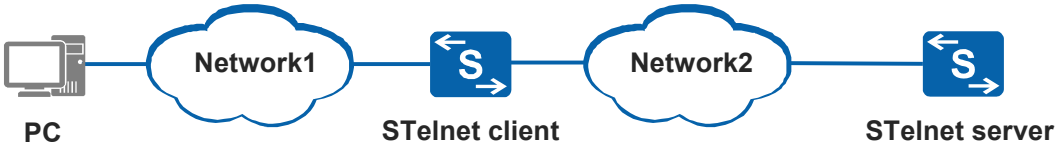
6.6.7 (Optional) Using STelnet to Log In to Another Device From the Local Device

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 6-9**, 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 6-9 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:

- Logging in to the device from a terminal
- Configuring a reachable route between the device and STelnet server
- Enabling the STelnet server function on the STelnet server
- Obtaining the SSH user name and password, server keys, and port number configured on the STelnet server

Procedure

Step 1 Generate a local key pair for the SSH client.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

NOTICE

When the device functions as an STelnet client to access the SSH server, the device can save a maximum of 20 public keys, which means that the device can access a maximum of 20 SSH servers at the same time. Run the **display ssh server-info** command to check the number of saved client public keys on the device. When the number of saved public keys exceeds 20 and the client needs to access other SSH servers, run the **undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** } command to delete the saved public keys. Note that after a public key is deleted, accessing the corresponding SSH server will fail (established connections remain unaffected).

1. Run:

   ```
   system-view
   ```

   The system view is displayed.

2. Run:

   ```
   rsa local-key-pair create or dsa local-key-pair create
   ```

   A local RSA or DSA 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 dsa local-key-pair public** command to view information about the public key in the generated RSA or DSA key pair. Configure the public key on the SSH server. For details, see **6.6.4 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, which allows the device to successfully connect to an SSH server without validating the SSH server's public key. The device then automatically saves the public key of the server for subsequent server authentication.

  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 method, 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

a. Run:

```
system-view
```

The system view is displayed.

b. Run:

```
rsa peer-public-key key-name [ encoding-type { der | openssh | pem } ]
or dsa peer-public-key key-name encoding-type { der | openssh | pem }
```

The RSA or DSA public key view is displayed.

Select a command to execute according to the type of the key on the server. For example, if an DSA key exists on the server, run the **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } command to enter the DSA public key view.

c. Run:

```
public-key-code begin
```

The public key editing view is displayed.

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 DSA 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 | dsa-key } key-name
```

The RSA or DSA 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** | **dsa-key** } command to unbind the RSA or DSA public key from the SSH server and then run the command to assign a new RSA or DSA public key to the SSH server.

Step 3 (Optional) Run:

```
ssh client key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 |
dh_group1_sha1 } *
```

A key exchange algorithm list is configured for the SSH client.

By default, an SSH server supports all key exchange algorithms.

NOTE

Do not add dh_group14_sha1 or dh_group1_sha1 to the list because they provide the lowest security among the supported key exchange algorithms.

Step 4 (Optional) Run:

```
ssh client cipher { 3des_cbc | aes128_cbc | aes128_ctr | aes256_cbc | aes256_ctr
| des_cbc } *
```

An encryption algorithm list is configured for the SSH client.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

By default, an SSH client supports five encryption algorithms: 3DES_CBC, AES128_CBC, AES256_CBC, AES128_CTR, and AES256_CTR.

NOTE

Do not add **des_cbc** or **3des_cbc** to the list because they provide the lowest security among the supported encryption algorithms.

Step 5 (Optional) Run:

```
ssh client hmac { md5 | md5_96 | sha1 | sha1_96 | sha2_256 | sha2_256_96 } *
```

An HMAC algorithm list is configured for the SSH client.

By default, an SSH client supports all HMC algorithms.

NOTE

Do not add md5, sha1, md5_96, sha1_96, or sha2_256_96 to the HMAC algorithm list because they provide the lowest security among the supported HMAC algorithms.

Step 6 Log in to another device.

- IPv4 mode: run the **stelnet** [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [[**-vpn-instance** *vpn-instance-name*] | [**identity-key** { **dsa** | **rsa** }] | [**user-identity-key** { **rsa** | **dsa** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-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*] [[**identity-key** { **dsa** | **rsa** }] | [**user-identity-key** { **rsa** | **dsa** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] * command to log in to another device.

Run either of the preceding commands based on the network address type.

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 and VPN instance name, select a key exchange algorithm, an encryption algorithm, and an HMAC algorithm, and enable the keepalive function on the client.

NOTE

- Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support **-a** *source-address* and **-i** *interface-type interface-number* parameter in the command.
- Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support support **-vpn-instance** *vpn-instance-name* parameter in the command.
- The algorithms DES, 3DES, MD5, MD5_96, SHA1, SHA1_96, SHA2_256, and SHA2_256_96 are insecure. It is recommended that you use the AES128 or AES256 encryption algorithm, which is more secure.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Checking the Configuration

- Run the **display ssh server-info** command on the SSH client to view all SSH servers and their public keys.

6.7 Common Operations After Login

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.

Clearing Online Users

You can disconnect an online user from a device by clearing the user on the corresponding user interface.

1. Run the **kill user-interface** { *ui-number* | *ui-type ui-number1* } command to clear an online user.
2. Run the **display users** command to view information about login users on a device.

Setting a Password for Switching User Levels

To run commands of levels higher than your user level, you need to switch to a higher user level and set a password.

1. Run the **system-view** command to enter the system view.
2. Run the **super password** [**level** *user-level*] [**cipher** *password*] command to set a password for switching user levels.

On networks that do not require high security, you can disable complexity check for passwords used to switch a user from a low user level to a higher one.

1. Run the **system-view** command to enter the system view.
2. Run the **super password complexity-check disable** command to disable complexity check for passwords used to switch a user from a low user level to a higher one.

Switching User Levels

You need to enter a password when switching from a low user level to a higher one.

1. Run the **super** [*level*] command to switch to a higher user level.
2. Enter the password as prompted.

   If the password is correct, you will switch to a higher user level. If you enter incorrect passwords three consecutive times, the system returns to the user view and the user level remains unchanged.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

If a user is switched to a higher user level using the **super** command, the system generates a trap and records the event in a log. If a user is switched to a lower user level, the system only records the event in a log.

Huawei switches use the combination of user name, password, and level to control users' operation rights. If you use the super command to switch user levels, this right control method will become invalid. Moreover, any user can use the super password of a higher level to obtain high-level operation rights. Therefore, you are not advised to use the super command to switch user levels.

Locking Configuration Rights

When multiple users log in to the system to perform configurations at the same time, conflicts occur. To avoid service exceptions, you can configure exclusive configuration rights to ensure that only one user can perform configurations at a time.

1. Run the **configuration exclusive** command to lock configuration rights for the current user.

   After you run the command, the configuration rights are exclusive to the current user and other users do not have configuration rights.

   This command applies to all views.

   If configuration rights are locked, a message is displayed when you attempt to lock the configuration rights again.

   NOTE

   Run the **display configuration-occupied user** command to check information about the user for whom configuration rights are locked.

2. Run the **system-view** command to enter the system view.
3. (Optional) Run the **configuration-occupied timeout** *timeout-value* command to set the timeout period for locking configuration rights.

   This command specifies the maximum period for locking configuration rights when no configuration command is issued. After the specified period times out, the system automatically unlocks the configuration rights and other users can perform configurations.

   The default timeout period is 30 seconds.

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.

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

2. Enter the lock password and confirm password as prompted.

```
<HUAWEI> lock
Please configure the login password (8-16)
Enter Password:
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.

By default, the minimum length of plain text passwords allowed by a device is 8 characters. You can set a longer password to increase password complexity and improve device security. Run the **set password min-length** *length* command to set the minimum length of plain text passwords allowed by the device.

To unlock the user interface, you must press **Enter** and enter the correct login password as prompted.

Executing User-View Commands in the System View

Some commands need to be executed in the user view. To execute these commands, you need to enter the user view. To facilitate user-view command execution, you can perform the following configuration. After the configuration is complete, you can execute user-view commands directly in the system view, without the need to switch views.

1. Run the **system-view** command to enter the system view.
2. Run the **run** *command-line* command to allow the execution of user-view commands in the system view.

   By default, the system does not allow the execution of user-view commands in the system view.

6.8 CLI Login Configuration Examples

6.8.1 Example for Configuring Login 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 6-10 Networking diagram for configuring login through a console port

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuration Roadmap

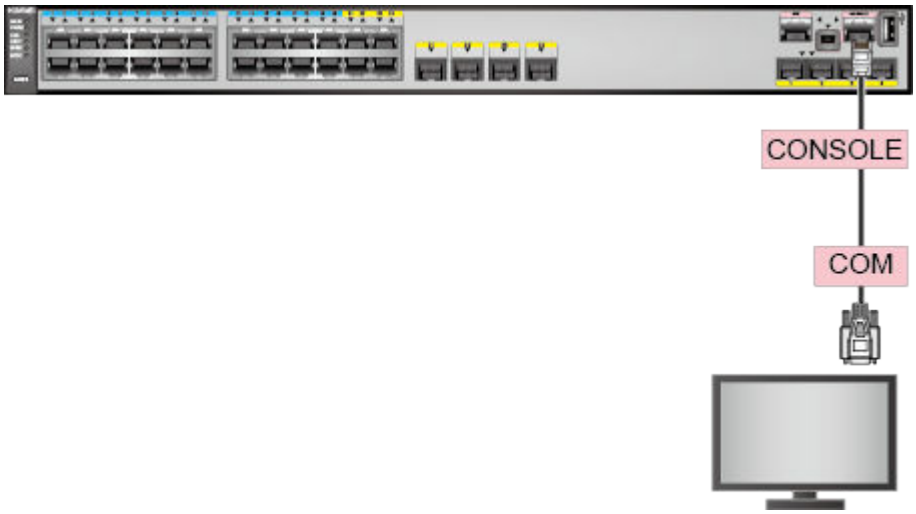
The configuration roadmap is as follows:

1. Use terminal emulation software to log in to the device through the console port.
2. Set an authentication mode for the console user interface.

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 6-11**.

Figure 6-11 Connecting to the device through the console port



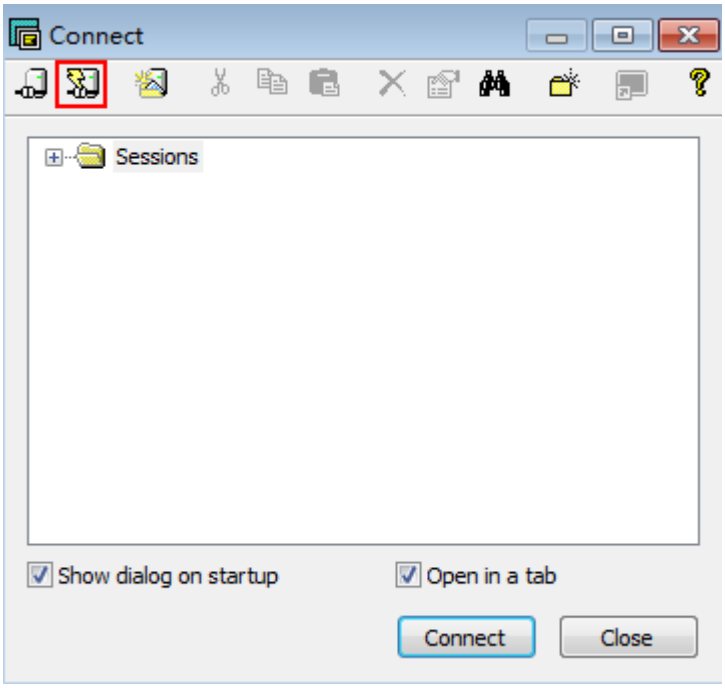
Step 2 Start the terminal emulation software on the PC. Create a connection, select the port for connection, and set communication parameters. (This section uses the third-party software SecureCRT as an example.)

1. Click to establish a connection, as shown in **Figure 6-12**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Figure 6-12 Establishing a connection



2. Set the port for connection and communication parameters, as shown in **Figure 6-13**.

   Select the port for connection. For example, you can view port information in **Device Manager** in the Windows operating system, and select the port for connection.

   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

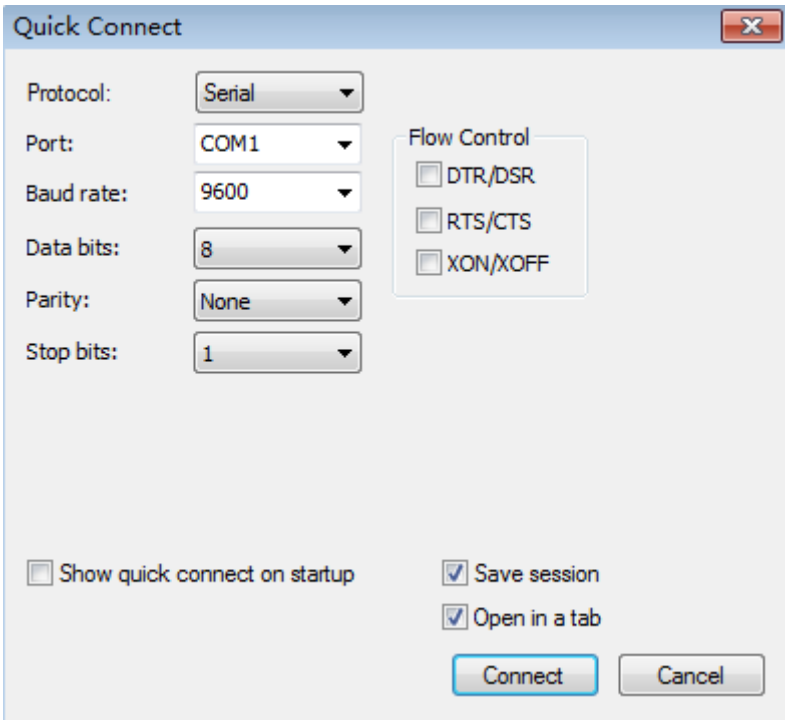
   By default, no flow control mode is configured on the device. Because RTS/CTS is selected in the software by default, you need to deselect RTS/CTS; otherwise, you cannot enter commands.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 6-13 Setting the port for connection and communication parameters



Step 3 Press **Enter**. 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>
```

NOTE

If you configure the console user interface after login through the console port, the configuration takes effect on your next login.

Step 4 Set an authentication mode for the console user interface.

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] user-interface console 0
[Switch-ui-console0] authentication-mode aaa
[Switch-ui-console0] user privilege level 15
[Switch-ui-console0] quit
[Switch] aaa
[Switch-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Switch-aaa] local-user admin1234 privilege level 15
[Switch-aaa] local-user admin1234 service-type terminal
```

After the preceding operations, you need to enter the user name **admin1234** and password **Helloworld@6789** to pass identity authentication before re-logging in to the device from the console user interface.

----End

Configuration Files

Switch configuration file

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
#
sysname Switch
#
aaa
 local-user admin1234 password irreversible-cipher %^%#aVW8S=aP=B<OWi1Bu'^R[=_!
~oR*85r_nNY+kA(I}[TiLiVGR-i/'DFGAI-O%^%#
 local-user admin1234 privilege level 15
 local-user admin1234 service-type terminal
#
user-interface con 0
 authentication-mode aaa
#
return
```

Related Content

Videos

Log In to a Switch Through the Console Port.

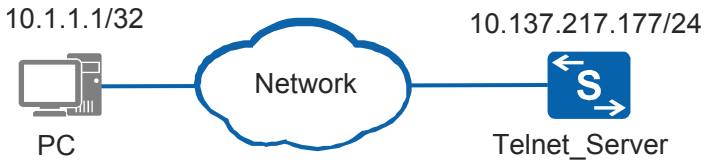
Log In to a Switch Through the MiniUSB Port.

6.8.2 Example for Configuring Telnet Login

Networking Requirements

As shown in **Figure 6-14**, the PC and device are reachable to each other. Users require that the device be remotely configured and managed in an easy way. To meet the requirement, configure AAA authentication for Telnet users on the server.

Figure 6-14 Networking diagram for configuring Telnet login



Configuration Roadmap

The configuration roadmap is as follows:

1. Log in to the device using Telnet to remotely maintain the device.
2. Configure the administrator user name and password, and configure an AAA authentication policy to ensure that only users passing the authentication can log in to the device.

Procedure

Step 1 Enable the server function.

```
<HUAWEI> system-view
[HUAWEI] sysname Telnet_Server
[Telnet_Server] telnet server enable
```

Step 2 Set parameters for the VTY user interface.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Set the maximum number of VTY user interfaces.

```
[Telnet_Server] user-interface maximum-vty 15
```

Set terminal attributes for the VTY user interface.

```
[Telnet_Server] user-interface vty 0 14
[Telnet_Server-ui-vty0-14] protocol inbound telnet
[Telnet_Server-ui-vty0-14] shell
[Telnet_Server-ui-vty0-14] idle-timeout 20
[Telnet_Server-ui-vty0-14] screen-length 0
[Telnet_Server-ui-vty0-14] history-command max-size 20
```

Set an authentication mode for the VTY user interface.

```
[Telnet_Server-ui-vty0-14] authentication-mode aaa
[Telnet_Server-ui-vty0-14] quit
```

Step 3 Configure the login user information.

Set an authentication mode for login users.

```
[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
```

Step 4 Log in to the client.

Run commands on the Windows Command Prompt of the PC to log in to the device using Telnet.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
```

Press **Enter**, and enter the configured user name and password in the login window. If authentication succeeds, the CLI is displayed, indicating that you have successfully logged in to the device. (The following information is only for reference.)

```
Login authentication


Username:admin1234
Password:
Info: The max number of VTY users is 15, and the number
      of current VTY users on line is 2.
      The current login time is 2012-08-06 18:33:18+00:00.
<Telnet_Server>
```

----End

Configuration Files

Telnet server configuration file

```
#
sysname Telnet_Server
#
telnet server enable
#
aaa
 local-user admin1234 password irreversible-cipher %^%#aVW8S=aP=B<OWi1Bu'^R[=_!
~oR*85r_nNY+kA(I}[TiLiVGR-i/'DFGAI-O%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
user-interface maximum-vty 15
user-interface vty 0 14
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 0
 protocol inbound telnet
#
return
```

Related Content

Videos

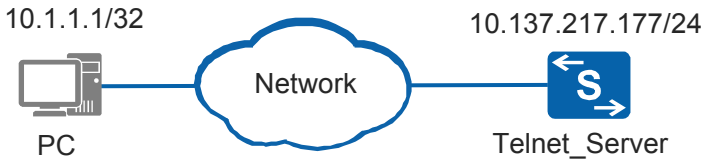
Remotely Log In to a Switch Using Telnet.

6.8.3 Example for Configuring a Security Policy to Limit Telnet Login

Networking Requirements

As shown in **Figure 6-15**, the PC and device are reachable to each other. Users require that the device be remotely configured and managed in an easy way. To meet the requirement, configure AAA authentication for Telnet users on the server and configure a security policy to allow only users meeting the policy to log in to the device.

Figure 6-15 Networking diagram for configuring Telnet login



Configuration Roadmap

The configuration roadmap is as follows:

1. Log in to the device using Telnet to remotely maintain the device.
2. Configure the administrator user name and password, and configure an AAA authentication policy to ensure that only users passing the authentication can log in to the device.
3. Configure a security policy to ensure that only users meeting the policy can log in to the device.

Procedure

Step 1 Enable the server function.

```
<HUAWEI> system-view
[HUAWEI] sysname Telnet_Server
[Telnet_Server] telnet server enable
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 2 Set parameters for the VTY user interface.

Set the maximum number of VTY user interfaces.

```
[Telnet_Server] user-interface maximum-vty 15
```

Specify the IP address of the host allowed to log in to the device.

```
[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 14
[Telnet_Server-ui-vty0-14] protocol inbound telnet
[Telnet_Server-ui-vty0-14] acl 2001 inbound
```

Set terminal attributes for the VTY user interface.

```
[Telnet_Server-ui-vty0-14] shell
[Telnet_Server-ui-vty0-14] idle-timeout 20
[Telnet_Server-ui-vty0-14] screen-length 0
[Telnet_Server-ui-vty0-14] history-command max-size 20
```

Set an authentication mode for the VTY user interface.

```
[Telnet_Server-ui-vty0-14] authentication-mode aaa
[Telnet_Server-ui-vty0-14] quit
```

Step 3 Configure the login user information.

Set an authentication mode for login users.

```
[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
```

Step 4 Log in to the client.

Run commands on the Windows Command Prompt of the PC to log in to the device using Telnet.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

Press **Enter**, and enter the configured user name and password in the login window. If authentication succeeds, the CLI is displayed, indicating that you have successfully logged in to the device. (The following information is only for reference.)

```
Login authentication


Username:admin1234
Password:
Info: The max number of VTY users is 8, and the number
      of current VTY users on line is 2.
      The current login time is 2012-08-06 18:33:18+00:00.
<Telnet_Server>
```

----End

Configuration Files

Telnet_Server configuration file

```
#
sysname Telnet_Server
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

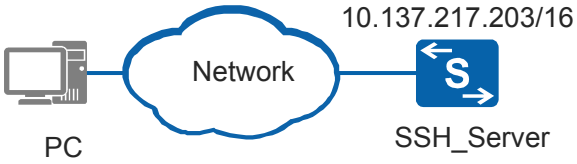

```
#
telnet server enable
#
acl number 2001
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^%#aVW8S=aP=B<OWi1Bu'^R[=_!
~oR*85r_nNY+kA(I}[TiLiVGR-i/'DFGAI-O%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface maximum-vty 15
user-interface vty 0 14
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 0
 protocol inbound telnet
#
return
```

6.8.4 Example for Configuring STelnet Login

Networking Requirements

Users may require secure remote login, but Telnet cannot provide a secure authentication method. To ensure remote login security, STelnet can be configured. As shown in **Figure 6-16**, the PC and SSH server are reachable to each other, and 10.137.217.203 is the IP address of the management interface on the SSH server. Configure a login user **client001** on the SSH server. The PC uses the account **client001** to log in to the SSH server through password authentication.

Figure 6-16 Networking diagram for configuring STelnet login



NOTICE

The STelnet V1 protocol has security vulnerabilities. It is recommended that you log in to the device using STelnet V2.

Configuration Roadmap

The configuration roadmap is as follows:

1. Install SSH server login software on the PC.
2. Generate a local key pair on the SSH server to implement secure data exchange between the server and client.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

3. Create SSH user **client001** on the SSH server.
4. Enable the STelnet service on the SSH server.
5. Set the service type of client001 to STelnet on the SSH server.
6. Configure client001 to log in to the SSH server through STelnet.

Procedure

Step 1 Generate a local key pair for the SSH server.

```
<HUAWEI> system-view
[HUAWEI] sysname SSH_Server
[SSH_Server] dsa local-key-pair create
Info: The key name will be:
HUAWEI_Host_DSA.

Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

Step 2 Create an SSH user on the server.

Configure the VTY user interface.

```
[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
```

Create SSH user **client001** and set the authentication mode to password authentication.

```
[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
```

Step 3 Enable the STelnet service on the SSH server.

```
[SSH_Server] stelnet server enable
```

Step 4 Set the service type of client001 to **STelnet** on the SSH server.

```
[SSH_Server] ssh user client001 service-type stelnet
```

Step 5 Verify the configuration.

Use the account **client001** to log in to the SSH server through password authentication.

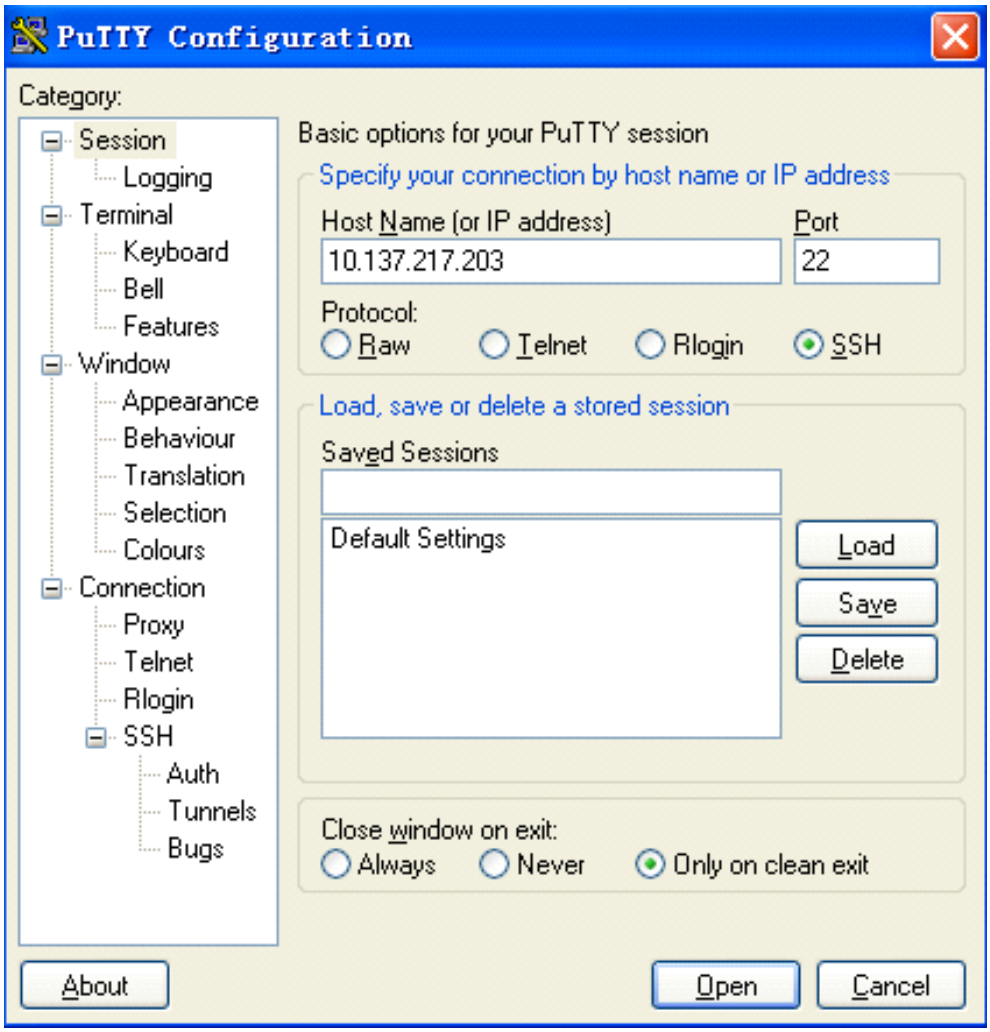
Log in to the device using PuTTY, enter the device's IP address, and select the SSH protocol.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 6-17 Logging in to the SSH server through PuTTY in password authentication mode



Click **Open**. In the displayed page, enter the user name and password and press **Enter** to log in to the SSH server. (The following information is only for reference.)

```
login as: client001
Sent username "client001"

client001@10.137.217.203's password:

Info: The max number of VTY users is 8, and the number
      of current VTY users on line is 5.
      The current login time is 2012-08-06 09:35:28+00:00.
<SSH_Server>
```

----End

Configuration Files

SSH_Server configuration file

```
#
sysname SSH_Server
#
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
aaa
 local-user client001 password irreversible-cipher %^%#aVW8S=aP=B<OWi1Bu'^R[=_!
~oR*85r_nNY+kA(I}[TiLiVGR-i/'DFGAI-O%^%#
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
stelnet server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type stelnet
#
user-interface vty 0 14
 authentication-mode aaa
#
return
```

Related Content

Videos

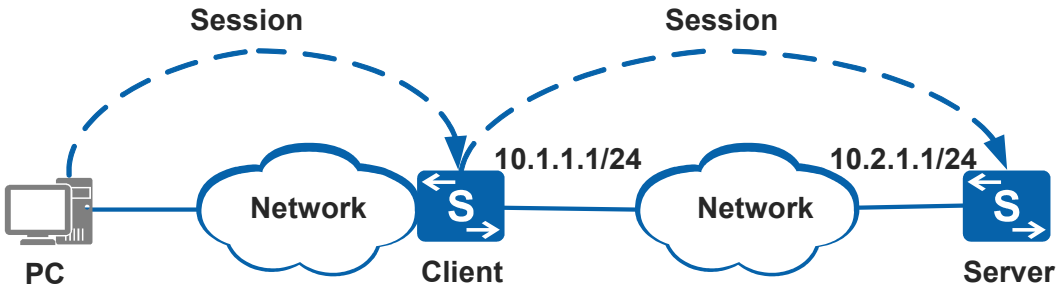
Remotely Log In to a Switch Using Telnet.

6.8.5 Example for Configuring the Device as the Telnet Client to Log In to Another Device

Networking Requirements

As shown in **Figure 6-18**, the PC and Client have reachable routes to each other; Client and Server have reachable routes to each other. The user needs to manage and maintain Server remotely. However, the PC cannot directly log in to Server through Telnet because it has no reachable route to Server. The user can log in to Client through Telnet, and then log in to Server from Client. To prevent unauthorized devices from logging in to Server through Telnet, an ACL needs to be configured to allow only the Telnet connection from Client to Server.

Figure 6-18 Networking diagram of configuring the device as the Telnet client to log in to another device



NOTICE

The Telnet protocol poses a security risk, and therefore the STelnet V2 protocol is recommended.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Telnet authentication mode on Server.
2. Configure the login user information on Server.
3. Configure the Server to allow Client access with ACL.
4. Log in to Server from Client through Telnet.

Procedure

Step 1 Configure the Telnet authentication mode and password on Server.

```
<HUAWEI> system-view
[HUAWEI] sysname Server
[Server] telnet server enable
[Server] user-interface vty 0 4
[Server-ui-vty0-4] user privilege level 15
[Server-ui-vty0-4] protocol inbound telnet
[Server-ui-vty0-4] authentication-mode aaa
[Server-ui-vty0-4] quit
```

Step 2 Configure the login user information.

```
[Server] aaa
[Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Server-aaa] local-user admin1234 service-type telnet
[Server-aaa] local-user admin1234 privilege level 3
[Server-aaa] quit
```

Step 3 Configure the Switch2 to allow Client access with ACL.

```
[Server] acl 2000
[Server-acl-basic-2000] rule permit source 10.1.1.1 0
[Server-acl-basic-2000] quit
[Server] user-interface vty 0 4
[Server-ui-vty0-4] acl 2000 inbound
[Server-ui-vty0-4] quit
```

NOTE

It is optional to configure an ACL for Telnet services.

Step 4 Verify the configuration.

After the preceding configuration, you can log in to Server from Client through Telnet. You cannot log in to Server from other devices.

```
<HUAWEI> system-view
[HUAWEI] sysname Client
[Client] quit
<Client> telnet 10.2.1.1
Trying 10.2.1.1 ...
Press CTRL+K to abort
Connected to 10.2.1.1 ...

Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.

Login authentication


Username:admin1234
Password:
<Server>
```

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuration Files

Server configuration file

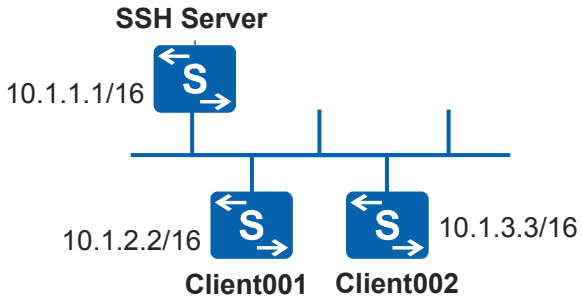
```
#
sysname Server
#
telnet server enable
#
acl number 2000
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^
%#gRNl~ukoL~0.WU)C2]~2a}Cz/Y0-u8M{j@Ql6/xHryO-Y7m{=A>kWc.-q}>*%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface vty 0 4
 acl 2000 inbound
 authentication-mode aaa
 user privilege level 15
 protocol inbound telnet
#
return
```

6.8.6 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 6-19**, two login users **client001** and **client002** are configured and they use the password and DSA authentication modes respectively to log in to the SSH server.

Figure 6-19 Networking diagram of logging in to another device through STelnet



NOTICE

The STelnet V1 protocol poses a security risk, and therefore the STelnet V2 mode is recommended.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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. 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] dsa local-key-pair create
Info: The key name will be: SSH Server_Host_DSA.
Info: The DSA host key named SSH Server_Host_DSA already exists.
Info: The key modulus can be any one of the following : 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys........
Info: Succeeded in creating the DSA host 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
  [SSH Server] ssh user client001 authentication-type password
  ```

- Create an SSH user named **client002**.

  # Create an SSH user named **client002** and configure the DSA authentication mode for the user.

  ```
  [SSH Server] ssh user client002
  [SSH Server] ssh user client002 authentication-type dsa
  ```

  # Generate a local key pair for Client002.

  ```
  <HUAWEI> system-view
  [HUAWEI] sysname client002
  [client002] dsa local-key-pair create
  Info: The key name will be: SSH Server_Host_DSA.
  Info: The DSA host key named SSH Server_Host_DSA already exists.
  Info: The key modulus can be any one of the following : 1024, 2048.
  Info: If the key modulus is greater than 512, it may take a few minutes.
  ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
Please input the modulus [default=2048]:
Info: Generating keys........
Info: Succeeded in creating the DSA host keys.
```

Check the public key in the DSA key pair generated on the client.

```
[client002] display dsa local-key-pair public
=========================================================
Time of Key pair created: 2014-03-03 16:51:28-05:13
Key name: client002_Host
Key modulus : 2048
Key type: DSA encryption Key
Key fingerprint: c0:52:b0:37:4c:b2:64:d1:8f:ff:a1:42:87:09:8c:6f
=========================================================
Key code:
30820109
  02820100
    CA97BCDE 697CEDE9 D9AB9475 9E004D15 C8B95116
    87B79B0C 5698C582 69A9F4D0 45ED0E53 AF2EDEC1
    A09DF4BE 459E34B6 6697B85D 2191A00E 92F3A5E7
    FB0E73E7 F0212432 E898D979 8EAA491E E2B69727
    4B51A2BE CD86A144 16748D1E 4847A814 3FE50862
    6EB1AD81 EB49A05E 64F6D186 C4E94CDB 04C53074
    B839305A 7F7BCE2C 606F6C91 EA958B6D AC46C12B
    8C2B1E03 98F1C09D 3AF2A69D 6867F930 DF992692
    9A921682 916273FC 4DD875D4 44BC371E DDBB8F6A
    C0A4CDB3 ADDAE853 DB86B9FA DB13CCA9 D8CF6EC1
    530CC2F5 697C4707 90829982 4339507F F354FAF9
    0F9CD2C2 F7D6FF3D 901D700F F0588104 856B9592
    71D773E2 E76E8EEB 431FB60D 60ABC20B
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAABAQDKl7zeaXzt6dmrlHWeAE0VyLlRFoe3mwxW
mMWCaan00EXtDlOvLt7BoJ30vkWeNLZml7hdIZGgDpLzpef7DnPn8CEkMuiY2XmO
qkke4raXJ0tRor7NhqFEFnSNHkhHqBQ/5QhibrGtgetJoF5k9tGGxOlM2wTFMHS4
OTBaf3vOLGBvbJHqlYttrEbBK4wrHgOY8cCdOvKmnWhn+TDfmSaSmpIWgpFic/xN
2HXURLw3Ht27j2rApM2zrdroU9uGufrbE8yp2M9uwVMMwvVpfEcHkIKZgkM5UH/z
VPr5D5zSwvfW/z2QHXAP8FiBBIVrlZJx13Pi526O60Mftg1gq8IL
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-dsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDKl7zeaXzt6dmrlHWeAE0VyLlRFoe3mwxWmMWCaan00EXtDl
OvLt7BoJ30vkWeNLZml7hdIZGgDpLzpef7DnPn8CEkMuiY2XmOqkke4raXJ0tRor7NhqFEFnSNHkhH
qBQ/
5QhibrGtgetJoF5k9tGGxOlM2wTFMHS4OTBaf3vOLGBvbJHqlYttrEbBK4wrHgOY8cCdOvKmnWhn
+TDfmSaSmpIWgpFic/
xN2HXURLw3Ht27j2rApM2zrdroU9uGufrbE8yp2M9uwVMMwvVpfEcHkIKZgkM5UH/
zVPr5D5zSwvfW/z2QHXAP8FiBBIVrlZJx13Pi526O60Mftg1gq8IL dsa-key
```

```
[SSH Server] dsa peer-public-key dsakey001 encoding-type der
[SSH Server-dsa-public-key] public-key-code begin
Info: Enter "DSA key code" view, return the last view with "public-key-code
end".
[SSH Server-dsa-key-code] 30820109
[SSH Server-dsa-key-code] 2820100
[SSH Server-dsa-key-code] CA97BCDE 697CEDE9 D9AB9475 9E004D15 C8B95116
[SSH Server-dsa-key-code] 87B79B0C 5698C582 69A9F4D0 45ED0E53 AF2EDEC1
[SSH Server-dsa-key-code] A09DF4BE 459E34B6 6697B85D 2191A00E 92F3A5E7
[SSH Server-dsa-key-code] FB0E73E7 F0212432 E898D979 8EAA491E E2B69727
[SSH Server-dsa-key-code] 4B51A2BE CD86A144 16748D1E 4847A814 3FE50862
[SSH Server-dsa-key-code] 6EB1AD81 EB49A05E 64F6D186 C4E94CDB 04C53074
[SSH Server-dsa-key-code] B839305A 7F7BCE2C 606F6C91 EA958B6D AC46C12B
[SSH Server-dsa-key-code] 8C2B1E03 98F1C09D 3AF2A69D 6867F930 DF992692
[SSH Server-dsa-key-code] 9A921682 916273FC 4DD875D4 44BC371E DDBB8F6A
[SSH Server-dsa-key-code] C0A4CDB3 ADDAE853 DB86B9FA DB13CCA9 D8CF6EC1
[SSH Server-dsa-key-code] 530CC2F5 697C4707 90829982 4339507F F354FAF9
[SSH Server-dsa-key-code] 0F9CD2C2 F7D6FF3D 901D700F F0588104 856B9592
[SSH Server-dsa-key-code] 71D773E2 E76E8EEB 431FB60D 60ABC20B
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[SSH Server-dsa-key-code] 203
[SSH Server-dsa-key-code] 10001
[SSH Server-dsa-key-code] public-key-code end
[SSH Server-dsa-public-key] peer-public-key end
```

Bind the DSA public key of the STelnet client to the SSH user client002 on the SSH server.

```
[SSH Server] ssh user client002 assign dsa-key dsakey001
```

Step 3 Enable the STelnet service on the SSH server.

Enable the STelnet service.

```
[SSH Server] stelnet server enable
```

Step 4 Configure the STelnet service type for the **client001** and **client002** users.

```
[SSH Server] ssh user client001 service-type stelnet
[SSH Server] ssh user client002 service-type stelnet
```

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
```

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
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] :y
Save the server's public key? [Y/N] :y
The server's public key will be saved with the name 10.1.1.1. Please wait...

Please select public key type for user authentication [R for RSA; D for DSA;
Enter for Skip publickey authentication; Ctrl_C for Can
cel], Please select [R, D, Enter or Ctrl_C]:d
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 DSA authentication mode.

```
[client002] stelnet 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 ...
Please select public key type for user authentication [R for RSA; D for DSA;
Enter for Skip publickey authentication; Ctrl_C for Can
cel], Please select [R, D, Enter or Ctrl_C]:d
<SSH Server>
```

If the user view is displayed, you have logged in successfully. If the message "Session is disconnected" is displayed, the login fails.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 6 Verify the configuration.

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                          :2.0
 SSH connection timeout               :60 seconds
 SSH server key generating interval   :0 hours
 SSH authentication retries           :3 times
 SFTP server                          :Disable
 Stelnet server                       :Enable
 Scp server                           :Disable
 SSH server source                    :0.0.0.0
 ACL4 number                          :0
 ACL6 number                          :0
```

Check information about SSH users.

```
[SSH Server] display ssh user-information
  User 1:
       User Name            : client001
       Authentication-type  : password
       User-public-key-name : -
       User-public-key-type : -
       Sftp-directory       : -
       Service-type         : stelnet
       Authorization-cmd    : No
  User 2:
       User Name            : client002
       Authentication-type  : dsa
       User-public-key-name : dsakey001
       User-public-key-type : dsa
       Sftp-directory       : -
       Service-type         : stelnet
       Authorization-cmd    : No
```

----End

Configuration Files

- SSH server configuration file

```
#
sysname SSH Server
#
dsa peer-public-key dsakey001 encoding-type der
 public-key-code begin
  30820109
    02820100
      CA97BCDE 697CEDE9 D9AB9475 9E004D15 C8B95116 87B79B0C 5698C582 69A9F4D0
      45ED0E53 AF2EDEC1 A09DF4BE 459E34B6 6697B85D 2191A00E 92F3A5E7 FB0E73E7
      F0212432 E898D979 8EAA491E E2B69727 4B51A2BE CD86A144 16748D1E 4847A814
      3FE50862 6EB1AD81 EB49A05E 64F6D186 C4E94CDB 04C53074 B839305A 7F7BCE2C
      606F6C91 EA958B6D AC46C12B 8C2B1E03 98F1C09D 3AF2A69D 6867F930 DF992692
      9A921682 916273FC 4DD875D4 44BC371E DDBB8F6A C0A4CDB3 ADDAE853 DB86B9FA
      DB13CCA9 D8CF6EC1 530CC2F5 697C4707 90829982 4339507F F354FAF9 0F9CD2C2
      F7D6FF3D 901D700F F0588104 856B9592 71D773E2 E76E8EEB 431FB60D 60ABC20B
    0203
      010001
 public-key-code end
peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher %^
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
%#gRNl~ukoL~0.WU)C2]~2a}Cz/Y0-u8M{j@Ql6/xHryO-Y7m{=A>kWc.-q}>*%^%#
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
stelnet server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type stelnet
ssh user client002
ssh user client002 authentication-type dsa
ssh user client002 assign dsa-key dsakey001
ssh user client002 service-type stelnet
#
user-interface vty 0 4
 authentication-mode aaa
#
return
```

- Client001 configuration file

```
#
sysname client001
#
ssh client first-time enable
#
return
```

- Client002 configuration file

```
#
sysname client002
#
ssh client first-time enable
#
return
```

6.9 CLI Login Common Misconfigurations

6.9.1 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 SecureCRT 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 6-20**. The default console port settings are as follows:

- Baud rate: 9600
- Data bits: 8
- Stop bits: 1
- Parity: None

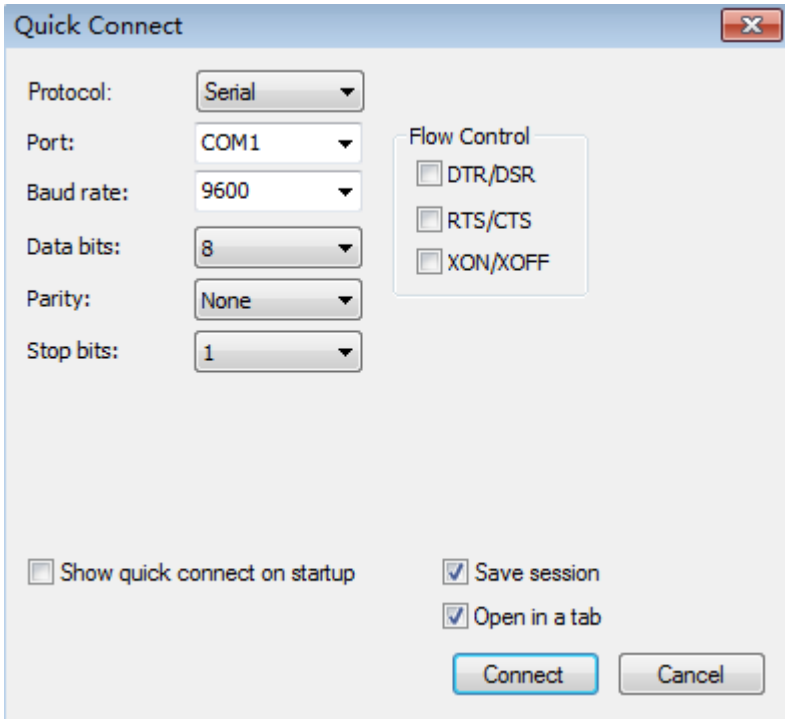
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Flow control: None

Figure 6-20 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

6.9.2 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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 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

6.9.3 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 or a DSA 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** or **display dsa 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** or **dsa local-key-pair create** command to create a key pair.

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**, **ssh user authentication-type**, and **ssh user**

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

service-type commands in the system view to create an SSH user and set an authentication mode and the service type 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

6.10 FAQ

6.10.1 What Is the Default Login Password?

- Logging in through the console port or Telnet

Table 6-7 Default passwords for console port or Telnet login in different versions

Version	Default User Name	Default Password	Default Level
V1R6C00-V1R6C05	None	None	None

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Version	Default User Name	Default Password	Default Level
V2R1C00-V2R9C00			

- Web login

Table 6-8 Default passwords for web login in different versions

Version	Default User Name	Default Password	Default Level
V1R6C00	admin	admin	0
V1R6C05		admin@huawei.com	
V2R1C00		admin	
V2R2C00		admin	
V2R3C00-V2R9C00		admin@huawei.com	

- BootROM menu login

Table 6-9 Default passwords for BootROM menu login to devices of different versions

Version	Default User Name	Default Password	Default Level
V1R6C00	None	huawei	None
V1R6C05		Admin@huawei.com	
V2R1C00-V2R9C00		Admin@huawei.com	

6.10.2 What If I Forget the Password for Console Port Login?

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.

Ensure that you have an STelnet/Telnet account and administrator rights. 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 Huawei@123
[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
[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/BootLoad Menu

NOTE

On S5710-X-LI, S5700S-28X-LI-AC, S5700S-52X-LI-AC, S5720SI, S5720S-SI, S5720EI, S5720HI, S6720EI, and S6720S-EI, you can clear the password for console port login through the BootLoad menu. On other switch models, you can clear the password through the BootROM menu.

You can use the BootROM/BootLoad menu of the device to clear the lost password for console port login. After starting the switch, 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/BootLoad password to enter the BootROM/BootLoad menu.

   ```
   Press Ctrl+B or Ctrl+E to enter BootROM menu ... 2
   password:      //Enter the BootROM/BootLoad password.
   ```

   NOTE

   Some models allow you to enter the BootROM/BootLoad menu by pressing **Ctrl+E**. Perform operations as prompted on the screen.

2. Select **Clear password for console user** on the BootROM/BootLoad menu to clear the password for console port login.
3. Select **Boot with default mode** on the BootROM/BootLoad menu to start the device as prompted.
4. After the device is started, log in through the console port. Authentication is not required when you log in. Set a password as prompted after login.
5. You can set an authentication mode and password for the console user interface according to service requirements. 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.

6.10.3 What If I Forget the Password for Telnet Login?

If you forget the Telnet login password, log in to the device through the console port and set a new password for Telnet login.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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] protocol inbound telnet   //By default, switches in V200R006 and
earlier versions support Telnet, and switches in V200R007 and later versions
support SSH.
[HUAWEI-ui-vty0] authentication-mode password
[HUAWEI-ui-vty0] set authentication password cipher Huawei@123
[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   //By default, switches in V200R006 and
earlier versions support Telnet, and switches in V200R007 and later versions
support SSH.
[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
```

6.10.4 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.

  NOTE

  This command is valid only for information displayed by the **display interface description** [*interface-type* [*interface-number*]] command.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

7 Web System Login Configuration

About This Chapter

7.1 Overview
7.2 Web System Login Configuration Tasks
7.3 Web System Login Default Configuration
7.4 Configuring Device Login Through the Web System (Simple Mode)
7.5 Configuring Device Login Through the Web System (Secure Mode)
7.6 Configuring Access Control on Web Users
7.7 Web System Login Configuration Examples
7.8 Web System Login Common Misconfigurations
7.9 FAQ

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

7.1 Overview

Definition

Web systems are used to manage devices. Before using a web system to manage a device, users need to log in to the system using the device's internal web server.

Purpose

You can manage a device using a web system or a command line interface (CLI). On a CLI, you must use commands to manage and maintain the device. The CLI method allows you to implement fine-grained device management, but you must familiarize yourself with required commands. The web system is easy to operate and allows you to manage and maintain the device on a GUI. However, the web system provides only basic routine maintenance and management functions. You can select a proper management method based on actual needs.

To use the CLI, you must log in to the device through a console port or a mini USB port, or using Telnet or STelnet. To use the web system, you must log in to the device through HTTPS.

For details on how to log in to a device through the console port or a mini USB port, or using Telnet or STelnet, see **6 CLI Login Configuration**.

Concepts

Before configuring web system login, familiarize yourself with the following concepts:

- **HTTP**

  Hypertext Transfer Protocol (HTTP) is used to transfer web page files over the Internet. It runs at the application layer of the TCP/IP protocol stack. The transport layer uses the connection-oriented TCP protocol. Due to the security vulnerability of HTTP, devices only allow you to log in to the web system through the more secure Hypertext Transfer Protocol Secure (HTTPS).

- **HTTPS**

  HTTPS uses secure sockets layer (SSL) to encrypt data exchanged between the client and device and defines access control policies based on certificate attributes. HTTPS enhances data integrity and transmission security, ensuring only authorized clients can log in to the device.

- **SSL policy**

  An SSL policy defines parameters that the device uses during startup, and is implemented during configuration of HTTPS. During configuration, the corresponding digital certificate on the device is loaded. The SSL policy takes effect only after it is applied to application layer protocols, such as HTTP.

- **Digital certificate**

  A digital certificate is issued by a certificate authority (CA) and uses a digital signature to bind a public key with an identity (applicant who possesses the certificate). The digital certificate includes information such as the applicant name, public key, digital signature of the CA, and validity period of the digital certificate. A digital certificate validates the identities of two communicating parties to improve communication reliability.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- **Certificate Authority (CA)**

  A CA issues, manages, and revokes digital certificates by checking the validity of digital certificate owners, issuing digital certificates to prevent eavesdropping and tampering, and managing keys. A worldwide trusted CA is called a root CA. The root CA can authorize other CAs as subordinate. CA identity needs to be verified and is described in a trusted-CA file.

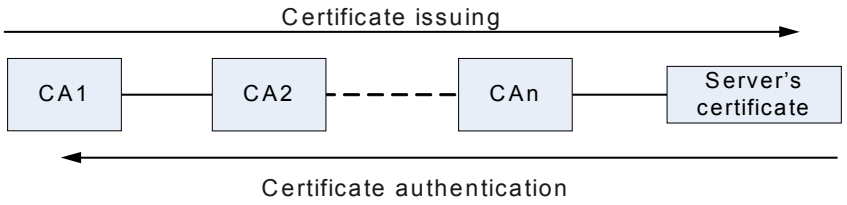
  For example, if CA1 is the root CA and issues a certificate for CA2, CA2 then issues a certificate for CA3. This process continues until the final server certificate is issued.

  Assume that CA3 issues the server certificate. A certificate authentication process on the client starts from server certificate authentication:

  - The client first verifies validity of the server certificate based on the CA3 certificate.
  - The client then checks CA2 certificate to verify validity of the CA3 certificate.
  - The client then checks CA1 certificate to verify validity of the CA2 certificate.
  - The server certificate passes the authentication only when the CA2 certificate is verified valid by the CA1 certificate.

  Figure 7-1 shows the certificate issuing and authentication processes.

Figure 7-1 Certificate issuing and authentication



- **Certificate Revocation List (CRL)**

  A CRL is issued by a CA and specifies a list of certificates that have been revoked. It should not be strongly relied upon.

  Each digital certificate has a limited lifetime and a CA can revoke a digital certificate to shorten its lifetime. The validity period of a certificate specified in the CRL is shorter than the original validity period of the certificate. If a CA revokes a digital certificate, the key pair defined in the certificate can no longer be used even if the digital certificate does not expire. When a certificate expires, it is deleted from the CRL to shorten it.

You can load the CRL and a certificate (trust certificate) with a higher level than the digital certificate on your PC. If not loaded, you are prompted to trust the server when establishing a connection with a web server. Once the connection is established successfully, the PC cannot immediately verify the digital certificate on the server. However, the confidentiality of data transmitted between the PC and server is ensured. To ensure that you are connecting to a valid web server, you can load a trust certificate and CRL on the PC. For details on how to load trust certificates, refer to the help information in the operating system.

7.2 Web System Login Configuration Tasks

You can configure login through the web system in simple mode or secure mode.

Table 7-1 describes configuration tasks of web system login.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 7-1 Configuration tasks of web system login

Scenario	Description	Section
Simple Mode Configure device login through the web system	The device provides a default SSL policy, and the web page file contains a randomly generated self-signed certificate. If the default SSL policy and self-signed certificate meet security requirements, you do not need to upload a digital certificate or configure an SSL policy. The configuration of this mode is simple but brings security risks. It applies to scenarios that do not have high security requirements.	**7.4 Configuring Device Login Through the Web System (Simple Mode)**
Secure Mode Configure device login through the web system	This mode requires more complex configuration but provides high security. It is recommended that you use this mode to configure device login through the web system. This mode involves manually configuring an SSL policy and helps ensure security.	**7.5 Configuring Device Login Through the Web System (Secure Mode)**
Configure access control on web users	To enhance security, you can configure access control on web users to specify clients that can log in to the device through the web system.	**7.6 Configuring Access Control on Web Users**

NOTE

The device does not provide lifetime management for the self-signed digital certificate, such as update and revocation. To ensure device and certificate security, it is recommended that you replace the self-signed certificate with a certificate authority (CA) certificate.

7.3 Web System Login Default Configuration

Table 7-2 lists the default configuration of web system login.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 7-2 Default configuration of web system login

Parameter	Default Setting
Web page file integrated into system software	Supported
Default SSL policy	Supported
HTTPS service	HTTPS IPv4: enabled HTTPS IPv6: disabled
Port number of the HTTPS server	443
Timeout period of an HTTPS connection	20 minutes
Web user	By default, the local user **admin** exists in the system, with the password **admin@huawei.com**, user level 0, and service type **http**.
Access control on web users	None

7.4 Configuring Device Login Through the Web System (Simple Mode)

Pre-configuration Tasks

Before configuring login through the web system (simple mode), configure a reachable route between a terminal and the device.

Configuration Process

The following configuration tasks must be performed in sequence.

7.4.1 Uploading and Loading a Web Page File

Context

The system software of the device contains a web page file, and the web page file is pre-loaded to the device before delivery. If you use this web page file, you do not need to perform the following configuration. To upgrade the web page file on the device, log in to Huawei official website to download an independent web page file, upload and load the file to the device.

NOTE

To obtain a web page file, visit **http://support.huawei.com/enterprise** and download the software package containing the web page file based on the product name and version. The file is named in the format **product name-software version number.web file version number.web.7z**.

After downloading the file, compare the downloaded web page file with that on the website to check whether their sizes are the same. If not, an error may occur during file download. Download the file again.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Upload the web page file.

You can upload the web page file using SFTP or other modes. For details, see **8.3 Local File Management**.

NOTE

After the file is uploaded to the device, run the **dir** command in the user view to check whether the uploaded file has the same size as that on the file server. If not, an error may occur during file upload. Upload the file again.

Step 2 Load the web page file.

1. Run the **system-view** command to enter the system view.
2. Run the **http server load** { *file-name* | **default** } command to load the web page file.

   By default, the web page file in system software is pre-loaded on the device.

   If **default** is specified, the web page file in the system software is loaded. If *file-name* is specified, an independent web page file is loaded.

   NOTE

   If the system software is upgraded from V200R006 or an earlier version to V200R007 or a later version, but the target software version conflicts with the configuration file for next startup, the device will cancel the configuration of loading the web page file in the original system software after the upgrade, and load the web page file integrated in the new system software by default.

----End

7.4.2 Enabling the HTTPS Service

Context

You can only log in to the web system after the HTTPS service is enabled. To enhance device security, you can change the port number of the HTTPS server to prevent attackers from accessing the server using the default port number. You can also save resources by setting a timeout period for an HTTPS connection when operations are not being performed.

By default, only the HTTPS IPv4 service (not HTTPS IPv6) is enabled on a device. On the HTTPS server, port 443 is used, the timeout period of an HTTPS connection is 20 minutes, and login requests from all interfaces are accepted. If you use the HTTPS IPv4 service, default port number, default timeout period, and accept login requests from all interfaces, do not perform the following configuration. To use the HTTPS IPv6 service, you need to enable it first.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
http [ ipv6 ] secure-server enable
```

The HTTPS service is enabled.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

By default, the HTTPS IPv4 service is enabled on a device while the HTTPS IPv6 service is disabled.

Step 3 Run:

```
http [ ipv6 ] secure-server port port-number
```

The port number of the HTTPS server is specified.

The default port number of the HTTPS server is 443.

Step 4 Run:

```
http server-source -i loopback interface-number
```

A loopback interface is specified as the source interface of the HTTPS server.

Before specifying a source interface for an HTTPS server, ensure that the loopback interface has been created. If not, the **http server-source** command cannot be executed.

Step 5 Run:

```
http timeout timeout
```

A timeout period is set for HTTPS connections.

The default timeout period is 20 minutes.

----End

7.4.3 Configuring a Web User and Logging In to the Web System

Context

A web user account can be configured based on the user name, password, level, and access type. After configuration, you can log in to the web system. Enter the user name and password to log in to a web system.

Procedure

Step 1 Configure a web user.

1. Run:

   ```
   system-view
   ```

   The system view is displayed.

2. Run:

   ```
   aaa
   ```

   The AAA view is displayed.

3. Run:

   ```
   local-user user-name password irreversible-cipher password
   ```

   A local user name and a password are configured.

   By default, the local user **admin** exists in the system, with the password **admin@huawei.com**.

4. Run:

   ```
   local-user user-name service-type http
   ```

   The access type of the local user is set to **HTTP**

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

By default, no access type is configured for a local user.

5. Run:

```
local-user user-name privilege level level
```

The local user level is set.

By default, the user level of the local user **admin** is 0, indicating a monitoring user.

Only level 3 users and higher are administrators with management rights. Level 2 users and below are monitoring users. Administrator users have all operation rights of a web page, and monitoring users can only perform ping and tracert operations.

After logging in to the web system, monitoring users receive a message, showing their current level and prompts them to raise their user level. **Figure 7-2** and **Figure 7-3** show the message displayed on the Classics and EasyOperation versions.

Figure 7-2 Message received by a monitoring user logging in to the Classics web system

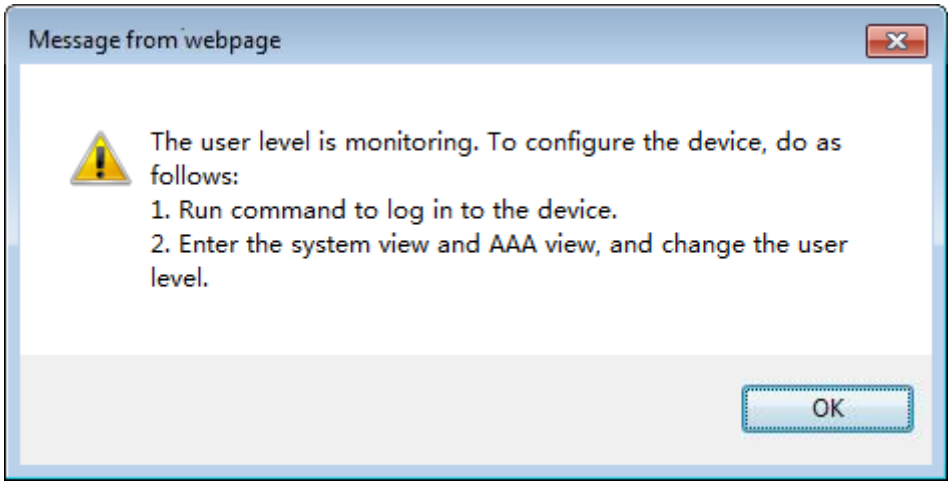
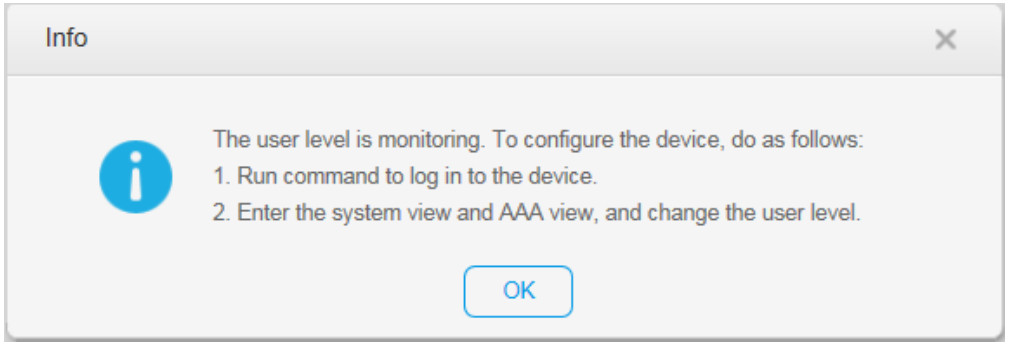


Figure 7-3 Message received by a monitoring user logging in to the EasyOperation web system



Step 2 Log in to the web system.

1. Open the web browser on a PC, enter **https:// *IP address*** in the address box, and press **Enter**. The web system login page is displayed. Enter the web user name and password and select a language for the web system, as shown in **Figure 7-4**.

   IP address specifies the device's management IP address, which can be an IPv4 or IPv6 address, depending on the HTTPS service type.

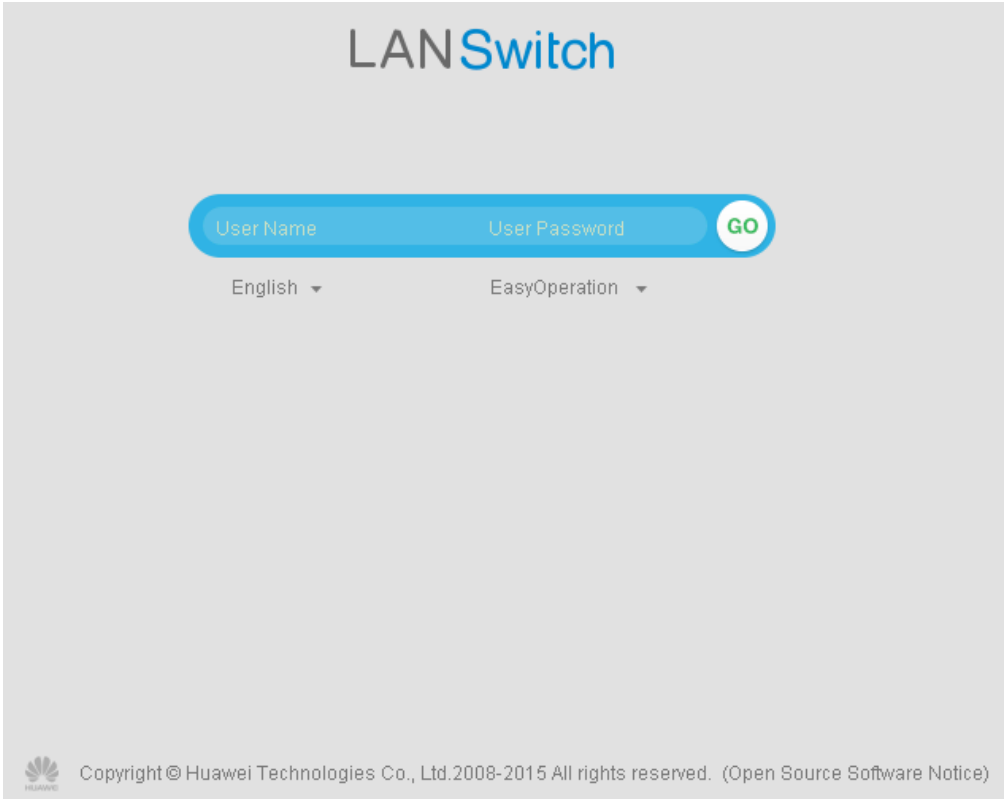
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

To ensure compatibility, a user logging in through HTTP is redirected to **https:// *IP address*** if the user enters **http:// *IP address*** in the address box.

Figure 7-4 Web system login page



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

- The operating system required for web system login must be the Windows 7.0, Windows 8.0, Windows 8.1, or iOS operating system. The iOS operating system supports only login to the EasyOperation web system, but does not support file uploading and downloading.
- The EasyOperation web system supports Internet Explorer 10.0 – 11.0, Firefox35.0 – 43.0, and Google Chrome 34.0 – 48.0. The Classics web system supports Internet Explorer 10.0 – 11.0 and Firefox35.0 – 43.0. In addition, JavaScript must be enabled in the browser. If your browser is not supported, the web page may be displayed incorrectly.
- When logging in to the web system using the Internet Explorer, ensure that active scripting in the **Security** tab page is enabled; otherwise, an exception may occur during web system login.
- The best resolution of the display for web system login is 1316px. If the resolution is less than 1280px, the system displays a prompt message.
- By default, the earliest SSL version used in SSL policies on the device is TLS1.1. When logging in to the device through the web system, ensure that the SSL version supported by the browser is the same as that supported by the device; otherwise, an exception may occur during web system login. It is recommended that you upgrade the browser based on the displayed page or modify the SSL configuration. Take the Internet Explorer as an example. Choose **Tools** > **Internet Options**, and click the **Advanced** tab to view and select the SSL version.
- If you use Internet Explorer 8.0 running on Windows XP to log in to the web system, you must configure the RC4 algorithm for the customized SSL cipher suite policy. Otherwise, you will be unable to log in to the web system. To perform this configuration, run the **set cipher-suite** { **tls1_ck_rsa_with_aes_256_sha** | **tls1_ck_rsa_with_aes_128_sha** | **tls1_ck_rsa_rc4_128_sha** | **tls1_ck_dhe_rsa_with_aes_256_sha** | **tls1_ck_dhe_dss_with_aes_256_sha** | **tls1_ck_dhe_rsa_with_aes_128_sha** | **tls1_ck_dhe_dss_with_aes_128_sha** | **tls12_ck_rsa_aes_256_cbc_sha256** } command.
- The web system identifies card information based on the **Item** value in the device's electronic label, but the device hardware driver determines whether to start the device based on the **BarCode** value. Since the values of **BarCode** and **Item** may not be the same, the web system may not read or display the card information.
- If you do not perform any operation after logging in to the web system, you cannot click the back button on the browser to return to the previous page.
- If you log in to the Web systems with the same IP address through multiple windows on a browser, only the latest login is saved. If the Web systems have the same IP address and the same port number, the latest login account is displayed on earlier web pages after all the windows are refreshed. If the Web systems have the same IP address but different port numbers, timeout messages are displayed on earlier web pages after all the windows are refreshed.
- If the software version of the device changes (for example, the device software is upgraded or rolled back), clear the browser cache before using the web system. Otherwise, the web page may be displayed incorrectly.
- You can click **Open Source software Notice** to view details of the open source software notice.

2. Select the layout of the web system.

   The EasyOperation version provides rich graphics and a more user-friendly UI on which users can perform monitoring, configuration, maintenance, and other network operations. The Classics version inherits the web page style of Huawei switches and provides comprehensive configuration and management functions.

   The EasyOperation version is used by default.

3. Access the password change page of the web system.

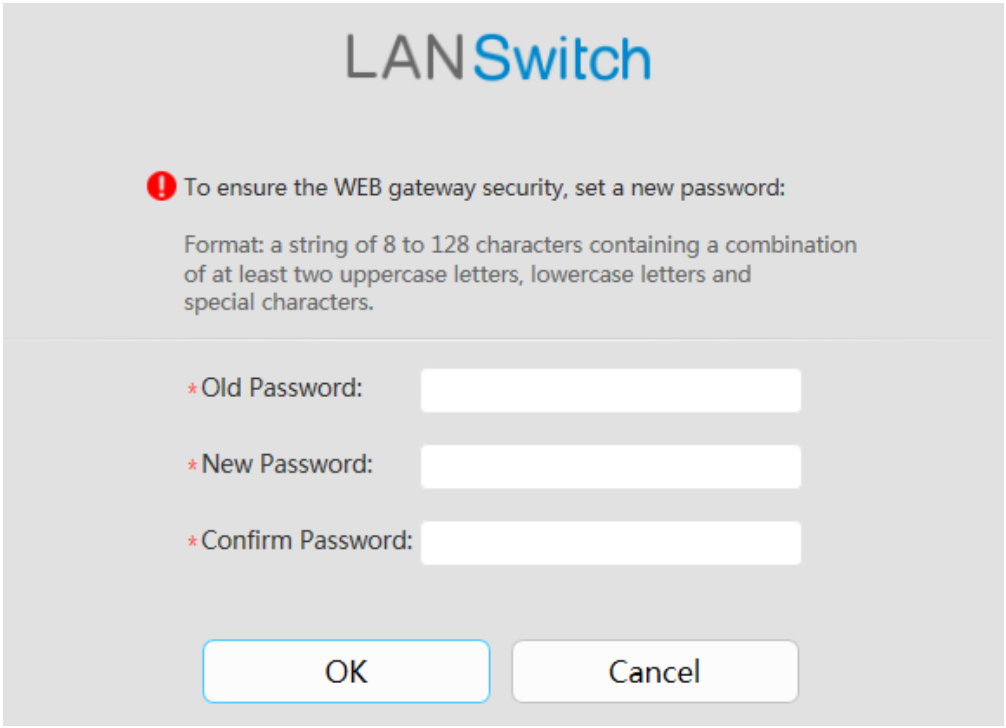
   On the web system login page, click **GO** or press **Enter** to access the password change page, as shown in **Figure 7-5**. Change the password and re-log in to the web system as prompted. You can manage and maintain the device after logging in to the web system.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 7-5 Password change page of the web system



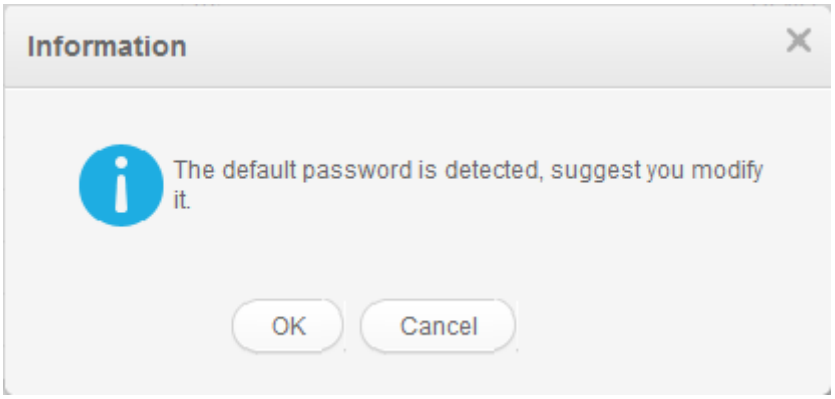
NOTE

- The password change page is displayed during the login process only the first time you log in to the web system.
- The password change page is also displayed if your password will expire or has expired. To access the web system main page, you must change the password.
- To improve security, a password must contain at least two types of the following: lowercase letters, uppercase letters, digits, and special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').

4. (Optional) Change the default user password.

   If you are logged in as an administrator and the password of the default user **admin** is **admin@huawei.com**, the system prompts you to change this password. **Figure 7-6** shows the prompt. Click **Confirm** to display the **User Management** page on which you can change the password of the default user. Changing this password is recommended to improve security.

Figure 7-6 Changing the default user



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

- Only when you log in to the web system as an administrator user (level 3 or higher), the dialog box is displayed.
- A secure password should contain at least two types of the following: lowercase letters, uppercase letters, numerals, special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').

----End

7.4.4 Checking the Configuration of Configuring Device Login Through the Web System (Simple Mode)

Context

After completing the configuration, run the following commands in any view on the CLI to check information about online web users and the HTTPS server.

Procedure

- Run the **display http user** [**username** *username*] command to check online web user information.
- Run the **display http server** command to check current HTTPS server information.

----End

7.5 Configuring Device Login Through the Web System (Secure Mode)

Pre-configuration Tasks

Before configuring login through the web system (secure mode), complete the following tasks:

- Configure a reachable route between a terminal and the device.
- Obtain a digital certificate and private key file from the CA.

Configuration Process

The following configuration tasks must be performed in sequence.

7.5.1 Uploading and Loading a Web Page File

Context

The system software of the device contains a web page file, and the web page file is pre-loaded to the device before delivery. If you use this web page file, you do not need to perform the following configuration. To upgrade the web page file on the device, log in to Huawei official website to download an independent web page file, upload and load the file to the device.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

To obtain a web page file, visit **http://support.huawei.com/enterprise** and download the software package containing the web page file based on the product name and version. The file is named in the format **product name-software version number.web file version number.web.7z**.

After downloading the file, compare the downloaded web page file with that on the website to check whether their sizes are the same. If not, an error may occur during file download. Download the file again.

Procedure

Step 1 Upload the web page file.

You can upload the web page file using SFTP or other modes. For details, see **8.3 Local File Management**.

NOTE

After the file is uploaded to the device, run the **dir** command in the user view to check whether the uploaded file has the same size as that on the file server. If not, an error may occur during file upload. Upload the file again.

Step 2 Load the web page file.

1. Run the **system-view** command to enter the system view.
2. Run the **http server load** { *file-name* | **default** } command to load the web page file.

   By default, the web page file in system software is pre-loaded on the device.

   If **default** is specified, the web page file in the system software is loaded. If *file-name* is specified, an independent web page file is loaded.

   NOTE

   If the system software is upgraded from V200R006 or an earlier version to V200R007 or a later version, but the target software version conflicts with the configuration file for next startup, the device will cancel the configuration of loading the web page file in the original system software after the upgrade, and load the web page file integrated in the new system software by default.

----End

7.5.2 Configuring an SSL Policy and Loading a Digital Certificate

Context

To provide enhanced security, you can acquire a trust digital certificate and private key file from the CA and manually configure an SSL policy.

The device supports certificates in PEM, ASN1, and PFX formats. Certificates have the same content regardless of format.

- The PEM (.pem) digital certificate is most commonly used. It applies to text transmission between systems.
- The ASN1 (.der) format is a universal digital certificate format and the default format for most browsers.
- The PFX (.pfx) format is a universal digital certificate format and a binary format that can be converted into PEM or ASN1 format.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Upload the digital certificate and private key file.

You can upload the digital certificate and private key file using SFTP or other modes and save them to the **security** directory. If this directory does not exist, run the **mkdir security** command to create it. For procedure on uploading files, see **8.3 Local File Management**.

NOTE

After the files are uploaded to the device, run the **dir** command in the user view to check if the uploaded files are the same size as those on the file server. If not, an error may have occurred. Upload the files again.

Step 2 Configure an SSL policy and load the digital certificate.

1. Run:

```
system-view
```

The system view is displayed.

2. (Optional) Customize SSL cipher suite.

a. Run:

```
ssl cipher-suite-list customization-policy-name
```

An SSL cipher suite policy is customized and the view of the cipher suite policy is displayed. If the SSL cipher suite policy already exists, the command directly displays its view.

By default, no customized SSL cipher suite policy is configured.

To improve system security, the device only supports secure algorithms. To improve compatibility, the device also allows you to customize cipher suite policies. To customize a cipher suite policy, run the **ssl cipher-suite** command.

b. Run:

```
set cipher-suite { tls1_ck_rsa_with_aes_256_sha |
tls1_ck_rsa_with_aes_128_sha | tls1_ck_rsa_rc4_128_sha |
tls1_ck_dhe_rsa_with_aes_256_sha | tls1_ck_dhe_dss_with_aes_256_sha |
tls1_ck_dhe_rsa_with_aes_128_sha | tls1_ck_dhe_dss_with_aes_128_sha |
tls12_ck_rsa_aes_256_cbc_sha256 }
```

The cipher suite for a customized SSL cipher suite policy is configured.

By default, no customized SSL cipher suite policy is configured.

To configure cipher suites for a customized SSL cipher suite policy, run the **ssl cipher-suite-list** command.

If a customized SSL cipher suite policy is being referenced by an SSL policy, the cipher suites in the customized cipher suite policy can be added, modified, or partially deleted. Deleting all of the cipher suites is not allowed.

c. Run:

```
quit
```

Return to the system view.

3. Run:

```
ssl policy policy-name
```

An SSL policy is created and the SSL policy view is displayed.

4. (Optional) Run:

```
ssl minimum version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 }
```

The minimum version of an SSL policy is set.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

By default, the minimum version of an SSL policy is TLS1.1.

5. (Optional) Run:

```
binding cipher-suite-customization customization-policy-name
```

A customized SSL cipher suite policy is bound to an SSL policy.

By default, no customized cipher suite policy is bound to an SSL policy. Each SSL policy uses a default cipher suite.

After a customized cipher suite policy is unbound from an SSL policy, the SSL policy uses one of the following default cipher suites:

- tls1_ck_rsa_with_aes_256_sha
- tls1_ck_rsa_with_aes_128_sha
- tls1_ck_dhe_rsa_with_aes_256_sha
- tls1_ck_dhe_dss_with_aes_256_sha
- tls1_ck_dhe_rsa_with_aes_128_sha
- tls1_ck_dhe_dss_with_aes_128_sha
- tls12_ck_rsa_aes_256_cbc_sha256

After a customized SSL cipher suite policy is bound to an SSL policy, the device uses an algorithm in the specified cipher suite to perform SSL negotiation.

The customized cipher suite policy to be bound to an SSL policy contains cipher suites.

If the cipher suite contains only one type of algorithm (RSA or DSS), the corresponding certificate must be loaded for the SSL policy. This facilitates SSL negotiation.

6. Load the digital certificate and specify the private key file.

Only one certificate or certificate chain can be loaded to an SSL policy. (A certificate chain is a list of trust certificates, starting from end entity's certificate and ending at the root CA certificate.) If a certificate or certificate chain has been loaded, run the **undo certificate load** command to unload the old certificate or certificate chain before loading a new one. Select the corresponding configuration based on the certificate type.

NOTE

When loading a certificate or certificate chain to an SSL policy, ensure that the length of the key pair in the certificate or certificate chain does not exceed 2048 bits. If the key pair length exceeds 2048 bits, the certificate or certificate chain cannot be uploaded to the device.

- Load a PEM certificate or certificate chain. Run either of the following commands based on whether a user obtains a digital certificate or certificate chain from the CA.
  - Run:

    ```
    certificate load pem-cert cert-filename key-pair { dsa | rsa } key-file key-filename auth-code cipher auth-code
    ```

    A PEM digital certificate is loaded and the private key file is specified.
  - Run:

    ```
    certificate load pem-chain cert-filename key-pair { dsa | rsa } key-file key-filename auth-code cipher auth-code
    ```

    A PEM certificate chain is loaded and the private key file is specified.
- Run:

  ```
  certificate load asn1-cert cert-filename key-pair { dsa | rsa } key-file key-filename
  ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

An ASN1 digital certificate is loaded and the private key file is specified.

- Run:

```
certificate load pfx-cert cert-filename key-pair { dsa | rsa } { mac
cipher mac-code | key-file key-filename } auth-code cipher auth-code
```

A PFX digital certificate is loaded and the private key file is specified.

NOTE

Before rolling V200R008 or a later version back to an earlier version, back up the SSL private key file.

----End

7.5.3 Enabling the HTTPS Service

Context

Enabling HTTPS service enhances device security, and preserves resources during timeout periods. To log in to the web system in secure mode, bind an SSL policy to the device and enable the HTTPS service. You can change the port number of the HTTPS server to prevent attackers from accessing the server using the default port number. In addition, you can set a timeout period for an HTTPS connection to prevent waste of web channel resources.

By default, only the HTTPS IPv4 service (not HTTPS IPv6) is enabled on a device. On the HTTPS server, port 443 is used, the timeout period of an HTTPS connection is 20 minutes, and login requests from all interfaces are accepted. If you use the HTTPS IPv4 service, default port number, default timeout period, and accept login requests from all interfaces, you only need to bind an SSL policy to the device. To use the HTTPS IPv6 service, you need to enable it first.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
http secure-server ssl-policy policy-name
```

An SSL policy is bound to the device.

policy-name specifies the SSL policy created in **7.5.2 Configuring an SSL Policy and Loading a Digital Certificate**.

Step 3 Run:

```
http [ ipv6 ] secure-server enable
```

The HTTPS service is enabled.

By default, the HTTPS IPv4 service is enabled on a device while the HTTPS IPv6 service is disabled.

Step 4 Run:

```
http [ ipv6 ] secure-server port port-number
```

The port number of the HTTPS server is specified.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

The default port number of the HTTPS server is 443.

Step 5 Run:

```
http server-source -i loopback interface-number
```

A loopback interface is specified as the source interface of the HTTPS server.

Before specifying a source interface for an HTTPS server, ensure that the loopback interface has been created. If the loopback interface is not created, the **http server-source** command cannot be correctly executed.

Step 6 Run:

```
http timeout timeout
```

A timeout period is set for HTTPS connections.

The default timeout period is 20 minutes.

----End

7.5.4 Configuring a Web User and Logging In to the Web System

Context

A web user account can be configured based on the user name, password, level, and access type. After configuration, you can log in to the web system. Enter the user name and password to log in to a web system.

Procedure

Step 1 Configure a web user.

1. Run:

   ```
   system-view
   ```

   The system view is displayed.

2. Run:

   ```
   aaa
   ```

   The AAA view is displayed.

3. Run:

   ```
   local-user user-name password irreversible-cipher password
   ```

   A local user name and a password are configured.

   By default, the local user **admin** exists in the system, with the password **admin@huawei.com**.

4. Run:

   ```
   local-user user-name service-type http
   ```

   The access type of the local user is set to **HTTP**

   By default, no access type is configured for a local user.

5. Run:

   ```
   local-user user-name privilege level level
   ```

   The local user level is set.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

By default, the user level of the local user **admin** is 0, indicating a monitoring user.

Only level 3 users and higher are administrators with management rights. Level 2 users and below are monitoring users. Administrator users have all operation rights of a web page, and monitoring users can only perform ping and tracert operations.

After logging in to the web system, monitoring users receive a message, showing their current level and prompts them to raise their user level. **Figure 7-7** and **Figure 7-8** show the message displayed on the Classics and EasyOperation versions.

Figure 7-7 Message received by a monitoring user logging in to the Classics web system

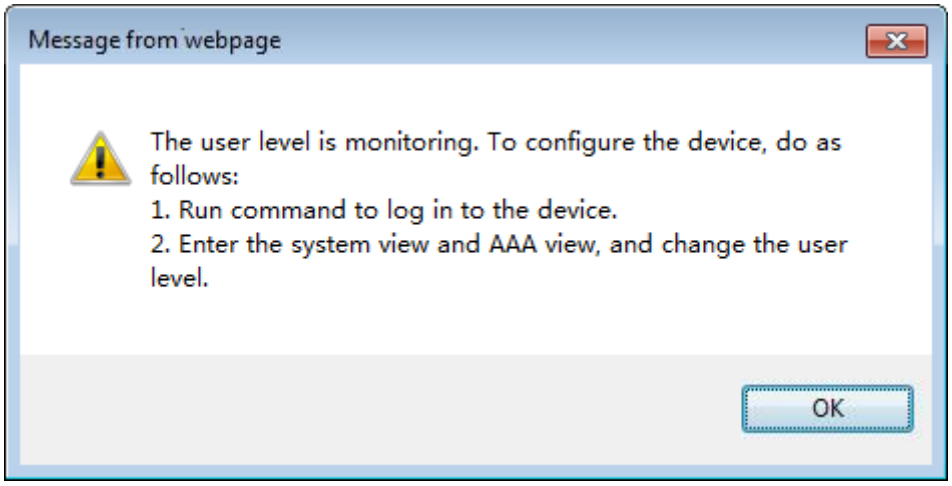
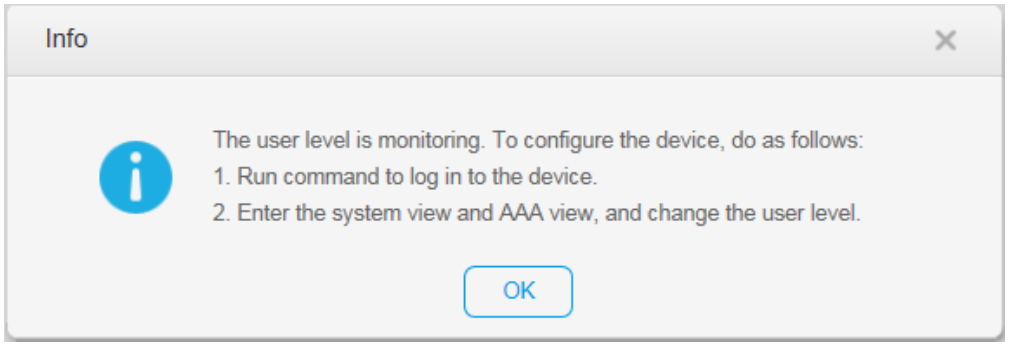


Figure 7-8 Message received by a monitoring user logging in to the EasyOperation web system



Step 2 Log in to the web system.

1. Open the web browser on a PC, enter **https:// *IP address*** in the address box, and press **Enter**. The web system login page is displayed. Enter the web user name and password and select a language for the web system, as shown in **Figure 7-9**.

   IP address specifies the device's management IP address, which can be an IPv4 or IPv6 address, depending on the HTTPS service type.

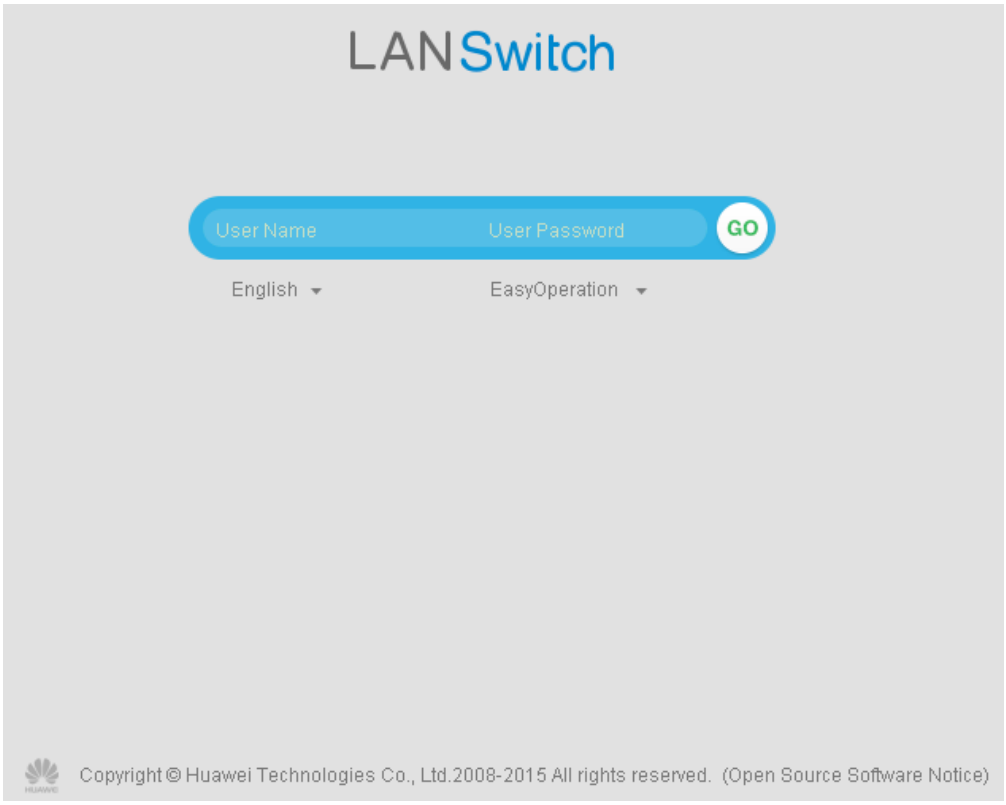
   To ensure compatibility, a user logging in through HTTP is redirected to **https:// *IP address*** if the user enters **http:// *IP address*** in the address box.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 7-9 Web system login page



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

- The operating system required for web system login must be the Windows 7.0, Windows 8.0, Windows 8.1, or iOS operating system. The iOS operating system supports only login to the EasyOperation web system, but does not support file uploading and downloading.
- The EasyOperation web system supports Internet Explorer 10.0 – 11.0, Firefox35.0 – 43.0, and Google Chrome 34.0 – 48.0. The Classics web system supports Internet Explorer 10.0 – 11.0 and Firefox35.0 – 43.0. In addition, JavaScript must be enabled in the browser. If your browser is not supported, the web page may be displayed incorrectly.
- When logging in to the web system using the Internet Explorer, ensure that active scripting in the **Security** tab page is enabled; otherwise, an exception may occur during web system login.
- The best resolution of the display for web system login is 1316px. If the resolution is less than 1280px, the system displays a prompt message.
- By default, the earliest SSL version used in SSL policies on the device is TLS1.1. When logging in to the device through the web system, ensure that the SSL version supported by the browser is the same as that supported by the device; otherwise, an exception may occur during web system login. It is recommended that you upgrade the browser based on the displayed page or modify the SSL configuration. Take the Internet Explorer as an example. Choose **Tools** > **Internet Options**, and click the **Advanced** tab to view and select the SSL version.
- If you use Internet Explorer 8.0 running on Windows XP to log in to the web system, you must configure the RC4 algorithm for the customized SSL cipher suite policy. Otherwise, you will be unable to log in to the web system. To perform this configuration, run the **set cipher-suite** { **tls1_ck_rsa_with_aes_256_sha** | **tls1_ck_rsa_with_aes_128_sha** | **tls1_ck_rsa_rc4_128_sha** | **tls1_ck_dhe_rsa_with_aes_256_sha** | **tls1_ck_dhe_dss_with_aes_256_sha** | **tls1_ck_dhe_rsa_with_aes_128_sha** | **tls1_ck_dhe_dss_with_aes_128_sha** | **tls12_ck_rsa_aes_256_cbc_sha256** } command.
- The web system identifies card information based on the **Item** value in the device's electronic label, but the device hardware driver determines whether to start the device based on the **BarCode** value. Since the values of **BarCode** and **Item** may not be the same, the web system may not read or display the card information.
- If you do not perform any operation after logging in to the web system, you cannot click the back button on the browser to return to the previous page.
- If you log in to the Web systems with the same IP address through multiple windows on a browser, only the latest login is saved. If the Web systems have the same IP address and the same port number, the latest login account is displayed on earlier web pages after all the windows are refreshed. If the Web systems have the same IP address but different port numbers, timeout messages are displayed on earlier web pages after all the windows are refreshed.
- If the software version of the device changes (for example, the device software is upgraded or rolled back), clear the browser cache before using the web system. Otherwise, the web page may be displayed incorrectly.
- You can click **Open Source software Notice** to view details of the open source software notice.

2. Select the layout of the web system.

   The EasyOperation version provides rich graphics and a more user-friendly UI on which users can perform monitoring, configuration, maintenance, and other network operations. The Classics version inherits the web page style of Huawei switches and provides comprehensive configuration and management functions.

   The EasyOperation version is used by default.

3. Access the password change page of the web system.

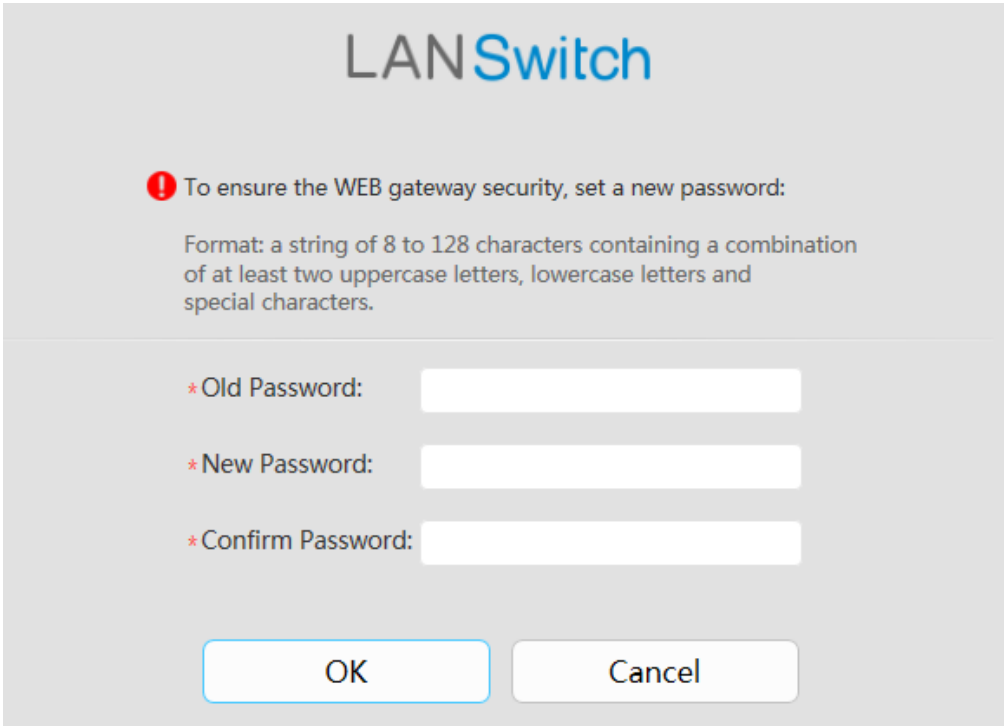
   On the web system login page, click **GO** or press **Enter** to access the password change page, as shown in **Figure 7-10**. Change the password and re-log in to the web system as prompted. You can manage and maintain the device after logging in to the web system.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 7-10 Password change page of the web system



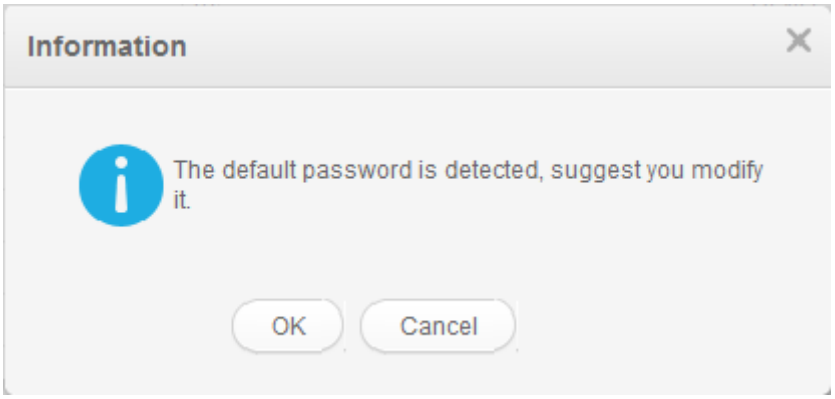
NOTE

- The password change page is displayed during the login process only the first time you log in to the web system.
- The password change page is also displayed if your password will expire or has expired. To access the web system main page, you must change the password.
- To improve security, a password must contain at least two types of the following: lowercase letters, uppercase letters, digits, and special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').

4. (Optional) Change the default user password.

   If you are logged in as an administrator and the password of the default user **admin** is **admin@huawei.com**, the system prompts you to change this password. **Figure 7-11** shows the prompt. Click **Confirm** to display the **User Management** page on which you can change the password of the default user. Changing this password is recommended to improve security.

Figure 7-11 Changing the default user



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

- Only when you log in to the web system as an administrator user (level 3 or higher), the dialog box is displayed.
- A secure password should contain at least two types of the following: lowercase letters, uppercase letters, numerals, special characters (such as ! $ # %). In addition, the password cannot contain spaces or single quotation marks (').

----End

7.5.5 Checking the Configuration of Configuring Device Login Through the Web System (Secure Mode)

Context

After completing the configuration, run the following commands in any view on the CLI to check information about the SSL policy, loaded digital certificate, online web users, and current HTTPS server.

Procedure

- Run the **display ssl policy** [*policy-name*] command to check the configured SSL policy and loaded digital certificate.
- Run the **display http user** [**username** *username*] command to check online web user information.
- Run the **display http server** command to check current HTTPS server information.

----End

7.6 Configuring Access Control on Web Users

Context

To further enhance security, you can configure an HTTPS access control list to allow only specified web users to log in to the device. Commands can also be run to force idle users from occupying resources for too long.

ACL/ACL6 rules:

- If the ACL/ACL6 rule is **permit**, clients matching the rule are permitted to set up HTTPS connections with the local device.
- If the ACL/ACL6 rule is **deny**, clients matching the rule are forbidden to set up HTTPS connections with the local device.
- If an ACL/ACL6 rule is configured but packets from a client do not match the rule, the client is not allowed to set up HTTPS connections with the local device.
- If no ACL/ACL6 rule is configured, any clients are permitted to set up HTTPS connections with the local device.

Procedure

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

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 2 Configure an ACL/ACL6 on the HTTPS server.

- Configure an HTTPS IPv4 ACL as follows:
  a. Run the **acl** [**number**] *acl-number* command to enter the ACL view.

     HTTPS IPv4 supports basic and advanced ACLs. If a basic ACL is configured, the value of *acl-number* ranges from 2000 to 2999. If an advanced ACL is configured, the value of *acl-number* ranges from 3000 to 3999.
  b. Configure an ACL.

     The commands for configuring basic and advanced ACLs are different.
     - Command for configuring a basic ACL:

       rule [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *
     - Command for configuring an advanced ACL:

       rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *
  c. Run the **quit** command to return to the system view.
  d. Run the **http acl** *acl-number* command to configure an HTTPS IPv4 ACL.

     By default, no ACL is configured on the HTTPS IPv4 server, that is, all web clients can set up HTTPS IPv4 connections with the server.
- Configure an HTTPS IPv6 ACL6 as follows:
  a. Run the **acl ipv6** [**number**] *acl6-number* command to enter the ACL6 view.

     HTTPS IPv6 supports basic and advanced ACL6s. If a basic ACL6 is configured, the value of *acl6-number* ranges from 2000 to 2999. If an advanced ACL6 is configured, the value of *acl6-number* ranges from 3000 to 3999.
  b. Configure an ACL6.

     The commands for configuring basic and advanced ACL6s are different.
     - Command for configuring a basic ACL6:

       rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *
     - Command for configuring an advanced ACL6:

       rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

c. Run the **quit** command to return to the system view.

d. Run the **http ipv6 acl** *acl-number* command to configure an HTTPS IPv6 ACL.

By default, no ACL6 is configured on the HTTPS IPv6 server, that is, all web clients can set up HTTPS IPv6 connections with the server.

Step 3 (Optional) Run the **free http user-id** *user-id* command to force a web user offline.

Currently, the device supports a maximum of five concurrent online web users. The value of *user-id* ranges from 89 to 93. If a user occupies the web channel resources but performs no operation in a long time, other users may fail to log in. To prevent this situation, run the command to force idle web users to go offline and release the occupied channel resources.

----End

7.7 Web System Login Configuration Examples

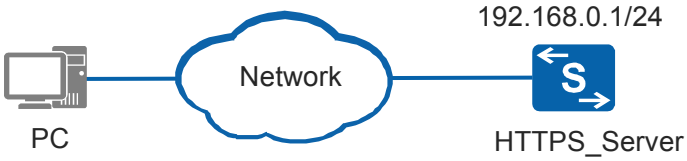
7.7.1 Example for Configuring Device Login Through the Web System (Secure Mode)

Networking Requirements

As shown in **Figure 7-12**, the device functions as an HTTPS server (an HTTPS IPv4 server is used as an example here) and is reachable to the PC. The management IP address of the HTTPS server is 192.168.0.1/24.

Users want to manage and maintain the device through the web system and have high security requirements. They have obtained the server digital certificate **1_servercert_pem_dsa.pem** and private key file **1_serverkey_pem_dsa.pem** from the CA.

Figure 7-12 Networking diagram for configuring device login through the web system (secure mode)



Configuration Roadmap

Loading an independent web page file is used as an example here. The configuration roadmap is as follows:

1. Securely upload necessary files to the server through SFTP, including the web page file, server digital certificate, and private key file.
2. Load the web page file and digital certificate.
3. Bind an SSL policy and enable the HTTPS service.
4. Configure a web user and enter the web login page.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Upload files to the device through SFTP.

Generate a local key pair on the server and enable the SFTP server function.

```
<HUAWEI> system-view
[HUAWEI] sysname HTTPS-Server
[HTTPS-Server] dsa local-key-pair create
Info: The key name will be: HTTPS-Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:2048
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
[HTTPS-Server] sftp server enable
```

Configure the VTY user interface on the server.

```
[HTTPS-Server] user-interface vty 0 4
[HTTPS-Server-ui-vty0-4] authentication-mode aaa
[HTTPS-Server-ui-vty0-4] protocol inbound ssh
[HTTPS-Server-ui-vty0-4] quit
```

Configure an SSH user, including its authentication mode, service type, service authorized directory and password, user level, and access type.

```
[HTTPS-Server] ssh user client001 authentication-type password
[HTTPS-Server] ssh user client001 service-type sftp
[HTTPS-Server] ssh user client001 sftp-directory flash:
[HTTPS-Server] aaa
[HTTPS-Server-aaa] local-user client001 password irreversible-cipher
Helloworld@6789
[HTTPS-Server-aaa] local-user client001 privilege level 15
[HTTPS-Server-aaa] local-user client001 service-type ssh
[HTTPS-Server-aaa] quit
[HTTPS-Server] quit
```

Log in to the HTTPS server through SFTP from the terminal and upload the digital certificate and web page file to the server.

The SSH client software must be installed on the terminal before login. Third-party software OpenSSH and Windows Command Prompt window are used as examples here.

NOTE

- Ensure that the OpenSSH version you use is compatible with the terminal's operating system; otherwise, you may fail to log in to the switch through SFTP.
- For details on how to install OpenSSH, see the instruction of the software.
- You need to use OpenSSH commands for login through OpenSSH. For details on how to use the OpenSSH commands, see the help document of the software.
- OpenSSH commands can be used in the Windows Command Prompt window only after the OpenSSH software is installed.

Open the Windows Command Prompt window and run the **sftp client001@192.168.0.1** command to enter the working directory of the SFTP server. You can access the device through SFTP. (The following information is for reference only.)

```
C:\Documents and Settings\Administrator> sftp client001@192.168.0.1
Connecting to 192.168.0.1...
The authenticity of host '192.168.0.1 (192.168.0.1)' can't be established.
DSA 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 '192.168.0.1' (DSA) to the list of known hosts.
User Authentication
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
Password:
sftp>
```

Upload the digital certificate and web page file from the terminal to the server.

```
sftp> put web.7z
Uploading web.7z to /web.7z
web.7z                                100%   1308478   4.6KB/s   00:11
sftp> put 1_servercert_pem_dsa.pem
Uploading 1_servercert_pem_dsa.pem to /1_servercert_pem_dsa.pem
1_servercert_pem_dsa.pem              100%   1302      4.6KB/s   00:02
sftp> put 1_serverkey_pem_dsa.pem
Uploading 1_serverkey_pem_dsa.pem to /1_serverkey_pem_dsa.pem
1_serverkey_pem_dsa.pem               100%   951       4.6KB/s   00:01
```

Run the **dir** command on the device to check whether the digital certificate and web page file exist in the current storage directory.

NOTE

If the sizes of the digital certificate and web page file in the current storage directory are different from sizes of those on the server, an error may have occurred during file transfer. Upload the files again.

Create the subdirectory **security** on the server and copy the digital certificate and private key file to the subdirectory.

```
<HTTPS-Server> mkdir security
<HTTPS-Server> copy 1_servercert_pem_dsa.pem security
<HTTPS-Server> copy 1_serverkey_pem_dsa.pem security
```

Run the **dir** command in the **security** subdirectory to check the digital certificate.

```
<HTTPS-Server> cd security
<HTTPS-Server> dir
Directory of flash:/security/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-          1,302  Apr 13 2011 14:29:31   1_servercert_pem_dsa.pem
    1  -rw-            951  Apr 13 2011 14:29:49   1_serverkey_pem_dsa.pem

65,233 KB total (7,287 KB free)
```

Step 2 Load the web page file and digital certificate.

Load the web page file.

```
<HTTPS-Server> system-view
[HTTPS-Server] http server load web.7z
```

Create an SSL policy and load the PEM digital certificate.

```
[HTTPS-Server] ssl policy http_server
[HTTPS-Server-ssl-policy-http_server] certificate load pem-cert
1_servercert_pem_dsa.pem key-pair dsa key-file 1_serverkey_pem_dsa.pem auth-code
cipher 123456
[HTTPS-Server-ssl-policy-http_server] quit
```

After the preceding configurations are complete, run the **display ssl policy** command on the HTTPS server to check detailed information about the loaded certificate.

```
[HTTPS-Server] display ssl policy

       SSL Policy Name: http_server
     Policy Applicants: Config-Webs
         Key-pair Type: DSA
 Certificate File Type: PEM
      Certificate Type: certificate
  Certificate Filename: 1_servercert_pem_dsa.pem
     Key-file Filename: 1_serverkey_pem_dsa.pem
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
            Auth-code: ******
                  MAC:
             CRL File:
      Trusted-CA File:
          Issuer Name:
  Validity Not Before:
   Validity Not After:
```

Step 3 Bind an SSL policy to the device and enable the HTTPS service.

Bind an SSL policy to the device.

```
[HTTPS-Server] http secure-server ssl-policy http_server
```

Enable the HTTPS service.

```
[HTTPS-Server] http secure-server enable
```

Step 4 Configure a web user and enter the web login page.

Configure a web user.

```
[HTTPS-Server] aaa
[HTTPS-Server-aaa] local-user admin password irreversible-cipher Helloworld@6789
[HTTPS-Server-aaa] local-user admin privilege level 15
[HTTPS-Server-aaa] local-user admin service-type http
[HTTPS-Server-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.

Enter the web login page.

Open the web browser on the PC, enter https://192.168.0.1 in the address box, and press **Enter** to enter the web login page, as shown in **Figure 7-13**.

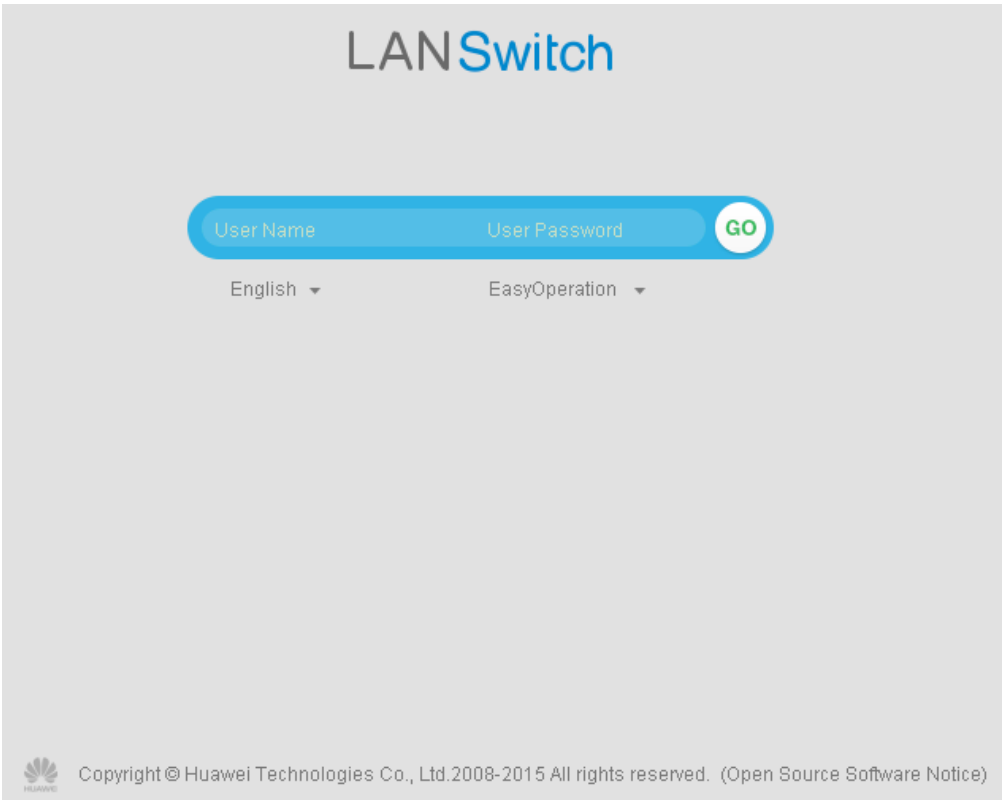
Enter the web user name and password and click **GO** or press **Enter** to enter the web system home page.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 7-13 Web system login page



Step 5 Verify the configuration.

After the configurations are complete, you can 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 the HTTPS server status.

```
[HTTPS-Server] display http server
   HTTP Server Status              : enabled
   HTTP Server Port                : 80(80)
   HTTP Timeout Interval           : 20
   Current Online Users            : 1
   Maximum Users Allowed           : 5
   HTTP Secure-server Status       : enabled
   HTTP Secure-server Port         : 443(443)
   HTTP SSL Policy                 : http_server
   HTTP IPv6 Server Status         : disabled
   HTTP IPv6 Server Port           : 80(80)
   HTTP IPv6 Secure-server Status  : disabled
   HTTP IPv6 Secure-server Port    : 443(443)
   HTTP server source address      : 0.0.0.0
```

----End

Configuration Files

HTTPS-Server configuration file

```
#
sysname HTTPS-Server
#
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
http server load web.7z
http secure-server ssl-policy http_server
#
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
 local-user client001 password irreversible-cipher %^%#L@[C7B11%"H&
\fS;qETS`zGI#RyJ%+A2KzP'.k[0tQ{=Cq5s43s&f^L\In6K%^%#
 local-user client001 privilege level 15
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
#
user-interface vty 0 4
 authentication-mode aaa
#
ssl policy http_server
 certificate load pem-cert 1_servercert_pem_dsa.pem key-pair dsa key-file
1_serverkey_pem_dsa.pem auth-code cipher %^%#0|:yF=]P~Afis516)rO,3Yu<@/3e]
KFg.q@LG50%%^%#
#
return
```

Related Content

Videos

Log In to a Switch Using the Web System.

Configure a Switch Using the Web System.

7.8 Web System Login Common Misconfigurations

7.8.1 Web System Login Failure

Symptom

In a web system login failure, the device and client can ping each other, but the device cannot be logged in through the web system.

Procedure

Step 1 Check whether the HTTPS service is enabled.

- HTTPS IPv4:

  By default, the HTTPS IPv4 service is enabled. Run the **display this** command in the system view to check whether the **undo http secure-server enable** command configuration exists. If it does, the HTTPS IPv4 service is disabled.

  You can run the **http secure-server enable** command in the system view to enable the HTTPS IPv4 service.

- HTTPS IPv6:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

By default, the HTTPS IPv6 service is disabled. You can run the **http ipv6 secure-server enable** command in the system view to enable the HTTPS IPv6 service.

Step 2 Check whether the number of online web users is at its the maximum.

Run the **display http user** command on the device to check whether the number of current online web users has reached 5.

Currently, the device supports a maximum of five concurrent online web users. If an idle user occupies web channel resources, other users may fail to log in. You can run the **free http user-id** *user-id* command to force the user offline.

Step 3 Check whether access control is configured for web users on the device.

- HTTPS IPv4:

  Run the **display this** command in the system view to check whether the **http acl** *acl-number* command configuration exists. If so, record the value of *acl-number*.

  Run the **display acl** *acl-number* command in any view to check whether the IPv4 address of the web client is denied in the ACL. If so, run the **undo rule** *rule-id* command in the ACL view to delete the **deny** rule. Then, modify the ACL and permit the IPv4 address of the web client.

- HTTPS IPv6:

  Run the **display this** command in the system view to check whether the **http ipv6 acl** *acl6-number* command configuration exists. If so, record the value of *acl6-number*.

  Run the **display acl ipv6** *acl6-number* command in any view to check whether the IPv6 address of the web client is denied in the ACL. If so, run the **undo rule** *rule-id* command in the ACL6 view to delete the **deny** rule. Then, modify the ACL6 and permit the IPv6 address of the web client.

Step 4 Check whether web user access type is correct.

Run the **display this** command in the AAA view to check whether the access type of the web user is HTTP. If **local-user** *user-name* **service-type http** exists in the command output, the access type of *user-name* is HTTP. If **local-user** *user-name* **service-type http** does not exist in the command output, run the **local-user** *user-name* **service-type http** command in the AAA view to set the access type of the web user to HTTP.

----End

7.9 FAQ

7.9.1 How Do I Obtain the Web Page File?

To obtain a web page file, visit **http://support.huawei.com/enterprise** and download the software package containing the web page file based on the product name and version. The file is named in the format **product name-software version number.web file version number.web.7z**.

After downloading the file, compare the downloaded web page file with that on the website to check whether their sizes are the same. If not, an error may occur during file download. Download the file again.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

7.9.2 Why Only a Few Options Are Available on the Web System?

The user level of the login web user is low.

Web users of level 2 or lower are monitoring users and can use only the ping and tracert functions. Web users of level 3 or higher are administrator users and have all operation rights of a web page.

You can run the **local-user** *user-name* **privilege level** *level* command in AAA view to set the user level of the login user to level 3 or higher. The login user then has all operation rights of a web page.

7.9.3 How Do I Change the Password for Web Login?

If you forget or want to change the web login password, log in to the switch through the console port, Telnet, or STelnet and set a new password after login.

NOTICE

The Telnet protocol has security vulnerabilities. It is recommended that you log in to the device through the console port or using STelnet V2.

Set the user name and password to **admin123** and **Huawei@123** respectively.

```
<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
```

7.9.4 What Is the Difference Between Web and HTTP?

Hypertext Transfer Protocol (HTTP) is used to transfer web page files over the Internet. It runs at the application layer of the TCP/IP protocol stack. The transport layer uses the connection-oriented TCP protocol.

Conclusively, HTTP is a protocol while web is a device management method. Using the web system to manage and maintain devices requires the HTTP protocol.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

8 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.

8.1 File System Overview

8.2 File Management Modes

8.3 Local File Management

8.4 File Management on Other Devices

8.5 File Management Configuration Examples

8.6 Common Misconfigurations

8.7 FAQ

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

8.1 File System Overview

File System

The file system manages files and directories on storage media. In the file system, you can create, delete, modify, and rename files or directories, and view file contents.

Storage Medium

The switch supports the flash memory.

Naming Rules for Files

A file name is a string of 1 to 160 case-insensitive characters without spaces. 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.

  In this format, **drive** indicates the storage medium and can be set to **flash:**.

  drive of devices in a stack can be set to:

  - **flash**: root directory of the flash memory of the master switch on a device in a stack.
  - **stack ID#flash**: root directory of the flash memory in a slot on a device in a stack.

    For example, **slot2#flash:** indicates the flash memory in slot 2.

  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. The relative path is related to the root directory or the current working directory. A relative path starting with a slash (/) is related to the root directory.

  - **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 /my/test/mytest.txt** command to find the **mytest.txt** file from a directory related to the root directory.

  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).

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

- In the file operation command format, **filename** indicates the file name.
- In the file operation command format, **directory** indicates the path (**drive + path**).

8.2 File Management Modes

The device can function as a server or client to manage files.

- When the device functions as a server, you can access the device from a terminal to manage files on the device and transfer files between the device and the terminal.
- 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.

In Trivial File Transfer Protocol (TFTP) mode, the device can function only as a client. In File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), Secure Copy Protocol (SCP), or File Transfer Protocol over SSL (FTPS) mode, the device can function both as a server and a client.

Table 8-1 describes the advantages and disadvantages of different file management modes.

Table 8-1 Advantages and disadvantages of file management modes

Mode	Usage Scenario	Advantage	Disadvantage
Device login	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.
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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Mode	Usage Scenario	Advantage	Disadvantage
TFTP	On the LAN of a lab, 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.	● In TFTP mode, the device can function only as a client. ● The TFTP mode supports only file transfer, but does not support interaction. ● 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. ● In SFTP mode, the SFTP and FTP functions are available on the device. (In FTPS mode, FTPS and FTP cannot be configured simultaneously.)	Configurations are complicated.
SCP	The SCP mode is applicable to the highly-efficient file upload and download scenarios with high network security requirements.	● Data is encrypted and protected. ● In SCP mode, files are uploaded or downloaded when the client is connected to the server, which is efficient.	Configurations are complicated (similar to SFTP configurations), and interactions are not supported.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Mode	Usage Scenario	Advantage	Disadvantage
FTPS	The FTPS mode is applicable to scenarios with high network requirements and no FTP function.	The FTPS mode uses the data encryption, user identity authentication, and message integrity check mechanisms to ensure the security of the TCP-based application-layer protocols.	● Configurations are complicated, and a set of certificates must be obtained from Certificate Authority (CA). ● To enable the FTPS function, disable the FTP function first.

Device login, FTP, and TFTP are easy to learn and configure. The following section describes the remaining modes in more detail.

SFTP Mode

As a part of Secure Shell (SSH), SFTP allows remote users to securely log in to the device and perform file management and transmission through the security channel provided by SSH. Therefore, SFTP improves data transmission security. In addition, the device can function as the SSH client to connect to the remote SSH server for secure file transmission.

SSH security features:

- Encrypted transmission: When an SSH connection is set up, two devices negotiate an encryption algorithm and a session key to ensure secure communications between them.
- Public key-based authentication: The device supports the RSA or DSA authentication mode.
- Server authentication: The SSH protocol authenticates a server based on the public key to defend against attacks from bogus servers.
- Interaction data check: The SSH protocol uses the CRC (for SSH1.5) or MD5-based MAC algorithm (for SSH2.0) to check the data integrity and authenticity. This mechanism protects the system from man-in-the-middle attacks.

Establishment of an SSH connection:

1. Negotiate the SSH version.

   The client and the server negotiate an SSH version by exchanging character strings that specify the SSH version.
2. Negotiate the algorithm.

   The server and the client negotiate the key exchange algorithm, encryption algorithm, and MAC algorithm for subsequent communications.
3. Exchange keys.

   Based on the key exchange algorithm, the server and the client obtain the same session key and session ID after calculation.
4. Authenticate users.

   The client sends an authentication request containing the user identity information to the server. If the authentication succeeds or expires, the client is disconnected from the server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

The public key-based and password-based authentication modes are supported.

- In public key-based (RSA or DSA) authentication mode, the client must generate the RSA or DSA key and send it to the server. When a user initiates an authentication request, the client randomly generates a text that is encrypted with the private key and sends it to the server. The server decrypts the text by using the public key. If decryption succeeds, the server considers this user trusted and grants this user access rights. If decryption fails, the client is disconnected from the server.
- Password-based authentication is implemented by the Authentication, Authorization and Accounting (AAA). Similar to Telnet and FTP, SSH supports local database authentication and remote RADIUS server authentication. The SSH server compares the user name and password of an SSH client with the preset ones. Authentication succeeds if both match.

5. Request a session.

   After user authentication is complete, the client sends a session request to the server. After receiving the request, the server processes it.

6. Enter the interactive session.

   After the session request is accepted, the SSH connection enters the interactive session mode. In this mode, data is transmitted bidirectionally.

NOTE

Before an SSH connection is set up, the local key pair (RSA or DSA key pair) must be generated on the server. The key pair is used to generate the session key and session ID and authenticate the server. This step is the key to SSH server configuration.

SCP Mode

Based on the SSH remote file copy function, SCP is used to copy, upload, and download files. SCP commands are easy to use, improving network maintenance efficiency.

FTPS Mode

FTPS combines FTP and Secure Sockets Layer (SSL). A client and server use SSL to authenticate each other and encrypt data to be transmitted. SSL ensures secure connections to FTP servers and greatly improve security of common FTP servers, enabling files of the device to be managed securely.

Concepts to learn before configuring the FTPS mode:

- CA

  CA is an entity that issues, manages, and abolishes digital certificates, and it authenticates identities of digital certificate owners. Root CAs are widely trusted in the world and authorize other lower-level CAs. CA identity information is provided in the file of a trusted CA.

  For example, CA1 is a root CA that issues a certificate to lower-level CA2, and CA2 issues the certificate to lower-level CA3. The certificate used by the server is issued by the lowest-level CA.

  If the certificate of the server is issued by CA3, the certificate is authenticated as follows: CA3 authenticates the certificate of the server. If the authentication succeeds, CA2 authenticates the certificate of CA3. If the authentication succeeds, the root CA authenticates the certificate of CA2. Only when the root authentication succeeds, the certificate used by the server is valid.

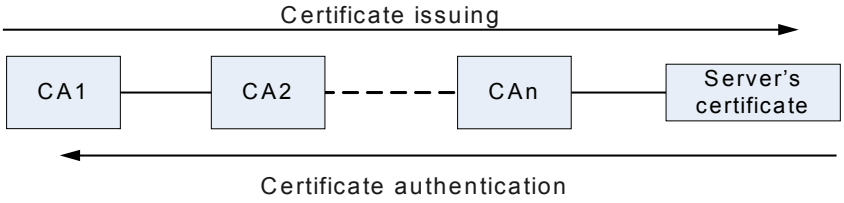
Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 8-1 shows the certificate issuing process and certificate authentication process.

Figure 8-1 Certificate issuing process and certificate authentication process



- Digital certificate

  A digital certificate is an electronic document which uses a digital signature to bind a public key with an identity. The digital certificate contains information such as the name of a person or an organization and the address. The certificate can be used to verify that a public key belongs to an individual.

  Users must obtain the public key of the message sending party to decode messages, and obtain the CA certificate of the message sending party to authenticate its identity.

- CRL

  The CA issues the Certificate Revocation List (CRL), containing a set of certificates that the CA regards as invalid.

  The CA can shorten the validity period of a certificate using a CRL. The certificate validity period specified by the CRL is shorter than the original certificate validity period. If the CA revocates a certificate in the CRL, the declaration about authorized key pair is revoked before the certificate expires. When the certificate expires, data related to the certificate is cleared from the CRL.

  Before using a certificate, the client checks the corresponding CRL.

Accessing a device functioning as the server or client:

- Access the device that functions as the FTP server on a terminal

  Configure an SSL policy, load the digital certificate, and enable the FTPS server function on the device that functions as the FTP server. Users can use the FTP client that supports SSL to access the FTP server to manage files.

- Access the FTP server using the device that functions as an FTP client

  Configure an SSL policy on the device that functions as the FTP client and load the trusted CA certificate to check the owner's identity.

8.3 Local File Management

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

8.3.1 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 has 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.

Procedure

- **Perform operations on directories.**

Table 8-2 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* | **/all-filesystems**]	-
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 8-3 Performing operations on files

Operation	Command	Description
Display the file content.	**more** *filename* [*offset*] [**all**]	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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 asks 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 asks you whether to overwrite the existing file.
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**] [**/quiet**] { *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* }	Running the **delete** command without the **/unreserved** keyword moves a file to the recycle bin. Run this command to restore this file.
Remove a file from the recycle bin.	**reset recycle-bin** [*filename* | *devicename*]	Remove a file from the recycle bin to permanently delete it.
Enter the system view.	**system-view**	-
Execute batch files.	**execute** *batch-filename*	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.

- **Perform operations on storage media.**

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

When the file system on a storage medium fails, the terminal prompts the user to rectify the fault.

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 formatting a storage medium.

Table 8-4 Performing operations on storage media

Operation	Command	Description
Repair a storage medium with a faulty file system.	**fixdisk** *drive*	If the system still reports the fault after this command is executed, the storage medium is damaged.
Format a storage medium.	**format** *drive*	If the storage medium is still unavailable after it is formatted, a physical exception occurs.

- **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 8-5 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

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

8.3.2 Managing Files When the Device Functions as an FTP Server

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

NOTICE

The FTP protocol brings security risks. The SFTPv2, SCP, or FTPS mode is recommended.

Table 8-6 describes the procedure for managing files when the device functions as an FTP server.

Table 8-6 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.	Perform these three steps in any sequence.
2	**Configure local FTP user information**	Configure local FTP user information including the service type, user level, and authorized directory.	
3	**(Optional) Configure the FTP ACL**	Configure the ACL rule and FTP basic ACL to improve FTP access security.	
4	**Connect to the device using FTP**	Connect to the device using FTP from the terminal.	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Default Parameter Settings

Table 8-7 Default parameter settings

Parameter	Default Value
FTP server function	Disabled
Listening port number	21
FTP user	No local user is created.

Procedure

- **Set FTP server parameters.**

Table 8-8 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 this 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(Optional) Configure the timeout duration of the FTP server.	**ftp** [**ipv6**] **timeout** *minutes*	By default, the idle timeout duration is 10 minutes. If no operation is performed on the FTP server during the timeout duration, the FTP client automatically disconnects from the FTP server.

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 8-9 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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.**

  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 FTP connections 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 8-10 (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*	-
Configure the ACL rule.	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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.
  - 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:\Documents and Settings\Administrator> 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.

  The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

  Users can perform the following operations in any sequence.

Table 8-11 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**	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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 one or more files.	**put** *local-filename* [*remote-filename*] Or **mput** *local-filenames*	● To upload a file, run the **put** command. ● To upload multiple files, run the **mput** command.
Download one or more files.	**get** *remote-filename* [*local-filename*] Or **mget** *remote-filenames*	● To download a file, run the **get** command. ● To download multiple files, run the **mget** command.
Set the file transfer mode to ASCII or Binary.	**ascii** Or **binary**	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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Set the data transmission mode to passive or active.	**passive** Or **undo passive**	Select one of them. The default data transmission mode is active.
View the online help about FTP commands.	**remotehelp** [*command*]	-
Enable the system prompt function.	**prompt**	By default, the prompt function is disabled.
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

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Checking the Configurations

- 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.

8.3.3 Managing Files When the Device Functions as an SFTP Server

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 or FTPS mode is recommended.

Table 8-12 describes the procedure for managing files when the device functions as an SFTP server.

Table 8-12 Managing files when the device functions as an SFTP server

No.	Task	Description	Remarks
1	**Set SFTP server parameters**	Generate local key pair, enable the SFTP server, and configure SFTP server parameters, including the listening port number, key pair updating time, SSH authentication timeout duration, and number of SSH authentication retries.	The three steps can be performed in any sequence.
2	**Configure 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 service type, authorized directory, and authentication mode on the SFTP server.	

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

No.	Task	Description	Remarks
4	**Connect to the device using SFTP**	Connect to the device using the SSH client software on the terminal.	-

Default Parameter Settings

Table 8-13 Default parameter settings

Parameter	Default Value
SFTP server function	Disabled
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
Number of SSH authentication retries	3
SSH user	No SSH user is created.
Type of service for SSH users	No service type is supported.
Authorized directory for SSH users	flash:

Procedure

- **Set SFTP server parameters.**

Table 8-14 Setting SFTP server parameters

Operation	Command	Description
Enter the system view.	**system-view**	-
Generate a local key pair.	**rsa local-key-pair create**, or **dsa local-key-pair create**.	Perform one of the operations based on the key type. After the key pair is generated, you can run the **display rsa local-key-pair public**, or **display dsa local-key-pair public** command to check the public key in the local key pair. **NOTE** Because a longer key pair provides higher security, you are advised to use key pairs of the largest length.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Enable the SFTP server function.	**sftp server enable**	By default, the SFTP server function is disabled.
(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** } *	By default, an SSH server supports all key exchange algorithms.
(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** } *	By default, an SSH server supports all key exchange algorithms.
(Optional) Configure an encryption algorithm list for the SSH server.	**ssh server cipher** { **3des_cbc** | **aes128_cbc** | **aes128_ctr** | **aes256_cbc** | **aes256_ctr** | **des_cbc** } *	By default, an SSH server supports the following encryption algorithms: 3DES_CBC, AES128_CBC, AES256_CBC, AES128_CTR, and AES256_CTR.
(Optional) Configure an HMAC algorithm list for the SSH server.	**ssh server hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** } *	By default, an SSH server supports the following HMAC algorithms: MD5, MD5_96, SHA1, SHA1_96, SHA2_256, and SHA2_256_96.
(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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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. This command takes effect only for SSH1.X. However, SSH1.X ensures poor security and is not recommended.
(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. When an SSH server is upgraded, the server's compatibility with earlier versions is the same as that in the configuration file.
(Optional) Configure an ACL.	**ssh** [**ipv6**] **server acl** *acl-number*	By default, no ACL is configured for the SSH server. An ACL is configured to determine which clients can log in to the current device through SSH.
(Optional) Configure the source IP address of the SSH server.	**ssh server-source -i loopback** *interface-number*	By default, the source interface of an SSH server is not specified. **NOTE** Before specifying the source interface of the SSH server, ensure that the loopback interface to be specified as the source interface has been created. If the loopback interface is not created, this command cannot be correctly executed.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

- When the local RSA 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 is 2048 bits.
- When the local DSA key pair is generated, only the host key pair is generated. The length of the host key pair can be 1024 or 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 8-15 Configuring the VTY user interface for SSH users to log in to the device

Operation	Command	Description
Enter the system view.	**system-view**	-
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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(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 **6.5.1 (Optional) Configuring Attributes for a VTY User Interface** or **6.6.1 (Optional) Configuring Attributes for a VTY User Interface**.

- **Configure SSH user information.**

  Configure SSH user information including the authentication mode. Authentication modes including RSA, password, password-rsa, DSA, password-dsa, and all are supported.

  - The password-rsa authentication mode consists of the password and RSA authentication modes.
  - The password-dsa authentication mode consists of the password and DSA authentication modes.
  - The all authentication mode indicates that SSH users only need to authenticated by DSA, password, or RSA.

Table 8-16 Configuring SSH user information

Operation	Command	Description
Enter the system view.	**system-view**	-
Create SSH users.	**ssh user** *user-name*	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Configure the authentication mode for SSH users.	**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **all** | **dsa** | **password-dsa** }	If SSH users are not created using the **ssh user** command, directly run the **ssh authentication-type default password** command to configure the default password authentication mode for users. This mode simplifies the configurations when a large number of users exist, because you need to configure only AAA users. **NOTE** In all authentication mode, the user priority depends on the authentication mode selected. ● If password authentication is selected, the user priority is the same as that specified on the AAA module. ● If RSA/DSA authentication is selected, the user priority depends on the priority of the VTY window used during user access. If all authentication is selected and an AAA user with the same name as the SSH user exists, user priorities may be different in password authentication and RSA/DSA authentication modes. Set relevant parameters as needed.
Set the service type to **SFTP** or **all** for SSH users.	**ssh user** *username* **service-type** { **sftp** | **all** }	By default, the service type of SSH users is empty.
Configure the authorized directory for SSH users.	**ssh user** *username* **sftp-directory** *directoryname*	The default SFTP service authorized directory is flash: for an SSH user.

- The password authentication mode is implemented based on the AAA. To log in to the device in the password-dsa, password, or password-rsa authentication mode, create a local user with the same user name in the AAA view.
- If the SSH user uses the password authentication mode, only the SSH server needs to generate the RSA or DSA key. If the SSH user uses the RSA or DSA authentication mode, both the SSH server and client need to generate the RSA or DSA key and configure the public key of the peer end locally.

Perform any of the following configurations according to authentication mode:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

- To configure password authentication for the SSH user, see **Table 8-17**.
- To configure RSA or DSA authentication for the SSH user, see **Table 8-18**.
- To configure password-RSA, password-dsa, authentication for the SSH user, configure an AAA user and set the RSA or DSA public key. For details, see **Table 8-17** and **Table 8-18**.

Table 8-17 Configuring password, password-dsa, or password-rsa authentication for the SSH user

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 service type for the local user.	**local-user** *user-name* **service-type ssh**	-
Configure the level for the local user.	**local-user** *user-name* **privilege level** *level*	-
Return to the system view.	**quit**	-

Table 8-18 Configuring DSA, RSA, password-dsa, or password-rsa authentication for the SSH user

Operation	Command	Description
Enter the system view.	**system-view**	-
Display the RSA or DSA public key view.	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] or **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	-
Display the public key editing view.	**public-key-code begin**	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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 client software that supports SSH. For detailed operations, see the SSH client software help. ● You must enter the RSA or DSA public key on the device that works as the SSH server.
Exit 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 *key-name* has been deleted in another view, 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 from the public key view.	**peer-public-key end**	-
Assign an RSA or DSA public key to an SSH user.	**ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** } *key-name*	-

- **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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 sftpuser@10.136.23.5
Connecting to 10.136.23.5...
The authenticity of host '10.136.23.5 (10.136.23.5)' can't be established.
DSA 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 '10.136.23.5' (DSA) to the list of known hosts.

User Authentication
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 8-19** 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.

  The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Table 8-19 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**	-
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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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*]	-

You can also use the next commands to download files from the SFTP server or upload files.

- IPv4 address : **sftp client-transfile** { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** *prefer_key-exchange*] | [**identity-key** { **rsa** | **dsa** }] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]
- IPv6 address : **sftp client-transfile** { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [[**prefer_kex** *prefer_key-exchange*] | [**identity-key** { **rsa** | **dsa** }] | [**prefer_ctos_cipher** dou *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

- **Disconnect the SFTP client from the SSH server.**

Operation	Command	Description
Disconnect the SFTP client from the SSH server.	**quit**	-

----End

Checking the Configurations

- Run the **display ssh user-information** [*username*] command to view SSH user information on the SSH server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

- 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.

8.3.4 Managing Files When the Device Functions as an SCP Server

Pre-configuration Tasks

Before connecting to the SCP 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 supporting SCP has been installed on the terminal.

Configuration Process

Table 8-20 describes the procedure for managing files when the device functions as an SCP server.

Table 8-20 Managing files when the device functions as an SCP server

No.	Task	Description	Remarks
1	**Set SCP server parameters**	Generate local key pair, enable the SCP server, and configure SCP server parameters, including the listening port number, key pair updating time, SSH authentication timeout duration, and number of SSH authentication retries.	Steps 1, 2, and 3 can be performed in any sequence.
2	**Configure 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 SSH users and set the authentication mode and service type on the SCP server.	
4	**Manage files when the device functions as an SCP server**	Upload and download files on the SCP client.	—

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Default Parameter Settings

Table 8-21 Default parameter settings

Parameter	Default Value
SCP server function	Disabled
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
Number of SSH authentication retries	3
SSH user	No SSH user is created.
Type of service for SSH users	No service type is supported.

Procedure

- **Set SCP server parameters.**

Table 8-22 Setting SCP server parameters

Operation	Command	Description
Enter the system view.	**system-view**	-
Generate a local key pair.	**rsa local-key-pair create**, or **dsa local-key-pair create**.	Perform one of the operations based on the key type. After the key pair is generated, you can run the **display rsa local-key-pair public**, or **display dsa local-key-pair public** command to check the public key in the local key pair. **NOTE** Because a longer key pair provides higher security, you are advised to use key pairs of the largest length.
Enable the SCP server function.	**scp server enable**	By default, the SCP server function is disabled.
(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** } *	By default, an SSH server supports all key exchange algorithms.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(Optional) Configure an encryption algorithm list for the SSH server.	**ssh server cipher** { **3des_cbc** | **aes128_cbc** | **aes128_ctr** | **aes256_cbc** | **aes256_ctr** | **des_cbc** } *	By default, an SSH server supports the following encryption algorithms: 3DES_CBC, AES128_CBC, AES256_CBC, AES128_CTR, and AES256_CTR.
(Optional) Configure an HMAC algorithm list for the SSH server.	**ssh server hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** } *	By default, an SSH server supports the following HMAC algorithms: MD5, MD5_96, SHA1, SHA1_96, SHA2_256, and SHA2_256_96.
(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.
(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. This command takes effect only for SSH1.X. However, SSH1.X ensures poor security and is not recommended.
(Optional) Configure the SSH authentication timeout duration.	**ssh server timeout** *seconds*	By default, the SSH authentication timeout duration is 60 seconds.
(Optional) Configure the source IP address of the SSH server.	**ssh server-source -i loopback** *interface-number*	By default, the source interface of an SSH server is not specified. **NOTE** Before specifying the source interface of the SSH server, ensure that the loopback interface to be specified as the source interface has been created. If the loopback interface is not created, this command cannot be correctly executed.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(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. When an SSH server is upgraded, the server's compatibility with earlier versions is the same as that in the configuration file.
(Optional) Configure an ACL.	**ssh** [**ipv6**] **server acl** *acl-number*	By default, no ACL is configured for the SSH server. An ACL is configured to determine which clients can log in to the current device through SSH.

- When the local RSA 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 is 2048 bits.
- When the local DSA key pair is generated, only the host key pair is generated. The length of the host key pair can be 1024 or 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 SCP. Attributes of the VTY user interface must be configured.

  Table 8-23 Configuring the VTY user interface for SSH users to log in to the device

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the VTY user interface view.	**user-interface vty** *first-ui-number* [*last-ui-number*]	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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 **6.5.1 (Optional) Configuring Attributes for a VTY User Interface** or **6.6.1 (Optional) Configuring Attributes for a VTY User Interface**.

- **Configure SSH user information.**

  Configure SSH user information including the authentication mode. Authentication modes including RSA, password, password-rsa, DSA, password-dsa, and all are supported.

  - The password-rsa authentication mode consists of the password and RSA authentication modes.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- The password-dsa authentication mode consists of the password and DSA authentication modes.
- The all authentication mode indicates that SSH users only need to authenticated by DSA, password, or RSA.

Table 8-24 Configuring SSH user information

Operation	Command	Description
Enter the system view.	**system-view**	-
Create SSH users.	**ssh user** *user-name*	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Configure the authentication mode for SSH users.	**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **all** | **dsa** | **password-dsa** }	If SSH users are not created using the **ssh user** command, directly run the **ssh authentication-type default password** command to configure the default password authentication mode for users. This mode simplifies the configurations when a large number of users exist, because you need to configure only AAA users. **NOTE** In all authentication mode, the user priority depends on the authentication mode selected. ● If password authentication is selected, the user priority is the same as that specified on the AAA module. ● If RSA/DSA authentication is selected, the user priority depends on the priority of the VTY window used during user access. If all authentication is selected and an AAA user with the same name as the SSH user exists, user priorities may be different in password authentication and RSA/DSA authentication modes. Set relevant parameters as needed.
Set the service type to **all** for SSH users.	**ssh user** *username* **service-type all**	By default, the service type of SSH users is empty.

- The password authentication mode is implemented based on the AAA. To log in to the device in the password-dsa, password, or password-rsa authentication mode, create a local user with the same user name in the AAA view.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

- If the SSH user uses the password authentication mode, only the SSH server needs to generate the RSA or DSA key. If the SSH user uses the RSA or DSA authentication mode, both the SSH server and client need to generate the RSA or DSA key and configure the public key of the peer end locally.

Perform any of the following configurations according to authentication mode:

- To configure password authentication for the SSH user, see **Table 8-25**.
- To configure RSA, or DSA authentication for the SSH user, see **Table 8-26**.
- To configure password-rsa, or password-dsa authentication for the SSH user, configure an AAA user and set the RSA, or DSA public key. For details, see **Table 8-25** and **Table 8-26**.

Table 8-25 Configuring password, password-dsa, or password-rsa authentication for the SSH user

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 service type for the local user.	**local-user** *user-name* **service-type ssh**	-
Configure the level for the local user.	**local-user** *user-name* **privilege level** *level*	-
Return to the system view.	**quit**	-

Table 8-26 Configuring DSA, RSA, password-dsa, or password-rsa authentication for the SSH user

Operation	Command	Description
Enter the system view.	**system-view**	-
Display the RSA or DSA public key view.	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] or **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	-
Display the public key editing view.	**public-key-code begin**	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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 client software that supports SSH. For detailed operations, see the SSH client software help. ● You must enter the RSA or DSA public key on the device that works as the SSH server.
Exit 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 *key-name* has been deleted in another view, 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 from the public key view.	**peer-public-key end**	-
Assign an RSA or DSA public key to an SSH user.	**ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** } *key-name*	-

- **Manage files when the device functions as an SCP server.**

  The SSH client software supporting SCP must be installed on the terminal to ensure that the terminal can connect to the device using SCP to upload or download 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Access the Windows CLI and run the commands supported by the OpenSSH to connect to the device using SCP to manage files. (The following information is only for reference.)

```
C:\Documents and Settings\Administrator> scp scpuser@10.136.23.5:flash:/
vrpcfg.zip vrpcfg-backup.zip
The authenticity of host '10.136.23.5 (10.136.23.5)' can't be established.
DSA 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 '10.136.23.5' (DSA) to the list of known hosts.

User Authentication
Password:
vrpcfg.zip                                    100% 1257     1.2KByte(s)/sec
00:00
Received disconnect from 10.136.23.5: 2: The connection is closed by SSH
server


C:\Documents and Settings\Administrator>
```

The user terminal uploads or downloads files while connecting to the SCP server and access the user local directory.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

----End

Checking the Configurations

- Run the **display ssh user-information** [*username*] command to view SSH user information on the SSH server.
- 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.

8.3.5 Managing Files When the Device Functions as an FTPS Server

Pre-configuration Tasks

Before connecting to the FTPS server to manage files, complete the following tasks:

- Ensure that routes are reachable between the terminal and the device.
- Ensure that the FTP client software supporting SSL has been installed on the terminal.

Configuration Process

Table 8-27 describes the procedure for managing files when the device functions as an FTPS server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 8-27 Managing files when the device functions as an FTPS server

No.	Task	Description	Remarks
1	**Upload the server digital certificate and private key**	Upload the digital certificate and private key to the device.	Step 1 must be performed before step 2. The other steps can be performed in any sequence.
2	**Configure the SSL policy and load the digital certificate**	Configure an SSL policy and load the digital certificate to the server.	
3	**Configure the FTPS server function and set FTP service parameters**	Configure an SSL policy for the FTPS server and set FTPS server parameters including the port number, source address, and timeout duration.	
4	**Configure local FTP user information**	Configure FTP local users including the service type and authorized directory.	
5	**Connect to the device using FTPS**	Connect to the device using FTPS on the terminal.	-

Default Parameter Settings

Table 8-28 Default parameter settings

Parameter	Default Value
SSL policy	No SSL policy is created for FTPS server.
FTPS server function	Disabled
Listening port number	21
FTP user	No local user is created.

Procedure

- **Upload the server digital certificate and private key.**

  Upload the server digital certificate and private key file to the **security** directory on the device in SFTP or SCP mode. If no **security** directory exists on the device, run the **mkdir** *directory* command to create one.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

The server must obtain a digital certificate (including the private key file) from a CA. The client that connects to the server must obtain a digital certificate from the CA to authenticate the validity of the server digital certificate.

NOTE

CA is an authority that issues and manages digital certificates. Digital certificates that are loaded to the FTPS server must be applied from a CA.

The device does not support life-cycle management on the self-signed certificate generated by the device, such as updating the certificate or revoking the certificate. You are advised to use your own certificate to ensure device and certificate security.

Digital certificates support the PEM, ASN1, and PFX formats.

- A PEM digital certificate has a file name extension .pem and is applicable to text transmission between systems.
- An ASN1 digital certificate has a file name extension .der and is the default format for most browsers.
- A PFX digital certificate has a file name extension .pfx and is a binary format that can be converted into the PEM or ASN1 format.

For details, see the description about uploading files in other modes.

- **Configure the SSL policy and load the digital certificate.**

  Load the digital certificate and specify the private key.

Table 8-29 Configuring the SSL policy and loading the digital certificate

Operation	Command	Description
Enter the system view.	**system-view**	-
(Optional) Customize SSL cipher suite.	**ssl cipher-suite-list** *customization-policy-name*	Customize an SSL cipher suite policy and enter the cipher suite policy view. By default, no customized SSL cipher suite policy is configured.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
	set cipher-suite { **tls1_ck_rsa_with_aes_256_sha** | **tls1_ck_rsa_with_aes_128_sha** | **tls1_ck_rsa_rc4_128_sha** | **tls1_ck_dhe_rsa_with_aes_256_sha** | **tls1_ck_dhe_dss_with_aes_256_sha** | **tls1_ck_dhe_rsa_with_aes_128_sha** | **tls1_ck_dhe_dss_with_aes_128_sha** | **tls12_ck_rsa_aes_256_cbc_sha256** }	Configure the cipher suites for a customized SSL cipher suite policy. By default, no customized SSL cipher suite policy is configured. If a customized SSL cipher suite policy is being referenced by an SSL policy, the cipher suites in the customized cipher suite policy can be added, modified, or partially deleted. Deleting all of the cipher suites is not allowed.
	quit	Return to the system view.
Create an SSL policy and enter the SSL policy view.	**ssl policy** *policy-name*	-
(Optional) Set a minimum version of an SSL policy.	**ssl minimum version** { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }	By default, the minimum version of an SSL policy is TLS1.1.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(Optional) Bind a customized SSL cipher suite policy to an SSL policy.	**binding cipher-suite-customization** *customization-policy-name*	By default, no customized cipher suite policy is bound to an SSL policy. Each SSL policy uses a default cipher suite. After a customized cipher suite policy is unbound from an SSL policy, the SSL policy uses one of the following cipher suites supported by default: ● tls1_ck_rsa_with_aes_256_sha ● tls1_ck_rsa_with_aes_128_sha ● tls1_ck_dhe_rsa_with_aes_256_sha ● tls1_ck_dhe_dss_with_aes_256_sha ● tls1_ck_dhe_rsa_with_aes_128_sha ● tls1_ck_dhe_dss_with_aes_128_sha ● tls12_ck_rsa_aes_256_cbc_sha256 If the cipher suite in the customized cipher suite policy bound to an SSL policy contains only one type of algorithm (RSA or DSS), the corresponding certificate must be loaded for the SSL policy to ensure successful SSL negotiation.
Load the digital certificate in the PEM format.	**certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*	Load the digital certificate in the PEM, ASN1, or PFX format.
Load the digital certificate in the ASN1 format.	**certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*	
Load the digital certificate in the PFX format.	**certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac cipher** *mac-code* | **key-file** *key-filename* } **auth-code cipher** *auth-code*	

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Load the digital certificate chain in the PEM format.	**certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*	**NOTE** ● You can load a certificate or certificate chain for only one SSL policy. Before loading a certificate or certificate chain, you must unload the existing certificate or certificate chain. ● When you configure an SSL policy to load a certificate or certificate chain, ensure that the maximum length of the key pair in the certificate or certificate chain is 2048 bits. If the length of the key pair exceeds 2048 bits, the certificate file or certificate chain file cannot be uploaded to the device. ● Before rolling V200R008 or a later version back to an earlier version, back up the SSL private key file.

- **Configure the FTPS server function and set FTP service parameters.**

  FTPS is based on the FTP protocol. You can enable the FTPS server function and set FTP service parameters.

  Table 8-30 Configuring the FTPS server function and setting FTP service 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 this 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.
Configure the SSL policy on the FTPS server.	**ftp secure-server ssl-policy** *policy-name*	The SSL policy configured on the FTP server is the same as that is created in the last step.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Enable the FTPS server function.	**ftp** [**ipv6**] **secure-server enable**	By default, the FTPS server function is disabled. **NOTE** To enable the security FTPS server function, you must disable the FTP server function.
(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 10 minutes. If no operation is performed on the FTP server during the timeout duration, the FTP client automatically disconnects from the FTP server.

NOTE

- If the FTPS service is enabled, the port number of the FTPS service cannot be changed. To change the port number, run the **undo ftp** [**ipv6**] **secure-server** command to disable the FTPS service first.
- After operations on files are complete, run the **undo ftp** [**ipv6**] **secure-server** to disable the FTPS server function to ensure the device security.

- **Configure local FTP user information.**

  Before performing operations on files using FTPS, configure the local user name and password, service type, and authorized directory on the FTPS server.

  Table 8-31 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*	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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.

- **Connect to the device using FTPS.**

  The FTP client software supporting SSL must be installed on the terminal to ensure that the terminal can connect to the FTPS server using third-party software to manage files.

  NOTE

  The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

----End

Checking the Configurations

- Run the **display ssl policy** command to view the SSL policy and digital certificate.
- Run the **display** [**ipv6**] **ftp-server** command to view the FTPS server status.
- Run the **display ftp-users** command to view information about the FTP users who log in to the FTP server.

8.4 File Management on Other Devices

8.4.1 Managing Files When the Device Functions as a TFTP Client

Pre-configuration Tasks

Before connecting to a device as a TFTP client to manage files, complete the following tasks:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- 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, SCP or FTPS mode is recommended.

Table 8-32 describes the procedure for managing files when the device functions as a TFTP client.

Table 8-32 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.	
3	**Run TFTP commands to upload or download files**	Upload and download files.	

Procedure

- **(Optional) Configure the TFTP client source address.**

  When specifying 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 8-33 (Optional) Configuring the TFTP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
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. By default, the TFTP client source address is the IP address of the outbound interface connecting to the TFTP server, and it is displayed as 0.0.0.0.

- **(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:

  - 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 8-34 (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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Configure the ACL rule.	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *	By default, no ACL rule is configured. **NOTE** Only the S5720EI, S5720SI, S5720S-SI, S5720HI, S6720S-EI, and S6720EI support **vpn-instance**.
Return to the system view.	**quit**	-
Configure the TFTP ACL.	**tftp-server** [**ipv6**] **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*]	● **get**: downloads a file. ● **put**: uploads a file. **NOTE** Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support **public-net** or **vpn-instance** *vpn-instance-name* parameter in the command.
IPv6 address	**tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-oi** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]	

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

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

Checking 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

8.4.2 Managing Files When the Device Functions as an FTP Client

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 brings security risks. The SFTPv2, SCP, or FTPS mode is recommended.

Table 8-35 describes the procedure for managing files when the device functions as an FTP client.

Table 8-35 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**	-	

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

No.	Task	Description	Remarks
5	**Disconnect the FTP client from the FTP server**	-	

Procedure

- **(Optional) Configure the FTP client source address.**

  When specifying 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.

  Table 8-36 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 8-37 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Connect to the FTP server in the FTP client view when the server uses an IPv4 address.	**ftp**	**NOTE** Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support **public-net** or **vpn-instance** *vpn-instance-name* parameter in the command.
	open [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	

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. (Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support this command.)
- 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 8-38 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* [*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.

  The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

  Users can perform the following operations in any sequence.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 8-39 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: < > ? \ :
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 one or more files.	**put** *local-filename* [*remote-filename*] Or **mput** *local-filenames*	● To upload a file, run the **put** command. ● To upload multiple files, run the **mput** command.
Download one or more files.	**get** *remote-filename* [*local-filename*] Or **mget** *remote-filenames*	● To download a file, run the **get** command. ● To download multiple files, run the **mget** command.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Set the file transfer mode to ASCII or Binary.	**ascii** Or **binary**	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 data transmission mode to passive or active.	**passive** Or **undo passive**	Select one of them. The default data transmission mode is active.
View the online help about FTP commands.	**remotehelp** [*command*]	-
Enable the system prompt function.	**prompt**	By default, the prompt function is disabled.
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.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Disconnect the FTP client from the FTP server and return to the FTP client view.	**close** or **disconnect**	

----End

Checking the Configurations

- Run the **display ftp-client** command to check source interface of the FTP client.

8.4.3 Managing Files When the Device Functions as an SFTP Client

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.

Configuration Process

Table 8-40 describes the procedure for managing files when the device functions as an SFTP client.

Table 8-40 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. **NOTE** You can set the SFTP client source address on the S1720GFR, S2720, S5700S-LI, S5710-X-LI, S5720SI, S5720S-SI, S5720HI, S5720EI, S6720S-EI, and S6720EI support only.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

No.	Task	Description	Remarks
2	**Generate a local key pair**	Generate a local key pair and configure the public key on the SSH server. Perform this task only when the device logs in to the SSH server in RSA or DSA 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 specifying 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.

  NOTE

  You can set the SFTP client source address on the S1720GFR, S2720, S5700S-LI, S5710-X-LI, S5720SI, S5720S-SI, S5720HI, S5720EI, S6720S-EI, and S6720EI support only.

  The SFTP client source address must be set to the loopback interface IP address or loopback interface.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Table 8-41 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. The client source address is set to the loopback interface IP address or loopback interface.

- **Generating a local key pair**

  NOTE

  Perform this step only when the device logs in to the SSH server in RSA or DSA authentication mode, not the password authentication mode.

Table 8-42 Generating a local key pair

Action	Command	Description
Enter the system view.	**system-view**	-
Generate the local key pair.	**rsa local-key-pair create**, or **dsa local-key-pair create**.	Select one from the following based on the type of key configured on the remote end. Run the **display rsa local-key-pair public**, or **display dsa local-key-pair public** command to view the public key in the local RSA or DSA key pair. Configure the public key on the SSH server.

- **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 8-43**.
  - 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 8-44**. This method ensures higher security but becomes more complex than the first method.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 8-43 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 8-44 Configuring the SSH client to assign the RSA or DSA public key to the SSH server

Action	Command	Description
Enter the system view.	**system-view**	-
Enter the RSA or DSA public key view.	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] or **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	Perform one of the operations based on the key type.
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 DSA public key that is generated on the server to the client.
Exit from the public key editing view.	**public-key-code end**	● If the key public hex-data is invalid, the public key cannot be generated after you run this command. ● If the specified key *key-name* 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Action	Command	Description
Return to the system view.	**peer-public-key end**	-
Bind the RSA or DSA public key to the SSH server.	**ssh client** *servername* **assign** { **rsa-key** | **dsa-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** | **dsa-key** } command to cancel the binding between the SSH server and RSA or DSA public key, and run this command to assign a new RSA or DSA 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 8-45 Running SFTP commands to connect to the SSH server

Operation	Command	Description
Enter the system view.	**system-view**	-
(Optional) Configure a key exchange algorithm list for the SSH client.	**ssh client key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** } *	By default, an SSH client supports all key exchange algorithms.
(Optional) Configure an encryption algorithm list for the SSH client.	**ssh client cipher** { **des_cbc** | **3des_cbc** | **aes128_cbc** | **aes256_cbc** | **aes128_ctr** | **aes256_ctr** } *	By default, an SSH client supports the following encryption algorithms: 3DES_CBC, AES128_CBC, AES256_CBC, AES128_CTR, and AES256_CTR.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(Optional) Configure an HMAC algorithm list for the SSH client.	**ssh client hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** } *	By default, an SSH client supports the following HMAC algorithms: MD5, MD5_96, SHA1, SHA1_96, SHA2_256, and SHA2_256_96.
IPv4 address	**sftp** [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**identity-key** { **dsa** | **rsa** }] | [**user-identity-key** { **rsa** | **dsa** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-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** ● Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support **public-net** or **-vpn-instance** *vpn-instance-name* parameter in the command. ● The aes128 algorithm is recommended to improve data transmission security.
IPv6 address	**sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [[**identity-key** { **dsa** | **rsa** }] | [**user-identity-key** { **rsa** | **dsa** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-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 8-46** 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.

  The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 8-46 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*]	-

You can also use the next commands to download files from the SFTP server or upload files.

- IPv4 address : **sftp client-transfile** { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** *prefer_key-exchange*] | [**identity-key** { **rsa** | **dsa** }] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher**

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

prefer_stoc_cipher] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

- IPv6 address : **sftp client-transfile** { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [[**prefer_kex** *prefer_key-exchange*] | [**identity-key** { **rsa** | **dsa** }] | [**prefer_ctos_cipher** dou *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

- **Disconnect the SFTP client from the SSH server.**

Operation	Command	Description
Disconnect the SFTP client from the SSH server.	**quit**	-

----End

Checking the Configuration

- Run the **display sftp-client** command to check source interface of the SFTP client. Only the S1720GFR, S2720, S5700S-LI, S5710-X-LI, S5720SI, S5720S-SI, S5720HI, S5720EI, S6720S-EI, and S6720EI support support the command.
- Run the **display ssh server-info** command to check the mappings between the SSH server and the public key.

8.4.4 Managing Files When the Device Functions as an SCP Client

Pre-configuration Tasks

Before connecting to a device as an SCP 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.

Configuration Process

Table 8-47 describes the procedure for managing files when the device functions as an SCP client.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Table 8-47 Procedure for managing files when the device functions as an SCP client

No.	Task	Description	Remarks
1	**(Optional) Configure the SCP client source address**	Configure the SCP client source address. The source address can be set to a source IP address or source interface information, ensuring communication security.	Steps 1, 2, and 3 can be performed in any sequence.
2	**Generate a local key pair**	Generate a local key pair and configure the public key on the SSH server. Perform this task only when the device logs in to the SSH server in RSA or DSA 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 SCP commands to connect to the SSH server**	-	

Procedure

- **(Optional) Configure the SCP client source address.**

  Table 8-48 (Optional) Configuring the SCP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the SCP client source address.	**scp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	By default, no source IP address is configured on the SCP client.

- **Generate a local key pair**

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

Perform this step only when the device logs in to the SSH server in RSA or DSA authentication mode, not the password authentication mode.

Table 8-49 Generating a local key pair

Action	Command	Description
Enter the system view.	**system-view**	-
Generate the local key pair.	**rsa local-key-pair create**, or **dsa local-key-pair create**.	Select one from the following based on the type of key configured on the remote end. Run the **display rsa local-key-pair public**, or **display dsa local-key-pair public** command to view the public key in the local RSA or DSA key pair. Configure the public key on the SSH server.

- **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 8-43**.
  - 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 8-44**. This method ensures higher security but becomes more complex than the first method.

Table 8-50 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 8-51 Configuring the SSH client to assign the RSA or DSA public key to the SSH server

Action	Command	Description
Enter the system view.	**system-view**	-
Enter the RSA or DSA public key view.	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] or **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	Perform one of the operations based on the key type.
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 DSA public key that is generated on the server to the client.
Exit from the public key editing view.	**public-key-code end**	● If the key public hex-data is invalid, the public key cannot be generated after you run this command. ● If the specified key *key-name* 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**	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Action	Command	Description
Bind the RSA or DSA public key to the SSH server.	**ssh client** *servername* **assign** { **rsa-key** | **dsa-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** | **dsa-key** } command to cancel the binding between the SSH server and RSA or DSA public key, and run this command to assign a new RSA or DSA public key to the SSH server.

- **Run SCP commands to connect to the SSH server.**

  Different from the SFTP mode, after the SCP connection is established, the client can directly upload files to or download files from the server.

  Table 8-52 Running SCP commands to connect to the SSH server

Operation	Command	Description
Enter the system view.	**system-view**	-
(Optional) Configure a key exchange algorithm list for the SSH client.	**ssh client key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** } *	By default, an SSH client supports all key exchange algorithms.
(Optional) Configure an encryption algorithm list for the SSH client.	**ssh client cipher** { **des_cbc** | **3des_cbc** | **aes128_cbc** | **aes256_cbc** | **aes128_ctr** | **aes256_ctr** } *	By default, an SSH client supports the following encryption algorithms: 3DES_CBC, AES128_CBC, AES256_CBC, AES128_CTR, and AES256_CTR.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(Optional) Configure an HMAC algorithm list for the SSH client.	**ssh client hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** } *	By default, an SSH client supports the following HMAC algorithms: MD5, MD5_96, SHA1, SHA1_96, SHA2_256, and SHA2_256_96.
IPv4 address	**scp** [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** } | **user-identity-key** { **rsa** | **dsa** } | { **-a** *source-address* | **-i** *interface-type interface-number* } | **-r** | **-cipher** *-cipher* | **-c**] * *sourcefile destinationfile*	Run either of the commands based on the IP address type. **NOTE** ● Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support **public-net** or **vpn-instance** *vpn-instance-name* parameter in the command.
IPv6 address	**scp ipv6** [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** } | **user-identity-key** { **rsa** | **dsa** } | **-a** *source-address* | **-r** | **-cipher** *-cipher* } | **-c**] * *sourcefile destinationfile* [**-oi** *interface-type interface-number*]	

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

----End

Checking the Configurations

- Run the **display scp-client** command to check source configurations on the SCP client.
- Run the **display ssh server-info** command to check the mappings between the SSH server and the public key.

8.4.5 Managing Files When the Device Functions as an FTPS Client

Pre-configuration Tasks

Before connecting to a device as an FTPS client to manage files, complete the following tasks:

- Ensure that routes are reachable between the current device and the FTPS server.
- Load the digital certificate on the FTPS server.
- Obtain the host name or IP address of the FTPS server, FTPS user name, and password.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Configuration Process

Table 8-53 describes the procedure for managing files when the device functions as an FTPS client.

Table 8-53 Procedure for managing files when the device functions as an FTPS client

No.	Task	Description	Remarks
1	**Upload the CA certificate and CRL file**	Upload required files to the device.	After the FTPS connection is established, perform steps 4 and 5 in any sequence.
2	**Configure the SSL policy and load the CA certificate and CRL file**	-	
3	**Connect to the FTPS server**	-	
4	**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.	
5	**(Optional) Change the login user**	-	
6	**Disconnect the FTP client from the FTP server**	-	

Procedure

- **Upload the CA certificate and CRL file.**

  Upload the CA certificate and CRL file to the **security** directory on the device in FTP, SFTP, or SCP mode. If no **security** directory exists on the device, run the **mkdir** *security* command to create one.

  NOTE

  - The FTPS client must obtain certificates from the CA to authenticate the digital certificate of the server.
  - The CRL is also issued by the CA. The CRL file lists serial numbers of certificates that are revoked. If the digital certificate is listed in the CRL file, the client cannot authenticate the server successfully and the FTPS connection fails.

  Digital certificates support the PEM, ASN1, and PFX formats.

  - A PEM digital certificate has a file name extension .pem and is applicable to text transmission between systems.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- An ASN1 digital certificate has a file name extension .der and is the default format for most browsers.
- A PFX digital certificate has a file name extension .pfx and is a binary format that can be converted into the PEM or ASN1 format.

The CRL file supports the ASN1 and PEM formats.

For details, see the description about uploading files in other modes.

- **Configure an SSL policy and load the CA certificate and CRL file.**

Table 8-54 Configuring an SSL policy and loading the CA certificate and CRL file

Operation	Command	Description
Enter the system view.	**system-view**	-
(Optional) Customize SSL cipher suite.	**ssl cipher-suite-list** *customization-policy-name*	Customize an SSL cipher suite policy and enter the cipher suite policy view. By default, no customized SSL cipher suite policy is configured.
	set cipher-suite { **tls1_ck_rsa_with_aes_256_sha** | **tls1_ck_rsa_with_aes_128_sha** | **tls1_ck_rsa_rc4_128_sha** | **tls1_ck_dhe_rsa_with_aes_256_sha** | **tls1_ck_dhe_dss_with_aes_256_sha** | **tls1_ck_dhe_rsa_with_aes_128_sha** | **tls1_ck_dhe_dss_with_aes_128_sha** | **tls12_ck_rsa_aes_256_cbc_sha256** }	Configure the cipher suites for a customized SSL cipher suite policy. By default, no customized SSL cipher suite policy is configured. If a customized SSL cipher suite policy is being referenced by an SSL policy, the cipher suites in the customized cipher suite policy can be added, modified, or partially deleted. Deleting all of the cipher suites is not allowed.
	quit	Return to the system view.
Create the SSL policy and enter the SSL policy view.	**ssl policy** *policy-name*	-
(Optional) Set a minimum version of an SSL policy.	**ssl minimum version** { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }	By default, the minimum version of an SSL policy is TLS1.1.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
(Optional) Bind a customized SSL cipher suite policy to an SSL policy.	**binding cipher-suite-customization** *customization-policy-name*	By default, no customized cipher suite policy is bound to an SSL policy. Each SSL policy uses a default cipher suite. After a customized cipher suite policy is unbound from an SSL policy, the SSL policy uses one of the following cipher suites supported by default: ● tls1_ck_rsa_with_aes_256_sha ● tls1_ck_rsa_with_aes_128_sha ● tls1_ck_dhe_rsa_with_aes_256_sha ● tls1_ck_dhe_dss_with_aes_256_sha ● tls1_ck_dhe_rsa_with_aes_128_sha ● tls1_ck_dhe_dss_with_aes_128_sha ● tls12_ck_rsa_aes_256_cbc_sha256 If the cipher suite in the customized cipher suite policy bound to an SSL policy contains only one type of algorithm (RSA or DSS), the corresponding certificate must be loaded for the SSL policy to ensure successful SSL negotiation.
Load the CA certificate in the PEM format.	**trusted-ca load pem-ca** *ca-filename*	Load the CA certificate in the PEM, ASN1 or PFX format. A maximum of four CA certificates can be loaded in an SSL policy. The loaded CA certificates are added to the existing CA list. **NOTE** Before rolling V200R008C00 or a later version back to an earlier version, back up the SSL private key file.
Load the CA certificate in the ASN1 format.	**trusted-ca load asn1-ca** *ca-filename*	
Load the CA certificate in the PFX format.	**trusted-ca load pfx-ca** *ca-filename* **auth-code cipher** *auth-code*	

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Operation	Command	Description
Load the CRL file.	**crl load** { **pem-crl** | **asn1-crl** } *crl-filename*	A maximum of two CRL files can be loaded in an SSL policy. The loaded CRL files are added to the existing CRL file list.

NOTE

- If only one CA certificate exists on the FTPS server, configure all CA certificates of upper levels on the client.
- If a certificate chain exists on the FTPS server, configure only the root certificate on the client.
- If the CRL file is not loaded, the FTPS connection is not affected, but the client cannot authenticate the digital certificate of the server. You are advised to load the CRL file and update it periodically.

- **Connect to the FTPS server.**

Table 8-55 Connecting to the FTPS server

Operation	Command	Description
IPv4 address	**ftp ssl-policy** *policy-name* [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	Select one of them based on the IP address type. **NOTE** Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support **public-net** or **vpn-instance** *vpn-instance-name* parameter in the command.
IPv6 address	**ftp ssl-policy** *policy-name* **ipv6** *host-ipv6-address* [*port-number*]	

When connecting to the FTPS server, run the **ftp** command to enter the FTP client view and the **open** command to implement FTP connection.

Users must enter the correct user name and password to enter the FTP client view and manage files on the server.

- **Run FTP commands to perform file-related operations.**

After connecting to the FTPS server, users can run FTP commands to perform file-related operations on the FTPS server.

NOTE

User rights are configured on the FTP server.

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Users can perform the following operations in any sequence.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 8-56 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: < > ? \ :
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 one or more files.	**put** *local-filename* [*remote-filename*] Or **mput** *local-filenames*	● To upload a file, run the **put** command. ● To upload multiple files, run the **mput** command.
Download one or more files.	**get** *remote-filename* [*local-filename*] Or **mget** *remote-filenames*	● To download a file, run the **get** command. ● To download multiple files, run the **mget** command.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Operation	Command	Description
Set the file transfer mode to ASCII or Binary.	**ascii** Or **binary**	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 data transmission mode to passive or active.	**passive** Or **undo passive**	Select one of them. The default data transmission mode is active.
View the online help about FTP commands.	**remotehelp** [*command*]	-
Enable the system prompt function.	**prompt**	By default, the prompt function is disabled.
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 FTP connection between the new user and FTPS server is the same as that established by running the **ftp ssl-policy** 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 FTPS client from the FTPS server.**

  Users can run different commands in the FTP client view to disconnect the FTPS client from the FTPS server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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

Checking the Configurations

- Run the **display ssl policy** command to check the SSL policy, CA certificate, and CRL file configured on the FTPS client.

8.5 File Management Configuration Examples

8.5.1 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.

Figure 8-2 Networking diagram for logging in to the switch for file operations

Procedure

Step 1 View files and subdirectories in the current directory.

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] quit
<Switch> dir
Directory of flash:/
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
  Idx  Attr     Size(Byte)  Date        Time        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
...
65,233 KB total (7,289 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
```

Copy the **vrpcfg.zip** file to **test** and rename **vrpcfg.zip** as **backup.zip**.

```
<Switch> copy vrpcfg.zip flash:/test/backup.zip
```

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        FileName
    0  -rw-          2,399  Mar 12 2012 11:16:44   backup.zip

65,233 KB total (7,285 KB free)
```

----End

Configuration File

Switch configuration file

```
#
sysname Switch
#
return
```

8.5.2 Example for Configuring the FTP Server

Networking Requirements

As shown in **Figure 8-3**, routes between the PC and the device functioning as an FTP server are reachable. 10.136.23.5 is the management IP address of the FTP server. To upgrade the device, you must upload the system software **devicesoft.cc** to and download the configuration file **vrpcfg.zip** from the FTP server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 8-3 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. Save the **vrpcfg.zip** file on the FTP server.
3. Connect to the FTP server from the PC.
4. 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
[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
[FTP_Server] quit
```

Step 2 Save the **vrpcfg.zip** file on the FTP server.

```
<FTP_Server> save
```

Step 3 Connect to the FTP server from the PC as user **admin1234** whose password is **Helloworld@6789** and transfer files in binary mode.

Assume that the PC runs the Windows 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 4 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: 23876556 bytes sent in 25.35Seconds 560.79Kbytes/sec.
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 5 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
    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-     23,876,556  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
...
65,233 KB total (7,289 KB free)
```

Access the FTP user's local directory on the PC and check the **vrpcfg.zip** file.

----End

Configuration File

FTP_Server configuration file

```
#
sysname FTP_Server
#
FTP server enable
#
aaa
 local-user admin1234 password irreversible-cipher %^%#P2m&M5d"'JHR7b~SrcHF\Z\,
2R"t&6V|zOLh9y$>M\bjG$D>%@Ug/<3I$+=Y%^%#
 local-user admin1234 privilege level 15
 local-user admin1234 ftp-directory flash:/
 local-user admin1234 service-type ftp
#
return
```

Related Content

Videos

Remotely Transfer Files Using FTP.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

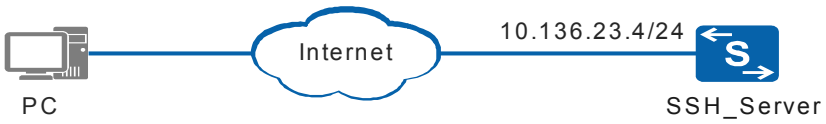
e-DOC 16A8F5D0-e
Proc 13409/2016

8.5.3 Example for Configuring the SFTP Server

Networking Requirements

As shown in **Figure 8-4**, routes between the PC and the device functioning as an SSH server are reachable. 10.136.23.4 is the management IP address on the SSH server. Configure the device as an SSH server so that the server can authenticate the client and encrypt data in bidirectional mode. This prevents man-in-middle attacks and MAC/IP address spoofing and ensures secure file transfer.

Figure 8-4 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, service type, authorized directory, user name, and password.
4. 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] dsa local-key-pair create
Info: The key name will be:
SSH_Server_Host_DSA.

Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus
[default=2048]:

Info: Generating
keys...

Info: Succeeded in creating the DSA host keys.
[SSH_Server] sftp server enable
```

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
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 3 Configure SSH user information including the authentication mode, service type, authorized directory, user name, and password.

```
[SSH_Server] ssh user client001 authentication-type password
[SSH_Server] ssh user client001 service-type sftp
[SSH_Server] ssh user client001 sftp-directory flash:
[SSH_Server] aaa
[SSH_Server-aaa] local-user client001 password irreversible-cipher Helloworld@6789
[SSH_Server-aaa] local-user client001 privilege level 15
[SSH_Server-aaa] local-user client001 service-type ssh
[SSH_Server-aaa] quit
```

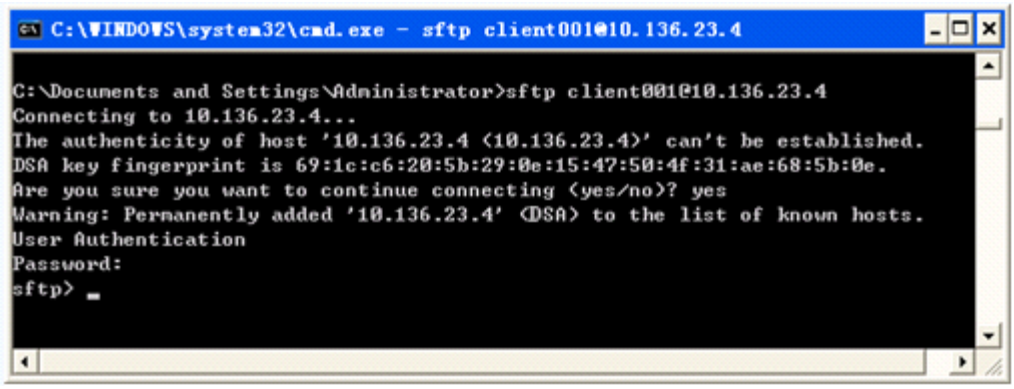
Step 4 Connect to the SSH server using the third-party software OpenSSH on the PC.

The Windows CLI can identify OpenSSH commands only when the OpenSSH is installed on the PC.

NOTE

Use the OpenSSH of a version matching the terminal operating system; otherwise, you may fail to access the switch through SFTP.

Figure 8-5 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

SSH_Server configuration file

```
#
sysname SSH_Server
#
aaa
 local-user client001 password irreversible-cipher %^%#P2m&M5d"'JHR7b~SrcHF\Z\,
2R"t&6V|zOLh9y$>M\bjG$D>%@Ug/<3I$+=Y%^%#
 local-user client001 privilege level 15
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
#
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
user-interface vty 0 14
 authentication-mode aaa
#
return
```

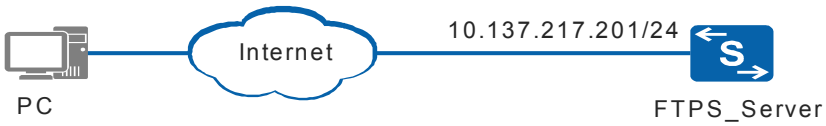
8.5.4 Example for Configuring the FTPS Server

Networking Requirements

As shown in **Figure 8-6**, routes between the PC and the device functioning as an FTPS server are reachable. 10.137.217.201 is the management IP address on the FTPS server.

The FTP server function does not provide security mechanisms. Data are transmitted in plain text, which cannot prevent man-in-middle attacks and MAC/IP address spoofing. To overcome this limitation, configure the SSL policy, data encryption, user identity authentication, and message integrity check mechanisms on the FTPS server to ensure secure file transfer. SSL ensures secure connection based on the FTP server function.

Figure 8-6 Networking diagram for managing files when the device functions as an FTPS server



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the FTP server function on the device and upload the digital certificate to the root directory on the device.
2. On the device, copy the digital certificate to the **security** directory, configure the SSL policy, and load the digital certificate so that the client can authenticate the server.
3. Enable the FTPS server function and configure the local FTP user.
4. Connect to the FTPS server using a third-party software.

Procedure

Step 1 Configure the FTP server function on the server and upload the digital certificate to the server.

Enable the FTP server function and configure FTP user information.

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Server
[FTPS_Server] ftp server enable
[FTPS_Server] aaa
[FTPS_Server-aaa] local-user admin password irreversible-cipher huawei@6789
[FTPS_Server-aaa] local-user admin service-type ftp
[FTPS_Server-aaa] local-user admin privilege level 3
[FTPS_Server-aaa] local-user admin ftp-directory flash:
[FTPS_Server-aaa] quit
[FTPS_Server] quit
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Access the Windows CLI and run the **ftp** *FTP server IP address* command to connect to the FTP server. Enter the correct user name and password to connect to the FTP server. Upload the digital certificate and private key to the FTP server.

Run the **dir** command on the FTP server to check the digital certificate and private key.

```
<FTPS_Server> dir
Directory of flash:/

Idx  Attr     Size(Byte)  Date        Time         FileName
    0  drw-              -  May 10 2011 05:05:40   src
    1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
    2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
    3  -rw-          1,302  May 10 2011 05:32:05   4_servercert_der_dsa.der
    4  -rw-            951  May 10 2011 05:32:44   4_serverkey_der_dsa.der
...
65,233 KB total (7,289 KB free)
```

Step 2 Configure the SSL policy and load the digital certificate.

Create the **security** directory and copy the digital certificate to the **security** directory.

```
<FTPS_Server> mkdir security/
<FTPS_Server> move 4_servercert_der_dsa.der security/
<FTPS_Server> move 4_serverkey_der_dsa.der security/
```

Run the **dir** command in the **security** directory to check the digital certificate and private key.

```
<FTPS_Server> cd security/
<FTPS_Server> dir
Directory of flash:/security/

  Idx  Attr     Size(Byte)  Date        Time         FileName
    0  -rw-          1,302  May 10 2011 05:44:34   4_servercert_der_dsa.der
    1  -rw-            951  May 10 2011 05:45:22   4_serverkey_der_dsa.der

65,233 KB total (7,289 KB free)
```

Configure the SSL policy and load the digital certificate in the ASN1 format.

```
<FTPS_Server> system-view
[FTPS_Server] ssl policy ftp_server
[FTPS_Server-ssl-policy-ftp_server] certificate load asn1-cert
4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
[FTPS_Server-ssl-policy-ftp_server] quit
```

Step 3 Enable the FTPS server function and configure the local FTP user.

Enable the FTPS server function.

NOTE

Disable the FTP server function before enabling the FTPS server function.

```
[FTPS_Server] undo ftp server
[FTPS_Server] ftp secure-server ssl-policy ftp_server
[FTPS_Server] ftp secure-server enable
```

Configure the local FTP user.

Use the **admin** user configured in the preceding step.

Step 4 Connect to the FTPS server using a third-party software.

For details, see related third-party documentation.

Step 5 Verify the configurations.

Run the **display ssl policy** command on the FTPS server to view detailed certificate information.

```
[FTPS_Server] display ssl policy
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
      SSL Policy Name: ftp_server
    Policy Applicants:
        Key-pair Type: DSA
Certificate File Type: ASN1
     Certificate Type: certificate
 Certificate Filename: 4_servercert_der_dsa.der
    Key-file Filename: 4_serverkey_der_dsa.der
            Auth-code:
                  MAC:
             CRL File:
      Trusted-CA File:
          Issuer Name:
  Validity Not Before:
   Validity Not After:
```

Run the **display ftp-server** command on the FTPS server to view the SSL policy name and the FTPS server status.

```
[FTPS_Server] display ftp-server
  FTP server is stopped
  Max user number                 5
  User count                      1
  Timeout value(in minute)        30
  Listening port                  21
  Acl number                      0
  FTP server's source address     0.0.0.0
  FTP SSL policy                  ftp_server
  FTP Secure-server is running
```

The FTP server supporting SSL can securely connect to the FTPS server, upload files, and download files.

----End

Configuration File

FTPS_Server configuration file

```
#
sysname FTPS_Server
#
FTP secure-server enable
ftp secure-server ssl-policy ftp_server
#
aaa
 local-user admin password irreversible-cipher %^%#P2m&M5d"'JHR7b~SrcHF\Z\,
2R"t&6V|zOLh9y$>M\bjG$D>%@Ug/<3I$+=Y%^%#
 local-user admin privilege level 3
 local-user admin ftp-directory flash:
 local-user admin service-type ftp
#
ssl policy ftp_server
 certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file
4_serverkey_der_dsa.der
#
return
```

8.5.5 Example for Configuring the TFTP Client

Networking Requirements

As shown in **Figure 8-7**, 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 8-7 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.
23876556 bytes received in 199 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.

```
<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-     23,876,556  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
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
...
65,233 KB total (7,289 KB free)
```

Access the working directory on the TFTP server and check the **vrpcfg.zip** file.

----End

Configuration File

None

8.5.6 Example for Configuring an FTP Client

Networking Requirements

As shown in **Figure 8-8**, 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 8-8 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.
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.
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
[ftp]
```

Step 3 Run FTP commands to download **devicesoft.cc** from and upload **vrpcfg.zip** to the FTP server.

```
[ftp] binary
[ftp] get devicesoft.cc
[ftp] put vrpcfg.zip
[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-     23,876,556  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
...
65,233 KB total (7,289 KB free)
```

Access the working directory on the FTP server and check the **vrpcfg.zip** file.

----End

Configuration File

None

8.5.7 Example for Configuring an SFTP Client

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 8-9**, routes between the SSH server and clients client001 and client002 are reachable. In this example, Huawei device functions as an SSH server.

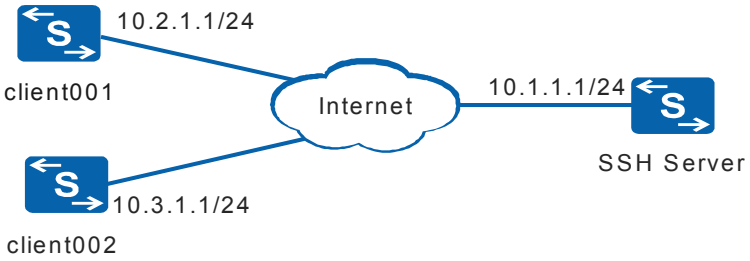
Client001 connects to the SSH server using the password authentication mode, and client002 using the DSA authentication mode.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 8-9 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 DSA 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] dsa local-key-pair create
Info: The key name will be: SSH
Server_Host_DSA.

Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus
[default=2048]:

Info: Generating
keys...

Info: Succeeded in creating the DSA host keys.
[SSH Server] sftp server enable
```

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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[SSH Server] ssh user client001
[SSH Server] ssh user client001 authentication-type password
[SSH Server] ssh user client001 service-type sftp
[SSH Server] ssh user client001 sftp-directory flash:
[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
```

Create an SSH user **client002** and set the authentication mode to **dsa** for the user.

```
[SSH Server] ssh user client002
[SSH Server] ssh user client002 authentication-type dsa
[SSH Server] ssh user client002 service-type sftp
[SSH Server] ssh user client002 sftp-directory flash:
```

Step 3 Generate a local key pair on client002 and configure the DSA public key of client002 on the SSH server.

Generate a local key pair on client002.

```
<HUAWEI> system-view
[HUAWEI] sysname client002
[client002] dsa local-key-pair create
Info: The key name will be: SSH
Server_Host_DSA.

Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus
[default=2048]:

Info: Generating
keys...

Info: Succeeded in creating the DSA host keys.
[client002] sftp server enable
```

Check the DSA public key of the client.

```
[client002] display dsa local-key-pair public

=====================================================
Time of Key pair created: 2014-03-03 19:11:04+00:00
Key name: client002_Host
Key type: DSA encryption Key
=====================================================
Key code:
30820109
  02820100
    C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC
    8EA252B0 E90A5001 1F2567C6 3952DEFD 95EF93C2
    D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187
    04FD6A03 C4FFDB58 04B3A0C4 B6E50528 AAE56FF9
    5F66EE00 8E4702DB AA764006 322E6F72 CC9C1A39
    462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA
    20C9CB60 98E5ACDA 2E98B55A 0299FBAB FE91EFA3
    E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
    2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685
    BD8D6325 CCBE3F32 85435E5B EB6A08DF 752B7EBD
    CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6
    D12B4BA3 6E9EF69F A5BED377 954709EB CE29A923
    04B347D7 29296E7D 3D5F69AB 4365AA2F
  0203
    010001

 Host public key for PEM format code:
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAABAQDH2S4n6IdF1JM6sfXaaSrEHVRL3I6iUrDp
ClABHyVnxjlS3v2V75PC136M37Nuf0NXwde6CXjdei9/cYcE/WoDxP/bWASzoMS2
5QUoquVv+V9m7gCORwLbqnZABjIub3LMnBo5Ri280OqTREEWeLojQEc+xFjfhPog
yctgmOWs2i6YtVoCmfur/pHvo+FV4GV8f/zUTqtx7KenPdeshHS3LdN9HHEMbhRX
2iAMR35FvDisdoW9jWMlzL4/MoVDXlvragjfdSt+vc4hz8vzrAw1Zx5azK/DbwtU
5kb20StLo26e9p+lvtN3lUcJ684pqSMEs0fXKSlufT1faatDZaov
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-dsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDH2S4n6IdF1JM6sfXaaSrEHVRL3I6iUrDpClABHyVnxjlS3v2V75
PC136M37Nuf0NXwde6CXjdei9/cYcE/WoDxP/bWASz
oMS25QUoquVv+V9m7gCORwLbqnZABjIub3LMnBo5Ri280OqTREEWeLojQEc
+xFjfhPogyctgmOWs2i6YtVoCmfur/pHvo+FV4GV8f/zUTqtx7KenPdeshHS3LdN9HHEMbhRX
2iAMR35FvDisdoW9jWMlzL4/MoVDXlvragjfdSt+vc4hz8vzrAw1Zx5azK/DbwtU5kb20StLo26e9p
+lvtN3lUcJ684pqSMEs0fXKSlufT1faatDZaov= dsa-key
```

Configure the DSA public key of client002 on the SSH server. (Information in bold in the **display** command output is the DSA public key of client002. Copy the information to the server.)

```
[SSH Server] dsa peer-public-key dsakey001 encoding-type der
[SSH Server-dsa-public-key] public-key-code begin
[SSH Server-dsa-key-code] 30820109
[SSH Server-dsa-key-code] 02820100
[SSH Server-dsa-key-code] C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC
[SSH Server-dsa-key-code] 8EA252B0 E90A5001 1F2567C6 3952DEFD 95EF93C2
[SSH Server-dsa-key-code] D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187
[SSH Server-dsa-key-code] 04FD6A03 C4FFDB58 04B3A0C4 B6E50528 AAE56FF9
[SSH Server-dsa-key-code] 5F66EE00 8E4702DB AA764006 322E6F72 CC9C1A39
[SSH Server-dsa-key-code] 462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA
[SSH Server-dsa-key-code] 20C9CB60 98E5ACDA 2E98B55A 0299FBAB FE91EFA3
[SSH Server-dsa-key-code] E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
[SSH Server-dsa-key-code] 2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685
[SSH Server-dsa-key-code] BD8D6325 CCBE3F32 85435E5B EB6A08DF 752B7EBD
[SSH Server-dsa-key-code] CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6
[SSH Server-dsa-key-code] D12B4BA3 6E9EF69F A5BED377 954709EB CE29A923
[SSH Server-dsa-key-code] 04B347D7 29296E7D 3D5F69AB 4365AA2F
[SSH Server-dsa-key-code] 0203
[SSH Server-dsa-key-code] 010001
[SSH Server-dsa-key-code] public-key-code end
[SSH Server-dsa-public-key] peer-public-key end
```

Bind the **client002** user to the DSA public key of client002.

```
[SSH Server] ssh user client002 assign dsa-key dsakey001
```

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.

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.

```
[client002] sftp 10.1.1.1
Please input the
username:client002
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
Trying
10.1.1.1 ...

Press CTRL+K to
abort

Connected to
10.1.1.1 ...

password:SSH_SERVER_CODE



Please select public key type for user authentication [R for RSA; D for DSA;
Enter for Skip publickey authentication; Ctrl_C for Cancel], Please select [R, D,
Enter or
Ctrl_C]:D



sftp-client>
```

Log in to the SSH server from client002 in DSA 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 ...

password:SSH_SERVER_CODE



Please select public key type for user authentication [R for RSA; D for DSA;
Enter for Skip publickey authentication; Ctrl_C for Cancel], Please select [R, D,
Enter or
Ctrl_C]:D



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
 Scp server                           :Disable
 SSH server source                    :0.0.0.0
 ACL4 number                          :0
 ACL6 number                          :0
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Check information about SSH users.

```
[SSH Server] display ssh user-information
  User 1:
       User Name             : client001
       Authentication-type   : password
       User-public-key-name  : -
       User-public-key-type  : -
       Sftp-directory        : flash:
       Service-type          : sftp
       Authorization-cmd     : No
  User 2:
       User Name             : client002
       Authentication-type   : dsa
       User-public-key-name  : dsakey001
       User-public-key-type  : dsa
       Sftp-directory        : flash:
       Service-type          : sftp
       Authorization-cmd     : No
```

----End

Configuration Files

- SSH server configuration file

```
#
sysname SSH Server
#
dsa peer-public-key dsakey001 encoding-type der
 public-key-code begin
  30820109
    02820100
      C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC 8EA252B0 E90A5001 1F2567C6
      3952DEFD 95EF93C2 D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187 04FD6A03
      C4FFDB58 04B3A0C4 B6E50528 AAE56FF9 5F66EE00 8E4702DB AA764006 322E6F72
      CC9C1A39 462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA 20C9CB60 98E5ACDA
      2E98B55A 0299FBAB FE91EFA3 E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
      2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685 BD8D6325 CCBE3F32 85435E5B
      EB6A08DF 752B7EBD CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6 D12B4BA3
      6E9EF69F A5BED377 954709EB CE29A923 04B347D7 29296E7D 3D5F69AB 4365AA2F
    0203
      010001
 public-key-code end
peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher %^%#P2m&M5d"'JHR7b~SrcHF\Z
\,2R"t&6V|zOLh9y$>M\bjG$D>%@Ug/<3I$+=Y%^%#
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
ssh user client002
ssh user client002 authentication-type dsa
ssh user client002 assign dsa-key dsakey001
ssh user client002 service-type sftp
ssh user client002 sftp-directory flash:
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
#
return
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Client001 configuration file

```
#
sysname client001
#
ssh client first-time enable
#
return
```

- Client002 configuration file

```
#
sysname client002
#
ssh client first-time enable
#
return
```

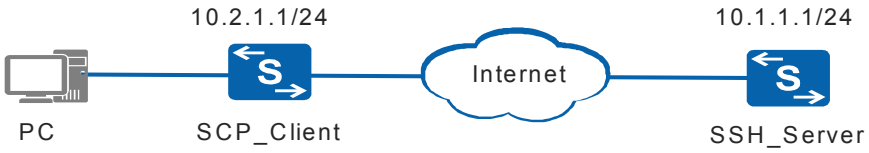
8.5.8 Example for Configuring an SCP Client

Networking Requirements

Compared with the SFTP protocol, the SCP protocol can authenticate user identity while transferring files, improving configuration efficiency.

As shown in **Figure 8-10**, routes between the device functioning as the SCP client and the SSH server are reachable. The SCP client can download files from the SSH server.

Figure 8-10 Networking diagram for managing files when the device functions as an SCP client



Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair on the SSH server.
2. Create an SSH user on the SSH server.
3. Enable the SCP function on the SSH server.
4. Download the **backup.cfg** file from the SSH server.

Procedure

Step 1 Generate a local key pair on the SSH server.

```
<HUAWEI> system-view
[HUAWEI] sysname SSH_Server
[SSH_Server] dsa local-key-pair create
Info: The key name will be:
SSH_Server_Host_DSA.

Info: The key modulus can be any one of the following : 1024,
2048.
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus
[default=2048]:

Info: Generating
keys...

Info: Succeeded in creating the DSA host keys.
```

Step 2 Create an SSH user on the SSH server.

Configure the VTY user interface.

```
[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
```

Create an SSH user **client001** and set the authentication mode to **password** and service type to **all**.

```
[SSH_Server] ssh user client001
[SSH_Server] ssh user client001 authentication-type password
[SSH_Server] ssh user client001 service-type all
```

Set the password of the **client001** user to **Helloworld@6789**.

```
[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
```

Step 3 Enable the SCP function on the SSH server.

```
[SSH_Server] scp server enable
```

Step 4 Download the **backup.cfg** file from the SSH server.

If the client connects to the SSH server for the first time, enable the initial authentication function on the client.

```
<HUAWEI> system-view
[HUAWEI] sysname SCP_Client
[SCP_Client] ssh client first-time enable
```

Use the aes256 encryption algorithm to download the **backup.cfg** file from the SSH server to the local user's directory.

```
[SCP_Client] scp -cipher aes256 client001@10.1.1.1:backup.cfg backup.cfg
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server has not been authenticated. Continue to access it? [Y/N]:y
Do you want to save the server's public key? [Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait.
..
Enter password:
backup.cfg                    100%        19174Bytes            7KByte(s)/sec
```

----End

Configuration File

- SSH_Server configuration file

```
#
sysname SSH_Server
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
#
aaa
 local-user client001 password irreversible-cipher %^%#P2m&M5d"'JHR7b~SrcHF\Z
\,2R"t&6V|zOLh9y$>M\bjG$D>%@Ug/<3I$+=Y%^%#
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
scp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type all
#
user-interface vty 0 14
 authentication-mode aaa
#
return
```

- SCP_Client configuration file

```
#
sysname SCP_Client
#
ssh client first-time enable
#
return
```

8.5.9 Example for Configuring an FTPS Client

Networking Requirements

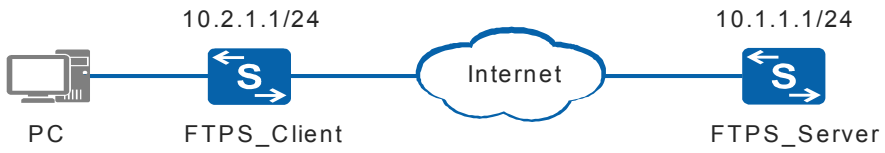
The FTP server function does not provide security mechanisms. Data are transmitted in plain text, which cannot prevent man-in-middle attacks and MAC/IP address spoofing. To overcome this limitation, configure the SSL policy, data encryption, user identity authentication, and message integrity check mechanisms on the FTPS server to ensure secure file transfer. SSL ensures secure connection based on the FTP server function.

As shown in **Figure 8-11**, routes between the device functioning as the FTPS client and the FTPS server are reachable. The FTPS client can securely connect to the FTPS server to manage files.

- On the FTPS client, configure the SSL policy and load the CA certificate to check the owner's identity.
- On the FTPS server, configure the SSL policy, load the digital certificate to check the owner's identity, and enable the FTPS server function.

Obtain required certificates for the FTPS client and server from the CA. In this example, Huawei device functions as the FTPS server.

Figure 8-11 Networking diagram for managing files when the device functions as an FTPS client



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Configuration Roadmap

The configuration roadmap is as follows:

1. Upload the certificates.
   - Upload the digital certificate and private key to the root directory on the FTPS server.
   - Upload the CA certificate to the root directory on the FTPS client.
2. Load the certificates and configure SSL policies.
   - On the FTPS server, copy the digital certificate to the **security** directory, configure the SSL policy, and load the digital certificate.
   - On the FTPS client, copy the CA certificate to the **security** directory, configure the SSL policy, and load the digital certificate.
3. Enable the FTPS server function and configure the local FTP user.
4. Run the FTP command to connect to the FTPS server and remotely manage files.

Procedure

Step 1 Upload the certificates.

- Configure the FTP function on the client and server and upload the certificates to the client and server. For details, see **8.3.2 Managing Files When the Device Functions as an FTP Server**.

  # Run the **dir** command on the FTPS server to check the digital certificate and private key.

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Server
[FTPS_Server] quit
<FTPS_Server> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time        FileName
    0  drw-              -  May 10 2011 05:05:40   src
    1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
    2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
    3  -rw-          1,302  Mar 13 2012 18:23:28   4_servercert_der_dsa.der
    4  -rw-            951  Mar 13 2012 18:30:20   4_serverkey_der_dsa.der
...

65,233 KB total (7,289 KB free)
```

  # Run the **dir** command on the client to check the CA certificate.

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Client
[FTPS_Client] quit
<FTPS_Client> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time        FileName
    0  -rw-        524,558  May 10 2011 04:50:39   private-data.txt
    1  -rw-          1,237  Mar 14 2012 07:46:24   cacert.der
    2  -rw-          1,241  Mar 14 2012 07:46:20   rootcert.der
    3  drw-              -  Apr 09 2011 19:46:14   src
    4  -rw-            421  Apr 09 2011 19:46:14   vrpcfg.zip
    5  -rw-      1,308,478  Apr 14 2011 19:22:45   we1.zip
    6  drw-              -  Apr 10 2011 01:35:54   logfile
    7  -rw-              4  Apr 19 2011 04:24:28   snmpnotilog.txt
    8  drw-              -  Apr 13 2011 11:37:40   lam
...
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
65,233 KB total (17,489 KB free)
```

Step 2 Configure the SSL policy and load the certificates.

- Perform the following operations on the FTPS server.

  # Create the **security** directory and move the digital certificate to the **security** directory.

```
<FTPS_Server> mkdir security/
<FTPS_Server> move 4_servercert_der_dsa.der security/
<FTPS_Server> move 4_serverkey_der_dsa.der security/
```

  # Run the **dir** command in the **security** directory to check the digital certificate and private key.

```
<FTPS_Server> cd security/
<FTPS_Server> dir
Directory of flash:/security/

  Idx  Attr     Size(Byte)  Date        Time        FileName
    0  -rw-          1,302  Mar 13 2012 18:23:28    4_servercert_der_dsa.der
    1  -rw-            951  Mar 13 2012 18:30:20    4_serverkey_der_dsa.der

65,233 KB total (7,289 KB free)
```

  # Configure the SSL policy and load the digital certificate in the ASN1 format.

```
<FTPS_Server> system-view
[FTPS_Server] ssl policy ftp_server
[FTPS_Server-ssl-policy-ftp_server] certificate load asn1-cert
4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
[FTPS_Server-ssl-policy-ftp_server] quit
```

  # Run the **display ssl policy** command on the FTPS server to view detailed certificate information.

```
[FTPS_Server] display ssl policy

      SSL Policy Name: ftp_server
    Policy Applicants:
        Key-pair Type: DSA
Certificate File Type: ASN1
     Certificate Type: certificate
 Certificate Filename: 4_servercert_der_dsa.der
    Key-file Filename: 4_serverkey_der_dsa.der
            Auth-code:
                  MAC:
             CRL File:
      Trusted-CA File:
          Issuer Name:
  Validity Not Before:
   Validity Not After:
```

- Perform the following operations on the FTPS client:

  # Create the **security** directory and move the CA certificate to the **security** directory.

```
<FTPS_Client> mkdir security/
<FTPS_Client> move cacert.der security/
<FTPS_Client> move rootcert.der security/
```

  # When the CA certificate is copied to the **security** directory, run the **dir** command in the **security** directory to check the CA certificate.

```
<FTPS_Client> cd security/
<FTPS_Client> dir
Directory of flash:/security/

  Idx  Attr     Size(Byte)  Date        Time        FileName
    0  -rw-          1,237  Mar 14 2012 07:46:24    cacert.der
    1  -rw-          1,241  Mar 14 2012 07:46:20    rootcert.der

65,233 KB total (17,489 KB free)
```

  # Configure the SSL policy and load the CA certificate.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
<FTPS_Client> system-view
[FTPS_Client] ssl policy ftp_client
[FTPS_Client-ssl-policy-ftp_client] trusted-ca load asn1-ca cacert.der
[FTPS_Client-ssl-policy-ftp_client] trusted-ca load asn1-ca rootcert.der
[FTPS_Client-ssl-policy-ftp_client] quit
```

Run the **display ssl policy** command on the FTPS client to view detailed certificate information.

```
[FTPS_Client] display ssl policy

      SSL Policy Name: ftp_client
    Policy Applicants:
        Key-pair Type:
Certificate File Type:
     Certificate Type:
 Certificate Filename:
    Key-file Filename:
            Auth-code:
                  MAC:
             CRL File:
      Trusted-CA File:
    Trusted-CA File 1: Format = ASN1, Filename = cacert.der
    Trusted-CA File 2: Format = ASN1, Filename = rootcert.der
```

Step 3 Enable the FTPS server function and configure the local FTP user.

Enable the FTPS server function.

NOTE

Disable the FTP server function before enabling the FTPS server function.

```
[FTPS_Server] undo ftp server
[FTPS_Server] ftp secure-server ssl-policy ftp_server
[FTPS_Server] ftp secure-server enable
```

Configure the local FTP user.

```
[FTPS_Server] aaa
[FTPS_Server-aaa] local-user admin password irreversible-cipher Helloworld@6789
[FTPS_Server-aaa] local-user admin service-type ftp
[FTPS_Server-aaa] local-user admin privilege level 3
[FTPS_Server-aaa] local-user admin ftp-directory flash:
[FTPS_Server-aaa] quit
```

You can use the user who uploads the certificates or create a new user.

Step 4 On the FTPS client, run the FTP command to connect to the FTPS server and remotely manage files.

```
[FTPS_Client] ftp ssl-policy ftp_client 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
234 AUTH command successfully, Security mechanism accepted.
200 PBSZ is ok.
200 Data channel security level is changed to private.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.

[ftp]
```

To connect to the FTPS server, enter the correct user name and password.

Step 5 Verify the configurations.

Run the **display ftp-server** command on the FTPS server to view the SSL policy name and the FTPS server status.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
[FTPS_Server] display ftp-server
  FTP server is stopped
  Max user number                 5
  User count                      1
  Timeout value(in minute)        30
  Listening port                  21
  Acl number                      0
  FTP server's source address     0.0.0.0
  FTP SSL policy                  ftp_server
  FTP Secure-server is running
```

Manage files remotely on the FTPS client.

----End

Configuration File

- FTPS_Server configuration file

```
#
sysname FTPS_Server
#
FTP secure-server enable
ftp secure-server ssl-policy ftp_server
#
aaa
 local-user admin password irreversible-cipher %^%#P2m&M5d"'JHR7b~SrcHF\Z\,
2R"t&6V|zOLh9y$>M\bjG$D>%@Ug/<3I$+=Y%^%#
 local-user admin privilege level 3
 local-user admin ftp-directory flash:
 local-user admin service-type ftp
#
ssl policy ftp_server
 certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file
4_serverkey_der_dsa.der
#
return
```

- FTPS_Client configuration file

```
#
sysname FTPS_Client
#
ssl policy ftp_client
 trusted-ca load asn1-ca cacert.der
 trusted-ca load asn1-ca rootcert.der
#
return
```

8.6 Common Misconfigurations

8.6.1 FTP Login Failure

Possible Causes

- 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- 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
  FTP SSL policy
  FTP Secure-server is stopped
```

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
  Acl number                      0
  FTP server's source address     0.0.0.0
  FTP SSL policy
  FTP Secure-server is stopped
```

If the listening port number is not 21, run the **ftp server port** command to set the listening port number to 21.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
<HUAWEI> system-view
[HUAWEI] undo ftp server
Warning: The operation will stop the FTP server. Continue? [Y/N]:y
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 setting 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 supports all service types. If you set the **service-type** parameter, only the service types that you set are available to the FTP user.

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

8.6.2 File Upload Failure

Possible Causes

- The source or destination directory contains characters not supported by the device, such as spaces.
- The server root directory does not have sufficient storage space.
- The MTU on the server or client is modified. The size of data frames sent by the server or client exceeds the maximum value of the peer device or a device on the transmission path. As a result, the data frames are discarded.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Procedure

Step 1 Check whether the source or destination directory contains characters not supported by the device, such as spaces.

The directory name cannot contain spaces and the following special characters: ~ * / \ : ' ".

If the directory contains any of these characters, modify the directory.

Step 2 Check whether the storage space of the server root directory is sufficient.

Run the **dir** command on the server to check the available space of the server root directory.

If the storage space is insufficient, run the **delete /unreserved** command in the user view to delete outdated files.

Step 3 Check whether the MTU on the server or client interface exceeds the maximum value supported by the device.

Run the **display this** command in the interface view on the server or client to check the MTU value. If no value is displayed, the default value 1500 is used.

If the MTU exceeds the maximum value of the server or client, run the **mtu** command in the interface view to set the MTU to a smaller value. For details on the largest frame size supported by a device, see "What Is the MTU of an Interface and What Is the Largest Frame Size Allowed on an Interface?" in *FAQs - Interface Management*.

----End

8.7 FAQ

8.7.1 How to View the Deleted Files in the System?

The device provides the recycle bin. The file that is deleted through the **delete** command can be saved in the recycle bin. The file is deleted permanently if you run the **delete/unreserved** command.

The **dir** command does not display the files that are placed into the recycle bin. The files in the recycle bin can be displayed through the **dir/all** command only. The name of the file in the recycle bin is bracketed by square brackets ([]).

8.7.2 Which SSH Version Does the Device Support?

The device supports SSH v1.99 and allows SSH clients of v1.x and v2.0 to connect to it.

The device can only function as the SSH client of v2.0. When the device functions as the SSH server, it allows SSH clients of v1.x and v2.0 to log in.

8.7.3 Why Local Users Must Be Configured on a Device When SSH Users Configure Remote Authentication?

Configuring local users on a device is optional. When the **ssh authentication-type default password** command is used on a device, you do not need to configure local users.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

8.7.4 How Can I Repair a Storage Device Where an Exception Occurred?

- The **dir** command displays information about the specified file or directory on the device. If the command output contains **unknown**, for example, 30,000 KB total (672 KB free, 25,560 KB used, **3,616 KB unknown**), run the **fixdisk** *device-name* command in the user view to release the **unknown** space.

  Do not run the **fixdisk** *device-name* command when the system works properly.
- If no file is displayed after you run the **dir** command, but the storage space is occupied, the following scenario may occur:

  Deleted files are in the recycle bin. Run the **dir /all** command to display all files, including deleted files that are contained in square brackets []. To restore these deleted files, run the **undelete** command. To deleted the files in the recycle bin, run the **reset recycle-bin** command.

NOTICE

- After you run the **fixdisk** *device-name* command, all the files and directories in the specified storage device will be deleted. Exercise caution when determining whether to run these commands because the files and directories cannot be restored after being deleted.
- The **fixdisk** *device-name* command cannot rectify device-level faults.

8.7.5 How to Delete the Files in the Recycle Bin?

Using the **reset recycle-bin** [*filename*] command, you can delete the files in the recycle bin. The files in the recycle bin cannot be restored after being deleted.

8.7.6 How Do I Upload or Download Files?

You can transfer files between two devices or between a device and a host through the console port, File Transfer Protocol (FTP), Secure Copy Protocol (SCP), Trivial File Transfer Protocol (TFTP), Secure File Transfer Protocol (SFTP), or FTP over Secure Sockets Layer (FTPS). The device and host can function as the server or client during file transfer. **Table 8-57** describes the application scenarios, advantages, and disadvantages of each file transfer mode. You can select one mode based on actual needs. For details on the file transfer modes, see "File Management" in the *Configuration Guide - Basic Configuration*.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 8-57 File transfer modes

File Transfer Mode	Application Scenario	Advantage	Disadvantage
Console port	Applies when the device is not deployed on a network or the management port of the device is damaged.	● Only one serial cable is required to connect a host and a device. ● This mode prevents security risks of the network.	The file transfer speed is low.
FTP	Applies to scenarios where there is no requirement for high security, for example, version upgrade scenario.	● This mode is easy to configure. ● This mode provides authorization and authentication functions.	Data is transmitted in plain text, resulting in potential security risks.
TFTP	On a lab local area network (LAN), you can perform online version upload or upgrade using TFTP. TFTP is used when the client and server do not need complex interactions.	TFTP consumes fewer memory resources than FTP.	TFTP does not provide authorization and authentication functions and transmits data in plain text. There are potential security risks because the devices are prone to viruses and network attacks.
SFTP	Applies to scenarios demanding high network security, for example, log download and configuration file backup scenarios.	Encryption and integrity check are performed for data, with high security.	The configuration is complex.
SCP	Applies to scenarios demanding high network security and high file upload/ download efficiency.	● Encryption and integrity check are performed for data, with high security. ● This mode features high efficiency because the same command is used to set up a connection between the client and server and complete the file upload/download operation simultaneously.	The configuration is complex (similar to that of the SFTP mode).

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

File Transfer Mode	Application Scenario	Advantage	Disadvantage
FTPS	Applies to scenarios where high network security is required and FTP cannot be used.	The FTPS protocol uses data encryption, identity authentication, and message integrity check to ensure security of TCP-based application layer protocols.	The configuration is complex, and you need to obtain a certificate from the Certificate Authority (CA) in advance.

NOTE

- The console port uses XModem as the transmission protocol. Select the correct transmission protocol when you transfer files.
- When TFTP is used, the device can function as the client only. When FTP, SFTP, SCP, or FTPS is used, the device can function as the client or server.
- When uploading system files to a device, ensure that the power supply of the device is normal. Otherwise, the files or the file system will be damaged. The device's storage media will be damaged or the device fails to work properly.
- The device cannot automatically download files from a server at a specified time using the console port, FTP, SFTP, SCP, TFTP, or FTPS.

8.7.7 How Do I Limit the FTP Upload or Download Speed?

The FTP protocol does not provide a rate limit mechanism. You can configure the rate limit on the communication interface of the FTP client or server to limit the FTP upload or download speed. For details, see "Traffic Policing, Traffic Shaping, and Interface-based Rate Limiting" in the *Configuration Guide - QoS*.

8.7.8 How Do I Check Whether an Uploaded File Is Complete?

After you upload a file, you can compare the file size before and after the file upload to check whether the uploaded file is complete. Before uploading the file, check and record the file size. After uploading the file, run the **dir** command to check the file size in the storage medium. If the file sizes are the same, the uploaded file is complete. If they are different, the uploaded file is incomplete. You need to run the **delete** command to delete the file and upload the file again.

```
<HUAWEI> dir /all
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time        FileName
    0  -rw-             14  Feb 27 2012 11:20:12   back_time_a
    1  -rw-             16  Dec 28 2011 13:10:56   abc.tbl
    2  drw-              -  Feb 25 2012 14:19:56   logfile
    3  drw-              -  Oct 31 2011 15:05:26   sysdrv
    4  drw-              -  Feb 25 2012 14:20:08   compatible
    5  drw-              -  Oct 31 2011 15:19:02   selftest
    6  -rw-             14  Feb 27 2012 11:20:12   back_time_b
    7  -rw-          9,637  Feb 25 2012 14:18:22   vrpcfg.cfg
    8  -rw-              4  Jan 18 2012 16:34:56   snmpnotilog.txt
    9  -rw-          1,968  Feb 25 2012 14:20:22   private-data.txt
   10  -rw-            637  Nov 04 2011 11:48:46   cacert.der
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
  11  -rw-          4,303  Feb 09 2012 21:16:06   vrpcfg1.cfg.bak
  12  -rw-            639  Nov 04 2011 11:49:04   rootcert.der
  13  drw-              -  Nov 04 2011 11:50:24   security
  14  -rw-             13  Nov 29 2011 20:33:40   tftp_test.txt
  15  -rw-     52,770,448  Dec 05 2011 17:00:06   basicsoft.cc
  16  -rw-     98,139,547  Jan 31 2012 16:11:52   devicesoft.cc
  17  -rw-        463,309  Jan 31 2012 15:55:40   rbsaveddata.txt

509,256 KB total (272,952 KB free)
```

Size(Byte) in the command output shows the file size.

8.7.9 What Are the Extensions of Different Types of Files?

Table 8-58 lists the extensions of different types of files.

Table 8-58 Extensions of different types of files

File Type	Extension
Web page file	.7z
License file	.dat
Configuration file	.cfg or .zip
System file	.cc
Patch file	.pat

8.7.10 Where Are Log Files Saved?

Log files of a switch are saved in the **syslogfile** or **logfile** folder in the flash memory.

```
<HUAWEI>dir            //Display all the files and folders in the flash
memory.
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-          1,766  Dec 24 2040 03:37:54   private-data.txt
    3  drw-              -  Dec 24 2040 03:40:12   syslogfile
    4  drw-              -  Dec 24 2040 03:37:58   compatible
   16  -rw-         10,571  Jan 04 2041 03:51:18   elabel-slot0.fls
……
<HUAWEI>cd logfile           //Access the logfile
folder.
<HUAWEI>dir
Directory of flash:/logfile/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         10,824  Jan 24 2042 09:15:04
logfile-2042-01-24-09-15-03.zip
    1  -rw-         15,334  Feb 03 2042 14:45:08
logfile-2042-02-03-14-45-08.zip
```

8.7.11 How Do I Delete Files?

Run the **delete** [**/unreserved**] [**/quiet**] { *filename* | *devicename* } [**all**] command to delete specified files including system files, configuration files, patch files, license files, and log files from a storage medium.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Delete a file from the storage medium.

```
<HUAWEI> delete test.txt
Delete flash:/test.txt?[Y/N]:y
Info: Deleting file flash:/test.txt...succeeded.
```

  NOTE

  - The actual output information may differ from the preceding information.
  - The **all** parameter is supported only in a stack. If you specify the **all** parameter, you can delete all the files in the corresponding directories on all member devices in a batch.
  - Do not delete running version files (including system software, patch files, web page files, and configuration files) in the CLI. You can use the BootROM menu to delete running version files. After a version file is deleted, the device cannot restart using the version file. Exercise caution when you delete a version file.

- Log files are stored in the **logfile** or **syslogfile** directory of the flash memory. You can access the **logfile** or **syslogfile** directory and then delete log files, or directly delete log files from the absolute path of the flash memory.

  # Access the **logfile** directory and then delete log files.

```
<HUAWEI> cd logfile/
<HUAWEI> delete logfile-2013-01-24-09-15-03.zip
Delete flash:/logfile/logfile-2013-01-24-09-15-03.zip?[Y/
N]:y
Info: Deleting file flash:/logfile/
logfile-2013-01-24-09-15-03.zip...succeeded.
```

  # Delete log files from the absolute path of the flash memory.

```
<HUAWEI> delete flash:/logfile/logfile-2013-01-24-09-15-03.zip
Delete flash:/logfile/logfile-2013-01-24-09-15-03.zip?[Y/
N]:y
Info: Deleting file flash:/logfile/
logfile-2013-01-24-09-15-03.zip...succeeded.
```

8.7.12 How Do I Transfer Files Between Two Switches?

To transfer files such as patch and configuration files between two switches, you can configure one switch as the server and the other as the client, and upload or download files between the server and client using FTP, TFTP, SFTP, SCP, or FTPS. For details about how to transfer files, see the *File Management* section in *Configuration Guide - Basic Configuration*.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

9 Configuring System Startup

About This Chapter

This chapter describes how to configure system startup and manage configuration files.

9.1 System Startup Overview
9.2 Managing Configuration Files
9.3 Configuring System Startup Files
9.4 Restarting the Device
9.5 Configuration Examples
9.6 FAQ

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

9.1 System Startup Overview

The system loads the system software and configuration file during startup. If a patch file is specified for next startup, the system also loads the specified patch file.

System startup scenarios include:

- Version upgrade

  Upgrade the system software to a later version. Upgrade the device to add new features, optimize existing features, or solve problems in the current version. To upgrade the device, load the upgrade system software and restart the device.

- Version rollback

  Downgrade the system software to an earlier version. Perform version rollback to restore normal service operating if an error occurs after the upgrade. You need to load the earlier version system software and restart the device.

- First startup

  When deploying a new device on a network, load an existing configuration file on the device to perform initial configuration quickly.

  A new device contains only default 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 **http://support.huawei.com/enterprise** and download the upgrade guide based on the product name and version.
- For details about commands used for device upgrade, see "Basic Configurations Commands - Upgrade Commands" in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Command Reference*.

System Software

The device software includes BootROM/BootLoad software and system software. After the device is powered on, it runs the BootROM/BootLoad 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/BootLoad software and system software are prerequisites for device startup and operation, providing support, management, and services for the device.

A device upgrade includes BootROM/BootLoad software upgrade and system software upgrade.

The BootROM/BootLoad software is included in the system software package (.cc file) of the device. The BootROM/BootLoad software is automatically upgraded during system software upgrade.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Configuration File

A configuration file is a collection of command lines. The current configurations are saved in the configuration file, and continue to take effect after the device restarts. You can view configurations in the configuration file or upload the file to other devices to implement batch configuration.

A configuration file is in text format and meets the following requirements:

- The configuration file saves configuration commands.
- The configuration file stores only non-default parameters to save the space.
- The commands used in the same command view form a section. Sections are separated by blank lines or comment lines beginning with comment signs (#). There can be one or multiple blank or comment lines.
- Sections are arranged in the following order: 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 commands in a configuration file must be expressed in their complete forms. Abbreviations are not allowed.
- Each command in a configuration file is wrapped using **\r\n**. No other invisible characters can be used to wrap commands.
- It is recommended that you transfer the configuration file to a device using FTP in binary mode.

The following table describes the factory configuration, configuration file, and current configuration.

Concept	Description	Command
Factory configuration	Factory configuration is the basic configuration on a new device, which enables the device to start and work properly when there is no configuration file or the configuration file is lost or damaged.	-
Configuration file	When the device is powered on, it reads the configuration file from the default directory to boot the system. The configuration in this file is called the initial configuration. If the default directory does not contain a configuration file, 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.
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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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

A configuration file can contain 30,000 command lines. If more than 30,000 commands are configured, some commands may be lost after an upgrade.

The maximum length of a command supported by the system 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 exceed the maximum length of 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.

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 numbers for users to identify, manage, and operate the patches.

Patch Classification

Patches are classified into hot and cold patches based on their impact on services.

- Hot patch (HP): does not interrupt services when being loaded and activated, which reduces upgrade costs and avoids upgrade risks.
- Cold Patch (CP): takes effect only after a reboot of the device. Services are interrupted during the reboot.

Patches are also classified into incremental and non-incremental patches based on patch dependency.

- 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.

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.

Patch State

Each patch has its own state that can only be changed using commands.

Table 9-1 describes patch states.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 9-1 Patch states

State	Description	Patch State 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 deactive state.
Deactive	When a patch is loaded to the patch area or stops running, the patch is in the deactive state.	You can perform either of the following operations on a patch in the deactive state: ● Uninstall the patch to delete it from the patch area. ● Run the patch file temporarily to change the state to active.
Active	When a patch is stored in the patch area and runs temporarily, the patch is in the active state. The active patch changes to the deactive state when the device is restarted.	You can perform one of the following operations on a patch in the active state: ● Uninstall the patch to delete it from the patch area. ● Stop running the patch to change the patch to the deactive state. ● Run the patch permanently to change the patch to the running state.
Running	When a patch is stored in the patch area and runs permanently, the patch is in the running state. The running patch remains in the running state when the device is restarted.	You can unload a patch in the running state so that it can be deleted from the patch area.

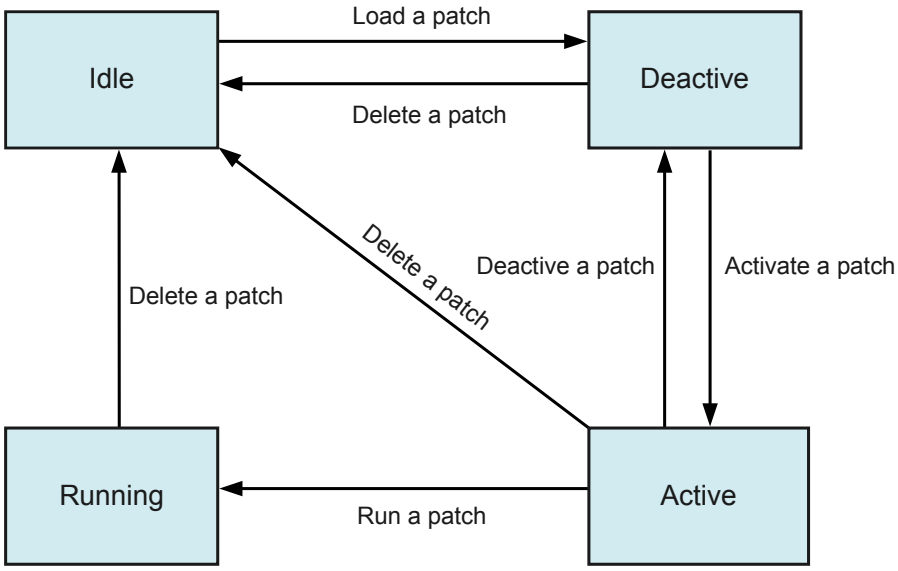
Figure 9-1 shows the transitions between different patch states.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Figure 9-1 Patch state transition



Installing Patches

Installing patches is a way of upgrading a device. You can install patches in the following ways:

- Install hot patches on a running device 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 *S1720&S2700&S5700&S6720 Series Ethernet Switches Command Reference*.
- Specify a patch file for next startup, which is described in this chapter. The patch file takes effect after the device restarts. The method is often used during a system upgrade.

9.2 Managing Configuration Files

Pre-configuration Tasks

Before managing configuration files, log in to the device.

Configuration Process

Perform one or multiple of the following tasks:

9.2.1 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

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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.
- Manually save the configuration.

NOTE

When the system is saving configuration files, other users are not allowed to perform configuration. When the current user is performing configuration, other users are not allowed to save configuration files.

Procedure

- Save the configurations automatically.
  a. Run:

     ```
     system-view
     ```

     The system view is displayed.
  b. Run:

     ```
     set save-configuration [ interval interval | cpu-limit cpu-usage | delay delay-interval ] *
     ```

     The system is configured to periodically save the configurations.

     By default, the system does not periodically save configurations.

     Before saving configurations, the system compares the configurations with those in the configuration file. Automatic saving of configurations is triggered in the following scenarios:

     - The configurations are inconsistent with those saved last time.
     - The configurations are the same as those saved last time, but changes have been made. For example, if a command is run and then its configurations are deleted, automatic saving of configurations will still be triggered although configurations are the same as those saved last time.

     The system cancels the automatic save operation when:

     - Content is being written into the configuration file.
     - The configurations are being recovered.
     - The CPU usage is excessively high.
  c. (Optional) Run:

     ```
     set save-configuration backup-to-server server server-ip [ vpn-instance vpn-instance-name ] transport-type { ftp | sftp } user user-name password password [ path folder ]
     ```

     or

     ```
     set save-configuration backup-to-server server server-ip transport-type [ vpn-instance vpn-instance-name ] tftp [ path folder ]
     ```

     The server information is configured. The information includes the IP address of the server to which the configuration is automatically saved, user name and password, the path to save the configuration file, and the mode in which the configuration file is transmitted to the server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

Before transferring the configuration file using TFTP, run the **tftp client-source** command to configure the loopback interface on the device as the client source address or source interface.

SFTP has higher security and is recommended for transferring the configuration file to the file server.

Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S6720S-EI, and S6720EI support the **vpn-instance** *vpn-instance-name* parameter in the command.

- 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 cards that are not running, to the current storage directory.

    - 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**. The **vrpcfg.zip** file is the default system configuration file with empty configurations in initial state.
    - 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

9.2.2 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 150 characters. If the different content contains fewer than 150 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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

9.2.3 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 displayed on the screen.
- Back up the configuration file to the storage device.
- Back up the configuration file using FTP, TFTP, FTPS, SFTP, or SCP.
- Run a command to back up the configuration file.

Procedure

- Copy the content displayed 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.

- Back up the configuration file to the storage device.

  The current configuration file can be backed up immediately to the flash memory of the device. After the device starts, run the following commands to back up the configuration file to the flash memory of the device:

  ```
  <HUAWEI> save config.cfg
  <HUAWEI> copy config.cfg backup.cfg
  ```

- Back up the configuration file using FTP, TFTP, FTPS, SFTP, or SCP.

  The device supports configuration file backup using FTP, TFTP, FTPS, SFTP, or SCP. Configuration file backup using FTP or TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file backup using FTPS, SFTP, or SCP is recommended. The following describes the configuration file backup process using FTP as an example. For details about TFTP, FTPS, SFTP, and SCP, see "File Management" in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - Basic Configuration*.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 flash memory directory.

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
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 flash memory:
[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, run the following command to set up an FTP connection to the device using the FTP client. In this example, 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 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.
```

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 flash:/config.cfg backup.cfg
```

e. Check whether the **config.cfg** and **backup.cfg** files have the same size. If they have the same size, you have successfully backed up the configuration file.

- Run a command to back up the configuration file.

  Run:

```
configuration copy startup to file file-name
```

  The startup configuration file is backed up to a specified file.

  The file name extension of the specified destination file must be .cfg or .zip. The extensions of the destination and backup files must be the same.

  If a file with the same name already exists, the system asks whether to replace the previous file. Press **Y** to replace the file or **N** not to do so.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

9.2.4 Recovering the Configuration File

Context

When incorrect configurations are performed and functions are abnormal, you can use one of the following methods to recover the configuration file:

- Recover the configuration file backed up in the storage device.
- Recover the configuration file using FTP, TFTP, FTPS, SFTP, or SCP.

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.

Procedure

- Recover the configuration file backed up in the .

  This step recovers the backup configuration file stored in the of the device to the current system configuration file. When the device is working properly, run the following command:

  ```
  <HUAWEI> copy flash:/backup.cfg flash:/config.cfg
  ```

- Recover the configuration file using FTP, TFTP, FTPS, SFTP, or SCP.

  The device supports configuration file recovery using FTP, TFTP, FTPS, SFTP, or SCP. Configuration file recovery using FTP or TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file recovery using FTPS, SFTP, or SCP is recommended. The following describes how to recover the configuration file backed up on a PC using FTP. For details about TFTP, FTPS, SFTP, and SCP, see "File Management" in the *S1720&S2700&S5700&S6720 Series Ethernet Switches Configuration Guide - Basic Configuration*.

  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 flash directory.

     ```
     <HUAWEI> system-view
     [HUAWEI] ftp server enable
     Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
     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 flash:
     [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, run the following command to set up an FTP connection to the device using the FTP client. In this example, 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.
     ```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
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 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.
```

d. Transfer the configuration file.

On the PC, run the **put** command to upload the configuration file to the specified path and save the file as **backup.cfg**.

```
ftp> put flash:/config.cfg 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, you have successfully recovered the configuration file.

----End

9.2.5 Executing a Configuration File

Procedure

- Run:

  configuration copy file *file-name* **to running**

  The commands in the specified configuration file are executed.

  The **configuration copy file to running** command allows you to execute all the commands in an existing configuration file at one time.

  Only one user can execute the **configuration copy file to running** command at one time.

  If configuration restoration occurs or a batch operation is performed, the **configuration copy file to running** command ends.

  If a command fails during the execution of the **configuration copy file to running** command, the system skips it and executes the next command.

----End

9.2.6 Clearing the Configuration

Context

You can use the following methods to clear the configuration in different scenarios:

- Clearing the configuration file: If the original configuration file does not match the system software after a system software upgrade, the configuration file is damaged, or an incorrect configuration file is loaded, you can clear the original configuration file and specify a new configuration file.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Clearing configurations on an interface at a time: To use a configured interface for another purpose, you need to delete configurations on the interface one by one. If a large number of configurations exist on the interface, deleting the configurations takes much time and increases maintenance workload. To reduce maintenance workload and simplify operation, you can clear all configurations on the interface at a time.
- Clearing inactive configurations on a switch: If a card is removed, the original configurations on the card are saved on the switch. If the standby/slave switch leaves a stack, the configurations on the switch are saved on the master switch. These invalid configurations are called inactive or offline configurations. You can run a command to clear all the inactive configurations on the switch to increase available space.

NOTICE

Configurations cannot be recovered after clearing. Therefore, exercise caution when deciding to run this command. You are advised to run this command under the guidance of technical support personnel.

Procedure

- Clear the configuration file.

  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.

  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 or do not save the configuration file after the file is not used for next startup, the device uses default factory configurations for startup.
  - If the next startup configuration file is empty, the device displays a message indicating that the file does not exist.
- Delete configurations on an interface at a time to restore the default configurations.

  For details, see **Table 9-2**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 9-2 Commands for deleting configurations on an interface at a time to restore the default configurations

View	Command	Description	Precautions
System view	**clear configuration interface** *interface-type interface-number*	Deletes the configuration information on the specified interface or restores the default settings. Make sure that the command is run in the system view and the specified interface type and number are correct. Otherwise, the configuration information on other interfaces may be deleted and services are interrupted.	Deleting configurations on an interface causes the interface to be shut down. Therefore, exercise caution when running the two commands.
Interface view	**clear configuration this**	Deletes the configuration information on the current interface or restores the default settings. The command is directly run in the interface view, which simplifies the operation. **NOTE** You cannot run this command in tunnel, or stack-port interface view.	

- Clear inactive configurations on the switch.
  a. Run:
  ```
  system-view
  ```
  The system view is displayed.
  b. Run:
  ```
  clear inactive-configuration all
  ```
  Inactive configurations on the switch are cleared.

----End

9.2.7 Setting Factory Configurations on the S1720GFR

Context

If an unknown error occurs on the device or the device runs slowly or unstably after it runs for a long period, you can restore factory configurations to restore the initial state.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTICE

Hold down **reset**. The factory configurations are restored after the device restarts. It is recommended that you perform this operation under the supervision of the technical support personnel.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
undo factory-configuration prohibit
```

The command enables the function of restoring the factory configuration of a device by holding down **reset**.

By default, you can hold down **reset** to restore the factory configuration.

Step 3 Run:

```
set factory-configuration operate-mode { reserve-configuration | delete-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.

By default, the system reserves the previous configuration file when restoring the factory configuration.

Step 4 Run the **display factory-configuration information** command to check whether the function of restoring the factory configuration by holding down **reset** is enabled and the mode of restoring the factory configuration.

Step 5 Hold down **reset** for more than 5 seconds and restart the device. Do not save the configuration when you restart the device.

----End

9.3 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:

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

- Start the device and log in to the device locally or remotely.
- Save the system startup files in the root directory of the device.

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 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.
- Do not change the configuration file manually and specify the configuration file for next startup. Otherwise, the device may not start normally.

Procedure

- Run:

  ```
  startup system-software system-file
  ```

  The system software to be loaded for next startup is specified.

  NOTE

  If the specified system software is in V200R005 or earlier versions (excluding V200R005C02), run the **reset boot password** command to restore the default BootLoad password and then specify the system software.

- Run:

  ```
  startup saved-configuration configuration-file
  ```

  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 | slot slot-id ]
  ```

  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

Checking the Configuration

After the configuration is complete, run the **display startup** command to view the system software, configuration file and patch file for next startup.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

9.4 Restarting the Device

Pre-configuration Tasks

To make sure the specified system software and files take effect, restart the device after system startup configuration is complete.

Before restarting the device, configure system startup files.

Context

Use either 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 a 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 records information about every restart, including the number of restart events, restart type, and restart time. Run the **display reboot-info** command to view restart information. Run **reset reboot-info** command to clear restart information.

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.

Procedure

- Restart the device immediately.

  In the user view, run the **reboot** [**fast** | **save diagnostic-information**] 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.
  - **save diagnostic-information** indicates that the system will save the diagnostic information to root directory of the storage device before restarting.

- Restart the device at a scheduled time.

  In the user view, run the **schedule reboot** { **at** *time* | **delay** *interval* [**force**] } command to restart the device at scheduled time.

  - **at** *time* specifies the specific time to restart the device.
  - **delay** *interval* [**force**] specifies the waiting time before restarting the device.

    If the **force** parameter is not specified, the system compares the configuration file with the current configuration. If the current configuration is different from the

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

configuration file, the system asks you whether to save the current configuration. After you complete the selection, the system prompts you to confirm the configured restart time. Enter **Y** or **y** to make the configured restart time take effect. If the **force** parameter is specified, the system does not display any message, and the restart time takes effect directly. The current configuration is not compared or saved.

----End

Checking the Configuration

- If scheduled restart is configured, run the **display schedule reboot** command to check the device restart configuration.

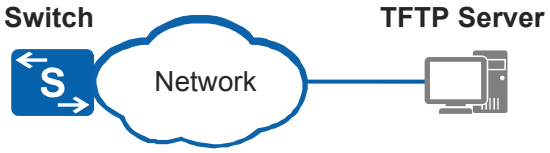
9.5 Configuration Examples

9.5.1 Example for Backing Up the Configuration File

Networking Requirements

As shown in **Figure 9-2**, 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 9-2 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 using TFTP.

NOTICE

Configuration file backup using TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file backup using FTPS, SFTP, or SCP 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.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
<HUAWEI> save config.cfg
```

Step 2 Back up the configuration file using 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 flash:/config.cfg backup.cfg
   ```

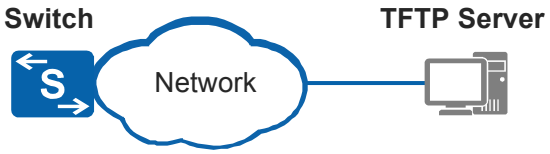
----End

9.5.2 Example for Recovering the Configuration File

Networking Requirements

As shown in **Figure 9-3**, 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 next startup.

Figure 9-3 Networking diagram of recovering the configuration file



Configuration Roadmap

The configuration roadmap is as follows:

1. Recover the configuration file backed up on the PC using TFTP.

   NOTICE

   Configuration file recovery using TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file recovery using FTPS, SFTP, or SCP is recommended. The following describes how to recover the configuration file backed up on a PC using TFTP.

2. Specify the recovered configuration file for next startup.

Procedure

Step 1 Recover the configuration file backed up on the PC using TFTP.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

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 next startup.

```
<HUAWEI> startup saved-configuration config.cfg
```

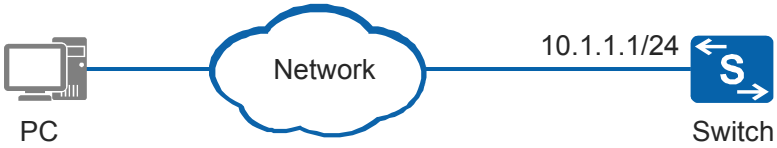
----End

9.5.3 Example of Configuring System Startup

Networking Requirements

As shown in **Figure 9-4**, 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 9-4 Networking diagram of configuring system startup



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.
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 Switch
[Switch] quit
<Switch> display startup
MainBoard:
  Configured startup system software:        flash:/basicsoft.cc
  Startup system software:                   flash:/basicsoft.cc
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
  Next startup system software:                flash:/basicsoft.cc
  Startup saved-configuration file:            flash:/vrpcfg.zip
  Next startup saved-configuration file:       flash:/vrpcfg.zip
  Startup paf file:                            NULL
  Next startup paf file:                       NULL
  Startup license file:                        NULL
  Next startup license file:                   NULL
  Startup patch package:                       NULL
  Next startup patch package:                  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.

```
<Switch> system-view
[Switch] ftp server enable
[Switch] aaa
[Switch-aaa] local-user huawei password irreversible-cipher Helloworld@6789
[Switch-aaa] local-user huawei service-type ftp
[Switch-aaa] local-user huawei ftp-directory flash:
[Switch-aaa] local-user huawei privilege level 15
[Switch-aaa] quit
[Switch] 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.

```
<Switch> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-        515,160  Oct 01 2008 00:06:14   bootrom.bin
    1  -rw-          1,799  Jan 01 2012 00:22:58   private-data.txt
    2  drw-              -  Jan 01 2012 00:25:20   logfile
    3  drw-              -  Jan 29 2012 00:00:54   resetinfo
    4  -rw-     26,493,884  Dec 31 2011 23:46:52   basicsoft.cc
    5  -rw-          1,111  Nov 29 2011 19:43:54   vrpcfg.zip
    6  drw-     27,403,824  Jul 16 2012 19:14:26   newbasicsoft.cc
...

65,233 KB total (8,284 KB free)
```

Step 2 Save the current configuration to the default storage device.

```
<Switch> 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.

```
<Switch> startup system-software newbasicsoft.cc
```

Step 4 Specify the configuration file for next startup.

```
<Switch> 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: flash:/**vrpcfg.zip**" will be displayed. This means that the **vrpcfg.zip** configuration file has been specified for next startup, so skip this step. To specify another file for next startup, perform this step.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Step 5 Checking the configuration

Run the following command to view the system software and configuration file for next startup.

```
<Switch> display startup
MainBoard:
  Configured startup system software:        flash:/basicsoft.cc
  Startup system software:                   flash:/basicsoft.cc
  Next startup system software:              flash:/newbasicsoft.cc
  Startup saved-configuration file:          flash:/vrpcfg.zip
  Next startup saved-configuration file:     flash:/vrpcfg.zip
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     NULL
  Next startup patch package:                NULL
```

Step 6 Restart the device.

Since the configuration file has been saved, run the **reboot fast** command to restart the device quickly.

```
<Switch> 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

```
#
FTP server enable
#
vlan batch 10
#
aaa
 local-user huawei password irreversible-cipher %#%#C"d3YGyf411I-z$.si9E-
TOVAw^&9Ttgw%WAr0'~XC9n/;goO~V9XdV6aOE'%#%#
 local-user huawei privilege level 15
 local-user huawei ftp-directory flash:
 local-user huawei service-type ftp
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

9.6 FAQ

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

9.6.1 How Can I Save the Device Configuration?

To retain the device configuration after a device is restarted, run the **save** command to save the current configuration before restarting the device.

- If NULL is used as the configuration file for the startup, the following information is displayed when you save the current configuration:

```
<HUAWEI> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Info: Please input the file name ( *.cfg, *.zip ) [vrpcfg.zip]:   //Enter the
name of the configuration file or press Enter. By default, the configuration
file is saved in vrpcfg.zip.
Now saving the current configuration to the slot 0....
Save the configuration successfully.
```

- If the configuration file used for the startup is not NULL, the following information is displayed when you save the current configuration:

```
<HUAWEI> 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...
Save the configuration successfully.
```

NOTE

The command outputs on your device may be different from that provided in this example.

9.6.2 How Can I Delete the Device Configuration?

To clear the current configuration and restore factory settings of a device, run the **reset saved-configuration** command to clear the configuration file for the next startup and then restart the device. If you are prompted to save the configuration, select **N** indicating that the device will not save the current configuration.

NOTICE

Exercise caution and follow the instructions of the technical support personnel when you run this command.

```
<HUAWEI> reset saved-configuration
Warning: The action will delete the saved configuration in the device.
The configuration will be erased to reconfigure. Continue? [Y/N]:y
Warning: Now clearing the configuration in the device.
Info: Succeeded in clearing the configuration in the device.
<HUAWEI> reboot
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next
startup saved-configuration file flash:/vrpcfg.zip. Continue? [Y/N]:n
Info: If want to reboot with saving diagnostic information, input 'N' and then
execute 'reboot save diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

NOTE

The command outputs on your device may be different from those provided in this example.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

9.6.3 What Files Will Be Displayed in the Flash Memory in Addition to the Default Startup System Software Package and Configuration File?

After a device is powered on, it initializes the configuration by reading the configuration file from the flash memory. When you run the **dir flash:** command in the user view, the following information is displayed:

```
<HUAWEI> dir flash:
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            812  Jan 01 2008 00:00:56   private-data.txt
    1  -rw-            948  Jan 01 2008 07:16:55   vrpcfg.zip
    2  -rw-         90,602  Jan 03 2008 03:58:15   v200r008sph001.pat
    3  -rw-      6,418,980  Jan 19 2008 20:19:42   s2700-v100r005.cc
    4  -rw-         12,240  Jan 03 2008 04:52:43   $_patchstate_reboot

14,632 KB total (8,228 KB free)
```

In the command output:

- The **private-data.txt** file saves service initialization data. Initialization data of some tasks is irrelevant to the configuration and is not recorded in the configuration file. The **private-data.txt** file records initialization data of these tasks, for example, the number of times the device restarts.
- The **$_patchstate_reboot** file records the patch status. This file is created after the device runs a patch and cannot be deleted. The file records the status of all patches, for example, the active state and running state.
- The **v200r008sph001.pat** is a patch file. The file name extension of patch files is .pat.

Sometimes, the flash memory saves a **notilogindex.txt** file. If a destination host is configured for Inform traps, the number recorded in this file is used as the initial serial number and filled in the Request ID field in Simple Network Management Protocol (SNMP) packets. The system starts a timer when the SNMP task starts and updates the file every 12 hours.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

10 BootROM Menu Operation

About This Chapter

This chapter describes the BootROM menu. During the device startup, you can press shortcut keys to access the BootROM menu to configure the startup file, upgrade components, and change the login password. Only the S1720GFR, S2720, S2750, S5700LI, S5700S-LI, and S5700S-28P-PWR-LI-AC support the BootROM menu.

10.1 BootROM Menu Overview

10.2 BootROM Main Menu

10.3 Serial Port Submenu

10.4 Startup Configuration Submenu

10.5 Ethernet Submenu

10.6 File System Submenu

10.7 Password Submenu

10.8 Deleting the Password for Login Through the Console Port

10.9 Configuration Example

10.10 FAQ

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

10.1 BootROM Menu Overview

The Boot Read-Only Memory (BootROM) is a set of programs fixed in the read-only memory (ROM) chip on a device's main card. The BootROM contains the basic input/output program, system settings, power on self-test (POST) program, and system self-startup program.

The BootROM program on the device composed of two menus:

- BootROM main menu: is the main menu of the BootROM. During the device startup, press **Ctrl+B** or **Ctrl+E** to access this menu. The BootROM main menu provides rich functions including file transfer, startup file configuration, file management, and change on BootROM and console port passwords.
- DIAG menu: You can enter this menu by pressing **Ctrl+E** in the BootROM main menu. This menu is used for equipment commissioning during the device production and assembly process. You are advised to use this menu under the supervision of technical support personnel. This manual does not provide description about this menu. For details, see *S1720&S2700&S5700&S6720 Series Ethernet Switches Troubleshooting*.

If the device properly starts, accessing the BootROM menu is not necessary. If either of the following situations occurs, you can use the BootROM menu to:

- Restore or upgrade the system when the system stops responding and the command line interface (CLI) cannot be displayed.
- Delete the password for logging in to the device using the console port when you forget the password.

The BootROM menu also allows you to back up the configuration file, format the storage device, and change the BootROM password.

NOTE

- To view the device startup process, log in to the device using the console port. Press shortcut keys as prompted to access a BootROM menu. For the method of login using the console port, see **6.3 Configuring Login Through a Console Port**. Access the equipment menu from the BootROM main menu. No option or message is provided, so you must remember the shortcut keys.
- Do not power off the device while managing the device using the BootROM; otherwise, the settings in the BootROM menu are lost.
- The screen display information varies depending on devices.

10.2 BootROM Main Menu

The BootROM main menu integrates main functions of the BootROM program.

During startup, the device loads the BootROM program and then the system software. Press **Ctrl+B** or **Ctrl+E** within three seconds when the following information is displayed to enter the BootROM main menu:

```
Press Ctrl+B or Ctrl+E to enter BootROM menu : 2

password:      //Enter the BootROM password.
```

To prevent unauthorized users from accessing the BootROM main menu, users are required to enter a password. The BootROM main menu password is **Admin@huawei.com** by default and possibly **huawei** on a device running earlier versions, which can be changed on the **10.7.1 Submenu for Changing the Password of the BootROM Menu** or using the **bootrom password change** command.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

NOTE

If a user enters incorrect BootROM passwords three consecutive times, the device will restart.

To ensure device security, change the password periodically.

If you press **Ctrl+T** when the device displays "Start memory Test ? ('Ctrl+T' is test):" during device startup, the device will perform a memory check.

When the correct BootROM password is entered, the BootROM main menu is displayed as follows:

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8):
```

Table 10-1 Description of the BootROM main menu

Item	Description
1. Boot with default mode	Starts the device with the default mode without the BootROM reboot phase. Select this option when fast device startup is required or when the operations in the BootROM menu do not involve the BootROM program.
2. Enter serial submenu	Enters the serial port submenu. In this submenu, you can download files through the serial port to the flash memory and upgrade the BootROM program. Advantage: The serial port can be directly connected without being configured. Disadvantage: The file transfer rate is slow.
3. Enter startup submenu	Enters the startup submenu. In this submenu, you can check or modify startup configurations.
4. Enter ethernet submenu	Enters the Ethernet submenu. In this submenu, you can download files to the flash memory through the Ethernet port or back up configuration files. Advantage: The file transfer rate is fast. Disadvantage: The network parameters and file server must have been configured to ensure reachable routes between the device and server.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
5. Enter filesystem submenu	Enters the file system submenu. In this submenu, you can manage and maintain the file system.
6. Enter password submenu	Enters the password submenu. In this menu, you can change the BootROM password or restore the default BootROM password.
7. Clear password for console user	Deletes the password for login through the console port. If the password for login through the console port is lost or forgotten, you can use this function to delete the password. After you log in to the device, reset this password.
8. Reboot	Restarts the BootROM by selecting **8. Reboot** and starts other components when parameter modification affects device initialization.
(Press Ctrl+E to enter diag menu)	Press **Ctrl+E** to enter the diagnosis menu. For details about the diagnosis menu, see BootROM Menu Overview in *S1720&S2700&S5700&S6720 Series Ethernet Switches Troubleshooting*.
Shortcut key	The BootROM menu provides two shortcut keys: **Ctrl+M** and **Ctrl+J**. The functions of the shortcut keys are as follows: **Ctrl+M** and **Ctrl+J**: The two shortcut keys can be used in any BootROM menu to provide functions similar to **Enter**.

10.3 Serial Port Submenu

The serial port can be used for transferring files when the management interface fails. The transmission rate on the serial port is low. The default transmission rate is 9600 bit/s. You are advised to set the transmission rate to 115200 bit/s before transferring files.

NOTE

The serial port uses the file transfer protocol XModem to transfer files. Select the correct transfer protocol to transfer files.

In the BootROM main menu, select 2 to access the serial port submenu.

```
        BootROM  MENU

1. Boot with default mode
2. Enter serial submenu
3. Enter startup submenu
4. Enter ethernet submenu
5. Enter filesystem submenu
6. Enter password submenu
7. Clear password for console user
8. Reboot
(Press Ctrl+E to enter diag menu)
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
Enter your choice(1-8): 2

          SERIAL  SUBMENU

    1. Update BootROM system
    2. Download file to Flash through serial interface
    3. Modify serial interface parameter
    4. Return to main menu

Enter your choice(1-4):
```

Table 10-2 Serial port submenu

Item	Description
1. Update BootROM system	Loads the BootROM program file using the serial port and upgrades the BootROM. **NOTE** Currently, the system software contains the upgrade file of the BootROM. When you upgrade the system software, the BootROM is automatically upgraded.
2. Download file to Flash through serial interface	Loads files to the flash memory using the serial port. A flash memory stores all files on a device, including the system software, configuration file, patch file, and log files generated during the device running.
3. Modify serial interface parameter	Allows you to modify parameters on the serial port. The default transmission rate is 9600 bit/s. The serial port supports the following transmission rates: ● 9600 bit/s (default) ● 19200 bit/s ● 38400 bit/s ● 57600 bit/s ● 115200 bit/s **NOTE** After changing the transmission rate on the serial port, synchronize the transmission rate on the PC with that on the serial port and reconnect the PC to the device.
4. Return to main menu	-

10.4 Startup Configuration Submenu

In the BootROM main menu, select 3 to access the startup configuration submenu.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 3

       Startup Configuration Submenu

    1. Display startup configuration
    2. Modify startup configuration
    3. Return to main menu

Enter your choice(1-3):
```

Table 10-3 Startup configuration submenu

Item	Description
1. Display startup configuration	Displays the current system software, configuration file, and patch file, and those used in the last startup. Before upgrading or rolling back the system, you can check whether the correct startup files are specified.
2. Modify startup configuration	Allows you to modify startup configuration information. Before upgrading or rolling back the system, you need to specify the system software, configuration file, and patch file.
3. Return to main menu	-

10.4.1 Checking the Startup Configuration

Before upgrading or rolling back the system, select 1 in the startup configuration submenu to check whether the correct startup files are specified.

```
       Startup Configuration Submenu

    1. Display startup configuration
    2. Modify startup configuration
    3. Return to main menu

Enter your choice(1-3): 1
Current startup configuration
  startup type      : Flash
  startup file      : s5700li-v200r002c00.cc
  configuration file:
vrpcfg.zip
  patch package     :

Last time startup state : Success
Latest successful startup configuration
  startup file      : s5700li-V200R009C00.cc
  configuration file:
vrpcfg.zip
  patch package     :
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 10-4 Output information description

Item	Description
Current startup configuration	The following shows current startup configuration information.
startup type	Startup storage device where the system software, configuration file, and patch file are stored. The device supports only the flash memory. The parameter value is **Flash**.
startup file	System software, in the format of .cc.
configuration file	Configuration file, in the format of .zip or .cfg.
patch package	Patch file, in the format of .pat.
Last time startup state	Last startup status. The value can be: ● Success ● Failed
Latest successful startup configuration	Configuration used in the last successful startup.

10.4.2 Modifying Startup Configuration Information

Context

When the system software on a device is damaged and you cannot log in to the device, you can use the BootROM to upload the system software, configuration file, and patch file, and configure the device to start using the uploaded files. In this way, you can restore the system software and upgrade the device.

NOTE

Before modifying startup configuration information, upload specified files to the flash memory using **10.3 Serial Port Submenu** or **10.5 Ethernet Submenu**.

Procedure

Step 1 In the startup configuration submenu, select 2.

```
       Startup Configuration Submenu

   1. Display startup configuration
   2. Modify startup configuration
   3. Return to main menu

Enter your choice(1-3): 2
```

Step 2 Select the startup storage device.

```
Note: startup file field can not be cleared
'.'=clear field; '^D'=quit; Enter=use current configuration
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
startup type(1: Flash)
  current: 1
  new    :
```

Currently, the device supports only the flash memory. No setting is required. Press **Enter**.

NOTE

Pay attention to the following:

- The area where the system software is stored cannot be cleaned.
- If you enter a dot (.), the existing storage device configuration is deleted. If the system software is not specified, the device cannot start. If the configuration file is not specified, the device starts using the factory settings.
- To return to the startup configuration submenu, press **Ctrl+D**.
- If you press **Enter**, the current configuration information is used without any change.

Step 3 Specify the system software.

```
Flash startup file (can not be cleared)
  current: s5700li-V200R009C00.cc
  new    :
```

Enter the name of the specified system software and press **Enter**. If the current system software is available and does not require reset, directly press **Enter**.

NOTE

- The specified system software must be available and stored in the flash memory; otherwise, the device fails to start. If the startup based on the specified system software fails for three consecutive times, the device starts using the system software in the last successful startup.
- If the system software to be specified is V200R008 or an earlier version, you must restore the default BootROM password first according to **Restoring the BootROM Password** and then specify the system software. Otherwise, the BootROM password may not be used or a fault occurs on the switch. If the BootROM password cannot be used after the downgrade, run the **reset boot password** command to restore the default BootROM password again.

Step 4 Specify the configuration file.

```
saved-configuration file
  current:
vrpcfg.zip
  new    :
```

Enter the name of the specified configuration file and press **Enter**. If the service configuration does not require reset, directly press **Enter**. By default, the device uses the configuration file **vrpcfg.zip**.

NOTE

The specified configuration file must be available and stored in the flash memory; otherwise, the device starts using the factory settings.

Step 5 Specify the patch file.

```
patch package
  current: s5700li-V200R009C00sph005.pat
  new    :
```

Enter the name of the patch file and press **Enter** to return to the startup configuration submenu. Press **Enter** if you do not need to upgrade the patch file. The submenu for modifying the flash description is displayed. By default, no patch file is specified.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

10.5 Ethernet Submenu

Before transferring files using the Ethernet submenu, deploy an FTP or TFTP server as the file server and connect the device to the FTP or TFTP server using the management interface.

NOTE

If no management interface is provided on a device, use the first port on the device to connect to the FTP or TFTP server. If the first port on a device is the combo port, use the electrical mode.

Compared with the rate for transferring files using the serial port, the file transfer using the Ethernet port is faster but requires the deployment of the FTP or TFTP server and an additional cable.

In the BootROM main menu, select 4 to access the Ethernet submenu.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 4

          ETHERNET  SUBMENU

    1. Update BootROM system
    2. Download file to Flash through ethernet interface
    3. Upload Configuration file to Ftp through ethernet interface
    4. Modify ethernet interface boot parameter
    5. Return to main menu

Be sure to select 4 to modify boot parameter before downloading!
Enter your choice(1-5):
```

Table 10-5 Ethernet submenu

Item	Description
1. Update BootROM system	Loads the BootROM program file using the Ethernet port and upgrades the BootROM. **NOTE** If the BootROM is in V200R005 or earlier versions (excluding V200R005C02), **restore the default BootROM password** and then upgrade the BootROM. The BootROM of the S5700LI cannot be updated to V200R001 or earlier versions using this submenu.
2. Download file to Flash through ethernet interface	Loads files to the flash memory using the Ethernet port.
3. Upload Configuration file to Ftp through ethernet interface	Uploads the configuration file to the FTP server for backup.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Item	Description
4. Modify ethernet interface boot parameter	Allows you to modify parameters on the Ethernet port. Properly set the parameters on the Ethernet port before uploading files using the Ethernet port. The Ethernet port here refers to the management interface on the device. Configure the IP address of the Ethernet port, files to be uploaded, and FTP user name and password, to connect the device to the FTP or TFTP server.
5. Return to main menu	-

10.5.1 Modifying Parameters on the Ethernet Port

Context

The BootROM allows you to connect a device to another device or a PC using FTP or TFTP to implement fast transfer of the system software, configuration file, and patch file. To ensure consistent parameters on both ends of an FTP or TFTP connection, set parameters on the Ethernet port (management interface) before setting up a connection.

Pre-configuration Tasks

In the BootROM menu, a device can function only as an FTP or TFTP client. Before transferring files using this menu, deploy an FTP or TFTP server as the file server and connect the server to the management interface on the device to ensure connectivity.

Procedure

Step 1 In the Ethernet submenu, select 4 to modify parameters on the Ethernet port.

```
          ETHERNET  SUBMENU

    1. Update BootROM system
    2. Download file to Flash through ethernet interface
    3. Upload Configuration file to Ftp through ethernet interface
    4. Modify ethernet interface boot parameter
    5. Return to main menu

Be sure to select 4 to modify boot parameter before downloading!
Enter your choice(1-5): 4

          BOOTLINE  SUBMENU

    1. Set TFTP protocol parameters
    2. Set FTP protocol parameters
    3. Return to ethernet menu

Enter your choice(1-3):
```

Step 2 Configure TFTP or FTP parameters based on the selected server type.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 10-6 Modifying parameters on the Ethernet port

Operation	Description
Entering characters **NOTE** The characters can contain only letters, numerals, underlines (_), and dots (.). Blanks are not allowed.	Indicates that the existing values need to be changed. Press **Enter** to confirm the operation.
Entering a dot (.)	Deletes existing information in the current view.
Pressing a hyphen (-)	Returns to the previous option.
Pressing **Ctrl+D**	Exists from the view for modifying parameters on the Ethernet port and returns to the Ethernet submenu.
Pressing **Enter**	Skips to the next option without any change.

- If a TFTP server is configured as the file server, select 1 to access the submenu for modifying TFTP parameters.

```
          BOOTLINE
SUBMENU


    1. Set TFTP protocol
parameters
    2. Set FTP protocol
parameters
    3. Return to ethernet
menu


Enter your choice(1-3):
1


'.' = clear field;  '-' = go to previous field;  ^D =
quit
Load File name      : s5700li-V200R009C00.cc
Switch IP address   :
192.168.1.15:ffffff00
Server IP address   : 192.168.1.40
```

Table 10-7 Submenu for modifying TFTP parameters

Item	Description
Load File name	File to be uploaded.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
Switch IP address	IP address of the management interface on the device. By default, the IP address of the management interface is 192.168.1.15:ffffff00. **NOTE** The IP addresses of the device and the TFTP server must be on the same network segment. A subnet mask is an 8-digit hexadecimal number and does not support the format of dotted decimal notation or mask length. The subnet mask is automatically identified by the device and does not need to be set manually.
Server IP address	IP address of the TFTP server.

- If an FTP server is configured as the file server, select 2 to access the submenu for modifying FTP parameters.

```
          BOOTLINE
SUBMENU


    1. Set TFTP protocol
parameters
    2. Set FTP protocol
parameters
    3. Return to ethernet
menu


Enter your choice(1-3):
2


'.' = clear field;  '-' = go to previous field;  ^D =
quit
Load File name      : s5700li-V200R009C00.cc
Switch IP address   :
192.168.1.15:ffffff00
Server IP address   :
192.168.1.40
FTP User Name       :
huawei
FTP User Password   :
```

Table 10-8 Submenu for modifying FTP parameters

Item	Description
Load File name	File to be uploaded.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
Switch IP address	IP address of the management interface on the device. By default, the IP address of the management interface is 192.168.1.15:ffffff00. **NOTE** The IP addresses of the device and the FTP server must be on the same network segment. A subnet mask is an 8-digit hexadecimal number and does not support the format of dotted decimal notation or mask length. The subnet mask is automatically identified by the device and does not need to be set manually.
Server IP address	IP address of the FTP server.
FTP User Name	User name for logging in to the FTP server.
FTP User Password	Password for logging in to the FTP server, in cipher text.

----End

10.6 File System Submenu

In the BootROM main menu, select 5 to access the file system submenu.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 5
         FILESYSTEM SUBMENU

    1. Erase Flash
    2. Format flash
    3. Delete file from Flash
    4. Rename file from Flash
    5. Display Flash files
    6. Update EPLD file
    7. Return to main menu

Enter your choice(1-7):
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 10-9 File system submenu

Item	Description
1. Erase Flash	Erases the flash memory. All information including the system software and configuration file are deleted from the flash memory. After the device is deployed in a new environment, you can erase the flash memory and reload the system software and configuration file. **NOTICE** After the flash memory is erased, the device cannot start. You need to reload the system software. Therefore, exercise caution before erasing the flash memory.
2. Format flash	Formats the flash memory. If the flash memory fails, format the flash memory to rectify the fault. If the fault persists, contact technical support personnel. **NOTICE** After the flash memory is formatted, the device cannot start. You need to reload the system software. Therefore, exercise caution before formatting the flash memory.
3. Delete file from Flash	Deletes files in the flash memory. **NOTE** After you select 3 in the file system submenu, all files in the flash memory are displayed. You can delete files as required.
4. Rename file from Flash	Renames files. **NOTE** After you select 4 in the file system submenu, all files in the flash memory are displayed. You can rename files as required.
5. Display Flash files	Displays all files in the flash memory. At the same time, the total size and remaining size of the flash memory are displayed.
6. Update EPLD file	Upgrades the EPLD. Before upgrading the EPLD, select the EPLD file for the upgrade, in the format of .bin.
8. Return to main menu	-

10.7 Password Submenu

In the BootROM main menu, select 6 to enter the password submenu.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 6

        PASSWORD  SUBMENU

    1. Modify BootROM password
    2. Reset BootROM password
    3. Return to main menu

Enter your choice(1-3):
```

Table 10-10 Password submenu description

Item	Description
1. Modify BootROM password	Changes the BootROM password. You can change the BootROM password to prevent unauthorized users from entering the BootROM menu.
2. Reset BootROM password	Restores the default BootROM password. The default BootROM password is **Admin@huawei.com**.
3. Return to main menu	-

10.7.1 Submenu for Changing the Password of the BootROM Menu

Context

The BootROM main menu password is **Admin@huawei.com** by default and possibly **huawei** on a device running earlier versions. You are advised to change the password to prevent unauthorized users from accessing the BootROM.

NOTE

You can also run the **bootrom password change** command to change the password of the BootROM main menu.

Procedure

- In the BootROM main menu, select 6 to enter the password submenu.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 6

       PASSWORD  SUBMENU

    1. Modify BootROM password
    2. Reset BootROM password
    3. Return to main menu

Enter your choice(1-3):
```

- In the password submenu, select 1 to enter the page for changing the BootROM password.

```
       PASSWORD  SUBMENU

    1. Modify BootROM password
    2. Reset BootROM password
    3. Return to main menu

Enter your choice(1-3): 1

Old password:     //Enter the old password.
New password:     //Enter the new password.
Verify:           //Enter the new password again.
```

----End

10.7.2 Restoring the BootROM Password

Context

You can select 2 Reset BootROM password in the password submenu to restore the default BootROM menu password. The BootROM main menu password is Admin@huawei.com by default and possibly **huawei** on a device running earlier versions.

NOTE

Restoring the default BootROM password using the BootROM menu achieves the same result as running the **reset boot password** command.

Procedure

- In the BootROM main menu, select 6 to enter the password submenu.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 6

       PASSWORD  SUBMENU
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    1. Modify BootROM password
    2. Reset BootROM password
    3. Return to main menu

Enter your choice(1-3):
```

- In the password submenu, select 2 to restore the default BootROM password.

```
        PASSWORD  SUBMENU

     1. Modify BootROM password
     2. Reset BootROM password
     3. Return to main menu

Enter your choice(1-3): 2

The password used to enter the boot menu will be restored to the default
password, continue? [Y/N]y

Succeeded in setting boot password to "Admin@huawei.com".
```

----End

10.8 Deleting the Password for Login Through the Console Port

Context

If you forget the password for logging in to the device using telnet or serial port, you cannot log in to the device. To address this issue, the BootROM menu provides a submenu for deleting the password for logging in using the serial port.

NOTE

If multiple devices establish a stack, you can log in to the stack system only after deleting the console port login password from the master switch. You are advised to start each member device and delete the console port login password on each device in sequence.

Procedure

- In the BootROM main menu, select 7 to clear the password for console users.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 7

Note: Clear password for console user? Yes or No(Y/N): y

Clear password for console user successfully. Choose "1" to boot, then set a
new password.
Note: Do not choose "8. Reboot" or power off the device, otherwise this
operation will not take effect.
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTICE

After the password is deleted, start the device using option 1 in the BootROM menu. Do not select 8 or power off the device; otherwise, the configuration becomes invalid.

----End

10.9 Configuration Example

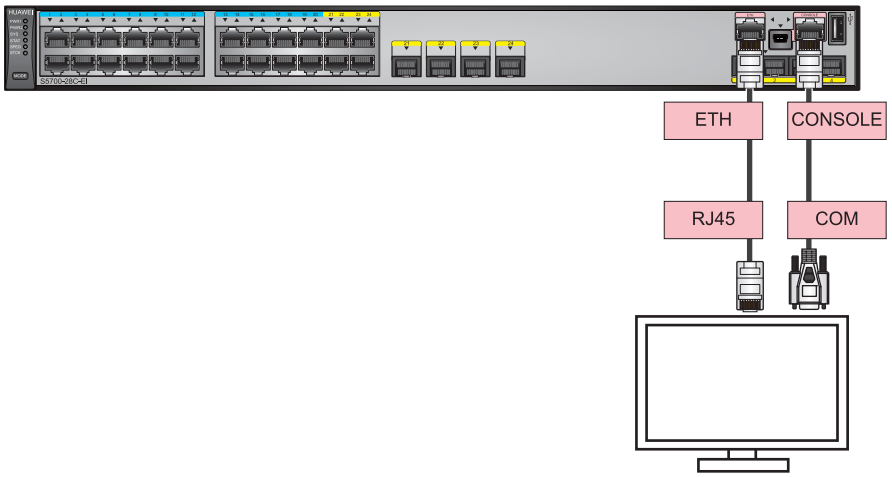
10.9.1 Example for Upgrading the System Software Using the BootROM Menu

Networking Requirements

As shown in **Figure 10-1**, the serial port on a PC connects to the console port on a switch, and the network adapter on the PC connects to the management interface on the switch. The terminal emulation software is used for logging in to the switch.

If the system software on a switch is faulty, you cannot log in. To address this issue, use the Ethernet submenu under the BootROM menu to upload system software and specify it as the next startup system software. This enables the switch to load the system software and start an upgrade.

Figure 10-1 Networking diagram of connecting a PC to the console port on a switch



NOTE

In this example, HyperTerminal is used as terminal emulation software. If other third-party terminal emulation software is used, see the corresponding software user guide or online help.

Configuration Roadmap

1. Deploy an FTP server and upload the target system software to the FTP working directory. In this example, configure the PC as the FTP server, and connect the network

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

adapter on the PC to the management interface on the switch for setting up subsequent FTP connections.

2. Restart the switch and access the BootROM main menu.
3. Set FTP parameters on the switch so that the switch can communicate with the FTP server. Use FTP to upload the target system software to the storage device on the switch.
4. In the startup configuration submenu, configure the uploaded system software as the next startup system software.

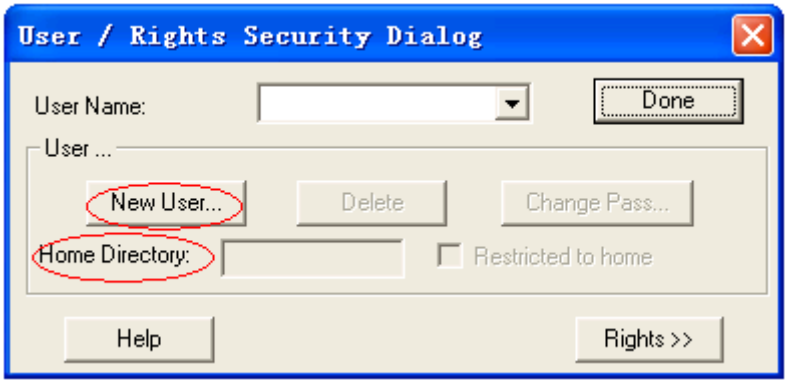
Procedure

Step 1 Configure the PC as the FTP server and copy the system software of the switch to the FTP working directory.

1. Configure the IP address, user name, password, and working directory for the FTP server.

   Run an FTP server program on the PC, for example, wftpd32. Choose **Security** > **Users/rights...**. In the dialog box that is displayed as shown in **Figure 10-2**, click **New User...**. In the dialog box that is displayed, set the user name to **user** and password to **huawei**. Set **Home Directory:** to **D:\BootROM**. Click **Done** to close the dialog box. Set the IP address of the PC to 192.168.1.6 and mask to 255.255.255.0.

   Figure 10-2 Configuring the FTP server



2. Upload the system software, such as S5700LI-V200R009C00.cc to the working directory (D:\BootROM) of the FTP server. The upload process is not mentioned here.

Step 2 Restart the switch. When the following information is displayed, press **Ctrl+B** or **Ctrl+E**, and then enter the password to access the BootROM main menu. The default BootROM password is **Admin@huawei.com**.

```
BIOS loading ...
Copyright (c) 2011-2013 HUAWEI TECH CO., LTD.
Basic BootROM version : 160 Compiled at May 14 2013, 21:19:01

Press Ctrl+B or Ctrl+E to enter BootROM menu ... 2
password:      //Enter the BootROM password.
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8):
```

Step 3 Set FTP parameters on the switch to set up an FTP connection with the PC.

1. In the BootROM main menu, select 4 to access the Ethernet submenu.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 4
```

2. In the Ethernet submenu, select 4 to modify parameters on the Ethernet port.

```
          ETHERNET  SUBMENU

    1. Update BootROM system
    2. Download file to Flash through ethernet interface
    3. Upload Configuration file to Ftp through ethernet interface
    4. Modify ethernet interface boot parameter
    5. Return to main menu

Enter your choice(1-5): 4

          BOOTLINE  SUBMENU

    1. Set TFTP protocol parameters
    2. Set FTP protocol parameters
    3. Return to ethernet menu

Enter your choice(1-3):
```

3. Select 2 to set FTP parameters on the switch.

```
          BOOTLINE  SUBMENU

    1. Set TFTP protocol parameters
    2. Set FTP protocol parameters
    3. Return to ethernet menu

Enter your choice(1-3): 2

'.' = clear field;  '-' = go to previous field;  ^D = quit
Load File name      : S5700LI-V200R001C00.CC S5700LI-V200R009C00.cc //Enter
the name of the system software to be loaded.
Switch IP address   : 192.168.1.15:ffffff00 192.168.1.3     //Enter the IP
address of the management interface on the switch.
Server IP address   : 192.168.1.1 192.168.1.6   //Enter the IP address of the
FTP server.
FTP User Name       : huawei user               //Enter the user name "user"
for logging in to the FTP server.
FTP User Password   :                           //Enter the password "huawei"
for logging in to the FTP server.

Starting to write BOOTLINE into flash ... done
```

Step 4 In the Ethernet submenu, select 2 to load the system software to the flash memory.

```
          ETHERNET  SUBMENU
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    1. Update BootROM system
    2. Download file to Flash through ethernet interface
    3. Upload Configuration file to Ftp through ethernet interface
    4. Modify ethernet interface boot parameter
    5. Return to main menu

Be sure to select 4 to modify boot parameter before downloading!
Enter your choice(1-5): 2
Attached TCP/IP interface to mottsec0.
Warning: no netmask specified.
Attaching network interface lo0... done.

Read file to sdram ..............Done
Writing Flash.....................................................................
.....................................................................................
.....................................................................done
File length: 13955100 bytes
Time taken : 118s
```

Step 5 Exit from the Ethernet submenu. In the BootROM main menu, select 3 to specify the loaded system software for the next startup.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 3

       Startup Configuration Submenu

    1. Display startup configuration
    2. Modify startup configuration
    3. Return to main menu

Enter your choice(1-3): 2
Note: startup file field can not be cleared
'.'=clear field; '^D'=quit; Enter=use current configuration

startup type(1: Flash)
  current: 1
  new    :       //No setting is required. Press "Enter".
Flash startup file (can not be cleared)
  current: S5700LI-V200R001C00.cc
  new    : S5700LI-V200R009C00.cc       //Enter the name of the system software
to be loaded.
saved-configuration file
  current: vrpcfg.zip
  new    :       //No setting is required. Press "Enter".
patch package
  current:
  new    :      //No setting is required. Press "Enter".
```

Step 6 Exit from the startup configuration submenu. In the BootROM main menu, select 1 to start the switch.

```
          BootROM  MENU

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 1
```

Step 7 Verify the configuration.

After the switch starts, run the **display version** command in the CLI to check whether the switch version is the target version.

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (S5700 V200R009C00)
Copyright (C) 2000-2014 HUAWEI TECH CO., LTD
HUAWEI S5700-28P-LI-AC Routing Switch uptime is 0 week, 0 day, 0 hours, 7 minutes

......
```

----End

10.10 FAQ

10.10.1 What Is the Default BootROM Password of the Switch?

When the system starts the BootROM, press **CTRL+B** or **CTRL+E** within 3 seconds and then enter the default password to enter the BootROM menu.

When a chassis switch runs a version earlier than V100R006C03, the default BootROM password is **9300**. When a chassis switch runs V100R006C03 or later, the default BootROM password is **Admin@huawei.com**.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

11 BootLoad Menu Operation

About This Chapter

The BootLoad menu on the device allows you to upgrade the system software and delete the password for logging in to the device using the console port. If the device fails to enter the command line interface (CLI), you can use the BootLoad menu to restore the initial status of the device. Only the S5710-X-LI, S5700S-28X-LI-AC, S5700S-52X-LI-AC, S5720SI, S5720S-SI, S5720EI, S5720HI, S6720EI, and S6720S-EI support the BootLoad menu.

11.1 BootLoad Main Menu

11.2 Startup Configuration Submenu

11.3 Ethernet Submenu

11.4 File System Submenu

11.5 Password Submenu

11.6 Submenu for Deleting the Password for Logging In Using the Serial Port

11.7 Configuration Example

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

11.1 BootLoad Main Menu

The BootLoad main menu integrates main functions of the BootLoad program.

During startup, the device loads the BootLoad program and then the system software. Press **Ctrl+B** or **Ctrl+E** within 3 seconds when the following information is displayed to enter the BootLoad main menu:

```
Press Ctrl+B or Ctrl+E to enter BootLoad menu : 2
Password:      //Enter the password
```

To ensure device security, users must enter password to enter the BootLoad main menu. This prevents unauthorized users from entering the BootLoad main menu. By default, the BootLoad menu password is **Admin@huawei.com**, which can be changed on the **11.5.1 Submenu for Changing the Password of the BootLoad Menu** or using the **bootrom password change** command.

NOTE

If a user enters incorrect BootLoad passwords three times, the device restarts.

To ensure device security, please change the password periodically.

If you press **Ctrl+T** when the device displays "Press Ctrl+T to Start Memory Test" during the device startup process, the device will perform a memory check.

When a correct BootLoad password is entered, the BootLoad main menu is displayed as follows:

```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8):
```

Table 11-1 Description of the BootLoad main menu

Item	Description
1. Boot with default mode	Starts the device with the default mode without the BootLoad reboot phase. Select this option when fast device startup is required or the operations in the BootLoad menu do not involve the BootLoad program, for example, modify bootload password.
2. Enter serial submenu	Enters the serial port submenu. S5710-X-LI, S5700S-28X-LI-AC, S5700S-52X-LI-AC, S5720SI, S5720S-SI, S5720EI, S5720HI, S6720EI, and S6720S-EI do not support this menu.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
3. Enter startup submenu	Enters the startup submenu. In this submenu, you can check or modify startup configurations.
4. Enter ethernet submenu	Enters the Ethernet submenu. In this submenu, you can download files to memories and storage devices through the Ethernet port or back-up configuration files. This operation features fast file transfer, but you must configure network parameters and file server to ensure reachable routes between the device and server.
5. Enter filesystem submenu	Enters the file system submenu. In this submenu, you can manage and maintain the file system.
6. Enter password submenu	Enters the password submenu. In this menu, you can change the BootLoad password or restore the default BootLoad password.
7. Clear password for console user	Deletes the password for login through the console port. When failing to log in to the device because you forget the password for login through the console port, you can delete the password. After you log in to the device, reset this password.
8. Reboot	Restarts the BootLoad by selecting **8. Reboot** and starts other components when parameter modification affects device initialization.
(Press Ctrl+E to enter diag menu)	Press **Ctrl+E** to enter the diagnosis menu. This menu is used by development personnel to perform device performance tests. It is recommended that users do not use this menu. For details about the diagnosis menu, see BootLoad Menu Overview in *S1720&S2700&S5700&S6720 Series Ethernet Switches Troubleshooting*.
Shortcut key	The BootLoad menu provides two shortcut keys: Ctrl+M and Ctrl+J. The two shortcut keys can be used in any BootLoad menu to provide functions similar to **Enter**.

11.2 Startup Configuration Submenu

In the BootLoad main menu, select 3 to access the startup configuration submenu.

```
          BootLoad Menu
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

```
    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 3

        Startup Configuration Submenu

     1. Display startup configuration
     2. Modify startup configuration
     3. Return to main menu

Enter your choice(1-3):
```

Table 11-2 Startup configuration submenu

Item	Description
1. Display startup configuration	Displays the current system software, configuration file, and patch file, and those used in the last startup. Before upgrading or rolling back the system, you can check whether the correct startup files are specified.
2. Modify startup configuration	Allows you to modify startup configuration information. Before upgrading or rolling back the system, you can specify the system software, configuration file, and patch file. **NOTE** Some S5720HI switches running V200R008 and later versions cannot be downgraded to V200R007C00SPC500.
3. Return to main menu	-

11.2.1 Display startup configuration

Before upgrading or rolling back the system, select 1 in the startup configuration submenu to check whether the correct startup files are specified.

```
       Startup Configuration Submenu

    1. Display startup configuration
    2. Modify startup configuration
    3. Return to main menu

Enter your choice(1-3): 1
Current startup configuration
  startup type      : Flash
  startup file      : s5720hi.cc
  configuration file:
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
vrpcfg.zip
  patch package     :

Last time startup state : Success
Latest successful startup configuration
  startup file      : s5720hi.cc
  configuration file:
vrpcfg.zip
  patch package     :
```

Table 11-3 Output information description

Item	Description
Current startup configuration	The following shows current startup configuration information.
startup type	Startup storage device where the system software, configuration file, and patch file are stored. The device supports only the flash memory. The parameter value is **Flash**.
startup file	System software, in the format of .cc.
configuration file	Configuration file, in the format of .zip or .cfg.
patch package	Patch file, in the format of .pat.
Last time startup state	Last startup status. The value can be: ● Success ● Failed
Latest successful startup configuration	Configuration used in the last successful startup.

11.2.2 Modifying Startup Configuration Information

Context

When the system software on a device is damaged and you cannot log in to the device, you can use the BootLoad to upload the system software, configuration file, and patch file, and configure the device to start using the uploaded files. In this way, you can restore the system software and upgrade the device.

NOTE

Before modifying startup configuration information, upload specified files to the flash memory using **11.3 Ethernet Submenu**.

Procedure

Step 1 In the startup configuration submenu, select 2 to enter the startup configuration submenu.

```
      Startup Configuration Submenu
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    1. Display startup configuration
    2. Modify startup configuration
    3. Return to main menu

Enter your choice(1-3): 2
```

Step 2 Select the startup storage device.

```
Note: startup file field can not be cleared
'.'=clear field; '^D'=quit; Enter=use current configuration

startup type(1: Flash)
  current: 1
  new    :
```

Currently, the device supports only the flash memory. No setting is required. .

Step 3 Specify the system software.

```
Flash startup file (can not be cleared)
  current: s5720hi.cc
  new    :
```

Enter the name of the specified system software and press **Enter**. If the current system software is available and does not require reset, directly press **Enter**.

NOTE

- The specified system software must be available and stored in the flash memory; otherwise, the device fails to start. If the startup based on the specified system software fails for three consecutive times, the device starts using the system software in the last successful startup.
- If the system software to be specified is V200R008 or an earlier version, you must restore the default BootLoad password first according to **Restoring the BootLoad Password** and then specify the system software. Otherwise, the BootLoad password may not be used or a fault occurs on the switch. If the BootLoad password cannot be used after the downgrade, run the **reset boot password** command to restore the default BootLoad password again.

Step 4 Specify the configuration file.

```
saved-configuration file
  current:
vrpcfg.zip
  new    :
```

Enter the name of the specified configuration file and press **Enter**. If the service configuration does not require reset, directly press **Enter**. By default, the device uses the configuration file **vrpcfg.zip**.

NOTE

The specified configuration file must be available and stored in the flash memory; otherwise, the device starts using the factory settings.

Step 5 Specify the patch file.

```
patch package
  current: s5720hi.cc-sph005.pat
  new    :
```

Enter the name of the patch file and press **Enter** to return to the startup configuration submenu. Press **Enter** if you do not need to upgrade the patch file. The submenu for modifying the flash description is displayed. By default, no patch file is specified.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

11.3 Ethernet Submenu

Before transferring files using the Ethernet submenu, deploy a File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server as the file server and connect the device to the FTP or TFTP server using the management interface.

NOTE

If no management interface is provided on a device, use the first interface on the device to connect to the FTP or TFTP server. If the first interface on a device is the combo interface, use the electrical mode.

Transferring files using an Ethernet interface is faster than using the serial port, but requires the deployment of an FTP or TFTP server and an additional cable.

In the BootLoad main menu, select 4 to access the Ethernet submenu.

```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 4

        ETHERNET  SUBMENU

     1. Update BootROM system
     2. Download file to Flash through ethernet interface
     3. Upload Configuration file to Ftp through ethernet interface
     4. Modify ethernet interface boot parameter
     5. Return to main menu

Enter your choice(1-5):
```

Table 11-4 Ethernet submenu

Item	Description
1. Update BootROM system	Loads the BootROM program file using the Ethernet interface and upgrades the BootROM.
2. Download file to Flash through ethernet interface	Loads files to the flash memory using the Ethernet interface.
3. Upload Configuration file to Ftp through ethernet interface	Uploads the configuration file to the FTP server for backup.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Item	Description
4. Modify ethernet interface boot parameter	Allows you to modify parameters on the Ethernet interface. Properly set the parameters on the Ethernet interface before uploading files using the Ethernet interface. The Ethernet interface here refers to the management interface on the device. Configure the IP address of the Ethernet interface, files to be uploaded, and FTP user name and password, to connect the device to the FTP server.
5. Return to main menu	-

11.3.1 Modifying Parameters on the Ethernet Interface

Context

The BootLoad allows you to connect a device to another device or a PC using FTP or TFTP to implement fast transfer for the system software, configuration file, and patch file. To ensure consistent parameters on both ends of the FTP or TFTP connection, set parameters on the Ethernet interface (management interface) before setting up a connection.

Pre-configuration Tasks

In the BootLoad menu, a device can function only as an FTP or TFTP client. Before transferring files in this menu, deploy an FTP or TFTP server as the file server and connect the server to the management interface on the device to ensure connectivity.

Procedure

Step 1 In the Ethernet submenu, select 4 to modify parameters on the Ethernet interface.

```
          ETHERNET  SUBMENU

    1. Update BootROM system
    2. Download file to Flash through ethernet interface
    3. Upload Configuration file to Ftp through ethernet interface
    4. Modify ethernet interface boot parameter
    5. Return to main menu

Be sure to select 4 to modify boot parameter before downloading!
Enter your choice(1-5): 4

          BOOTLINE  SUBMENU

    1. Set TFTP protocol parameters
    2. Set FTP protocol parameters
    3. Return to ethernet menu

Enter your choice(1-3):
```

Step 2 Configure TFTP or FTP parameters based on the selected server type.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Table 11-5 Modifying parameters on the Ethernet interface

Operation	Description
Entering characters **NOTE** The characters can contain only letters, numerals, underlines (_), and dots (.). Blanks are not allowed.	Indicates that the existing values need to be changed. Press **Enter** to confirm the operation.
Entering a dot (.)	Deletes existing information in the current view.
Pressing a hyphen (-)	Returns to the previous option.
Pressing **Ctrl+D**	Exists from the view for modifying parameters on the Ethernet interface and returns to the Ethernet submenu.
Pressing **Enter**	Skips to the next option without any change.

- If a TFTP server is configured as the file server, select 1 to access the submenu for modifying TFTP parameters.

```
          BOOTLINE
SUBMENU


    1. Set TFTP protocol
parameters
    2. Set FTP protocol
parameters
    3. Return to ethernet
menu


Enter your choice(1-3):
1


'.' = clear field;  '-' = go to previous field;  ^D =
quit

Load File name      : s5720hi.cc
Switch IP address   : 192.168.1.15
Server IP address   : 192.168.1.40
```

Table 11-6 Submenu for modifying TFTP parameters

Item	Description
Load File name	File to be uploaded.
Switch IP address	Configures the management IP address on the device. By default, the management IP address is 192.168.1.15. **NOTE** The IP addresses of the device and the TFTP server must be on the same network segment.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
Server IP address	IP address of the TFTP server.

- If an FTP server is configured as the file server, select 2 to access the submenu for modifying FTP parameters.

```
          BOOTLINE
SUBMENU


    1. Set TFTP protocol
parameters
    2. Set FTP protocol
parameters
    3. Return to ethernet
menu


Enter your choice(1-3):
2


'.' = clear field;  '-' = go to previous field;  ^D =
quit

Load File name      : s5720hi.cc
Switch IP address   : 192.168.1.15
Server IP address   :
192.168.1.40
FTP User Name       : huawei
FTP User Password   :
```

Table 11-7 Submenu for modifying FTP parameters

Item	Description
Load File name	File to be uploaded.
Switch IP address	Configures the management IP address on the device. By default, the management IP address is 192.168.1.15. **NOTE** The IP addresses of the device and the FTP server must be on the same network segment.
Server IP address	IP address of the FTP server.
FTP User Name	User name for logging in to the FTP server.
FTP User Password	Password for logging in to the FTP server, in cipher text.

----End

11.4 File System Submenu

In the BootLoad main menu, select 5 to access the file system submenu.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 5

        FILESYSTEM SUBMENU

     1. Erase Flash
     2. Format flash
     3. Delete file from Flash
     4. Rename file from Flash
     5. Display Flash files
     6. Update EPLD file
     7. Return to main menu

Enter your choice(1-7):
```

Table 11-8 File system submenu

Item	Description
1. Erase Flash	Erases the flash memory. All information including the system software and configuration file are deleted from the flash memory. After the device is deployed in a new environment, you can erase the flash memory and reload the system software and configuration file. **NOTICE** After the flash memory is erased, the device cannot start. You need to reload the system software. Therefore, exercise caution before erasing the flash memory.
2. Format flash	Formats the flash memory. If the flash memory fails, format the flash memory to rectify the fault. If the fault persists, contact technical support personnel. **NOTICE** After the flash memory is formatted, the device cannot start. You need to reload the system software. Therefore, exercise caution before formatting the flash memory.
3. Delete file from Flash	Deletes files in the flash memory. **NOTE** After you select 3 in the file system submenu, all files in the flash memory are displayed. You can delete files as required.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Item	Description
4. Rename file from Flash	Renames files. **NOTE** After you select 4 in the file system submenu, all files in the flash memory are displayed. You can rename files as required.
5. Display Flash files	Displays all files in the flash memory. At the same time, the total size and remaining size of the flash memory are displayed.
6. Update EPLD file	Upgrades the EPLD. Before upgrading the EPLD, select the EPLD file for the upgrade, in the format of .bin.
7. Return to main menu	-

11.5 Password Submenu

In the BootLoad main menu, select 6 to enter the password submenu.

```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 6

        PASSWORD  SUBMENU

     1. Modify bootload password
     2. Reset bootload password
     3. Return to main menu

Enter your choice(1-3):
```

Table 11-9 Password submenu description

Item	Description
1. Modify bootload password	Changes the BootLoad password. You can change the BootLoad password to prevent unauthorized users from entering the BootLoad menu.
2. Reset bootload password	Restores the default BootLoad password. The default BootLoad password is **Admin@huawei.com**.
3. Return to main menu	-

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

11.5.1 Submenu for Changing the Password of the BootLoad Menu

Context

By default, the password for accessing the BootLoad main menu is **Admin@huawei.com**. You are advised to change the password to prevent unauthorized users from accessing the BootLoad.

NOTE

You can also run the **bootrom password change** command to change the password of the BootLoad main menu.

Procedure

- In the BootLoad main menu, select 6 to enter the password submenu.

```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 6

        PASSWORD  SUBMENU

     1. Modify bootload password
     2. Reset bootload password
     3. Return to main menu

Enter your choice(1-3):
```

- In the password submenu, select 1 to enter the page for changing the BootLoad password.

```
        PASSWORD  SUBMENU

     1. Modify bootload password
     2. Reset bootload password
     3. Return to main menu

Enter your choice(1-3): 1

Old password:     //Enter the old password.
New password:     //Enter the new password.
Verify:           //Enter the new password again.
```

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

11.5.2 Restoring the BootLoad Password

Context

You can select 2 Reset bootload password in the password submenu to restore the default BootLoad menu password. The default BootLoad password is **Admin@huawei.com**.

NOTE

Restoring the default BootLoad password using the BootLoad menu achieves the same result as running the **reset boot password** command.

Procedure

- In the BootLoad main menu, select 6 to enter the password submenu.

```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 6
        PASSWORD  SUBMENU

     1. Modify bootload password
     2. Reset bootload password
     3. Return to main menu

Enter your choice(1-3):
```

- In the password submenu, select 2 to restore the default BootLoad password.

```
        PASSWORD  SUBMENU

     1. Modify bootload password
     2. Reset bootload password
     3. Return to main menu

Enter your choice(1-3): 2

The password used to enter the boot menu will be restored to the default
password, continue? [Y/N]y
Succeeded in setting boot password to "Admin@huawei.com".
```

----End

11.6 Submenu for Deleting the Password for Logging In Using the Serial Port

Context

If you forget the password for logging in to the device using telnet or serial port, you cannot log in to the device. To address this issue, the BootLoad menu provides a submenu for deleting the password for logging in using the serial port.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

NOTE

If multiple devices establish a stack, you can log in to the stack system only after deleting the console port login password from the master switch. You are advised to start each member device and delete the console port login password on each device in sequence.

Procedure

- In the BootLoad main menu, select 7.

```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 7

Note: Clear password for console user? Yes or No(Y/N): y
Clear password for console user successfully.
Note: Choose "1. Boot with default mode" to boot, then set a new password
```

NOTICE

After the password is deleted, start the device using option 1 in the BootLoad menu. Do not select 8 or power off the device; otherwise, the configuration becomes invalid.

----End

11.7 Configuration Example

11.7.1 Upgrading the System Software Using the BootLoad Menu

Networking Requirements

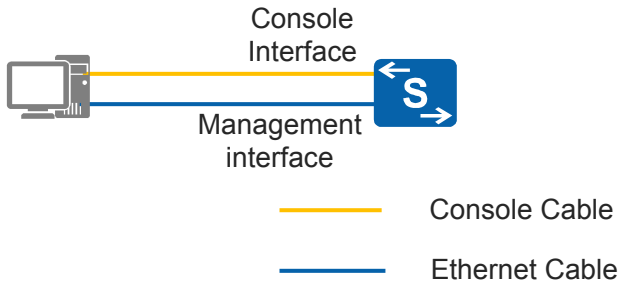
As shown in **Figure 11-1**, a PC is connected to the console interface on a switch and allows users to log in to the switch using terminal emulation software. The network adapter on the PC is connected to the Ethernet interface (management interface) on the switch.

The system software on the switch is faulty, and you cannot log in. To address this issue, you need to use the Ethernet submenu under the BootLoad menu to upload system software and specify it as the next startup system software. In this way, the switch can load the system software and start an upgrade.

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

Figure 11-1 Networking diagram of connecting a PC to a switch



NOTE

In this example, HyperTerminal is used as terminal emulation software. If other third-party terminal emulation software is used, see the corresponding software user guide or online help.

Configuration Roadmap

1. Deploy an FTP server and upload the target system software to the FTP working directory. In this example, configure the PC as the FTP server.
2. Restart the switch and access the BootLoad menu.
3. Set FTP parameters on the switch so that the switch can communicate with the FTP server. Use FTP to upload the target system software to the flash memory on the switch.
4. In the modify ethernet interface boot parameter, configure the uploaded system software as the next startup system software.

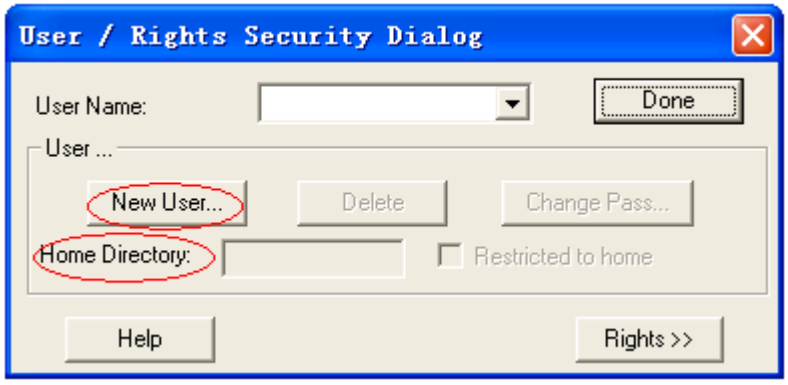
Procedure

Step 1 Configure the PC as the FTP server and copy the system software of the switch to the FTP working directory.

Configure the IP address, user name, password, and working directory for the FTP server.

Run an FTP server program on the PC, for example, **wftpd32**. Choose **Security** > **Users/rights...**. In the dialog box that is displayed as shown in **Figure 11-2**, click **New User...**. In the dialog box that is displayed, set the user name to **user** and password to **huawei**. Set **Home Directory**: to **D:\BootLoad**. Click **Done** to close the dialog box. Set the IP address of the PC to 192.168.1.6 and mask to 255.255.255.0.

Figure 11-2 Configuring the FTP server



Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

Upload the system software, such as S5720EIV200R009C00.cc, to **D:\BootLoad**. The upload process is not mentioned here.

Step 2 Restart the switch. When the following information is displayed, press **Ctrl+B** or **Ctrl+E** and enter the password to access the BootLoad menu. The default BootLoad password is **Admin@huawei.com**.

```
Press Ctrl+B or Ctrl+E to enter BootLoad menu : 2

Password:      //Enter the BootLoad password.
The default password is used now. Change the password.

          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8):
```

Step 3 Set FTP parameters on the switch for setting up an FTP connection with the PC.

In the BootLoad menu, select 4 to access the Ethernet submenu.

```
          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 4

        ETHERNET  SUBMENU

     1. Update BootROM system
     2. Download file to Flash through ethernet interface
     3. Upload Configuration file to Ftp through ethernet interface
     4. Modify ethernet interface boot parameter
     5. Return to main menu

Enter your choice(1-5):
```

In the Ethernet submenu, select 4 and modify the Ethernet parameters.

```
        ETHERNET  SUBMENU

     1. Update BootROM system
     2. Download file to Flash through ethernet interface
     3. Upload Configuration file to Ftp through ethernet interface
     4. Modify ethernet interface boot parameter
     5. Return to main menu

Enter your choice(1-5): 4

        BOOTLINE  SUBMENU
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
     1. Set TFTP protocol parameters
     2. Set FTP protocol parameters
     3. Return to ethernet menu

Enter your choice(1-3):
```

In the Bootline submenu, select 2 and configure the network parameters and system software name on the Ethernet interface.

```
        BOOTLINE  SUBMENU

     1. Set TFTP protocol parameters
     2. Set FTP protocol parameters
     3. Return to ethernet menu

Enter your choice(1-3): 2

'.' = clear field;  '-' = go to previous field;  ^D = quit

Load File name      : S5720EIV200R009C00.cc   //Enter the name of the system
software to be loaded.
Switch IP address   : 192.168.1.2   //Enter the IP address of the management
interface on the device.
Server IP address   : 192.168.1.6   //Enter the server IP address.
FTP User Name       : user   //Enter the server user name.
FTP User Password   :   //Enter the server password.
```

Step 4 After the parameters are set, return to the Ethernet submenu. Select 2 and load the system software to the flash memory.

```
        BOOTLINE  SUBMENU

     1. Set TFTP protocol parameters
     2. Set FTP protocol parameters
     3. Return to ethernet menu

Enter your choice(1-3): 3

        ETHERNET  SUBMENU

     1. Update BootROM system
     2. Download file to Flash through ethernet interface
     3. Upload Configuration file to Ftp through ethernet interface
     4. Modify ethernet interface boot parameter
     5. Return to main menu

Enter your choice(1-5): 2

Use ftp to download file : S5720EIV200R009C00.cc , please wait for a moment......
If it can't be finished for a long time, please enter Ctrl+\ to break and check
the network configuration.
Successfully download S5720EIV200R009C00.cc
```

Step 5 Exit the Ethernet submenu. Select 3 in the BootLoad menu and specify the loaded system software as the next startup file.

```
        ETHERNET  SUBMENU

     1. Update BootROM system
     2. Download file to Flash through ethernet interface
     3. Upload Configuration file to Ftp through ethernet interface
     4. Modify ethernet interface boot parameter
     5. Return to main menu

Enter your choice(1-5): 5

          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 3

        Startup Configuration Submenu

     1. Display startup configuration
     2. Modify startup configuration
     3. Return to main menu

Enter your choice(1-3): 2

Note: startup file field can not be cleared
'.'=clear field; '^D'=quit; Enter=use current configuration

startup type(1: Flash)
  current: 1
  new    :   //Press Enter. It does not need to be set.

Flash startup file (can not be cleared)
  current: s5720ei-V200R009C00SPC100B310.cc
  new    : S5720EIV200R009C00.cc    //Specify the loaded system software as the
next startup file.

saved-configuration file
  current: backupz.zip
  new    :   //Press Enter. It does not need to be set.

patch package
  current:
  new    :   //Press Enter. It does not need to be set.
```

Step 6 Exit the startup submenu. In the BootLoad menu, select 1 to start the switch.

```
        Startup Configuration Submenu

     1. Display startup configuration
     2. Modify startup configuration
     3. Return to main men

Enter your choice(1-3): 3

          BootLoad Menu

    1. Boot with default mode
    2. Enter serial submenu
    3. Enter startup submenu
    4. Enter ethernet submenu
    5. Enter filesystem submenu
    6. Enter password submenu
    7. Clear password for console user
    8. Reboot
    (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 1
```

Step 7 Check the configuration.

After the switch starts, run the **display version** command in the CLI to check whether the switch version is the target version.

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (S5720 V200R009C00)
Copyright (C) 2000-2014 HUAWEI TECH CO., LTD
HUAWEI S5720-50X-EI-46S-AC Routing Switch uptime is 0 week, 0 day, 0 hour, 2
```


Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016


```
minutes

......
```

The preceding command output shows that the system software version is **S5720 V200R009C00**, indicating that the system software is successfully upgraded.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0

e-DOC 16A8F5D0-e
Proc 13409/2016

12 Checking Declaration Information of an Open Source Software

Context

The declaration information of an open source software includes the following items:

- Warranty Disclaimer
- Copyright Notice
- Written Offer

Procedure

- Run the **display copyright** command to check declaration information of an open source software.

----End

Copyright © Huawei Technologies Co., Ltd.

Documento assinado digitalmente. Para verificar as assinaturas, acesse www.tc.df.gov.br/autenticidade e informe o edoc 16A8F5D0