



Quidway S5300 Series Ethernet Switches
V100R002C02

Configuration Guide - Basic Configuration

Issue	01
Date	2008-12-26
Part Number	

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

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

Copyright © Huawei Technologies Co., Ltd. 2008. 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



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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 the statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

About This Document.....	1
1 Logging In to the S-switch.....	1-1
1.1 Introduction.....	1-2
1.1.1 Methods of Logging In to the S-switch.....	1-2
1.1.2 Logical Relationships Between Configuration Tasks.....	1-2
1.2 Logging In to the S-switch Through the Console Interface.....	1-2
1.2.1 Establishing the Configuration Task.....	1-2
1.2.2 Logging In to the S-switch Through the Console Interface.....	1-3
1.3 Logging In to the S-switch Through Telnet.....	1-8
1.3.1 Establishing the Configuration Task.....	1-8
1.3.2 Logging In to the S-switch Through Telnet.....	1-9
1.4 Logging In to the S-switch Remotely Through Telnet.....	1-10
1.4.1 Establishing the Configuration Task.....	1-10
1.4.2 Logging In to the S-switch Remotely Through Telnet.....	1-11
1.5 Logging In to the S-switch Through SSH.....	1-11
1.5.1 Establishing the Configuration Task.....	1-11
1.5.2 Logging In to the S-switch Through SSH.....	1-11
2 How to Use Command Lines.....	2-1
2.1 Command Views.....	2-2
2.1.1 Command View Classifications.....	2-2
2.1.2 Hierarchies of Command Views.....	2-2
2.1.3 Common Views.....	2-3
2.2 Command Levels.....	2-5
2.2.1 Introduction to Command Levels.....	2-5
2.2.2 Relations Between Command Levels and User Levels.....	2-6
2.2.3 Command Level Switching.....	2-7
2.3 Command Line Online Help.....	2-8
2.3.1 Full Help.....	2-8
2.3.2 Partial Help.....	2-8
2.4 Editing Command Lines.....	2-9
2.5 Changing the Language of Displayed Information.....	2-10
2.6 Controlling Information Displayed in a CLI.....	2-10

2.7 Using History Commands.....	2-10
2.8 Shortcut Keys.....	2-11
3 Common Operations and Configurations.....	3-1
3.1 Introduction.....	3-2
3.1.1 Introduction to Common Operations.....	3-2
3.1.2 Introduction to Common Configurations.....	3-2
3.1.3 Logical Relationships Between Configuration Tasks.....	3-2
3.1.4 Common Operations.....	3-2
3.1.5 Locking a User Interface.....	3-4
3.1.6 Sending Information Between User Interfaces.....	3-4
3.1.7 Cutting off the Connection Between User Interfaces.....	3-4
3.2 Basic System Configuration.....	3-4
3.2.1 Setting the Name of the S-switch	3-5
3.2.2 Setting the System ClockS-switch	3-5
3.2.3 Switching a Language Mode.....	3-5
3.3 Changing Command Levels and User Levels.....	3-6
3.3.1 Changing User Levels.....	3-6
3.3.2 Extending Command Levels.....	3-6
3.3.3 Extending User Levels.....	3-6
3.4 Common Telnet Operations.....	3-7
3.4.1 Initiating a Telnet Connection.....	3-7
3.4.2 Cutting off a Telnet Connection.....	3-8
4 Managing Login Users.....	4-1
4.1 Introduction.....	4-2
4.1.1 User Login Modes.....	4-2
4.1.2 User Interface.....	4-2
4.1.3 User Authentication.....	4-3
4.1.4 Telnet Terminal Services.....	4-5
4.1.5 SSH Terminal Services.....	4-6
4.1.6 References.....	4-8
4.1.7 Logical Relationships Between Configuration Tasks.....	4-9
4.2 Configuring the Console Interface as the User Interface.....	4-9
4.2.1 Establishing the Configuration Task.....	4-9
4.2.2 (Optional) Configuring the Attributes of the User Interface.....	4-10
4.2.3 (Optional) Configuring User Authentication.....	4-11
4.2.4 (Optional) Setting User Levels.....	4-13
4.2.5 Checking the Configuration.....	4-13
4.3 Configuring Telnet Users.....	4-13
4.3.1 Establishing the Configuration Task.....	4-14
4.3.2 (Optional) Configuring the Attributes of the VTY User Interface.....	4-15
4.3.3 Configuring the VTY User Interface to Support the Telnet Service.....	4-17
4.3.4 Assigning an IP Address to the Telnet Server.....	4-17

4.3.5 Configuring User Authentication.....	4-17
4.3.6 Setting User Levels.....	4-19
4.3.7 Checking the Configuration.....	4-20
4.4 Configuring SSH Login Users.....	4-20
4.4.1 Establishing the Configuration Task.....	4-21
4.4.2 (Optional) Configuring the Attributes of the VTY Interface.....	4-21
4.4.3 Configuring the VTY User Interface to Support the SSH Service.....	4-23
4.4.4 Assigning an IP Address to the SSH Server.....	4-24
4.4.5 Configuring the Password Authentication Mode for SSH Login Users.....	4-24
4.4.6 Configuring the RSA Authentication Mode for SSH Login Users.....	4-24
4.4.7 (Optional) Setting the SSH Timer and Authentication Times.....	4-25
4.4.8 Checking the Configuration.....	4-26
4.5 Maintaining User Interfaces and Terminal Services.....	4-26
4.6 Configuration Examples.....	4-27
4.6.1 Example for Configuring the Telnet Login User on the Ethernet.....	4-27
4.6.2 Example for Configuring the SSH Login User.....	4-29
5 Managing the File System.....	5-1
5.1 Introduction.....	5-2
5.1.1 File System.....	5-2
5.1.2 File Transfer Modes.....	5-3
5.1.3 Logical Relationships Between Configuration Tasks.....	5-3
5.2 Managing the File System.....	5-3
5.2.1 Changing the Prompt Mode of the File System.....	5-4
5.2.2 Managing the Flash Memory.....	5-4
5.2.3 Managing File Directories.....	5-4
5.2.4 Managing Files.....	5-5
5.2.5 Executing the Batch File.....	5-5
5.3 Transferring Files with the S-switch Acting as the FTP Server.....	5-6
5.3.1 Establishing the Configuration Task.....	5-6
5.3.2 Enabling the FTP Server.....	5-6
5.3.3 Configuring Authentication and Authorization for Users Logging In to the FTP Server.....	5-7
5.3.4 (Optional) Setting the Timeout Period of the FTP Server.....	5-7
5.3.5 Checking the Configuration.....	5-8
5.4 Transferring Files with the S-switch Acting as the FTP Client.....	5-8
5.4.1 Establishing the Configuration Task.....	5-8
5.4.2 Logging In to the FTP Server.....	5-9
5.4.3 Cutting Off an FTP Connection.....	5-9
5.4.4 Switching the User Logging In to the FTP Server.....	5-9
5.4.5 Displaying Online Help About an FTP Command.....	5-10
5.4.6 Managing the Directory on the FTP Server.....	5-10
5.4.7 Managing Files on the FTP Server.....	5-10
5.4.8 Setting the File Transfer Mode.....	5-11

5.5 Transferring Files with the S-switch Acting as the TFTP Client.....	5-11
5.5.1 Establishing the Configuration Task.....	5-11
5.5.2 Setting the Range of Usable TFTP Servers.....	5-12
5.5.3 Initiating a TFTP Connection and Downloading Files.....	5-12
5.5.4 Initiating a TFTP Connection and Uploading Files.....	5-12
5.5.5 Checking the Configuration.....	5-13
5.6 Maintaining the File System.....	5-13
5.6.1 Debugging the File System.....	5-13
5.6.2 Debugging the FTP Server.....	5-13
5.7 Configuration Examples.....	5-14
5.7.1 Example for Transferring Files Through FTP with the S-switch Acting as the FTP Server.....	5-14
5.7.2 Example for Transferring Files Through FTP with the S-switch Acting as the FTP Client.....	5-16
5.7.3 Example for Transferring Files Through TFTP.....	5-17
5.7.4 Example for Integrated Operations of the File System.....	5-18
6 Managing Configuration Files.....	6-1
6.1 Introduction.....	6-2
6.1.1 Configuration Files.....	6-2
6.1.2 Logical Relationships Between Configuration Tasks.....	6-2
6.2 Checking the Configuration.....	6-2
6.2.1 Checking the Current Configuration.....	6-2
6.2.2 Checking Saved Configurations.....	6-2
6.3 Common Operations for the Configuration File.....	6-3
6.3.1 Saving the Current Configuration File.....	6-3
6.3.2 Clearing the Configuration File.....	6-3
6.3.3 Comparing Configuration Files.....	6-4
6.4 Configuring the Configuration File for the Next Startup.....	6-4

Figures

Figure 1-1 Logging In to the S-switch.....	1-3
Figure 1-2 Setting up a connection.....	1-4
Figure 1-3 Configuring the interface for connection.....	1-5
Figure 1-4 Specifying parameters.....	1-6
Figure 1-5 Selecting the terminal type.....	1-7
Figure 1-6 Logging In to the S-switch Through Telnet.....	1-8
Figure 1-7 Logging in to S-switch through a directly-connected PCS-switch.....	1-10
Figure 2-1 Hierarchies of command views.....	2-3
Figure 2-2 User Authority.....	2-7
Figure 3-1 Cutting off a cascading Telnet connection.....	3-8
Figure 4-1 S-switch providing the Telnet server service.....	4-5
Figure 4-2 S-switch providing the Telnet client service.....	4-6
Figure 4-3 S-switch providing cascading Telnet service.....	4-6
Figure 4-4 Local SSH connection between the PC and the S-switch.....	4-7
Figure 4-5 Remote login on the Ethernet.....	4-27
Figure 4-6 SSH local configuration.....	4-29
Figure 5-1 Managing files on the S-switch.....	5-2
Figure 5-2 Using FTP to upload files when the S-switch acts as the FTP server.....	5-14
Figure 5-3 Using FTP to download files when the S-switch acts as the FTP client.....	5-16
Figure 5-4 Using TFTP to download files when the S-switch acts as the TFTP client.....	5-17
Figure 5-5 Configuring the integrated file system.....	5-19

Tables

Table 1-1 Parameters.....	1-6
Table 2-1 Views and categories.....	2-2
Table 2-2 User levels.....	2-7
Table 2-3 Using history commands.....	2-11
Table 2-4 Shortcut keys.....	2-12
Table 4-1 User login modes.....	4-2
Table 4-2 Types of user interfaces.....	4-3
Table 4-3 Classifying users.....	4-4
Table 4-4 Authentication modes for login users.....	4-4
Table 4-5 Debugging Terminal Services.....	4-26

About This Document

Purpose

This document provides configuration procedures and examples for the basic features of the S-switch.

This document covers the following topics:

- Feature description
- Data preparations
- Pre-configuration tasks
- Configuration procedures
- Checking the configuration
- Configuration examples

This document helps you grasp the configuration procedures and application scenarios of the basic features of the S-switch.

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
S5300	V100R002C02

Intended Audience

This document is intended for:

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

Organization



This document provides basic knowledge of the software and hardware of the S-switch and describes user login procedures.




Chapter	Description
1 Logging In to the S-switch	Describes how to log in to the S-switch from a client.
2 How to Use Command Lines	Describes how to use command lines.
3 Common Operations and Configurations	Describes basic operations and configurations.
4 Managing Login Users	Describes how to log in to user interfaces, how to configure and maintain Telnet and Secure Shell (SSH) terminal services, and how to log in to the S-switch through an AUX interface. This chapter also provides configuration examples.
5 Managing the File System	Describes the basics of the file system, how to upload and download files through the File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP), and how to manage configuration files. This chapter also provides configuration examples and troubleshooting procedures.
6 Managing Configuration Files	Describes basic concepts and operations of configuration files.

Conventions

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.

Symbol	Description
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 TIP	Indicates a tip that may help you address a problem or save your time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

General Conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in Boldface . For example, log in as user Root .
<i>Italic</i>	Book titles are in <i>Italics</i> .
Courier New	Examples of information displayed on the screen are in Courier New.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x y ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none 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 alternative items are grouped in square brackets and separated by vertical bars. Several or none is selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

GUI Conventions

Convention	Description
boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard Operations

Convention	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+Alt+A means the three keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, F means the two keys should be pressed in turn.

Mouse Operations

Convention	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Update History

Updates between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Updates in Issue 01 (2008-12-26)

This is the first release.

1 Logging In to the S-switch

About This Chapter

This chapter describes how to log in to the S-switch from a client.

[1.1 Introduction](#)

This section describes how to log in to the S-switch and logical relations between configuration tasks.

[1.2 Logging In to the S-switch Through the Console Interface](#)

This section describes how to log in to the S-switch through the console interface.

[1.3 Logging In to the S-switch Through Telnet](#)

This section describes how to log in to the S-switch through Telnet.

[1.4 Logging In to the S-switch Remotely Through Telnet](#)

This section describes how to log in to the S-switch remotely through Telnet.S-switch

[1.5 Logging In to the S-switch Through SSH](#)

This section describes how to log in to the S-switch through Secure Shell (SSH).

1.1 Introduction

This section describes how to log in to the S-switch and logical relations between configuration tasks.

[1.1.1 Methods of Logging In to the S-switch](#)

[1.1.2 Logical Relationships Between Configuration Tasks](#)

1.1.1 Methods of Logging In to the S-switch

To manage and configure the S-switch, you need to log in to the S-switch.

You can log in to the S-switch through various types of interfaces such as console interfaces, service interfaces, and AUX interfaces. You can log in to the S-switch in the following methods:

- Console interface
- Telnet
- SSH
-

1.1.2 Logical Relationships Between Configuration Tasks

If you log in to the S-switch initially or need to log in to it later on site, perform [1.2 Logging In to the S-switch Through the Console Interface](#).

For logging in to the S-switch through other methods, see the configuration procedure in [4 Managing Login Users](#) to complete the configuration. Then, perform the following as required:

- [1.3 Logging In to the S-switch Through Telnet](#)
- [1.4 Logging In to the S-switch Remotely Through Telnet](#)
- [1.5 Logging In to the S-switch Through SSH](#)

1.2 Logging In to the S-switch Through the Console Interface

This section describes how to log in to the S-switch through the console interface.

[1.2.1 Establishing the Configuration Task](#)

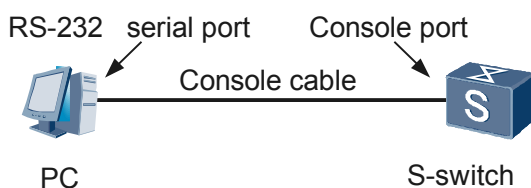
[1.2.2 Logging In to the S-switch Through the Console Interface](#)

1.2.1 Establishing the Configuration Task

Applicable Environment

As shown in [Figure 1-1](#), you need to log in to the S-switch through the console interface.

Figure 1-1 Logging In to the S-switch



 **NOTE**

If the S-switch is powered on for the first time and you need to manage and configure the S-switch, you can log in to the S-switch through only the console interface.

Pre-configuration Tasks

Before logging in to the S-switch through the console interface, complete the following tasks:

- Connecting the PC and the S-switch properly
- Starting the S-switch properly

Data Preparations

None.

1.2.2 Logging In to the S-switch Through the Console Interface

Context

When establishing the configuration environment through the console interface, you can log in to the S-switch through the HyperTerminal in Windows.

Procedure

Step 1 Start the HyperTerminal.

Choose **Start > All Program > Accessories > Communications > HyperTerminal** to start the HyperTerminal in Windows XP.

Step 2 Set up a connection.

See [Figure 1-2](#). Enter the name of the new connection in the **Name** text box and then choose one icon. Then, click **OK**.

Figure 1-2 Setting up a connection**Step 3** Configure an interface for connection.

In the **Connect To** dialog box, as shown in [Figure 1-3](#), select an interface from the drop-down list box according to the actual interface on the PC or terminal. Next, click **OK**.

Figure 1-3 Configuring the interface for connection

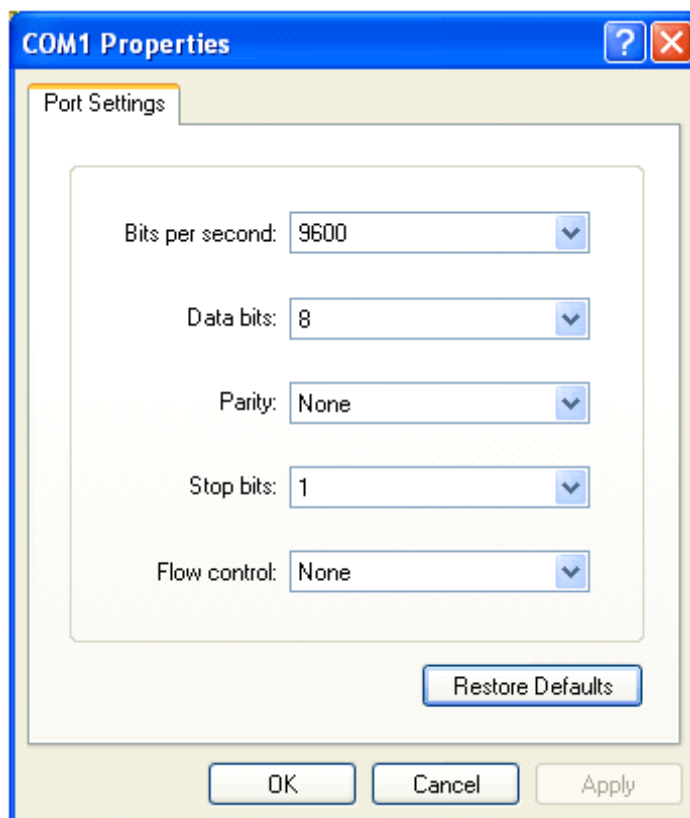


Step 4 Set communication parameters.

When the **COM1 Properties** dialog box is displayed as shown in [Figure 1-4](#), specify the parameters listed in [Table 1-1](#).

 **NOTE**

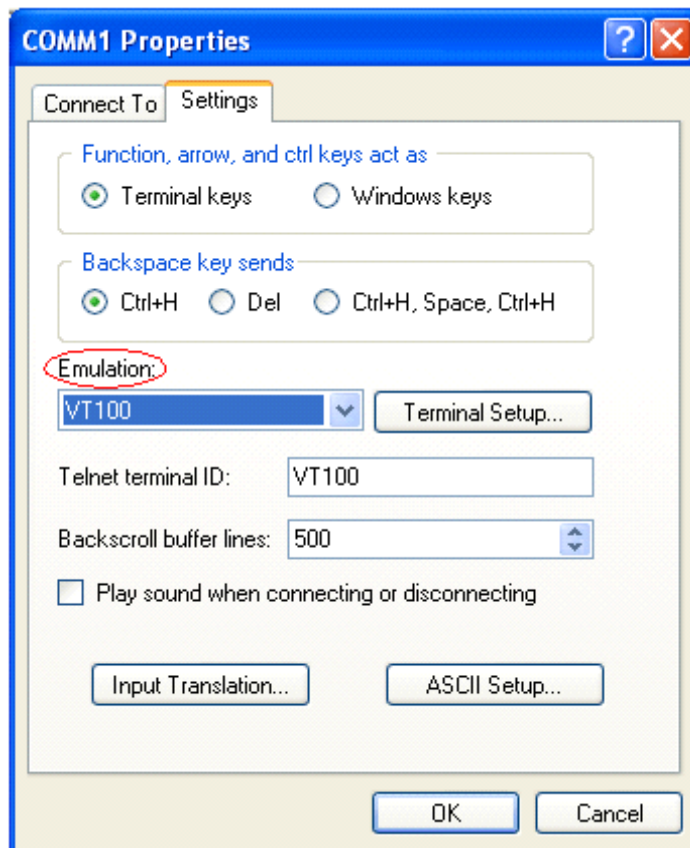
In other Windows operating systems, bits per second may be described as baud rate and data stream control may be described as traffic control.

Figure 1-4 Specifying parameters**Table 1-1** Parameters

Parameter	Value
Bit per second (baud rate)	9600
Data bit	8
Parity check	None
Stop bit	1
Flow control (traffic control)	None

- Step 5** After the HyperTerminal starts, choose **FileAttributes** to display the **COMM1 Properties** dialog box, as shown in **Figure 1-5**. On the **Setting** tab, select VT100 in the **Emulation** drop-down list box. Click **OK** to complete the setting.

Figure 1-5 Selecting the terminal type



----End

Postrequisite

After the preceding configurations are complete, press **Enter**. If the prompt <Quidway> is displayed on the screen, it indicates that the Command Line Interface (CLI) is displayed. In this case, you can enter commands to configure or manage the S-switch. For details on configuration procedures, see the following sections.

1.3 Logging In to the S-switch Through Telnet

This section describes how to log in to the S-switch through Telnet.

1.3.1 Establishing the Configuration Task

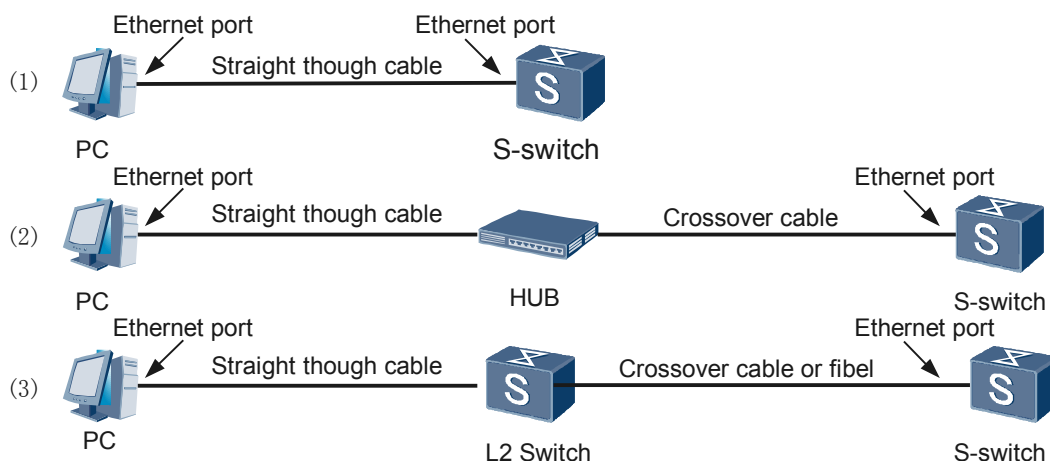
1.3.2 Logging In to the S-switch Through Telnet

1.3.1 Establishing the Configuration Task

Applicable Environment

As shown in [Figure 1-6](#), you need to log in to the S-switch through an Ethernet or MEth interface in Telnet mode.

Figure 1-6 Logging In to the S-switch Through Telnet



- The Ethernet interface on the PC or terminal is connected to the Ethernet or MEth interface on the S-switch.
- The Ethernet interface on the PC or terminal is connected to the Ethernet or MEth interface on the S-switch through a hub.
- The Ethernet interface on the PC or terminal is connected to the Ethernet or MEth interface on the S-switch through another switch.

Pre-configuration Tasks

Before logging in to the S-switch through Telnet, complete the following tasks:

- Connecting the PC and S-switch properly
- Starting the S-switch properly
- If you need to log in to the S-switch through an Ethernet interface, you must add the Ethernet interface to a VLAN and assign an IP address and mask to the VLAN IF interface.
- Set the parameters of the Telnet server. For the configuration procedure, see [4 Managing Login Users](#).

Data Preparations

To log in to the S-switch through Telnet, you need the following data.

No.	Data
1	IP address of the Telnet server

1.3.2 Logging In to the S-switch Through Telnet

Context

Before logging in to the S-switch through Telnet, you can connect the S-switch through the Telnet client in Windows.

Procedure

Step 1 Start Command Prompt.

Choose **Start > Programs > Accessories > Command Prompt**. The Command Prompt window is displayed.

The Command Prompt window displays the following messages:

```
Microsoft Windows XP [Version 5.1.2600]
(c) Copyright 1985-2001 Microsoft Corp.

C:\>
```

Step 2 Display the Telnet client.

At the prompt C:\>, enter **Telnet**. The Command Prompt window displays the following messages:

```
Microsoft Windows XP [Version 5.1.2600]
(c) Copyright 1985-2001 Microsoft Corp.

C:\> telnet
```

Press **Enter** to display the Telnet client. The Command Prompt window displays the following messages:

```
Welcome to Microsoft Telnet Client

Escape character is 'CTRL+]'

Microsoft Telnet>
```

Step 3 Connect the Telnet server.

At the prompt Microsoft Telnet>, enter the following command to connect the Telnet server.

open { *ip-address* | *host-name* } [*port*]

ip-address: specifies the IP address of the Telnet server.

host-name: specifies the host name of the Telnet server.

port: specifies the port of the Telnet server. The default value is 23.

For example:

Connect the S-switch at 1.1.1.1. The default port number is 23.

Welcome to Microsoft Telnet Client

Escape character is 'CTRL+J'

Microsoft Telnet> open 1.1.1.1

```
*****
*           All rights reserved (2007-2008)           *
*   Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*****
```

Note: The max number of VTY users is 5, and the current number
of VTY users on line is 1.

<Quidway>

----End

1.4 Logging In to the S-switch Remotely Through Telnet

This section describes how to log in to the S-switch remotely through Telnet.S-switch

1.4.1 Establishing the Configuration Task

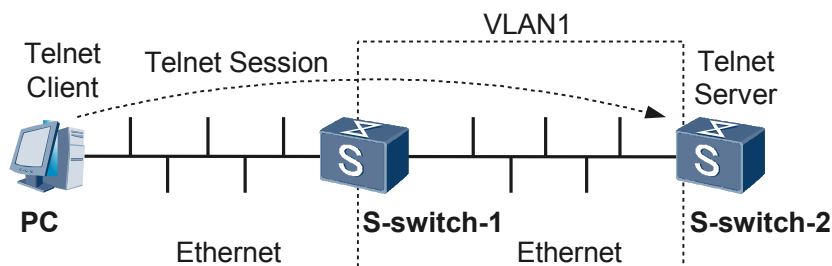
1.4.2 Logging In to the S-switch Remotely Through Telnet

1.4.1 Establishing the Configuration Task

Applicable Environment

As shown in [Figure 1-7](#), you need to log in to the S-switch remotely through Telnet to configure and manage the S-switch through a PC or a terminal.S-switch

Figure 1-7 Logging in to S-switch through a directly-connected PCS-switch



Pre-configuration Tasks

Before logging in to the S-switch remotely through Telnet, complete the following tasks:

- Connecting the PC and S-switch properly
- Starting the S-switch properly
- Configuring a direct or indirect route between the PC and S-switch

Data Preparations

To log in to the S-switch remotely through Telnet, you need the following data.

No.	Data
1	IP address of the Telnet server

1.4.2 Logging In to the S-switch Remotely Through Telnet

For details on how to log in to the S-switch remotely and directly through Telnet, see [1.3.2 Logging In to the S-switch Through Telnet](#). For details on how to log in to the S-switch in the cascade login method, see [1.3.2 Logging In to the S-switch Through Telnet](#).

1.5 Logging In to the S-switch Through SSH

This section describes how to log in to the S-switch through Secure Shell (SSH).

[1.5.1 Establishing the Configuration Task](#)

[1.5.2 Logging In to the S-switch Through SSH](#)

1.5.1 Establishing the Configuration Task

Applicable Environment

You need to log in to the S-switch through an Ethernet interface in SSH mode.

Pre-configuration Tasks

Before logging in to the S-switch through SSH, complete the following tasks:

- Obtaining the private key and username for login
- Connecting the PC and S-switch properly
- Starting the S-switch properly

Data Preparations

None.

1.5.2 Logging In to the S-switch Through SSH

Run the client software that supports SSH 1.5 on the PC or the terminal and enter the login interface. Enter the username, and then you can log in to the S-switch.

2 How to Use Command Lines

About This Chapter

This section describes how to use command lines.

[2.1 Command Views](#)

This section describes hierarchies of command views and relations between command views and interfaces.

[2.2 Command Levels](#)

This section describes command levels, user levels, and the relation between them.

[2.3 Command Line Online Help](#)

This section describes two types of online help: full help and partial help.

[2.4 Editing Command Lines](#)

This section describes the basic editing function of the CLI.

[2.5 Changing the Language of Displayed Information](#)

This section describes how to change the language of displayed information.

[2.6 Controlling Information Displayed in a CLI](#)

This section describes how to control displayed information.

[2.7 Using History Commands](#)

This section describes how to use history commands.

[2.8 Shortcut Keys](#)

This section describes the shortcut keys of the S-switch.

2.1 Command Views

This section describes hierarchies of command views and relations between command views and interfaces.

Command view is the interface where command line can be input.

The CLI on the Huawei Versatile Routing Platform (VRP) system are classified into different command views. Each command is enrolled in one or more command views. The commands can only run in the proper views.

2.1.1 Command View Classifications

2.1.2 Hierarchies of Command Views

2.1.3 Common Views

2.1.1 Command View Classifications

As shown in [Table 2-1](#), command views are classified into basic views, system management views, LAN views, WAN views, MPLS views, VPN views, IP routing views, QoS views, and security views according to their features and the modules to which they belong.

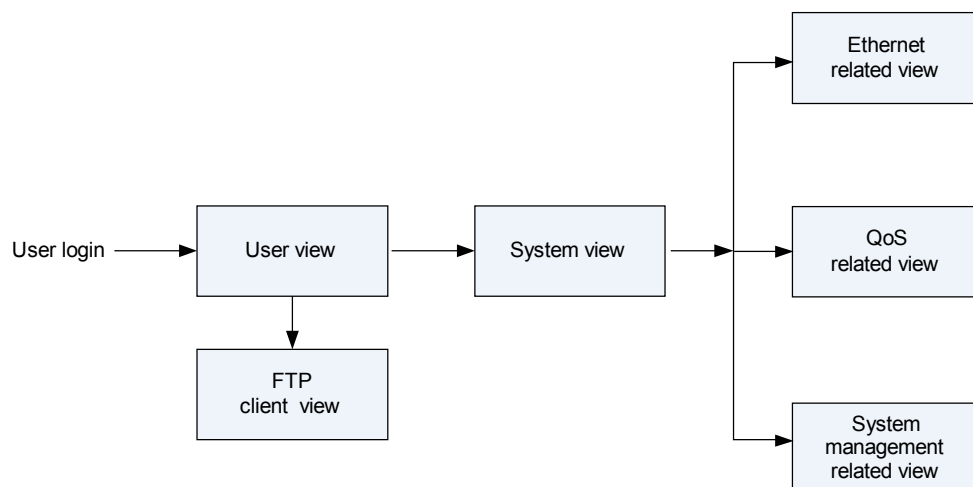
Table 2-1 Views and categories

View	Category
Basic views	User view, system view, VTY user interface view, public key editing view, public key view, and ACL view
System management views	HGMP cluster view, FTP client view, AAA view, AAA domain view, HWTACACS template view, RADIUS template view, accounting scheme view, recording scheme view, authentication scheme view, and authorization scheme view
LAN views	GE interface view, Eth-Trunk interface view, VLAN view, VLANIF interface view, RRPP domain view, RBRP view, MST domain view,
QoS related view	Policy view, class view and traffic classification view

2.1.2 Hierarchies of Command Views

Command views, which have both differences and relations among them apply to different configurations. For example, when you log in to the S-switch, the user view is displayed. In this view, you can view the running status and statistics or monitor the device. Then, you can run the **system-view** command to enter the system view and enter commands to enter related protocol and interface views. [Figure 2-1](#) shows the hierarchies of command views.

Figure 2-1 Hierarchies of command views



2.1.3 Common Views

User View

Item	Description
Function	Displays the operation status and statistics about the S-switch.S-switch
Entry command	Enters the user view after setting up a connection.
Prompt upon entry	<Quidway>
quit	<Quidway> quit
Prompt upon quit	None.

System View

Item	Description
Function	Sets the system parameters of the S-switch. After entering the system view, you can enter other views to configure the S-switch.S-switch
Entry command	<Quidway> system-view
Prompt upon entry	[Quidway]
quit	[Quidway] quit
Prompt upon quit	<Quidway>

Ethernet Interface Views

- GE interface view

Item	Description
Function	Set parameters of a Gigabit Ethernet interface and manage the Gigabit Ethernet interface.S-switch
Entry command	[Quidway] interface gigabitethernet <i>X/Y/Z</i>
Prompt upon entry	[Quidway-GigabitEthernet <i>X/Y/Z</i>]
quit	[Quidway- GigabitEthernet <i>X/Y/Z</i>] quit
Prompt upon quit	[Quidway]

NOTE

X/Y/Z specifies the number of a Gigabit Ethernet interface to be configured. It is in the format of slot number/subcard number/interface sequence number.

VLAN Views

Item	Description
Function	Adds an interface to or deletes an interface from a VLAN, and enables the multicast function in the VLAN.
Entry command	[Quidway] vlan 1
Prompt upon entry	[Quidway-vlan1]
quit	[Quidway-vlan1] quit
Prompt upon quit	[Quidway]

VLANIF Interface View

Item	Description
Function	Assigns IP addresses to VLANIF interfaces and manages the VLANIF interfaces.
Entry command	[Quidway] interface vlanif 1
Prompt upon entry	[Quidway-Vlanif1]
quit	[Quidway-Vlanif1] quit

Item	Description
Prompt upon quit	[Quidway]



NOTE

The value 1 indicates the number of a VLANIF interface to be configured. You must create a VLAN before entering the VLANIF interface view.

2.2 Command Levels

This section describes command levels, user levels, and the relation between them.

2.2.1 Introduction to Command Levels

2.2.2 Relations Between Command Levels and User Levels

2.2.3 Command Level Switching

2.2.1 Introduction to Command Levels

System commands are protected at four levels numbered from 0 to 3. A greater number indicates a higher level.

- 0: visit level
- 1: monitoring level
- 2: configuration level
- 3: management level

You can change the command level as required. For more commands, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.



NOTE

Users that log in to the system are also classified into four levels corresponding to the four command levels. A user can use only the commands whose levels are equal to or lower than the level of the user. For user levels, see "[2.2.2 Relations Between Command Levels and User Levels](#)."

Commands at the Visit Level

Commands at the visit level include commands for network diagnosis, such as the **ping** and **tracert** commands, and the commands used to access other devices. You cannot save the configuration file after using commands at this level.

By default, commands at the visit level include the following:

Level	Usable Commands
Visit level	cluster, language-mode, ping, quit, super, telnet, tracert

Commands at the Monitoring Level

You can use commands at the monitoring level to maintain the system and diagnose faults. You cannot save the configuration file after using commands at this level.

By default, commands at the monitoring level include the following:

Level	Usable Commands
Monitoring level	debugging, display, reset, send, terminal , and so on

Commands at the Configuration Level

Commands at the configuration level, which include routing commands and commands at each network layer, provide network services for users.

By default, commands at the configuration level include the following:

Level	Usable Commands
Configuration level	cluster-ftp, cluster-tftp, compare, mpls, ntpd, reset, save, system-view , and so on

Commands at the Management Level

Commands at the management level are for the basic operation and supporting modules of the system. These commands support provision of services.

By default, commands at the management level include the following:

Level	Usable Commands
Management level	cd, clock, copy, delete, dir, fixdisk, format, free, ftp, lock, mkdir, more, move, patch, pwd, reboot, rename, rmdir, schedule, startup, undelete, tftp , and so on

2.2.2 Relations Between Command Levels and User Levels

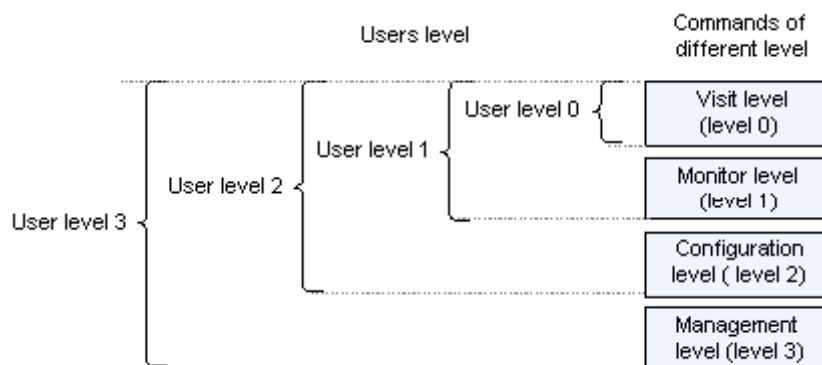
Users that log in to the S-switch are managed according to their levels. Similar to the command levels, users are classified into four levels numbered from 0 to 3. [Table 2-2](#) shows the user levels.

Table 2-2 User levels

Level	Name	Usable Commands
0	Visit level	language-mode , ping , quit , super , telnet , tracert , and so on
1	Monitoring level	debugging , display , language-mode , ping , quit , reset , send , super , telnet , terminal , tracert , undo , and so on
2	Configuration level	All configuration commands except for file system commands, the FTP command, and the TFTP command
3	Management level	All commands

After logging in to the S-switch, users obtain the authority that is determined by their own levels. A user can use only the commands whose levels are equal to or lower than the user level. **Figure 2-2** shows the user authority.

Figure 2-2 User Authority



For example, users at the configuration level can use only commands at the visit level, monitoring level, and configuration level. Users at the management level can use commands at all levels. When users switch to a higher level, authentication is required to prevent unauthorized users from logging in.

2.2.3 Command Level Switching

The S-switch has two types of command level classifications: level 0 to level 3 and level 0 to level 15. By default, the classification of level 0 to level 3 is adopted. If you need to manage the authority in a refined manner or interconnect the S-switch with non-Huawei devices, you can adopt the classification of level 0 to level 15.

If the classification of level 0 to level 3 is changed to that of level 0 to level 5, the visit and monitoring levels are retained. The configuration level, however, is upgraded to level 10 and the management level to level 15. In the classification of level 0 to level 15, no corresponding

command is at level 2 to level 9 or level 11 to level 14. You can thus set a command to any of these levels to manage the user authority in a refined manner.

2.3 Command Line Online Help

This section describes two types of online help: full help and partial help.

2.3.1 Full Help

2.3.2 Partial Help

2.3.1 Full Help

You can obtain full help from a command view in the following methods:

- In a command view, enter `?` to obtain all the commands in this command view and descriptions of the commands.
`<Quidway> ?`
- Enter a command and a `?` separated by a space. If a keyword is in place of the `?`, all keywords and their descriptions are listed. Here is an example.
`<Quidway> language-mode ?`
chinese Chinese environment
english English environment
`<Quidway> language-mode chinese ?`
`<cr>`
`<Quidway> language-mode chinese`
chinese and english are keywords. Chinese environment and English environment are the descriptions of the two keywords.
`<cr>` indicates that no key word or parameter is in this position and you can press **Enter** to repeat the command in the next command line.
- Enter a command and a `?` separated by a space. If a parameter is in place of the `?`, all parameters and their descriptions are listed. Here is an example.
`<Quidway> system-view`
`[Quidway] sysname ?`
TEXT Host name(1 to 30 characters)
TEXT is a parameter and Host name (1 to 30 characters) is the description.

2.3.2 Partial Help

You can obtain partial help from a command view in the following methods:

- Enter a character string closely followed by a `?`. All commands that begin with this character string are listed.
`<Quidway> d?`
debugging delete dir display
- Enter a command and a character string closely followed by a `?`. All key words of the command beginning with this string are listed.
`<Quidway> display v?`
version vlan
- Enter the first letters of a key word of a command and press **Tab**. Then, the key word is displayed completely. The first letters, however, must uniquely identify the key word. Otherwise, after **Tab** is continuously pressed, different key words are displayed, from which you can select one as required.

If you run the **language-mode chinese** command in the user view, all the preceding help messages are displayed in Chinese.

If commands entered pass the syntax check, the commands are correctly run. Otherwise, the system prompts error messages.

Error Information in English	Cause
Unrecognized command	Indicates that no command is found.
	Indicates that no keyword is found.
	Indicates that the parameter type is incorrect.
	Indicates that the parameter value is out of the permitted range.
Incomplete command	Indicates that the command input is incomplete.
Too many parameters	Indicates that the parameters input are excessive.
Ambiguous command	Indicates that the parameters entered are ambiguous.

2.4 Editing Command Lines

This section describes the basic editing function of the CLI.

You can edit commands in a CLI that supports multi-line edit. Each command can contain up to 255 characters.

Key	Function
Common key	Presses the key to insert a character in the place of the cursor and moves the cursor to the right if the editing buffer is not fully occupied.
Backspace	Deletes a character before the cursor and moves the cursor backward.
← or Ctrl+B	Moves the cursor to the left by the space of a character.
→ or Ctrl+F	Moves the cursor to the right by the space of a character.

Key	Function
Tab	<p>Presses Tab after entering an incomplete key word and the system runs the partial help.</p> <ol style="list-style-type: none">1. If only one key word matches the entered one, the system replaces the entered one with the complete key word and displays it in a new line with the cursor a space behind.2. If there are several matches or no match at all, the system displays the prefix first. You can press Tab to switch from one matched key word to another. In this case, the cursor closely follows the end of a word and you can press a spacebar and enter the next word.3. If an incorrect key word is entered, press Tab and it is displayed in a new line being unchanged.

2.5 Changing the Language of Displayed Information

This section describes how to change the language of displayed information.

The prompt and help information in a CLI can be displayed either in Chinese or in English. You can switch between the two languages by using the **language-mode** command.

2.6 Controlling Information Displayed in a CLI

This section describes how to control displayed information.

A CLI can control displayed information in the following methods:

- When information displayed is more than a full screen, the pause function can be applied. You have three options:

Key	Function
"Ctrl+C"	Stops displaying information and running commands.
Spacebar	Continues to display the next screen of information.
Enter	Continues to display the next line of information.

2.7 Using History Commands

This section describes how to use history commands.

The CLI can automatically save used commands. You can invoke and run history commands at any time.

By default, the system saves 10 history commands for each user. Operations of history commands are shown in [Table 2-3](#).

Table 2-3 Using history commands

Action	Command or Key	Result
Display history commands.	display history-command	Commands entered are displayed.
Access the previous history command.	Up cursor key ↑ or Ctrl+P	If there is an earlier history command, the latest history command is retrieved. Otherwise, an alarm is generated.
Access the next history command.	Down cursor key ↓ or Ctrl+N	If there is a later history command, the next history command is retrieved. Otherwise, the command is cleared and an alarm is generated.

 **NOTE**

On the HyperTerminal of Windows 9X, the cursor key ↑ is invalid, because the key is defined differently. In this case, you can use the shortcut keys Ctrl+P instead of the cursor key ↑.

When you use the history command function, note the following:

- The history commands saved on the S-switch are the same as what you have entered. For example, if you enter an incomplete command, the saved command is incomplete.
- If you run a command for several times, the earliest usage of the command is saved. If a command is entered in different forms, all inputs are recorded.

For example, the **display ip routing-table** command is used for several times, only the earliest usage is saved. If **display ip routing** and **display ip routing-table** are used, both of them are saved.

2.8 Shortcut Keys

This section describes the shortcut keys of the S-switch.

As shown in [Table 2-4](#), the CLI provides shortcut keys with specific functions.

 **NOTE**

Different terminal software defines shortcut keys in different ways. Therefore, the shortcut keys on the terminal may differ from that listed in this section.

Table 2-4 Shortcut keys

Key	Function
CTRL_A	Moves the cursor to the beginning of the current line.
CTRL_B	Moves the cursor to the left by the space of a character.
CTRL_C	Terminates the running function.
CTRL_D	Deletes the character where the cursor lies.
CTRL_E	Moves the cursor to the end of the current line.
CTRL_F	Moves the cursor to the right by the space of a character.
CTRL_H	Deletes a character on the left of the cursor.
CTRL_K	Terminates the outbound connection.
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_V	Pastes the contents on the clipboard.
CTRL_W	Deletes a string or a character on the left of the cursor.
CTRL_Y	Deletes all characters on the right of the cursor.
CTRL_Z	Returns to the user view.
CTRL_]	Terminates the inbound connection or redirects the connection.
ESC_B	Moves the cursor to the left by the space of a word.
ESC_D	Deletes a word on the right of the cursor.
ESC_F	Moves the cursor to the right by the space of a word.

3 Common Operations and Configurations

About This Chapter

This section describes common operations and configurations.

[3.1 Introduction](#)

This section describes common operations and configurations.

[3.2 Basic System Configuration](#)

This section describes basic system configuration on the S-switch.

[3.3 Changing Command Levels and User Levels](#)

This section describes how to change command levels and user levels.

[3.4 Common Telnet Operations](#)

This section describes how to initiate and cut off a Telnet connection.

3.1 Introduction

This section describes common operations and configurations.

[3.1.1 Introduction to Common Operations](#)

[3.1.2 Introduction to Common Configurations](#)

[3.1.3 Logical Relationships Between Configuration Tasks](#)

[3.1.4 Common Operations](#)

This section describes common operations on the S-switch.

[3.1.5 Locking a User Interface](#)

[3.1.6 Sending Information Between User Interfaces](#)

[3.1.7 Cutting off the Connection Between User Interfaces](#)

3.1.1 Introduction to Common Operations

This chapter describes common operations on the S-switch, including entering and quitting views, and displaying statistics on the system. None of these operations affects the configuration file of the S-switch.

3.1.2 Introduction to Common Configurations

You need to perform certain common configurations on the S-switch. For example, you need to specify the name of the S-switch, set time, select a language mode, and manage user levels and command levels. All these configurations are recorded in the configuration file.

3.1.3 Logical Relationships Between Configuration Tasks

There is no logical relations between configuration tasks. You can perform any configuration task as required.

3.1.4 Common Operations

This section describes common operations on the S-switch.

Entering the System View

After logging in to the S-switch, you enter the user view. To enter the system view, run the following command.

Action	Command
Enter the system view from the user view.	system-view

Enter the system view.

```
<Quidway> system-view
[Quidway]
```

Quitting the Current View

To quit the current view, run the following commands in any view.

Action	Command
Return to a lower level command view.	quit
Return to the user view from any other view.	return

NOTE

- Using the **quit** command in the user view, you quit the system view.
- Using the **quit** command or the **return** command in the system view, you return to the user view.
- The shortcut keys **Ctrl+Z** function the same as the **return** command.

Displaying the System Status

Using the **display** commands, you can view the system status. The **display** commands include:

- Commands used to display the system configuration
- Commands used to display the system running status

For details on the commands related to different protocols and interfaces, refer to related chapters. This section describes only the **display** commands related to the system status.

Commands Used to Display the System Configuration

To display the system configuration, run the following commands in any view.

Action	Command
Display the system clock.	display clock
Display the current configuration.	display current-configuration
Display the operation configuration of the current view.	display this

Commands Used to Display the System Running Status

To display the system running status, run the following commands in any view.

Action	Command
Display terminal users.	display users [all]
Display the system version.	display version [<i>slot-id</i>]

3.1.5 Locking a User Interface

When you leave the operation terminal temporarily, you can lock the user interface to prevent unauthorized users from logging in to it.

You need to enter a password to lock or unlock the user interface.

Do as follows in the user view.

Action	Command
Lock a user interface.	lock

3.1.6 Sending Information Between User Interfaces

To send information between user interfaces, run the following command in the user view.

Action	Command
Send information between user interfaces.	send { all <i>ui-type ui-number</i> <i>number</i> }

3.1.7 Cutting off the Connection Between User Interfaces

To cut off the connection between user interfaces, run the following command in the user view.

Action	Command
Cut off the connection between user interfaces.	free user-interface { <i>ui-type ui-number</i> <i>number</i> }

3.2 Basic System Configuration

This section describes basic system configuration on the S-switch.

[3.2.1 Setting the Name of the S-switch](#)

[3.2.2 Setting the System ClockS-switch](#)

3.2.3 Switching a Language Mode

3.2.1 Setting the Name of the S-switch

Context

Do as follows on the S-switch whose name needs to be set.

Procedure

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

Step 2 Run the **sysname** *host-name* command to set the name of the S-switch.

The default name of the S-switch is **Quidway**.

----End

3.2.2 Setting the System ClockS-switch

Do as follows in the user view on the S-switch.

Action	Command
Set the Universal Time Coordinated (UTC).	clock datetime time
Set the daylight time.	clock daylight-saving-time <i>time-zone-name</i> one-year <i>start-time start-date end-time end-date offset</i>
Set the time zone.	clock timezone <i>time-zone-name</i> { add minus } <i>offset</i>

To ensure that the S-switch works with other devices smoothly, you must set the system time properly. You can set a time zone and daylight time on the S-switch.

3.2.3 Switching a Language Mode

Do as follows in the user view on the S-switch.

Action	Command
Switch to the Chinese mode.	language-mode chinese
Switch to the English mode.	language-mode english

S-switchHelp information on the S-switch can be displayed either in English or in Chinese. By default, help information is displayed in English.

3.3 Changing Command Levels and User Levels

This section describes how to change command levels and user levels.

3.3.1 Changing User Levels

3.3.2 Extending Command Levels

3.3.3 Extending User Levels

3.3.1 Changing User Levels

Action	Command
Change the user level.	super [<i>level</i>]

To switch to a higher user level, you must enter a correct password.

NOTE

When you switch to a higher user level by using the **super** command, the system automatically generates a trap and records the change in the log. A change to a lower user level is only recorded in the log.

3.3.2 Extending Command Levels

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **command-privilege level rearrange** command to extend command levels in batches.
- Step 3** Run the **command-privilege level level view view-name command-key** command to set the level of a command.

Using the **command-privilege** command, you can set the levels of multiple commands and specify their command views.

NOTE

Each command has its view and priority. Usually, you need not set the view and priority of a command.

If you set no password for switching to 15 user levels before running the **command-privilege level rearrange** command, the system prompts you to set a super password. The system also prompts you to continue command level extension. You must select **N** and set the password. If you select **Y** first, command levels are extended in batches. In this case, only the console interface user can extend its levels.

----End

3.3.3 Extending User Levels

Context

If the command levels are extended to 0 - 15, the user levels must also be extended from 0 - 3 to 0 - 15.

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** [*ui-type*] *first-ui-number* [*last-ui-number*] command to enter the user interface view.
- Step 3** Run the **user privilege level** *level* command to extend user levels.
- End

3.4 Common Telnet Operations

This section describes how to initiate and cut off a Telnet connection.

3.4.1 Initiating a Telnet Connection

3.4.2 Cutting off a Telnet Connection

3.4.1 Initiating a Telnet Connection

Action	Command
Initiate a Telnet connection.	telnet { <i>host-ip-address</i> <i>host-name</i> } [<i>port-number</i>]

This function applies to users of all levels. To initiate a Telnet connection to a device with a specified address or name, you can use the **telnet** command in the user view.

For example,

```
<S-switch-A> telnet 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+T to abort
Connected to 10.1.1.1 ...
*****
*           All rights reserved (2007-2008)           *
*           Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
* Notice:                                           *
*           This is a private communication system.   *
*           Unauthorized access or use may lead to prosecution. *
*****

Login authentication

Password:
Note: The max number of VTY users is 15, and the current number
      of VTY users on line is 8.
```

```
<S-switch-B>
```

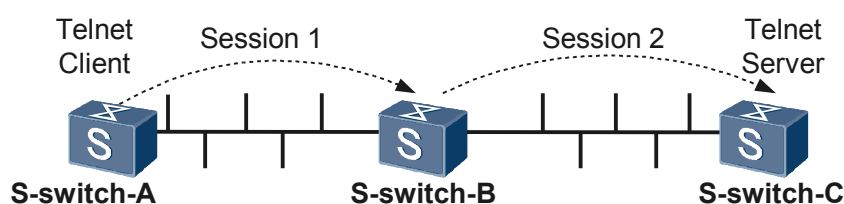
After the correct password is entered, the system prompts that you have logged in to S-switch-B.

3.4.2 Cutting off a Telnet Connection

You can use the **quit** command or shortcut keys to cut off a Telnet connection.

For example, a user logs in to S-switch-A from a PC through Telnet, and then uses the **telnet** command on S-switch-A to log in to S-switch-B. After that, the user uses the **telnet** command on S-switch-B to log in to S-switch-C. The three S-switches form a cascade.

Figure 3-1 Cutting off a cascading Telnet connection



- Run the **quit** command in the user view on S-switch-C whose IP address is 20.1.1.1 to return to S-switch-B. The following information is displayed:

```
<S-switch-C> quit
Note: The max number of VTY users is 5, and the current number
      of VTY users on line is 0.
The connection was closed by the remote host!
<S-switch-B>
```

Run the **quit** command in the user view on S-switch-B whose IP address is 10.1.1.1 to return to S-switch-A. The following information is displayed:

```
<S-switch-B> quit
Note: The max number of VTY users is 5, and the current number
      of VTY users on line is 0.
The connection was closed by the remote host!
<S-switch-A>
```

NOTE

If the network is interrupted when you are pressing the shortcut keys, the instruction fails to reach the Telnet server.

- Use the shortcut keys **Ctrl+]**, whose function is the same as that of the **quit** command. Press **Ctrl+]** in any view on S-switch-C to return to S-switch-B. The following information is displayed:

```
<S-switch-C> (press <CTRL+>])
Note: The max number of VTY users is 5, and the current number
      of VTY users on line is 0.
The connection was closed by the remote host!
<S-switch-B>
```

- Use the shortcut keys **Ctrl+K**.

If the server fails and the client cannot detect the failure, the server cannot respond to any instruction from the client. In this case, you can press **Ctrl+K** on the client. The client then disconnects the Telnet connection and quits the connection process. Press **Ctrl+K** in any view on S-switch-C to disconnect the Telnet connection and quit the connection process. The following information is displayed:

<S-switch-C> (press <Ctrl_K>)
<S-switch-A>

4 Managing Login Users

About This Chapter

This chapter describes how to manage the user interface, configure the Telnet terminal service, configure the SSH terminal service and maintain the terminal service, and remotely log in to the S-switch from the AUX interface. This chapter also provides examples of terminal services.

[4.1 Introduction](#)

This section describes the login modes and concepts.

[4.2 Configuring the Console Interface as the User Interface](#)

This section describes how to log in to the S-switch to configure the S-switch.

[4.3 Configuring Telnet Users](#)

This section describes how to remotely log in to the S-switch through Telnet to configure the S-switch.

[4.4 Configuring SSH Login Users](#)

When higher security is required, you can log in to the S-switch through SSH to configure the S-switch.

[4.5 Maintaining User Interfaces and Terminal Services](#)

This section describes how to maintain user interfaces and terminal services.

[4.6 Configuration Examples](#)

This section provides examples for user login.

4.1 Introduction

This section describes the login modes and concepts.

[4.1.1 User Login Modes](#)

[4.1.2 User Interface](#)

[4.1.3 User Authentication](#)

[4.1.4 Telnet Terminal Services](#)

[4.1.5 SSH Terminal Services](#)

[4.1.6 References](#)

[4.1.7 Logical Relationships Between Configuration Tasks](#)

4.1.1 User Login Modes

To configure, monitor, and maintain the local or remote S-switch, you need log in to the S-switch to configure:

- User interface where users can control the S-switch
- Authentication mode that ensures the secure login
- Terminal services that provide various protocols

Table 4-1 shows the login modes supported by the S-switch.

Table 4-1 User login modes

Login Mode	Application	Description
Console interface	Local maintenance	See this chapter.
AUX interface	Remote maintenance	See this chapter.
Telnet	Local and remote maintenance	See this chapter.
SSH	Local and remote maintenance	See this chapter.
FTP	Local and remote maintenance	Refer to the chapter "File Management."

You need to manage users and control user rights in a reasonable way and ensure the security for the information transmitted.

4.1.2 User Interface

A user interface (UI) enables users to log in to the S-switch. Through a user interface, you can configure the parameters on all physical and logical interfaces that work in asynchronous and interactive modes. In this manner, you can manage, authenticate, and authorize the login users.

Types of User Interfaces

Table 4-2 shows the types of user interfaces supported by the S-switch.

Table 4-2 Types of user interfaces

Type	Application	Description
CON	Local login through the console interface	It is a linear interface conforming to the EIA/TIA-232 standard. The type of the interface is DCE. Each Switch Control Unit (SCU) provides a console interface.
VTY	Local or remote login through Telnet or Secure Shell (SSH)	VTY is a kind of virtual interface indicating a logical terminal line. When users log in to S-switch by the mode of Telnet, FTP or SSH, a VTY connection is created.

User Interface Numbering

You can number a user interface in the following ways:

- **Relative numbering**
Relative numbering indicates that the interfaces of the same type are numbered. The relative numbering uniquely specifies a user interface of the same type.
The format of the relative numbering is: user interface type + number. It must comply with the following rules:
 - Number of the CON interface: console0
 - Default number of the VTY: vty0, vty1, vty2, vty3, and vty4
- **Absolute numbering**
Default numbers of 0, 33, 34...38 are uniquely and respectively specified for the user interfaces of CON and VTY. You can enter a specific user interface view by entering any of these numbers.

4.1.3 User Authentication

When the S-switch is powered on for the first time, no authentication information for login is available in the system. In this case, you can log in to the S-switch through the console interface without being authenticated.

If a user logs in to the S-switch through Telnet from an Ethernet interface, the login user must be authenticated for the sake of security. If the authentication succeeds, the user can log in to the S-switch to configure and maintain the S-switch.

To manage users that try to log in to the S-switch, these users are assigned passwords and classified into different levels.

Classifying Users

According to the service types and rights assigned to the login users, the users are classified, as shown in [Table 4-3](#).

Table 4-3 Classifying users

User Type	Description	Authentication
Super users	Log in to the S-switch through the console interface and have all rights.	Not authenticated for the first login but recommended later on
Telnet users	Log in to the S-switch through Telnet on the Ethernet interface and have limited rights. A Telnet connection is set up between the user terminal and the S-switch.	Recommended
SSH users	Log in to the S-switch through SSH on the Ethernet interface and have limited rights. An SSH connection is set up between the user terminal and the S-switch.	Recommended
FTP users	Log in to the S-switch through FTP on the Ethernet interface and have limited rights. An FTP connection is set up between the user terminal and the S-switch.	Recommended

The rights that can be obtained by users logging in to the S-switch through Telnet, SSH, and FTP depends on the priority of the user interface through which they log in. The S-switch provides multiple services for a user. To ensure both login convenience and security, login users must be classified, and then assigned levels.

For details on configuring FTP users, refer to the chapter "File Management".

Authenticating Login Users

After users are configured on the S-switch, the system authenticates the users when they log in to the S-switch. The S-switch provides three authentication modes, as shown in [Table 4-4](#).

Table 4-4 Authentication modes for login users

Authentication Mode	Description
Non-authentication	Users can log in to the S-switch without entering the username and password. There is a great security risk.
Password authentication	Users can log in to the S-switch by entering the password rather than the username. The security is ensured to a certain extent.

Authentication Mode	Description
AAA local authentication	Users need to enter both the username and password to log in to the S-switch. The S-switch then authenticates the users according to the locally configured user information. This further improves the security. It applies to the users logging in to the S-switch through the console interface and Telnet.

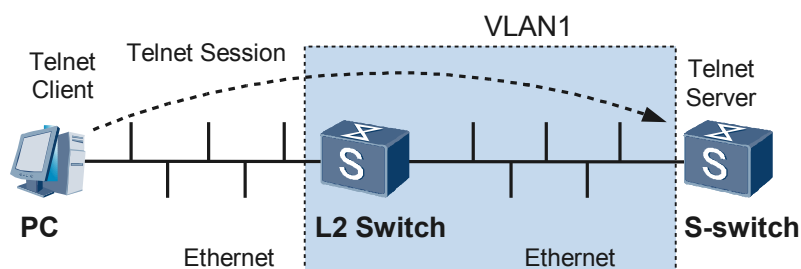
4.1.4 Telnet Terminal Services

The Telnet protocol is an application layer protocol in the TCP/IP protocol suite. It supports remote login and virtual terminal services through the TCP connections. The S-switch provides the following Telnet services.

Telnet Server

By default, the S-switch functions as the Telnet server. The Telnet client program can be run on the user terminal, as shown in [Figure 4-1](#).

Figure 4-1 S-switch providing the Telnet server service



Users can log in to the S-switch through Telnet to configure and manage the S-switch. If the user logs in to the S-switch through the Layer 2 switch, the IP addresses of the PC and the S-switch must be in the same network segment. In addition, the Layer 2 switch and the S-switch must belong to the same Virtual Local Area Network (VLAN).

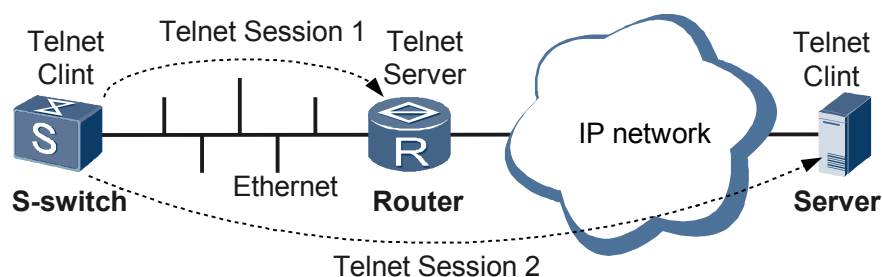
NOTE

To configure the remote S-switch, you must set the attributes of the Telnet terminal service, including: (Item List) Character entry mode No echo at the local end Terminal type of VT100 Telnet works normally only when the attributes of the client and server are the same.

For details on configuring VLANs, refer to the chapter "VLAN Configuration" in the *Quidway S5300 Series Ethernet Switches Configuration Guide – Ethernet*.

Telnet Client

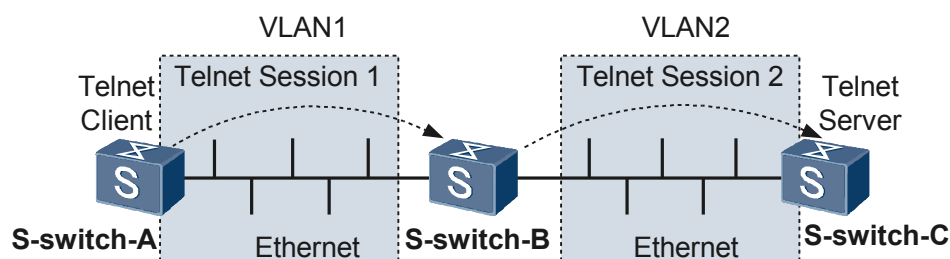
An S-switch functions as the Telnet client to initiate a connection and a router or an application server functions as the Telnet server, as shown in [Figure 4-2](#).

Figure 4-2 S-switch providing the Telnet client service

If the S-switch logs in to the router through Telnet to configure and manage the router, the IP addresses of the S-switch and the router must be in the same network segment. If the S-switch logs in to the application server through Telnet to configure and manage the server, the IP addresses of the S-switch and the router must be in the same network segment and can interconnect at the network layer.

Cascading Telnet Server

As shown in [Figure 4-3](#), the S-switch can function as either the client or the server.

Figure 4-3 S-switch providing cascading Telnet service

S-switch-A logs in to S-switch-B through Telnet. Then, S-switch-B logs in to S-switch-C through Telnet. In this manner, the three S-switches form a cascading login structure. Here, S-switch-A is the client of S-switch-B, and S-switch-B is the client of S-switch-C.

S-switch-A and S-switch-B are required to belong to the same VLAN, and their IP addresses should be in the same network segment. This is the same with S-switch-B and S-switch-C.

NOTE

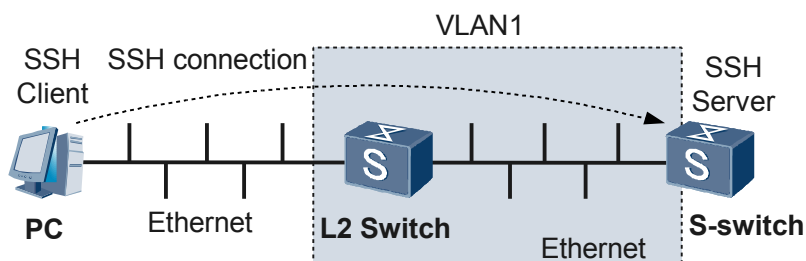
If S-switch-A logs in to S-switch-C directly through Telnet, the three S-switchs must be in the same VLAN and their IP addresses must be in the same network segment.

4.1.5 SSH Terminal Services

Introduction to SSH

As shown in [Figure 4-4](#), SSH is an application layer protocol in the TCP/IP protocol suite. It is used for remote login and virtual terminal on the network of which the security is not guaranteed. Based on TCP connections, SSH guarantees security and provides authentication for transmitted information, preventing the following attacks: (Item List) IP address spoofing Interception of the plain text password Denial of Service (DoS)

Figure 4-4 Local SSH connection between the PC and the S-switch



SSH adopts the client/server model and sets up multiple secure transmission channels. The S-switch, as the SSH server, can be connected to multiple PCs that function as SSH clients. A Layer 2 switch may exist between the PC and the SSH server.

In actual networking, the IP addresses of the PC and the S-switch must be in the same network segment, and the Layer 2 switch and the S-switch must be in the same VLAN.

Currently, there are three SSH versions including v1.0, v1.5, and v2.0. The v2.0 and v1.0 are compatible but the v2.0 and v1.5 are incompatible.

Advantages of SSH

Different from Telnet terminal services, SSH provides secure remote access on the network without guaranteed security. The advantages are as follows:

- Supporting Revest-Shamir-Adleman Algorithm (RSA) authentication
- Supporting Data Encryption Standard (DES) and 3DES
- Supporting the encrypted transfer of the username or password
- Supporting the encrypted transfer of interactive data

SSH adopts RSA. After the public key and the private key are generated according to the encryption principle of the asymmetric encryption system, the following information is transmitted with security between the SSH client and the SSH server: (Item List) Key Username Password Interactive data

Setting Up an SSH Connection

The procedure for setting up an SSH connection is as follows:

1. Negotiating the SSH version

The SSH client initiates a TCP connection by sending a request to the SSH server. After the TCP connection is set up, the SSH server and the SSH client negotiate the SSH version. If the version of the client matches that of the server, the negotiation of the key starts; otherwise, the SSH server cuts off the TCP connection.

2. Negotiating the key

In this step, the key algorithm is negotiated and the session key is computed.

The SSH server generates the RSA key randomly and sends the public key to the SSH client.

The SSH client computes the session key according to the RSA public key received and the random number generated locally. Then, the SSH client encrypts the random number

by using the public key at the SSH server, and sends the encrypted random number to the SSH server.

The SSH server decrypts the data received from the SSH client by using the private key, and obtains the random number at the SSH client. Then, the SSH server compares the random number and its own public key. After that, the session key is computed.

 **NOTE**

After calculation, the SSH server and client obtain the same session key that is used to avoid the insecurity.

3. Authenticating the user identity

After computing the session key, the SSH server authenticates the SSH client.

The SSH client sends information about the identity to the SSH server. If the server is configured not to authenticate a user, the request for session starts. Otherwise, the server authenticates a user.

The SSH server authenticates a user in one of the following ways:

- Password authentication: The SSH server compares the username and password of an SSH client with those pre-configured in the system. If they are matched, the authentication succeeds.
- RSA authentication
 - The RSA public key of the SSH client is pre-configured on the SSH server.
 - The SSH client, as one RSA public key member, sends modulo to the SSH server.
 - The SSH server checks the validity of the public key members and generates a random number. Then, the SSH server encrypts the random number using the RSA public key of the client and sends it to the SSH client.
 - Both the server and the client compute the data used for authentication according to the random number.
 - After computation, the SSH client sends the data back to the server.
 - The SSH server then compares the data with that obtained through local computation. If the two are the same, the authentication succeeds. Otherwise, the authentication fails.

After a certain authentication mode is configured on the SSH server, the client sends an authentication request to the server. If the authentication succeeds or the connection with the server expires, the client is cut off from the server.

4. Initiating a session request

After being authenticated, the SSH client sends a request for a session to the server. The server receives and processes the request, and the session starts.

5. Performing an interactive session

Both the SSH client and server use the session key to encrypt and decrypt the interactive data. They communicate with each other with high security until the session is over.

4.1.6 References

For details about terminal services, refer to:

- RFC 854: Telnet Protocol Specification
- RFC 857: Telnet Echo Option
- RFC 858: Telnet Suppress Go Ahead Option

- RFC 1091: Telnet Terminal-Type Option
- Draft-Ylonen-SSH-Protocol-00

4.1.7 Logical Relationships Between Configuration Tasks

To log in to the S-switch safely and successfully, you should:

- Determine the type of the user interface and configure its parameters.
- Classify user levels and configure authentication information of login users.
- Configure various types of terminal services.

4.2 Configuring the Console Interface as the User Interface

This section describes how to log in to the S-switch to configure the S-switch.

[4.2.2 \(Optional\) Configuring the Attributes of the User Interface](#), [4.2.3 \(Optional\) Configuring User Authentication](#), and [4.2.4 \(Optional\) Setting User Levels](#) are not listed in sequence and can be configured as required.

[4.2.1 Establishing the Configuration Task](#)

[4.2.2 \(Optional\) Configuring the Attributes of the User Interface](#)

[4.2.3 \(Optional\) Configuring User Authentication](#)

[4.2.4 \(Optional\) Setting User Levels](#)

[4.2.5 Checking the Configuration](#)

4.2.1 Establishing the Configuration Task

Applicable Environment

You need to log in to a local S-switch through the console interface to configure and manage the S-switch.

Pre-configuration Tasks

Before configuring the console interface as the user interface, complete the following tasks:

- Powering the S-switch on normally
- Setting the HyperTerminal on the PC correctly

Data Preparation

To configure the console interface as the user interface, you need the following data.

No.	Data
1	(Optional) Auto-run commands
2	(Optional) Number of rows on a screen of the terminal display

No.	Data
3	(Optional) Size of the history command buffer
4	(Optional) Timeout period for login users
5	Type and number of a user interface
6	(Optional) Authentication mode, authentication password, service type, and user level
7	Default level of a user interface
8	(Optional) Password for switching user levels

4.2.2 (Optional) Configuring the Attributes of the User Interface

Configuring the Attributes of the User Interface

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface { 0 | console 0 }** command to enter the user interface view.
- Step 3** Run the **screen-length screen-length** command to set the number of rows on a screen of the terminal display.
- Step 4** Run the **history-command max-size size** command to set the size of the history command buffer.

By default, terminal services are enabled on all user interfaces. The maximum length of a screen on the terminal display defaults to 24 rows, and the history command buffer can store up to 10 commands.

Step 3 and **Step 4** are not listed in sequence.

----End

Configuring the Parameters of the User Interface

Context

Do as follows on the S-switch.

Procedure

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

Step 2 Run the **user-interface { 0 | console 0 }** command to enter the user interface view.

Step 3 Run the **idle-timeout minutes [seconds]** command to set the timeout period of login users.

By default, the timeout period for login users is 10 minutes. That is, if users perform no operation on the S-switch within 10 minutes after login, the terminal connection is cut off. If you run the **idle-timeout 0 0** command, no timeout period is set to cut off the connection.

----End

Configuring Asynchronous Communications Parameters of the User Interface

Context

Do as follows on the S-switch.

Procedure

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

Step 2 Run the **user-interface { 0 | console 0 }** command to enter the user interface view.

Step 3 Run the **speed speed-value** command to set the transmission rate.

Step 4 Run the **parity { none | even | odd | mark | space }** command to set the parity bit.

[Step 3](#) and [Step 4](#) are not listed in sequence.

----End

4.2.3 (Optional) Configuring User Authentication

Configuring the Non-Authentication Mode for Login Users

Context

Do as follows on the S-switch.

Procedure

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

Step 2 Run the **user-interface { 0 | console 0 }** command to enter the user interface view.

Step 3 Run the **authentication-mode none** command to configure the non-authentication mode.

After this configuration is performed, you can log in to the S-switch without being authenticated. This lowers the security of the system. Thus, this mode is not recommended.

----End

Configuring the Password Authentication Mode for Login Users

Context



NOTE

In the case of the password authentication mode, you must set a password to log in to the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface { 0 | console 0 }** command to enter the user interface view.
- Step 3** Run the **authentication-mode password** command to configure the password authentication mode.
- Step 4** Run the **set authentication password { cipher | simple } password** command to set the password for user authentication.

----End

Configuring the AAA Local Authentication Mode for Login Users

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface { 0 | console 0 }** command to enter the user interface view.
- Step 3** Run the **authentication-mode aaa** command to configure the Authentication, Authorization, and Accounting (AAA) authentication mode.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **aaa** command to enter the AAA view.
- Step 6** Run the **local-user user-name password { simple | cipher } password** command to create the local username and password.
- Step 7** (Optional) Run the **local-user user-name service-type { ftp | ppp | ssh | telnet | terminal } *** command to set the service type for local users.
- Step 8** Run the **local-user user-name level level** command to set the user level.
- Step 9** Run the **authentication-scheme authentication-scheme-name** command to create an authentication scheme and enter the authentication scheme view.
- Step 10** Run the **authentication-mode local** command to set the AAA local authentication mode.

After setting the username or password, service type, and login level, you can perform [Step 9](#) and [Step 10](#) to configure the local authentication.

When a user logs in to the S-switch, the commands that the user can run depend on the user level and the user interface level. If both of the two levels need to be configured, you can access the

system according to the user level. For example, if Tom's user level is 3, but the default level of VTY0 interface is 1, Tom can use the commands at or below level 3. If no user level is set for Tom, he can only use the commands at or below level 1.

----End

4.2.4 (Optional) Setting User Levels

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface { 0 | console 0 }** command to enter the user interface view.
- Step 3** Run the **user privilege level *level*** command to set the default level of the user interface.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **super password [level *user-level*] { simple | cipher } *password*** command to set the password for switching the user level.

In the case of the non-authentication or password authentication mode, the commands that a login user can run are determined by the user interface level. By default, the CON user interface is at level 3. That is, the users that log in to the S-switch through the console interface are at level 3, and the users that log in to the S-switch through other interfaces are at level 0.

If users that log in to the S-switch are at a lower level, they can use the password set in Step 5 to switch to a higher level.

----End

4.2.5 Checking the Configuration

Action	Command
Check information about the user interface.	display users [all]
Check physical attributes and certain configurations of the user interface.	display user-interface [<i>ui-type ui-number</i> <i>number</i>] [summary]

4.3 Configuring Telnet Users

This section describes how to remotely log in to the S-switch through Telnet to configure the S-switch.

[4.3.2 \(Optional\) Configuring the Attributes of the VTY User Interface](#), [4.3.3 Configuring the VTY User Interface to Support the Telnet Service](#), [4.3.4 Assigning an IP Address to the Telnet Server](#), [4.3.5 Configuring User Authentication](#), and [4.3.6 Setting User Levels](#) are not listed in sequence and can be configured as required.

[4.3.1 Establishing the Configuration Task](#)

[4.3.2 \(Optional\) Configuring the Attributes of the VTY User Interface](#)[4.3.3 Configuring the VTY User Interface to Support the Telnet Service](#)[4.3.4 Assigning an IP Address to the Telnet Server](#)[4.3.5 Configuring User Authentication](#)[4.3.6 Setting User Levels](#)[4.3.7 Checking the Configuration](#)

4.3.1 Establishing the Configuration Task

Applicable Environment

To configure and manage the S-switch through an Ethernet interface, you can log in to the S-switch through Telnet. In this case, the S-switch must provide the Telnet terminal service.

You can log in to the S-switch through Telnet from other devices or log in to other devices from the S-switch. All the configurations are performed according to the role that the S-switch plays in the Telnet terminal service.

Pre-configuration Tasks

Before configuring the Telnet terminal service, complete the following tasks:

- Powering the S-switch on normally
- Setting the HyperTerminal on the PC correctly

Data Preparation

To configure the Telnet terminal service, you need the following data.

No.	Data
1	(Optional) Auto-run commands
2	(Optional) Number of rows on a screen of the terminal display
3	(Optional) Size of the history command buffer
4	(Optional) Timeout period for login users
5	(Optional) Prompt message of login authentication and configuration
6	(Optional) Maximum number of VTY user interfaces and limit of calling in and calling out
7	ID of the VLAN and VLANIF interfaces at the server side
8	IP address and mask of the server
9	(Optional) Authentication information about the login user on the server
10	IP address and host name of the Telnet connection at the client side

No.	Data
11	(Optional) TCP port number of the Telnet connection at the client side

4.3.2 (Optional) Configuring the Attributes of the VTY User Interface

Configuring the Attributes of the VTY User Interface

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- You can configure either a single VTY user interface or multiple VTY user interfaces.
- Step 3** Run the **screen-length** *screen-length* command to set the number of rows on a screen of the terminal display.
- Step 4** Run the **history-command max-size** *size* command to set the size of the history command buffer.

By default, terminal services are enabled on all user interfaces. The maximum length of a screen on the terminal display defaults to 24 rows, and the history command buffer can store up to 10 commands.

Step 3 and **Step 4** are not listed in sequence.

----End

Configuring the Parameters of the VTY User Interface

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **auto-execute command** *command* command to configure the auto-run commands.

When a user logs in to the S-switch, the system automatically run the command specified by *command* in the **auto-execute command** command. After the command is run, the connection

with the user is cut off. Usually, the **Telnet** command is set to run automatically when a user logs in to the S-switch. The user thus can log in to the specified host.

Step 4 Run the **idle-timeout** *minutes* [*seconds*] command to set the timeout period of login users.

By default, the timeout period for login users is 10 minutes. That is, if users perform no operation on the S-switch within 10 minutes after login, the terminal connection is cut off. If you run the **idle-timeout 0 0** command, no timeout period is set to cut off the connection.

----End

Configuring Prompt Interfaces for Login Users

Context

Do as follows on the S-switch.

Procedure

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

Step 2 Run the **header login** { **file** *file-name* | **information** *text* } command to set the prompt information for login authentication.

Step 3 Run the **header shell** { **file** *file-name* | **information** *text* } command to set the prompt information for the configuration.

The prompt information is a passage of text messages displayed on the system after the authentication succeeds.

----End

Setting the Number of VTY User Interfaces

Context

Do as follows on the S-switch.

Procedure

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

Step 2 Run the **user-interface maximum-vty** *type-number* command to set the maximum number of VTY connections.

Step 3 Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.

Step 4 Run the **acl** *acl-number* { **inbound** | **outbound** } command to configure the calling in and calling out capabilities of a VTY connection.

----End

4.3.3 Configuring the VTY User Interface to Support the Telnet Service

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **shell** command to enable the Terminal service.
- Step 4** Run the **protocol inbound telnet** command to configure the user interface to support the Telnet service.

By default, the VTY user interface supports the Telnet service.

----End

4.3.4 Assigning an IP Address to the Telnet Server

Context



NOTE

IP addresses of the Telnet client and Telnet server must belong to the same network segment.

Assigning an IP Address to the Ethernet Interface on the Telnet Server

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan** *vlan-id* command to create a VLAN and enter the VLAN view.
- Step 3** Run the **port interface-type** { *interface-number* [**to** *interface-number*] } &<1-10> command to configure VLANIF interfaces.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **interface** **vlanif** *vlan-id* command to enter the VLANIF interface view.
- Step 6** Run the **ip address** *ip-address* { *mask* | *mask-length* } command to assign an IP address to the VLANIF interface.

The S-switch only transmits services at Layer 2; therefore, to process Telnet terminal services, a VLANIF interface must be created and assigned an IP address.

You should first create a VLAN and specify the range of VLANIF interfaces. Then, you can enter the specified VLAN interface view to assign the IP address for a Telnet connection. Regardless of whether the S-switch functions as the server or client, the S-switch must be assigned an IP address and connected to other devices through VLANIF interfaces.

----End

4.3.5 Configuring User Authentication

Configuring the Non-Authentication Mode for Login Users

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **authentication-mode none** command to configure the non-authentication mode.

After this configuration is performed, you can log in to the S-switch without being authenticated. This lowers the security of the system. Thus, this mode is not recommended.

----End

Configuring the Password Authentication Mode for Login Users

Context



NOTE

In the case of the password authentication mode, you must set a password to log in to the S-switch.

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **authentication-mode password** command to configure the password authentication mode.
- Step 4** Run the **set authentication password** { **cipher** | **simple** } *password* to set the password for user authentication.

----End

Configuring the AAA Local Authentication Mode for Login Users

Context

Do as follows on the S-switch.

Procedure

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

- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **authentication-mode aaa** command to configure the AAA authentication mode.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **aaa** command to enter the AAA view.
- Step 6** Run the **local-user** *user-name* **password** { **simple** | **cipher** } *password* command to create the local username and password.
- Step 7** (Optional) Run the **local-user** *user-name* **service-type** { **ftp** | **ppp** | **ssh** | **telnet** | **terminal** } * command to set the service type for local users.
- Step 8** Run the **local-user** *user-name* **level** *level* command to set the user level.
- Step 9** Run the **authentication-scheme** *authentication-scheme-name* command to create an authentication scheme and enter the authentication scheme view.
- Step 10** Run the **authentication-mode local** command to set the AAA local authentication mode.

After setting the username or password, service type, and login level, you can take Step 9 and Step 10 to configure the local authentication.

When you log in to the S-switch, you can use the commands of which the levels are determined by the user level and the user interface level. If both levels need to be configured, you can access the system according to the user level. For example, if Tom's user level is 3, but the default level of VTY0 interface is 1, Tom can use the commands at or below level 3. If no user level is set for Tom, he can only use the commands at or below level 1.

----End

Configuring the AAA Server for Authenticating Login Users

Context

For details on using the AAA server to authenticate login users, refer to the chapter "AAA Configuration" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*.

4.3.6 Setting User Levels

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **user privilege level** *level* command to set the level of the commands that users logging in through the current user interface can use.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **super password** [*level* *user-level*] { **simple** | **cipher** } *password* command to set the password for switching the user level.

In the case of non-authentication or password authentication mode, the user logging in to the S-switch can use the commands of which the levels are determined by the user interface level. By default, the CON user interface is at level 3. That is, the users that log in to the S-switch through the console interface are at level 3, and the users that log in to the S-switch through other interfaces are at level 0.

If users that log in to the S-switch are at a lower level, they can use the password set in Step 5 to switch to a higher level.

----End

4.3.7 Checking the Configuration

Action	Command
Check information about the user interface.	display users [all]
Check the maximum number of VTY user interfaces.	display user-interface maximum-vty
Check physical attributes and certain configurations of the user interface.	display user-interface [<i>ui-type ui-number</i> <i>number</i>] [summary]
Check the status of all the established TCP connections.	display tcp status

4.4 Configuring SSH Login Users

When higher security is required, you can log in to the S-switch through SSH to configure the S-switch.

[4.4.2 \(Optional\) Configuring the Attributes of the VTY Interface](#), [4.4.3 Configuring the VTY User Interface to Support the SSH Service](#), [4.4.4 Assigning an IP Address to the SSH Server](#), [4.4.5 Configuring the Password Authentication Mode for SSH Login Users](#), and [4.4.6 Configuring the RSA Authentication Mode for SSH Login Users](#) are configured on the SSH server. [4.4.3 Configuring the VTY User Interface to Support the SSH Service](#) and [4.4.4 Assigning an IP Address to the SSH Server](#) are not listed in sequence. You can choose an authentication mode from [4.4.5 Configuring the Password Authentication Mode for SSH Login Users](#).

[4.4.1 Establishing the Configuration Task](#)

[4.4.2 \(Optional\) Configuring the Attributes of the VTY Interface](#)

[4.4.3 Configuring the VTY User Interface to Support the SSH Service](#)

[4.4.4 Assigning an IP Address to the SSH Server](#)

[4.4.5 Configuring the Password Authentication Mode for SSH Login Users](#)

[4.4.6 Configuring the RSA Authentication Mode for SSH Login Users](#)

[4.4.7 \(Optional\) Setting the SSH Timer and Authentication Times](#)

[4.4.8 Checking the Configuration](#)

4.4.1 Establishing the Configuration Task

Applicable Environment

When higher security is required, you can use SSH terminal services to configure and manage the S-switch through the Ethernet interface.

Pre-configuration Tasks

Before configuring the SSH terminal service, complete the following tasks:

- Powering the S-switch on normally
- Setting the HyperTerminal on the PC correctly
- Generating RSA public key by using the client software that supports SSH1.5

Data Preparation

To configure the SSH terminal service, you need the following data.

No.	Data
1	(Optional) Auto-run commands
2	(Optional) Number of rows on a screen of the terminal display
3	(Optional) Size of the history command buffer
4	(Optional) Timeout period for login users
5	(Optional) Prompt message of login authentication and configuration
6	(Optional) Maximum number of VTY user interfaces and limit of calling in and calling out
7	ID of the VLAN and VLANIF interfaces
8	IP address and mask at the server side
9	(Optional) Authentication information about the login user at the server side
10	RSA public key
11	(Optional) Update interval, timeout period, and retry times for the SSH key

4.4.2 (Optional) Configuring the Attributes of the VTY Interface

Configuring the Attributes of the User Interface

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- You can configure either a single VTY user interface or multiple VTY user interfaces.
- Step 3** Run the **screen-length** *screen-length* command to set the number of rows on a screen of the terminal display.
- Step 4** Run the **history-command max-size** *size* command to set the size of the history command buffer.
- By default, terminal services are enabled on all user interfaces. The maximum length of a screen on the terminal display defaults to 24 rows, and the history command buffer can store up to 10 commands.
- Step 3 and Step 4 are not listed in sequence.
- End

(Optional) Configuring the Parameters of the User Interface

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **auto-execute command** *command* command to configure the auto-run commands.
- When a user logs in to the S-switch, the system automatically run the command specified by *command* in the **auto-execute command** command. After the command is run, the connection with the user is cut off. Usually, the **Telnet** command is set to run automatically when a user logs in to the S-switch. The user thus can log in to the specified host.
- Step 4** Run the **idle-timeout** *minutes* [*seconds*] command to set the timeout period for login users.
- By default, the timeout period for login users is 10 minutes. That is, if users perform no operation on the S-switch within 10 minutes after login, the terminal connection is cut off. If you run the **idle-timeout 0 0** command, no timeout period is set to cut off the connection.
- End

Configuring a Prompt Interface for Login Users

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **header login** { **file** *file-name* | **information** *text* } command to set the prompt for login authentication.
- Step 3** Run the **header shell** { **file** *file-name* | **information** *text* } command to set the prompt information for the configuration.

The prompt information is a passage of text messages displayed on the system after the authentication succeeds.

----End

Configuring a VTY User Interface

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface maximum-vty** *type-number* command to set the maximum number of VTY connections.
- Step 3** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 4** Run the **acl** *acl-number* { **inbound** | **outbound** } command to configure the calling in and calling out capabilities of a VTY connection.

----End

4.4.3 Configuring the VTY User Interface to Support the SSH Service

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **user-interface** { *ui-number* | **vty** *first-number* [*last-number*] } command to enter the VTY user interface view.
- Step 3** Run the **authentication-mode aaa** command to configure the AAA authentication mode.
- Step 4** Run the **shell** command to enable the terminal service.
- Step 5** Run the **protocol inbound ssh** command to configure the VTY user interface to support the SSH service.

----End

4.4.4 Assigning an IP Address to the SSH Server

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan** *vlan-id* command to create a VLAN and enter the VLAN view.
- Step 3** Run the **port interface-type** { *interface-number* [**to** *interface-number*] } &<1-10> command to configure VLANIF interfaces.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **interface** **vlanif** *vlan-number* command to enter the VLANIF interface view.
- Step 6** Run the **ip address** *ip-address* { *mask* | *mask-length* } command to assign an IP address to the VLANIF interface.

The S-switch only transmits services at Layer 2; therefore, to process SSH terminal services, a VLANIF interface must be created and assigned an IP address.

You should first create a VLAN and specify the range of VLANIF interfaces. Then, you can enter the specified VLAN interface view to assign the IP address for an SSH connection. Regardless of whether the S-switch functions as the server or client, the S-switch needs to be assigned an IP address.

For details on configuring VLANs, refer to the chapter "VLAN Configuration" in the *Quidway S5300 Series Ethernet Switches Configuration Guide – Ethernet*.

----End

4.4.5 Configuring the Password Authentication Mode for SSH Login Users

Context

Before configuring SSH, you must use the local RSA key pair generated in [Step 2](#). *user-name* configured in [Step 3](#) must be the same as the local username configured on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **rsa local-key-pair create** command to create a local RSA key pair.
- Step 3** Run the **ssh user** *user-name* **authentication-type password** command to configure the password authentication mode for SSH login users.

----End

4.4.6 Configuring the RSA Authentication Mode for SSH Login Users

Context

Before configuring SSH, you must use the local RSA key pair generated in [Step 2](#). Then, you can perform [Step 8](#) and [Step 9](#) in turn to enter the public key view and public key edit view where you can copy the RSA public key generated by the SSH client to the configuration interface of the S-switch. Finally, you can take [Step 13](#) to assign the RSA public key to a specified user.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **rsa local-key-pair create** command to create a local RSA key pair.
 - Step 3** Run the **aaa** command to enter the AAA view.
 - Step 4** Run the **local-user user-name password { simple | cipher } password** command to create local users.
 - Step 5** Run the **local-user user-name service-type ssh** command to configure the local user to be the SSH user.
 - Step 6** Run the **quit** command to return to the system view.
 - Step 7** Run the **ssh user user-name authentication-type rsa** command to configure the RSA authentication mode for SSH login users.
 - Step 8** Run the **rsa peer-public-key key-name** command to enter the public key view.
 - Step 9** Run the **public-key-code begin** command to enter the public key edit view.
 - Step 10** Enter the value of *key-string* to set the RSA public key.
 - Step 11** Run the **public-key-code end** command to return to the RSA public key view.
 - Step 12** Run the **peer-public-key end** command to return to the system view.
 - Step 13** Run the **ssh user user-name assign rsa-key key-name** command to assign the public key to the SSH user.
- End

4.4.7 (Optional) Setting the SSH Timer and Authentication Times

Context

[Step 2](#) to [Step 4](#) are optional and are not listed in sequence.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ssh server rekey-interval hours** command to set the update time of the SSH key. By default, the update time of the key is 0. That is, the key is not updated.
- Step 3** Run the **ssh server timeout seconds** command to set the timeout period for SSH authentication. By default, the timeout period for authentication is 60 seconds.

Step 4 Run the **ssh server authentication-retries** *times* command to set the retry times of SSH authentication. By default, the retry times of authentication is 3.

----End

4.4.8 Checking the Configuration

Action	Command
Check information about the user interface.	display users [all]
Check the maximum number of VTY user interfaces.	display user-interface maximum-vty
Check physical attributes and certain configurations of the user interface.	display user-interface [<i>ui-type ui-number</i> <i>number</i>] [summary]
Check the public key of the key pair of the host and the server.	display rsa local-key-pair public
Check the RSA public key at the client.	display rsa peer-public-key [brief name <i>key-name</i>]
Check information about the SSH status and session.	display ssh server { session status }
Check information about the SSH user.	display ssh user-information [<i>user-name</i>]

4.5 Maintaining User Interfaces and Terminal Services

This section describes how to maintain user interfaces and terminal services.



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When a user interface fault or a user authentication fault occurs, run the following debugging commands in the user view to locate the fault. For details on how to enable the debugging, refer to the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*.

Table 4-5 Debugging Terminal Services

Action	Command
Enable the debugging of Telnet.	debugging telnet

Action	Command
Enable the debugging of SSH.	debugging ssh server { all vty index }
Enable the debugging of RSA.	debugging rsa
Enable the debugging of VTY.	debugging vty { fsm negotiate }

4.6 Configuration Examples

This section provides examples for user login.

4.6.1 Example for Configuring the Telnet Login User on the Ethernet

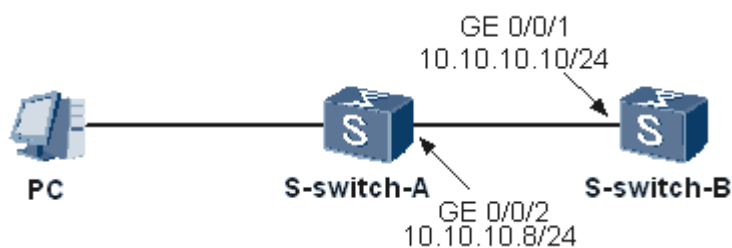
4.6.2 Example for Configuring the SSH Login User

4.6.1 Example for Configuring the Telnet Login User on the Ethernet

Networking Requirements

As shown in [Figure 4-5](#), after logging in to S-switch-A, the user logs in to S-switch-B through Telnet by using the default interface numbered 23.

Figure 4-5 Remote login on the Ethernet



Configuration Roadmap

Assign IP addresses to S-switch-A and S-switch-B and configure the Telnet authentication mode and password on the S-switch-B. Enter the password when you log in to S-switch-B from S-switch-A.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID
- IP address and the interface number of S-switch-A that functions as the Telnet client
- IP address and the interface number of S-switch-B that functions as the Telnet server
- Authentication mode and password

Configuration Procedure

1. Assign IP addresses.

Assign an IP address to S-switch-A that functions as the Telnet client.

```
<S-switch-A> system-view
[S-switch-A] vlan 2
[S-switch-A-vlan2] port GigabitEthernet 0/0/2
[S-switch-A-vlan2] quit
[S-switch-A] interface vlanif 2
[S-switch-A-Vlanif2] ip address 10.10.10.8 255.255.255.0
[S-switch-A-Vlanif2] quit
[S-switch-A]
```

Assign an IP address to S-switch-B that functions as the Telnet server.

```
<S-switch-B> system-view
[S-switch-B] vlan 2
[S-switch-B-vlan2] port GigabitEthernet 0/0/1
[S-switch-B-vlan2] quit
[S-switch-B] interface vlanif 2
[S-switch-B-Vlanif2] ip address 10.10.10.10 255.255.255.0
[S-switch-B-Vlanif2] quit
[S-switch-B]
```

2. Configure the authentication mode and password for logging in to S-switch-B through Telnet.

```
<S-switch-B> system-view
[S-switch-B] user-interface vty 0 4
[S-switch-B-ui-vty0-4] authentication-mode password
[S-switch-B-ui-vty0-4] set authentication password simple 123456
[S-switch-B-ui-vty0-4] quit
[S-switch-B]
```

3. Verify the configuration.

Log in to S-switch-B from S-switch-A through Telnet.

```
<S-switch-A> telnet 10.10.10.10
Trying 10.10.10.10 ...
Press CTRL+K to abort
Connected to 10.10.10.10 ...
*****
*                All rights reserved (2000-2005)                *
*      Without the owner's prior written consent,              *
* no decompiling or reverse-engineering shall be allowed.      *
* Notice:                                                        *
*      This is a private communication system.                  *
*      Unauthorized access or use may lead to prosecution.      *
*****
Login authentication

Password:
Note: The max number of VTY users is 5, and the current number
      of VTY users on line is 1.
<S-switch-B>
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 2
#
interface Vlanif2
ip address 10.10.10.8 255.255.255.0
#
interface GigabitEthernet0/0/2
```

```

        port default vlan 2
    #
    return

```

- Configuration file of S-switch-B


```

                #
                sysname S-switch-B
                #
                vlan batch 2
                #
                interface Vlanif2
                ip address 10.10.10.10 255.255.255.0
                #
                interface GigabitEthernet0/0/1
                port default vlan 2
                #
                user-interface vty 0 4
                set authentication password simple 123456
                #
                return
            
```

4.6.2 Example for Configuring the SSH Login User

Networking Requirements

As shown in [Figure 4-6](#), a local connection between the terminal that functions as the SSH client and the S-switch is set up. The client software that supports SSH1.5 is run on the terminal. Two login users are to be set: One is named client001; its password is Huawei; the authentication mode is password. The other is named client002; the authentication mode is RSA; the public key quidway002 is assigned to it. The user interface supports only the SSH protocol.

Figure 4-6 SSH local configuration



Configuration Roadmap

Set the password for the user client001 to log in to the S-switch. The user client002 uses the client software that supports SSH1.5 to generate an RSA public key. No password is needed for the user client002 to log in to the S-switch.

Data Preparation

To complete the configuration, you need the following data:

- Client software that supports SSH1.5
- RSA public key
- IP address of the S-switch

Configuration Procedure

1. Generate the local key pair.

```

[S-switch] rsa local-key-pair create
The key name will be: S-switch_Host

```

```
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
.....+++++++
.....+++++++
.....+++++++
.....+++++++
.....+++++++
```

NOTE

If the local key pair is generated, you can skip this configuration.

2. Configure the user client001; set the password to huawei1; set the authentication mode to password. The user interface supports only the SSH protocol.

```
[S-switch] user-interface vty 0 4
[S-switch-ui-vty0-4] authentication-mode aaa
[S-switch-ui-vty0-4] protocol inbound ssh
[S-switch-ui-vty0-4] quit
[S-switch] aaa
[S-switch-aaa] local-user client001 password simple huawei1
[S-switch-aaa] quit
[S-switch] ssh user client001 authentication-type password
```

3. Configure the user client002; set the password to huawei2; set the authentication mode to RSA. The user interface supports only the SSH protocol.

```
[S-switch] aaa
[S-switch-aaa] local-user client002 password simple huawei2
[S-switch-aaa] quit
[S-switch] ssh user client002 authentication-type rsa
```

4. Generate the RSA public key by using the client software that supports SSH1.5.

The detailed configuration is not mentioned here.

5. Send the RSA public key generated on the client software that supports SSH1.5 to the server.

```
[S-switch] rsa peer-public-key quidway002
Enter "RSA public key" view, return system view with "peer-public-key end".
[S-switch-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[S-switch-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[S-switch-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[S-switch-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[S-switch-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[S-switch-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[S-switch-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[S-switch-rsa-key-code] public-key-code end
[S-switch-rsa-public-key] peer-public-key end
[S-switch] ssh user client002 assign rsa-key quidway002
```

6. Run the client software that supports SSH1.5 on the terminal which has reserved the RSA private key.

The detailed configuration is not mentioned here.

Configuration Files

```
#
sysname S-switch
#
rsa peer-public-key quidway002
public-key-code begin
308186028180739A291ABDA704F5D93DC8FDF84C4274631991C164B0DF178C55FA833591C7D47D5381
D09CE82913D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE40861B74A0E135523CCD74CAC61
F8E58C452B2F3F2DA0DCC48E3306367FE187BDD944018B3B69F3CBB0A573202C16BB2FC1ACF3EC8F82
8D55A36F1CDDC4BB45504F020125
public-key-code end
```

```
peer-public-key end
#
aaa
local-user client001 password simple huawei1
local-user client002 password simple huawei2
authentication-scheme default
#
authorization-scheme default
#
accounting-scheme default
#
domain default
#
#
ssh user client002 assign rsa-key quidway002
ssh user client001 authentication-type password
ssh user client002 authentication-type RSA
#
user-interface con 0
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return
```


5 Managing the File System

About This Chapter

This chapter describes the basics of the file system, and how to upload and download files through the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) and manage configuration files. This chapter also provides configuration examples and troubleshooting.

[5.1 Introduction](#)

This section describes the concepts of file system management.

[5.2 Managing the File System](#)

This section describes how to manage the Flash memory, directories, or files on the S-switch.

[5.3 Transferring Files with the S-switch Acting as the FTP Server](#)

This section describes how to connect the S-switch to the FTP server for transferring files.

[5.4 Transferring Files with the S-switch Acting as the FTP Client](#)

This section describes how to connect the S-switch to the FTP client for transferring files.

[5.5 Transferring Files with the S-switch Acting as the TFTP Client](#)

This section describes how to download or upload files through TFTP.

[5.6 Maintaining the File System](#)

This section describes how to debug the file system or the FTP server.

[5.7 Configuration Examples](#)

This section provides examples for managing the file system.

5.1 Introduction

This section describes the concepts of file system management.

5.1.1 File System

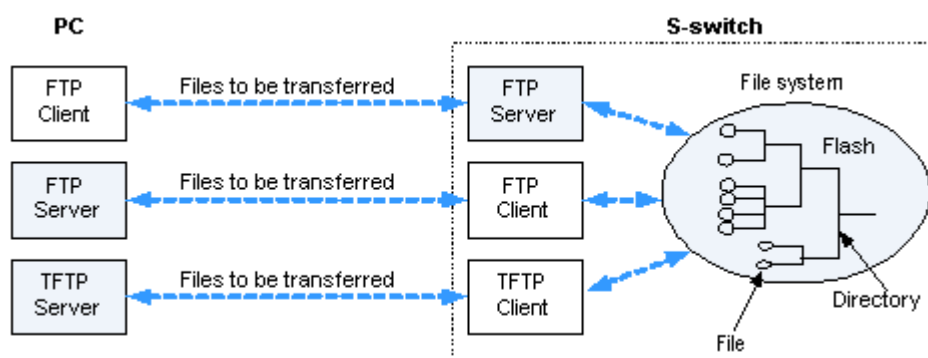
5.1.2 File Transfer Modes

5.1.3 Logical Relationships Between Configuration Tasks

5.1.1 File System

Figure 5-1 shows how the file system works on the S-switch.

Figure 5-1 Managing files on the S-switch



The flash memory of the S-switch supports the file system. It is a tree structure consisting of directories and files. The S-switch can use both FTP and TFTP to transfer files.

Flash

On the S-switch, you can manage the Flash memory by:

- Formatting the Flash memory
- Fixing the damaged Flash memory
- Creating, deleting, or changing the directories or files in the Flash memory

NOTE

The file name is a string of 3 to 64 characters when having the extension name added, or 1 to 64 characters when having no extension name added. The file name consists of the driver name, :, /, directory name, file name, or combination of them.

No space is allowed to name the file.

System Software and Configuration File

The system software facilitates the S-switch with an operating platform where you can deal with different functions and services. It is a binary program file. The configuration file contains the parameters for booting the S-switch. It is a text file. The system software and configuration file can be stored in the Flash memory.

5.1.2 File Transfer Modes

FTP

FTP is an application layer protocol and provides TCP-based reliable transfer services.

The S-switch provides the following FTP functions:

- FTP server
- You can run the FTP client program on a PC to log in to the S-switch. As the FTP server, the S-switch authenticates its users. Users that pass the authentication can access the Flash memory and upload or download files.
- FTP client
- You can log in to the FTP server from the S-switch through FTP. After passing the authentication, you can manage files on the FTP server, and upload files to the FTP server or download files to the Flash memory from the FTP server on the S-switch.

Two types of codes are applicable for transferring FTP files: binary and ASCII. Binary codes are used to transfer program files; ASCII codes are used to transfer text files.

TFTP

TFTP is a simple file transfer protocol based on the User Datagram Protocol (UDP). Compared with FTP, TFTP excludes the interfaces for complicated interactions or access. TFTP excludes authentication control, either. Thus, TFTP is applicable in the environment without complicated interactions between a client and a host.

As the TFTP client, the S-switch initiates TFTP connections and upload files to the FTP server or download files to the Flash memory from the FTP server on the S-switch.

- To upload files, the S-switch sends the write request (WRQ) to the TFTP server. After the server grants the request, the client sends data packets to the server and waits for an ACK packet from the server.
- To download files, the S-switch sends the read request (RRQ) to the TFTP server. The server then grants the request and sends data packets to the client. After receiving the data packets, the client sends an ACK packet to the server.

Currently, TFTP can transfer files only in binary mode.

5.1.3 Logical Relationships Between Configuration Tasks

For details on how to manage the file system, see [5 Managing the File System](#).

To transfer files between the client and server, you need:

- [5.3 Transferring Files with the S-switch Acting as the FTP Server](#)
- [5.4 Transferring Files with the S-switch Acting as the FTP Client](#)
- [5.5 Transferring Files with the S-switch Acting as the TFTP Client](#)

5.2 Managing the File System

This section describes how to manage the Flash memory, directories, or files on the S-switch.

[5.2.1 Changing the Prompt Mode of the File System](#)[5.2.2 Managing the Flash Memory](#)[5.2.3 Managing File Directories](#)[5.2.4 Managing Files](#)[5.2.5 Executing the Batch File](#)

5.2.1 Changing the Prompt Mode of the File System

Procedure

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

Step 2 Run the **file prompt { alert | quiet }** command to change the prompt mode of the file system.

The S-switch provides the following prompt modes of the file system:

- Alert
If the operation of a user such as deleting a file may cause data loss or data damage, the S-switch prompts a message for the user to confirm whether to perform the operation.
- Quiet
The S-switch does not prompt any message.

By default, the S-switch adopts the prompt mode of alert.

----End

5.2.2 Managing the Flash Memory

Context



CAUTION

All the files and directories in the flash are deleted when you run the **format flash:** command. So, confirm the action before you use the command.

[Step 1](#) and [Step 2](#) are optional and are not listed in sequence.

Procedure

Step 1 Run the **fixdisk flash:** command to fix the abnormal Flash memory.

Step 2 Run the **format flash:** command to format the Flash memory.

----End

5.2.3 Managing File Directories

Context

[Step 1](#) to [Step 5](#) are optional and are not listed in sequence.

Procedure

- Step 1** Run the **cd** { *path* | *..* | */* } command to enter a specified file directory.
 - Step 2** Run the **dir** [*/all*] [*filename* | **flash:**] command to view the directories and files in the current file directory.
 - Step 3** Run the **mkdir** *directory* command to create a directory.
 - Step 4** Run the **rmdir** *directory* command to delete a directory.
 - Step 5** Run the **pwd** command to view the current file directory.
- End

5.2.4 Managing Files

Context

[Step 1](#) to [Step 9](#) are optional and are not listed in sequence.

Procedure

- Step 1** Run the **dir** [*/all*] [*filename* | **flash:**] command to view the directories and files in the current file directory.
 - Step 2** Run the **copy** *source-filename destination-filename* command to copy a file.
 - Step 3** Run the **move** *source-filename destination-filename* command to move a file.
 - Step 4** Run the **rename** *source-filename destination-filename* command to rename a file.
 - Step 5** Run the **more** *filename* [*offset*] command to display a file.
 - Step 6** Run the **delete** { *filename* | **flash:** } command to move the file to the recycle bin of the S-switch.
 - Step 7** Run the **delete /unreserved** { *filename* | **flash:** } command to delete a file permanently.
 - Step 8** Run the **undelete** *filename* command to restore a deleted file.
 - Step 9** Run the **reset recycle-bin** [*filename*] command to delete the file in the recycle bin permanently.
- End

5.2.5 Executing the Batch File

Procedure

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

Step 2 Run the `execute batch-filename` command to execute the batch file.

----End

5.3 Transferring Files with the S-switch Acting as the FTP Server

This section describes how to connect the S-switch to the FTP server for transferring files.

[5.3.2 Enabling the FTP Server](#), [5.3.3 Configuring Authentication and Authorization for Users Logging In to the FTP Server](#), and [5.3.4 \(Optional\) Setting the Timeout Period of the FTP Server](#) are not listed in sequence.

[5.3.1 Establishing the Configuration Task](#)

[5.3.2 Enabling the FTP Server](#)

[5.3.3 Configuring Authentication and Authorization for Users Logging In to the FTP Server](#)

[5.3.4 \(Optional\) Setting the Timeout Period of the FTP Server](#)

[5.3.5 Checking the Configuration](#)

5.3.1 Establishing the Configuration Task

Applicable Environment

To transfer files with the S-switch, you can take the S-switch as the FTP server to upload files to the S-switch through the FTP client, or download files from the S-switch such as the VRP or configuration file.

When the S-switch acts as the FTP server, it authenticates user IDs to ensure security of files.

Pre-configuration Tasks

Before transferring files through FTP, complete the following tasks:

- Assigning IP addresses to interfaces
- Configuring a reachable route between the S-switch and the FTP client

Data Preparation

To take the S-switch as the FTP server to transfer files, you need the following data.

No.	Data
1	Authentication information of the login user
2	(Optional) Timeout period of the FTP server

5.3.2 Enabling the FTP Server

Procedure

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

Step 2 Run the **ftp server enable** command to enable the FTP server.

----End

5.3.3 Configuring Authentication and Authorization for Users Logging In to the FTP Server

Context

user-name in Step 3 to Step 5 must be the same.

For details on Authentication, Authorization, and Accounting (AAA) or managing local users, refer to the chapter "AAA Configuration" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*.

Procedure

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

Step 2 Run the **aaa** command to enter the AAA view.

Step 3 Run the **local-user user-name password { cipher | simple } password** command to set the name and password of an FTP login user.

Step 4 Run the **local-user user-name ftp-directory directory** command to configure the file directory for the FTP login user.

The parameter of *directory* should exist in the S-switch and include the whole path. For example, if the directory is named "FTP" and located at the root of the flash memory, *directory* is "flash:/FTP".

Step 5 (Optional) Run the **local-user user-name service-type ftp** command to set the service type for the FTP login user.

----End

5.3.4 (Optional) Setting the Timeout Period of the FTP Server

Procedure

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

Step 2 Run the **ftp timeout timeout** command to set the timeout period of the FTP server.

By default, the timeout period of the FTP server is 30 minutes.

----End

5.3.5 Checking the Configuration

Action	Command
Check information about the FTP server.	display ftp-server
Check information about FTP login users.	display ftp-users

Run the preceding command, and you can obtain the following information:

- FTP has been enabled on the S-switch and parameters of the FTP server have been configured correctly.
- All the FTP login users are displayed on the S-switch.

5.4 Transferring Files with the S-switch Acting as the FTP Client

This section describes how to connect the S-switch to the FTP client for transferring files.

[5.4.1 Establishing the Configuration Task](#)

[5.4.2 Logging In to the FTP Server](#)

[5.4.3 Cutting Off an FTP Connection](#)

[5.4.4 Switching the User Logging In to the FTP Server](#)

[5.4.5 Displaying Online Help About an FTP Command](#)

[5.4.6 Managing the Directory on the FTP Server](#)

[5.4.7 Managing Files on the FTP Server](#)

[5.4.8 Setting the File Transfer Mode](#)

5.4.1 Establishing the Configuration Task

Applicable Environment

To transfer files with the S-switch, you can take the S-switch as the FTP client to download or upload files such as the VRP or configuration file through the FTP server.

Pre-configuration Tasks

Before transferring files in FTP mode, complete the following tasks:

- Assigning IP addresses to interfaces
- Configuring a reachable route between the S-switch and the FTP server

Data Preparation

To take the S-switch as the FTP client to transfer files, you need the following data.

No.	Data
1	Authentication information about the logging in to the server

5.4.2 Logging In to the FTP Server

Procedure

- Step 1** Run the **ftp** [*ftp-server* [*port-number*]] command to set up a connection with the FTP server and enter the FTP client view.

If *host* is not specified, you can only enter the FTP client view. To set up FTP connections, you need to enter the username and password of the FTP user that has been configured on the FTP server.

- Step 2** (Optional) Run the **open** *ftp-server* [*port-number*] command to set up a connection with the FTP server.

You can perform step 2 only after the S-switch enters the FTP client view and no FTP connection has been set up.

----End

5.4.3 Cutting Off an FTP Connection

Procedure

- Step 1** Run the command of **close** or **disconnect** to cut off a connection with the FTP server and remain in the FTP client view.

- Step 2** Run the command of **bye** or **quit** to cut off a connection with the FTP server and return to the user view.

This configuration can be performed only in the FTP client view.

----End

5.4.4 Switching the User Logging In to the FTP Server

Procedure

- Step 1** Run the **ftp** [*ftp-server* [*port-number*]] command to set up a connection with the FTP server and enter the FTP client view.

- Step 2** Run the **user** *user-name* [*password*] command to switch the user logging in to the FTP server and re-log in to the FTP server.

----End

5.4.5 Displaying Online Help About an FTP Command

Procedure

- Step 1** Run the **ftp** [*ftp-server* [*port-number*]] command to set up a connection with the FTP server and enter the FTP client view.
- Step 2** Run the **remotehelp** [*command*] command to display online help about an FTP command.
- End

5.4.6 Managing the Directory on the FTP Server

Context

[Step 2](#) to [Step 7](#) are optional and are not listed in sequence.

Procedure

- Step 1** Run the **ftp** [*ftp-server* [*port-number*]] command to set up a connection with the FTP server and enter the FTP client view.
- Step 2** Run the **cd** *path* command to change the working path of the FTP server.
- Step 3** Run the **cdup** command to change the working path of the FTP server to the parent directory.
- Step 4** Run the **pwd** command to display the working path of the FTP server.
- Step 5** Run the **lcd** command to display the working path of the FTP client.
- Step 6** Run the **mkdir** *remote-directory* command to create a directory on the FTP server.
- Step 7** Run the **rmdir** *remote-directory* command to delete a directory on the FTP server.
- End

5.4.7 Managing Files on the FTP Server

Context

[Step 2](#) to [Step 6](#) are optional and are not listed in sequence.

Procedure

- Step 1** Run the **ftp** [*ftp-server* [*port-number*]] command to set up a connection with the FTP server and enter the FTP client view.
- Step 2** Run the **ls** [*remote-filename*] [*local-filename*] command to query information about a specified directory or file on the FTP server.
- Step 3** Run the **dir** [*remote-filename*] [*local-filename*] command to query detailed information about a specified directory or file on the FTP server.

Step 4 Run the **delete** *remote-filename* command to delete a specified file on the FTP server.

Step 5 Run the **get** *remote-filename* [*local-filename*] command to download files from the FTP server.

Step 6 Run the **put** *local-filename* [*remote-filename*] command to upload files to the FTP server.

----End

5.4.8 Setting the File Transfer Mode

Context

[Step 2](#) and [Step 3](#) are optional and are not listed in sequence.

Procedure

Step 1 Run the **ftp** [*ftp-server* [*port-number*]] command to set up a connection with the FTP server and enter the FTP client view.

Step 2 Run the **ascii** | **binary** command to set the format for FTP to transfer data.

By default, FTP transmits data in **ascii** format. That is, FTP adopts the passive mode.

Step 3 Run the **passive** command to configure the passive transfer mode.

----End

5.5 Transferring Files with the S-switch Acting as the TFTP Client

This section describes how to download or upload files through TFTP.

[5.5.1 Establishing the Configuration Task](#)

[5.5.2 Setting the Range of Usable TFTP Servers](#)

[5.5.3 Initiating a TFTP Connection and Downloading Files](#)

[5.5.4 Initiating a TFTP Connection and Uploading Files](#)

[5.5.5 Checking the Configuration](#)

5.5.1 Establishing the Configuration Task

Applicable Environment

To transfer files with the S-switch, you can use the TFTP mode. In TFTP mode, the S-switch is taken as the TFTP client to log in to the TFTP server to download or upload files, such as the VRP or configuration file.

Pre-configuration Tasks

Before taking the S-switch to transfer files through TFTP, complete the following tasks:

- Assigning IP addresses to interfaces
- Configuring a reachable route between the S-switch and TFTP server

Data Preparation

To take the S-switch to transfer files through TFTP, you need the following data.

No.	Data
1	Authentication information for logging in to the server

5.5.2 Setting the Range of Usable TFTP Servers

Procedure

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

Step 2 Run the **tftp-server acl acl-number** command to set the range of usable TFTP servers.

After this configuration is performed, if you do not use the **acl** command to set up the ACL numbered *acl-number*, the S-switch cannot access any TFTP server.

For details on the **acl** command, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

----End

5.5.3 Initiating a TFTP Connection and Downloading Files

Procedure

Run the **tftp hostname get source-filename [destination-filename]** command to initiate a TFTP connection and download files.

----End

5.5.4 Initiating a TFTP Connection and Uploading Files

Procedure

Run the **tftp hostname put source-filename [destination-filename]** command to initiate a TFTP connection and upload files.

----End

5.5.5 Checking the Configuration

Action	Command
Check the range of usable TFTP servers.	display current-configuration
	display acl acl-number

Run the preceding commands, and you can obtain the following information: The ACL number has been configured correctly. In an ACL rule, the range of usable TFTP servers has been set correctly.

5.6 Maintaining the File System

This section describes how to debug the file system or the FTP server.

5.6.1 Debugging the File System

5.6.2 Debugging the FTP Server

5.6.1 Debugging the File System



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When an operation fault of the file system occurs, run the following debugging command in the user view to locate the fault. For details on how to enable the debugging, refer to Chapter 4 "Debugging and Diagnosis". For details on the **debugging** command, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

Action	Command
Debug the file system.	debugging vfs { flash low }

5.6.2 Debugging the FTP Server



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When an operation fault of the FTP server occurs, run the following debugging command in the user view to locate the fault. For details on how to enable the debugging, refer to the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*. For details on the **debugging** command, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

Action	Command
Debug the FTP server.	debugging ftp-server

5.7 Configuration Examples

This section provides examples for managing the file system.

[5.7.1 Example for Transferring Files Through FTP with the S-switch Acting as the FTP Server](#)

[5.7.2 Example for Transferring Files Through FTP with the S-switch Acting as the FTP Client](#)

[5.7.3 Example for Transferring Files Through TFTP](#)

[5.7.4 Example for Integrated Operations of the File System](#)

5.7.1 Example for Transferring Files Through FTP with the S-switch Acting as the FTP Server

Networking Requirements

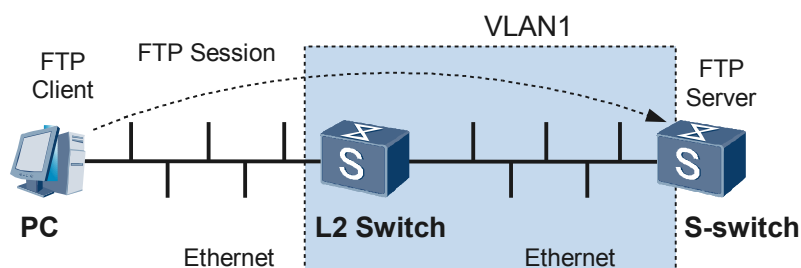
The PC is taken as the FTP client of which the IP address is 10.1.1.1/24.

The S-switch acts as the FTP server. VLAN 10 is created on the S-switch and GigabitEthernet 0/0/1 is added to VLAN 10. The IP address 10.1.1.2/24 is assigned to VLANIF 10.

The PC uploads the system software and configuration file to the S-switch.

Networking diagram

Figure 5-2 Using FTP to upload files when the S-switch acts as the FTP server



Configuration Procedure

1. Create VLAN 10 on the S-switch and assign the IP address 10.1.1.2/24 to VLANIF 10.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] port GigabitEthernet 0/0/1
[Quidway-vlan10] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.2 24
[Quidway-Vlanif10] quit
```

2. Start the FTP server on the S-switch, and set the FTP username to **ftpuser** and password to **ftppwd**.

```
[Quidway] ftp server enable
[Quidway] aaa
[Quidway-aaa] local-user ftpuser password simple ftppwd
[Quidway-aaa] local-user ftpuser service-type ftp
[Quidway-aaa] local-user ftpuser ftp-directory flash:/
[Quidway-aaa] return
```

3. Back up the configuration file and system software on the S-switch.

```
<Quidway> copy vrpcfg.cfg flash:/backup.cfg
<Quidway> copy 8031.cc flash:/8031bak.cc
```

4. From the PC, initiate a connection to the S-switch with username **tpuser** and password **ftppwd**.

Take Windows XP on the FTP client as an example.

```
C:\WINDOWS\Desktop> ftp 10.1.1.2
Connected to 10.1.1.2.
220 FTP-Server Microsoft FTP Service (Version 5.0).
User (10.1.1.1:(none)): ftpuser
331 Password required for ftpuser.
Password:*****
230 User logged in.
ftp>
```

5. Set the binary file transfer mode and view the local directory on the PC.

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

6. Upload the system software and configuration file to the S-switch.

```
ftp> put d006.cc d006.cc
ftp> put vrpcfg.cfg vrpcfg.cfg
ftp> quit
C:\WINDOWS\Desktop>
```

Configuration Files

```
#
sysname Quidway
#
FTP server enable
#
vlan batch 10
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
port default vlan 10
#
aaa
local-user ftpuser password simple ftppwd
local-user ftpuser service-type ftp
local-user ftpuser ftp-directory flash:/
#
return
```

5.7.2 Example for Transferring Files Through FTP with the S-switch Acting as the FTP Client

Networking Requirements

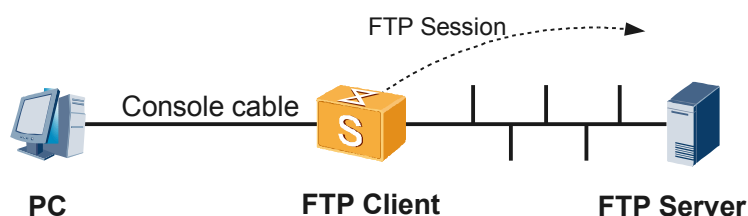
The remote server at 10.1.1.2 serves as the FTP server.

The S-switch acts as the FTP client. Interfaces ranging from GigabitEthernet 0/0/1 to GigabitEthernet 0/0/4 can be used to set up FTP connections and they share an IP address 10.1.1.1.

The S-switch downloads the latest system software and configuration file from the FTP server.

Networking Diagram

Figure 5-3 Using FTP to download files when the S-switch acts as the FTP client



Configuration Procedure

1. Enable FTP on the remote FTP server. Add an FTP user named **ftpuser** and set the password to **ftppwd**.
2. Create VLAN 10 on the S-switch and assign the IP address 10.1.1.1 to VLANIF10.

```

<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] port GigabitEthernet 0/0/1 to 0/0/4
[Quidway-vlan10] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 24
  
```

3. Back up the configuration file and system software on the S-switch.

```

<Quidway> copy vrpcfg.cfg flash:/backup.cfg
<Quidway> copy 8031.cc flash:/8031bak.cc
  
```

4. From the S-switch, initiate a connection to the FTP server with username **tpuser** and password **ftppwd**.

```

<Quidway> ftp 10.1.1.2
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP-Server v2.5 for WinSock ready...
User(10.1.1.1:(none)):ftpuser
331 User name okay, need password.
Password:*****
230 User logged in, proceed.
[ftp]
  
```

5. On the S-switch, set the binary file transfer mode and view the flash directory.

```

[ftp] binary
200 Type set to I.
  
```

- ```
[ftp] lcd flash:/
% Local directory now flash:.
```
6. The S-switch downloads the latest system software and configuration file from the remote FTP server.
- ```
[ftp] get d006.cc d006.cc
[ftp] get vrpcfg.cfg vrpcfg.cfg
[ftp] quit
<Quidway>
```

Configuration Files

```
#
 sysname Quidway
#
 vlan batch 10
#
 interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
 interface GigabitEthernet0/0/1
 port default vlan 10
#
 interface GigabitEthernet0/0/2
 port default vlan 10
#
 interface GigabitEthernet0/0/3
 port default vlan 10
#
 interface GigabitEthernet0/0/4
 port default vlan 10
#
return
```

5.7.3 Example for Transferring Files Through TFTP

Networking Requirements

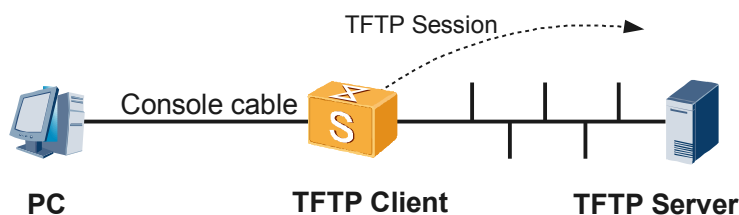
The S-switch cannot function as the TFTP server. The remote server at 10.1.1.2 functions as the TFTP server.

The S-switch acts as an TFTP client. VLAN 10 is created on the S-switch, and GigabitEthernet0/0/1, GigabitEthernet0/0/2, GigabitEthernet0/0/3, and GigabitEthernet0/0/4 are added to VLAN 10. The IP address 10.1.1.1/24 is assigned to VLANIF 10.

The S-switch downloads the system software and configuration file from the PC.

Networking Diagram

Figure 5-4 Using TFTP to download files when the S-switch acts as the TFTP client



Configuration Procedure

1. Enable TFTP on the remote server to ensure that the TFTP application software is started.
2. Create VLAN 10 on the S-switch and assign the IP address 10.1.1.2/24 to VLANIF 10.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] port GigabitEthernet 0/0/1 to 0/0/4
[Quidway-vlan10] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 24
```

3. Back up the configuration file and system software on the S-switch.

```
<Quidway> copy vrpcfg.cfg flash:/backup.cfg
<Quidway> copy 8031.cc flash:/8031bak.cc
```

4. On the S-switch, initiate a connection to the TFTP server and download the latest system software.

```
<Quidway> tftp 10.1.1.2 get 8031.cc 8031new.cc
Transfer file in binary mode.
Now begin to download file from remote tftp server, please wait for a while...
```

Configuration Files

```
#
sysname Quidway
#
vlan batch 10
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface GigabitEthernet0/0/2
port default vlan 10
#
interface GigabitEthernet0/0/3
port default vlan 10
#
interface GigabitEthernet0/0/4
port default vlan 10
#
return
```

5.7.4 Example for Integrated Operations of the File System

Networking Requirements

Two S-switches, S-switch-A and S-switch-B, need the same configurations. S-switch-A has been configured successfully and the current configurations on S-switch-A are saved as **config.cfg**. The **config.cfg** file of S-switch-A needs to be backed up on a PC and S-switch-B is configured the same as S-switch-A.

The IP address of the PC is 1.1.1.1/8; the PC is connected to GigabitEthernet 0/0/1 of S-switch-A and GigabitEthernet 0/0/1 of S-switch-B.

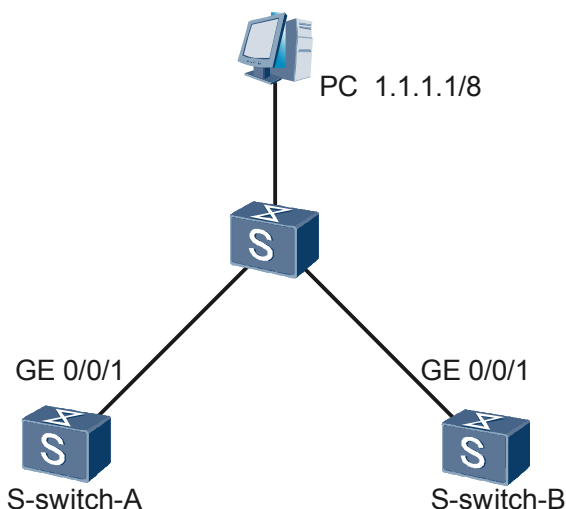
The configuration roadmap is as follows:

- On S-switch-A, save the current configuration as the file as the **config.cfg** file for the next startup.

- Enable the FTP server on S-switch-A. Log in to the S-switch-A through the FTP client program from the PC and download the **config.cfg** file to the PC.
- Enable TFTP application software on the PC. Log in to the PC from S-switch-B through the **tftp** command and download the **config.cfg** file to the flash on S-switch-B.
- Specify the **config.cfg** file as the configuration file for the next startup of S-switch-B.

Networking Diagram

Figure 5-5 Configuring the integrated file system



Configuration Procedure

1. On S-switch-A, save the current configuration as **config.cfg**.

```
<S-switch-A> save config.cfg
```

Are you sure to save the configuration to flash:/config.cfg?[Y/N]:y
Now saving the current configuration to the device.....
Info:Save the current config to flash:/config.cfg successfully!
2. Specify the **config.cfg** file as the configuration file for the next startup of S-switch-A.

```
<S-switch-A> startup saved-configuration config.cfg
```
3. Enable the FTP server on S-switch-A.

```
<S-switch-A> system-view  
[S-switch-A] ftp server enable
```

Info:Start FTP server
4. On S-switch-A, configure an FTP user with username **ftp** and password **123**, and allow the user to access directory **flash**.

```
[S-switch-A] aaa  
[S-switch-A-aaa] local-user ftp password simple 123  
[S-switch-A-aaa] local-user ftp service-type ftp  
[S-switch-A-aaa] local-user ftp ftp-directory flash:
```
5. Create VLAN 10 on S-switch-A and add GigabitEthernet 0/0/1 to VLAN 10. Assign the IP address 1.1.1.2/8 to VLANIF 10.

```
[S-switch-A-aaa] quit  
[S-switch-A] vlan 10  
[S-switch-A-vlan10] port GigabitEthernet 0/0/1  
[S-switch-A-vlan10] quit  
[S-switch-A] interface vlanif 10  
[S-switch-A-Vlanif10] ip address 1.1.1.2 8
```
6. Run the FTP client program on the PC; log in to S-switch-A through FTP and download "config.cfg" to the hard disk C on the PC.

```
C:\> ftp 1.1.1.2
Connected to 1.1.1.2.
220 FTP service ready.
User (1.1.1.2:(none)): ftp
331 Password required for ftp.
Password: ***
230 User logged in.
ftp> get config.cfg
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.
ftp: 1500 bytes received in 0.00Seconds 1500000.00Kbytes/sec.
ftp> bye
221 Server closing.
C:\>
```

7. Create VLAN 20 on S-switch-B and add GigabitEthernet 0/0/1 to VLAN 20. Assign the IP address 1.1.1.3/8 to VLANIF 20.

```
<S-switch-B> system-view
[S-switch-B] vlan 20
[S-switch-B-vlan20] port GigabitEthernet 0/0/1
[S-switch-B-vlan20] quit
[S-switch-B] interface vlanif 20
[S-switch-B-Vlanif20] ip address 1.1.1.3 8
[S-switch-B-Vlanif20] return
<S-switch-B>
```

8. Enable TFTP application software on the PC and change the current directory of TFTP server to hard disk C.

9. On S-switch-B, run the **tftp 1.1.1.1 get config.cfg** command to download the **config.cfg** file from the PC.

```
<S-switch-B> tftp 1.1.1.1 get config.cfg
Transfer file in binary mode.
Now begin to download file from remote tftp server, please wait for a while...
/
TFTP:      1500 bytes received in 1 seconds.
File downloaded successfully.
```

10. Check the configuration file for the startup of S-switch-B.

```
<S-switch-B> display startup
MainBoard:
Configured startup system software:      flash:/S-switch.cc
Startup system software:                  flash:/S-switch.cc
Next startup system software:             flash:/S-switch.cc
Startup saved-configuration file:         flash:/save.cfg
Next startup saved-configuration file:    flash:/save.cfg
```

11. Specify the **config.cfg** file as the configuration file for the next startup of S-switch-B and reboot S-switch-B.

```
<S-switch-B> startup saved-configuration config.cfg
<S-switch-B> reboot
```

12. Check the configuration file for startup of S-switch-B and permanently delete the previous **save.cfg** file.

```
<S-switch-B> display startup
MainBoard:
Configured startup system software:      flash:/S-switch.cc
Startup system software:                  flash:/S-switch.cc
Next startup system software:             flash:/S-switch.cc
Startup saved-configuration file:         flash:/config.cfg
Next startup saved-configuration file:    flash:/config.cfg
<S-switch-B> delete /unreserved save.cfg
The contents cannot be recycled!!! Delete flash:/save.cfg?[Y/N]:y
%Deleting file flash:/save.cfg...
Deleting file permanently from flash will take a long time if needed.....Done!
```

Configuration Files

- S-switch-A

```
#
 sysname S-switch-A
#
 FTP server enable
#
 vlan batch 10
#
 interface Vlanif10
 ip address 1.1.1.2 255.0.0.0
#
 interface GigabitEthernet0/0/1
 port default vlan 10
#
aaa
 local-user ftpuser password simple 123
 local-user ftp service-type ftp
 local-user ftpuser ftp-directory flash:/
#
return
```

- S-switch-B

```
#
 sysname S-switch-B
#
 vlan batch 20
#
 interface Vlanif20
 ip address 1.1.1.3 255.0.0.0
#
 interface GigabitEthernet0/0/1
 port default vlan 20
#
return
```


6 Managing Configuration Files

About This Chapter

This section describes basic concepts and operations of configuration files.

[6.1 Introduction](#)

This section describes configuration files and logical relationships between configuration tasks.

[6.2 Checking the Configuration](#)

This section describes how to check the configuration on the S-switch.

[6.3 Common Operations for the Configuration File](#)

This section describes how to save, clear, and compare configuration files.

[6.4 Configuring the Configuration File for the Next Startup](#)

This section describes how to configure the configuration file for the next startup.

6.1 Introduction

This section describes configuration files and logical relationships between configuration tasks.

6.1.1 Configuration Files

6.1.2 Logical Relationships Between Configuration Tasks

6.1.1 Configuration Files

The contents and format of the configuration file are as follows:

- File contents

The configuration file is composed of command lines. Only non-default command lines and command lines with non-default parameters are saved in the configuration file.

- File format

The command lines in the file are organized on the basis of command views. The commands of the same command view are grouped into a section. Sections are separated from each other by comment lines starting with # signs. The configuration file is ended with "return."

**NOTE**

The sections are arranged in the order of global configurations, interface configurations, protocol configurations, and user interface configurations.

6.1.2 Logical Relationships Between Configuration Tasks

There is no logical relation between configuration tasks. You can perform any configuration task as required.

6.2 Checking the Configuration

This section describes how to check the configuration on the S-switch.

6.2.1 Checking the Current Configuration

6.2.2 Checking Saved Configurations

6.2.1 Checking the Current Configuration

Procedure

Run the **display current-configuration interface** [*interface-type* [*interface-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*] command to check the current configuration.

You can view current configuration in all views through this command.

----End

6.2.2 Checking Saved Configurations

Procedure

Run the **display saved-configuration [last]** command to check saved configurations.

You can check the configuration file to be loaded in the next startup or loaded in this startup of the S-switch through this command.

If the optional parameter **last** is not specified, the configuration file to be loaded in the next startup is displayed. If the optional parameter **last** is specified, the configuration file loaded in this startup is displayed.

----End

6.3 Common Operations for the Configuration File

This section describes how to save, clear, and compare configuration files.

[6.3.1 Saving the Current Configuration File](#)

[6.3.2 Clearing the Configuration File](#)

[6.3.3 Comparing Configuration Files](#)

6.3.1 Saving the Current Configuration File

Context

To save the current configuration file, do as follows on the S-switch.

Procedure

Run the **save [config-filename]** command to save the current configuration file.

You can change the current configuration file of the S-switch through command lines. You can also use the **save** command to save the changed file to the flash memory as the initial configuration file for the next startup.

NOTE

If you do not specify the file name when you save the configuration file for the first time, the system prompts you whether to save the configuration file as **vrpcfg.cfg**.

----End

6.3.2 Clearing the Configuration File

Context

To clear the configuration file, do as follows on the S-switch.

Procedure

Run the **reset saved-configuration** command to clear the loaded configuration file.

You can clear the loaded configuration file of the S-switch through this command. As a result, if no configuration file is specified through the **startup saved-configuration** command, or if

the current configuration is not saved through the **save** command, the S-switch will use the default parameters for initialization next time you boot the S-switch.

You need to reset the configuration file in the flash memory in the following cases:

- The upgraded software of the S-switch mismatches the configuration file.
- The configuration file is damaged or an incorrect configuration file is loaded.

----End

6.3.3 Comparing Configuration Files

Procedure

Run the **compare configuration** [*current-line-number save-line-number*] command to compare the current configuration file with the initial configuration file.

----End

6.4 Configuring the Configuration File for the Next Startup

This section describes how to configure the configuration file for the next startup.

Context

To configure the configuration file for the next startup, do as follows on the S-switch.

Procedure

Run the **startup saved-configuration** *config-filename* command to configure the configuration file for the next startup of the S-switch.

When the S-switch is powered on, it reads the configuration file from the flash memory to boot the system. The configuration in the file used for booting is called the initial configuration. If no configuration file is stored in the flash memory, the S-switch uses the default parameters.

The configuration file that is effective during the operation of the S-switch is called the current configuration.

----End