



Quidway S5300 Series Ethernet Switches
V100R002C02

Configuration Guide - Device Management

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 Checking the Status of the S-switch.....	1-1
1.1 Introduction.....	1-2
1.2 Checking the Status of the S-switch.....	1-2
1.2.1 Checking Information About the S-switch.....	1-2
1.2.2 Checking the Version of the S-switch.....	1-2
1.2.3 Checking the Electronic Labels.....	1-3
1.2.4 Checking Temperature.....	1-3
1.2.5 Checking the CPU Usage.....	1-3
1.2.6 Checking the Memory Usage.....	1-4
1.2.7 Checking Alarms.....	1-4
1.2.8 Checking the Status of an Interface.....	1-5
1.3 Using the Regular Expression.....	1-5
1.3.1 Introduction.....	1-6
1.3.2 Usage of the Regular Expression.....	1-6
1.3.3 Examples for Using the Regular Expression.....	1-9
2 Monitoring the Device Through the Information Center.....	2-1
2.1 Introduction.....	2-2
2.1.1 Functions of the Information Center.....	2-2
2.1.2 Types of Information.....	2-2
2.1.3 Severity Levels of Information.....	2-3
2.1.4 Information Channels and Output Directions.....	2-4
2.1.5 Format of a Log.....	2-5
2.2 Configuring the Information Center.....	2-7
2.2.1 Establishing the Configuration Task.....	2-8
2.2.2 Enabling the Information Center.....	2-8
2.2.3 (Optional) Naming the Information Channel.....	2-8
2.2.4 Defining the Information Channel.....	2-9
2.2.5 (Optional) Configuring the Timestamp for the Output Information.....	2-9
2.2.6 Checking the Configuration.....	2-9
2.3 Sending Information of the Information Center.....	2-10
2.3.1 Sending Information to the Console.....	2-10

2.3.2 Sending Information to the Telnet Terminal.....	2-11
2.3.3 Sending Information to the SNMP Agent.....	2-11
2.3.4 Sending Information to the Log Buffer.....	2-12
2.3.5 Sending Information to the Trap Buffer.....	2-12
2.3.6 Sending Information to the Log Host.....	2-12
2.3.7 Checking the Configuration.....	2-12
2.4 Maintaining the Information Center.....	2-13
2.5 Configuration Examples.....	2-13
2.5.1 Example for Configuring the Information Center.....	2-13
3 Mirroring.....	3-1
3.1 Introduction.....	3-3
3.1.1 Mirroring Functions.....	3-3
3.1.2 Logical Relationships Between Configuration Tasks.....	3-6
3.1.3 Specifications.....	3-6
3.2 Configuring Interface-based Local SPAN.....	3-7
3.2.1 Establishing the Configuration Task.....	3-7
3.2.2 Configuring Interface-based Local SPAN.....	3-7
3.2.3 Checking the Configuration.....	3-8
3.3 Configuring Interface-based RSPAN.....	3-8
3.3.1 Establishing the Configuration Task.....	3-8
3.3.2 Configuring Interface-based RSPAN.....	3-9
3.3.3 Checking the Configuration.....	3-11
3.4 Canceling Interface Mirroring.....	3-11
3.4.1 Establishing the Configuration Task.....	3-11
3.4.2 Establishing the Configuration Task.....	3-13
3.4.3 Configuring VLAN-based RSPAN.....	3-14
3.4.4 Establishing the Configuration Task.....	3-14
3.5 Configuring VLAN-based RSPAN.....	3-15
3.5.1 Configuring VLAN-based RSPAN on the Source S-switch.....	3-15
3.5.2 Configuring an RSPAN VLAN and Attributes of Its Interfaces on an Intermediate S-switch.....	3-16
3.5.3 Configuring an Observing Interface for RSPAN on the Destination S-switch.....	3-16
3.5.4 Checking the Configuration.....	3-16
3.5.5 Canceling VLAN Mirroring.....	3-16
3.5.6 Establishing the Configuration Task.....	3-16
3.5.7 Canceling VLAN Mirroring.....	3-17
3.6 Checking the Configuration.....	3-17
3.6.1 Configuring Local SPAN Based on MAC Addresses.....	3-17
3.6.2 Establishing the Configuration Task.....	3-18
3.6.3 Configuring Local SPAN Based on MAC Addresses.....	3-18
3.6.4 Checking the Configuration.....	3-19
3.7 Configuring RSPAN Based on MAC Addresses.....	3-19
3.7.1 Establishing the Configuration Task.....	3-19

3.7.2 Configuring RSPAN Based on MAC Addresses.....	3-20
3.7.3 Checking the Configuration.....	3-21
3.8 Canceling Mirroring Based on MAC Addresses.....	3-21
3.8.1 Establishing the Configuration Task.....	3-22
3.8.2 Canceling Mirroring Based on MAC Addresses.....	3-22
3.8.3 Checking the Configuration.....	3-22
3.9 Configuring Flow-based Local SPAN.....	3-23
3.9.1 Establishing the Configuration Task.....	3-23
3.9.2 Setting Traffic Classification Rules.....	3-23
3.9.3 Configuring Flow Mirroring.....	3-25
3.9.4 Creating and Applying a Traffic Policy.....	3-26
3.9.5 Checking the Configuration.....	3-26
3.10 Configuring Flow-based RSPAN.....	3-27
3.10.1 Establishing the Configuration Task.....	3-27
3.10.2 Setting Traffic Classification Rules.....	3-28
3.10.3 Configuring Flow-based RSPAN.....	3-28
3.10.4 Creating and Applying a Traffic Policy.....	3-29
3.10.5 Checking the Configuration.....	3-29
3.11 Canceling Flow Mirroring.....	3-30
3.11.1 Establishing the Configuration Task.....	3-30
3.11.2 Canceling Flow Mirroring.....	3-30
3.11.3 Checking the Configuration.....	3-31
3.12 Canceling an RSPAN VLAN.....	3-31
3.12.1 Establishing the Configuration Task.....	3-31
3.12.2 (Optional)Canceling an RSPAN VLAN.....	3-32
3.12.3 Verify the configuration.....	3-32
3.13 Changing or Deleting an Observing Interface.....	3-32
3.13.1 Establishing the Configuration Task.....	3-33
3.13.2 (Optional) Deleting an Observing Interface.....	3-33
3.13.3 (Optional) Changing an Observing Interface.....	3-33
3.13.4 Checking the Configuration.....	3-34
3.14 Configuring CPU Cache.....	3-34
3.14.1 Establishing the Configuration Task.....	3-34
3.14.2 (Optional) Setting an ACL Rule.....	3-35
3.14.3 Configuring CPU Cache.....	3-35
3.14.4 Checking the Configuration.....	3-35
3.15 Configuring CPU Mirroring.....	3-36
3.15.1 Establishing the Configuration Task.....	3-36
3.15.2 (Optional) Configuring an ACL Rule.....	3-37
3.15.3 Configuring an Observing Interface.....	3-37
3.15.4 Configuring CPU Mirroring.....	3-37
3.15.5 Checking the Configuration.....	3-38

3.16 Maintaining Mirroring.....	3-38
3.16.1 Clearing the Statistics on CPU Cache.....	3-38
3.17 Configuration Examples.....	3-39
3.17.1 Example for Configuring Interface-based Local SPAN.....	3-39
3.17.2 Example for Configuring VLAN-based Local SPAN.....	3-41
3.17.3 Example for Configuring Local SPAN Based on MAC Addresses.....	3-42
3.17.4 Example for Configuring Flow-based Local SPAN.....	3-44
3.17.5 Example for Configuring Interface-based RSPAN.....	3-47
3.17.6 Example for Configuring CPU Cache.....	3-51
3.17.7 Example for Changing an Observing Interface.....	3-53
4 Debugging and Diagnosis.....	4-1
4.1 Introduction.....	4-2
4.2 Debugging the S-switch.....	4-2
4.2.1 Precautions on Debugging the S-switch.....	4-2
4.2.2 Enabling Debugging.....	4-2
4.2.3 Disabling Debugging.....	4-2
4.2.4 Sending Debugging Information to the Console and VTY.....	4-3
4.3 Using the ping Command.....	4-3
4.3.1 Introduction.....	4-3
4.3.2 Usage of the ping Command.....	4-4
4.4 Running the tracert Command.....	4-4
4.4.1 Introduction to the tracert Command.....	4-5
4.4.2 Usage of the tracert Command.....	4-5
4.5 Maintaining the S-switch.....	4-6
4.6 Configuration Examples.....	4-6
4.6.1 Example for Running the ping Command and the tracert Command.....	4-6
5 Restarting and Resetting.....	5-1
5.1 Introduction.....	5-2
5.1.1 Process of Starting the S-switch.....	5-2
5.1.2 Process of Starting the BootROM.....	5-2
5.1.3 Logical Relationships Between Configuration Tasks.....	5-3
5.2 Restarting the S-switch Immediately.....	5-3
5.2.1 Restarting the S-switch Immediately Through Command Lines.....	5-4
5.2.2 Restarting the S-switch Through the Power Button on the S-switch.....	5-4
5.3 Restarting the S-switch at a Fixed Time.....	5-4
6 Auto-Config Configuration.....	6-1
6.1 Introduction.....	6-2
6.1.1 Auto-Config Overview.....	6-2
6.1.2 Auto-Config Supported by the S-switch.....	6-2
6.1.3 Logical Relationships Between Configuration Tasks.....	6-2
6.1.4 History.....	6-2

6.2 Specifying the Configuration File for the Next Startup.....6-2

6.2.1 Establishing the Configuration Task.....6-3

6.2.2 Enabling Auto-Config.....6-3

6.2.3 Deleting the Configuration File for the Next Startup.....6-3

6.2.4 Restarting the S-switch.....6-4

6.2.5 Checking the Configuration.....6-4

Figures

Figure 2-1 Function of the information center.....	2-2
Figure 2-2 Networking of sending logs to the log host.....	2-13
Figure 3-1 Schematic diagram of interface mirroring.....	3-4
Figure 3-2 Schematic diagram of flow mirroring.....	3-4
Figure 3-3 Schematic diagram of RSPAN.....	3-5
Figure 3-4 Networking diagram of interface-based local SPAN.....	3-39
Figure 3-5 Networking diagram of VLAN-based local SPAN.....	3-41
Figure 3-6 Networking diagram of local SPAN based on MAC addresses.....	3-43
Figure 3-7 Networking diagram of flow-based local SPAN.....	3-45
Figure 3-8 Networking diagram of interface-based RSPAN.....	3-48
Figure 3-9 Networking for configuring CPU cache.....	3-52
Figure 3-10 Networking for changing the observing interface.....	3-54
Figure 4-1 Principle of the ping command.....	4-4
Figure 4-2 Format of ICMP echo request and echo reply packets.....	4-4
Figure 4-3 Principle of the trace route command.....	4-5
Figure 4-4 Networking diagram of running the ping command and the tracert command.....	4-7
Figure 5-1 Process of starting the S-switch.....	5-2

Tables

Table 1-1 Names and descriptions of alarms.....1-4

Table 1-2 Description of metacharacters.....1-6

Table 1-3 Description of the **display** commands that can use the regular expression.....1-7

Table 2-1 Severity levels of information.....2-3

Table 2-2 Information channels and output directions.....2-4

Table 2-3 Format of a log.....2-5

Table 2-4 Module name list.....2-5

About This Document

Purpose

This document describes procedures and provides examples for configuring the Device Management features of the S-switch.

This document covers the following topics:

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

This document guides you through the configuration and applicable environment of the Device Management 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 monitoring engineers
- System maintenance engineers

Organization





This document is organized as follows.


Chapter	Description
1 Checking the Status of the S-switch	This chapter describes the function and usage of the display command and regular expression.
2 Monitoring the Device Through the Information Center	This chapter describes the basics of the information center, and provides the configuration procedures and examples for the information center.
3 Mirroring	This chapter describes the principle of mirroring, and the procedures for configuring interface mirroring and flow mirroring.
4 Debugging and Diagnosis	This chapter describes the basics of debugging, and the common commands for fault diagnosis.
5 Restarting and Resetting	This chapter introduces the basics of the BootROM software and the Versatile Routing Platform (VRP) system software, and describes how to restart the S-switch.
6 Auto-Config Configuration	This chapter describes basic concepts and configuration procedures of Auto-Config.

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.
 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.

Symbol	Description
 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 italics.
Courier New	Terminal display is in Courier New. The messages input on terminals by users that are displayed are in boldface.

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 ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, 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

Format	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, A means the two keys should be pressed in turn.

Mouse Operation

Action	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 versions 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 Checking the Status of the S-switch

About This Chapter

This chapter describes the function and usage of the **display** commands and the regular expression.

[1.1 Introduction](#)

This section describes the function of the **display** commands in checking the status of the device.

[1.2 Checking the Status of the S-switch](#)

This section describes how to check the status of the S-switch by using the **display** commands.

[1.3 Using the Regular Expression](#)

This section describes the principle, concept, and usage of the regular expression.

1.1 Introduction

This section describes the function of the **display** commands in checking the status of the device.

1.2 Checking the Status of the S-switch

This section describes how to check the status of the S-switch by using the **display** commands.

[1.2.1 Checking Information About the S-switch](#)

[1.2.2 Checking the Version of the S-switch](#)

[1.2.3 Checking the Electronic Labels](#)

[1.2.4 Checking Temperature](#)

[1.2.5 Checking the CPU Usage](#)

[1.2.6 Checking the Memory Usage](#)

[1.2.7 Checking Alarms](#)

[1.2.8 Checking the Status of an Interface](#)

1.2.1 Checking Information About the S-switch

Context

You can run the **display** command in any view to check information about the S-switch. *slot-id* can be specified to check information about the components in a specified slot.

The displayed information includes the type of the device, startup time, startup mode, CPU frequency, size of the memory, size of the flash memory, and types and status of the cards in all slots.

Do as follows on the S-switch.

Procedure

Run the **display device** [*slot-id*] command to check information about the S-switch.

----End

1.2.2 Checking the Version of the S-switch

Context

You can run the **display version** command in any view to check the version of the S-switch. *slot-id* can be specified to check the version of the card in a specified slot.

The displayed information includes the type of the card, startup time, version of the hardware, and version of the software.

Do as follows on the S-switch.

Procedure

Run the **display version** [*slot-id*] command to check the version of the card.

----End

1.2.3 Checking the Electronic Labels

Context

You can run the **display elabel** command in any view to check the electronic labels. *slot-id* can be specified to check information about the label of the card in a specified slot.

You can run the **display elabel** command to check information about the hardware code. The hardware code provides necessary basis for such services as network installation, network upgrade, network expansion, device management and maintenance, and device replacement in batches.

The displayed information includes: type of the card, bar code, Bill of Material (BOM) code, English description, production date, supplier name, issuing number, Common Language Equipment Identification (CLEI) code, and sales BOM code.

Do as follows on the S-switch.

Procedure

Run the **display elabel** [*slot-id*] command to check the electronic labels.

----End

1.2.4 Checking Temperature

Context

You can run the command in any view to check the current working temperature of the S-switch.

You can run the **temperature threshold** command to set alarm temperature threshold for the Switch Control Unit or temperature-sensing Service Interface Card (SIC). For details on the procedure, refer to the *Quidway S5300 Series Ethernet Switches - Command Reference*.

Do as follows on the S-switch.

Procedure

Run the **display environment** command to check the temperature of the S-switch.

----End

1.2.5 Checking the CPU Usage

Context

Do as follows on the S-switch.

Procedure

Run the **display cpu-usage key-task** command to check the statistics about the CPU usage.

----End

1.2.6 Checking the Memory Usage

Context

Do as follows on the S-switch.

Procedure

Run the **display memory-usage [slot slot-id]** command to check the statistics of the CPU usage.

You can run the command in any view to check the statistics of the memory usage of the S-switch.

----End

1.2.7 Checking Alarms

Context

[Table 1-1](#) shows details of the alarms.

Table 1-1 Names and descriptions of alarms

Item	Description
Action	Indicates hot switchover.
Cause	Indicates the cause of hot switchover.
Date	Indicates the date of an alarm.
Time	Indicates the time of an alarm.
Action	Indicates the installation or removal of an SIC.
Slot	Indicates the number of the slot in which an SIC is installed or removed.
Date	Indicates the date of installing or removing of an SIC.

Item	Description
Time	Indicates the time of installing or removing of an SIC.
CardType	Indicates the type of an SIC.
Alarm	Indicates the type of an alarm.
Slot	Indicates the slot number of the card on which an alarm is generated.
Date	Indicates the date of an alarm.
Time	Indicates the time of an alarm.
Location	Indicates the location of an alarm.

Procedure

Run the **display alarm urgent** [**slot** *slot-id* | **time** *interval*] command to check alarms during the operation of the device.

You can run the command in any view to check alarms on the S-switch. Alarms can be classified into alarms of hot backup or restart, alarms of hot swap of SICs, and other alarms.

----End

1.2.8 Checking the Status of an Interface

Checking the Status of a Specified Interface

Do as follows on the S-switch.

1. Run the **display interface** *interface-type interface-number* command to check the status of a specified interface.

Information about the status of an interface contains the running status, basic configuration of the interface, and statistics of the transmission of packets.

Checking the Status of an Interface in the Current Interface View

Do as follows on the S-switch.

1. Run the **system-view** command to enter the system view.
2. Run the **interface** *interface-type interface-number* command to enter the interface view.
3. Run the **display this interface** command to check the status of the interface in the current interface view.

1.3 Using the Regular Expression

This section describes the principle, concept, and usage of the regular expression.

[1.3.1 Introduction](#)[1.3.2 Usage of the Regular Expression](#)[1.3.3 Examples for Using the Regular Expression](#)

1.3.1 Introduction

The regular expression specifies a rule of information matching. You can use the regular expression to match the targets and filter information to be displayed when a batch of information is ready for displaying.

To set up matching rules more flexibly, you can use metacharacters with special meanings in the regular expression. [Table 1-2](#) lists the metacharacters in common use.

Table 1-2 Description of metacharacters

Metacharacter	Description
\	Indicates an escape character.
.	Matches any single character except "\n", including spaces.
*	The character before it appears 0 times or multiple consecutive times in the target.
+	The character before it appears once or multiple consecutive times in the target.
	The characters to the left and right of it are in "or" relationship.
^	The characters after it must appear at the beginning of the target.
\$	The characters before it must appear at the end of the target.
[xyz]	Matches any character in the square bracket.
[^xyz]	Matches any character except those in the square brackets. The "^" is before the characters.
[a-z]	Matches any character within the specified range.
[^a-z]	Matches any character out of the specified range.
{n}	The "n" is a non-negative integer. It matches the "n" times of the consecutive appearing.
{n,}	The "n" is a non-negative integer. It matches at least "n" times of the consecutive appearing.
{n,m}	The "m" and "n" are both non-negative integers, and the "n" is equal to or smaller than the "m". Matches the times ranging from "n" to "m" of the consecutive appearing. Note that there is no space between "n" and comma, and between comma and "m".

1.3.2 Usage of the Regular Expression

Specifying the Filtering Mode Through Commands

The regular expression is used in the **display** commands listed in [Table 1-3](#) to filter the information to be displayed. For details on the commands, refer to the *Quidway S5300 Series Ethernet Switches - Command Reference*.

Table 1-3 Description of the **display** commands that can use the regular expression

Command	Description
display arp [dynamic static] [{ begin exclude include } <i>regular-expression</i>]	The display arp command checks the Address Resolution Protocol (ARP) mapping table.
display current-configuration [{ begin exclude include } <i>regular-expression</i>]	Run the display current-configuration command to check configuration parameters in effect.
display current-configuration configuration [<i>configuration-type</i>] [{ begin exclude include } <i>regular-expression</i>]	
display current-configuration interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]	
display interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]	Run the display interface command to check running status of the interface, basic configuration of the interface, and statistics of the transmission of packets.
display logbuffer [level <i>severity</i> size <i>size</i>] * [{ exclude include } <i>regular-expression</i>]	Run the display logbuffer command to check information recorded in the log buffer.

To filter the terminal display of the **display** commands, you can choose one of the three modes:

- **begin**: displays all of the lines beginning with the character string that matches the specified regular-expression.
- **exclude**: displays all of the lines with the character string that does not match the specified regular-expression.
- **include**: displays all of the lines with the character string that matches the specified regular-expression.

Specifying Filtering Mode on a Split Screen

If a lot of information is displayed on a split screen, you can enter the following escape characters and the corresponding character strings when "---- More ----" is prompted.

- **"/**: functions the same as **begin**.
- **"-**: functions the same as **exclude**.
- **"+**: functions the same as **include**.

For example, when running the **display** command to check the current configuration, you can display all the lines that match the keyword **interface**.

```
<Quidway> display current-configuration
#
 sysname Quidway
#
 vlan batch 1 3
#
 cluster enable
 ntdp enable
 ndp enable
#
  lsp-trigger host
#
 interface Vlanif1
#
 interface Vlanif3
  ip address 1.1.1.3 255.255.255.0
  arp expire-time 60
#
 interface Ethernet0/0/1
#
 interface Ethernet0/0/2
#
 interface Ethernet0/0/3
  port default vlan 3
  ---- More ----
```

When "---- More ----" is prompted, enter + and **interface**.

+interface

Then click **Enter**, and the terminal displays the following information:

```
Filtering...
interface LoopBack0
user-interface con 0
user-interface vty 0 4
<Quidway>
#
 sysname Quidway
#
 vlan batch 1
#
 traffic classifier a
  if-match l2-protocol mpls
#
 interface Vlanif1
  ip address 192.168.32.15 255.255.0.0
#
 interface Ethernet0/0/1
  port default vlan 1
#
 interface Ethernet0/0/2
#
 interface Ethernet0/0/3
#
 interface Ethernet0/0/4
#
 interface Ethernet0/0/5
#
 interface Ethernet0/0/6
  ---- More ----
```

When "---- More ----" is prompted, enter + and **interface**.

+interface

Then click **Enter**, and the terminal displays as follows:

```
Filtering...
interface LoopBack0
user-interface con 0
user-interface vty 0 4
<Quidway>
#
 sysname Quidway
#
 vlan batch 1
#
 traffic classifier a
  if-match l2-protocol mpls
#
 interface Vlanif1
  ip address 192.168.32.15 255.255.0.0
#
 interface Ethernet0/0/1
  port default vlan 1
#
 interface Ethernet0/0/2
#
 interface Ethernet0/0/3
#
 interface Ethernet0/0/4
#
 interface Ethernet0/0/5
#
 interface Ethernet0/0/6
---- More ----
```

1.3.3 Examples for Using the Regular Expression

Checking the Current Configuration

Run the **display current-configuration** command to check the current configuration.

```
<Quidway> display current-configuration
```

Example for begin

Check the configurations beginning with "aaa".

```
<Quidway> display current-configuration | begin aaa
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
 user-interface maximum-vty 15
 user-interface con 0
 user-interface vty 0 14
 authentication-mode none
 user privilege level 15
#
return
```

Example for include

Check all the configurations that matches "aaa".

```
<Quidway> display current-configuration | include aaa
aaa
authentication-scheme default
#
authorization-scheme default
#
accounting-scheme default
#
domain default
#
#
user-interface maximum-vty 15
user-interface con 0
user-interface vty 0 14
authentication-mode none
user privilege level 15
#
return
```

Example for exclude

Check all the configuration that does not match "interface".

```
<Quidway> display current-configuration | exclude interface
#
 sysname Quidway
#
 vlan batch 1
#
 traffic classifier a
 if-match l2-protocol mpls
#
 ip address 192.168.32.15 255.255.0.0
#
 port default vlan 1
#
 negotiation auto
#
 negotiation auto
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
 authentication-mode none
 user privilege level 15
#
return
```

Example for a Single Metacharacter

Use the metacharacter "|" to check all the lines of the configuration that matches "interface" and "vlan".

```
<Quidway> display current-configuration | include interface | vlan
vlan batch 1
interface Vlanif1
interface Ethernet0/0/1
 port default vlan 1
interface Ethernet0/0/2
interface Ethernet0/0/3
interface Ethernet0/0/4
```

```
interface Ethernet0/0/5
interface Ethernet0/0/6
interface Ethernet0/0/7
interface Ethernet0/0/8
interface Ethernet0/0/9
interface Ethernet0/0/10
interface Ethernet0/0/11
interface Ethernet0/0/12
interface Ethernet0/0/13
interface Ethernet0/0/14
interface Ethernet0/0/15
interface Ethernet0/0/16
interface Ethernet0/0/17
interface Ethernet0/0/18
interface Ethernet0/0/19
interface Ethernet0/0/20
interface Ethernet0/0/21
interface Ethernet0/0/22
interface Ethernet0/0/23
interface Ethernet0/0/24
interface GigabitEthernet0/0/1
interface GigabitEthernet0/0/2
interface GigabitEthernet0/0/3
interface GigabitEthernet0/0/4
interface NULL0
interface LoopBack1
user-interface maximum-vty 15
user-interface con 0
user-interface vty 0 14
```

Example for Multiple Metacharacters

Use the metacharacter "|" and "\$" to check all the lines of the configuration that matches "interface" and ends with "default".

```
<Quidway> display current-configuration | include interface | default$
interface Vlanif1
interface Vlanif2
interface Ethernet0/0/1
interface Ethernet0/0/2
interface Ethernet0/0/3
interface Ethernet0/0/4
interface Ethernet0/0/5
interface Ethernet0/0/6
interface Ethernet0/0/7
interface Ethernet0/0/8
interface Ethernet0/0/9
interface Ethernet0/0/10
interface Ethernet0/0/11
interface Ethernet0/0/12
interface Ethernet0/0/13
interface Ethernet0/0/14
interface Ethernet0/0/15
interface Ethernet0/0/16
interface Ethernet0/0/17
interface Ethernet0/0/18
interface Ethernet0/0/19
interface Ethernet0/0/20
interface Ethernet0/0/21
interface Ethernet0/0/22
interface Ethernet0/0/23
interface Ethernet0/0/24
interface GigabitEthernet0/0/1
interface GigabitEthernet0/0/2
interface NULL0
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
```

```
user-interface maximum-vty 15
user-interface con 0
user-interface aux 0
user-interface vty 0 14
```

2 Monitoring the Device Through the Information Center

About This Chapter

This chapter describes the basics of the information center, introduces the procedure for managing the information center and monitoring the device, and provides configuration examples.

[2.1 Introduction](#)

This section describes the basic principle and concepts of the information center.

[2.2 Configuring the Information Center](#)

This section describes how to manage and configure the information center.

[2.3 Sending Information of the Information Center](#)

This section describes how to send information to the specified direction.

[2.4 Maintaining the Information Center](#)

This section describes how to clear the statistics.

[2.5 Configuration Examples](#)

This section provides examples for configuring the information center.

2.1 Introduction

This section describes the basic principle and concepts of the information center.

2.1.1 Functions of the Information Center

2.1.2 Types of Information

2.1.3 Severity Levels of Information

2.1.4 Information Channels and Output Directions

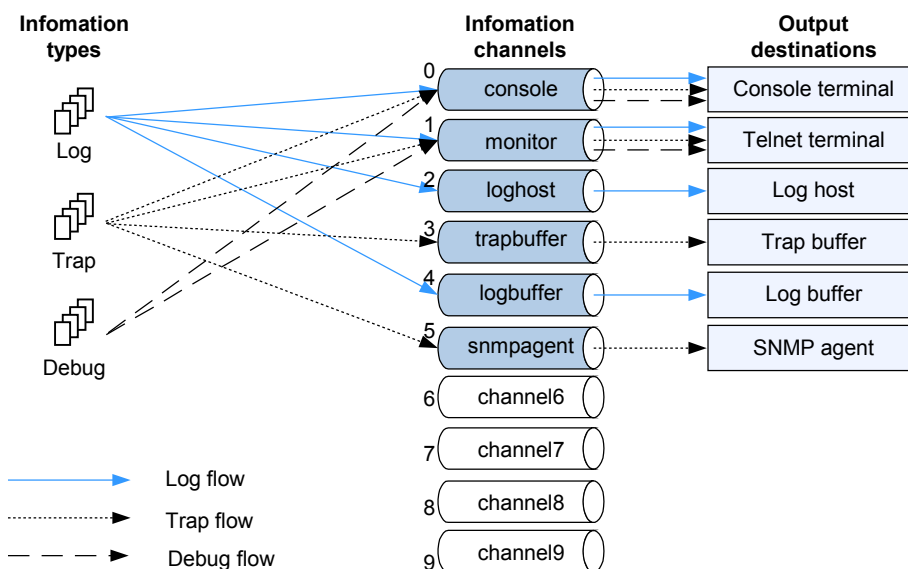
2.1.5 Format of a Log

2.1.1 Functions of the Information Center

The information center on the S-switch collects and classifies debugging information, logs, and traps sent by the functional modules. Thus, it facilitates information filtering.

The information center sends the module information of different configurations and severity levels to different channels. Then the information center releases information on the basis of the information channels and the output direction. **Figure 2-1** shows how the information center works.

Figure 2-1 Function of the information center



2.1.2 Types of Information

The information center can receive and process the following types of information:

- Debugging information
- Logs

- Traps

2.1.3 Severity Levels of Information

Information is classified into eight levels on the basis of its severity or emergency degree. The severer the information, the smaller the severity threshold. [Table 2-1](#) shows the detailed information.

Table 2-1 Severity levels of information

Severity Level	Name	Description
1	Emergency	A fatal fault occurs in the device so that the system fails to run normally and the device must be restarted. For example, the device is restarted because of abnormal programs, or the memory is detected faulty.
2	Alert	A grave fault occurs in the device, which requires urgent response. For example, the memory usage of the device reaches utmost.
3	Critical	A grave fault occurs in the device so that measures are taken to analyze or process it. The following situations belong to this category: The memory usage is lower than the lower limit; the temperature is lower than the alarming limit; Bidirectional Forwarding Detection (BFD) detects that the device is unreachable or faults generated by the device itself occur.
4	Error	Improper operation or abnormal process of the device, which does not inflict heavy losses on the follow-up services, is still worth intense attention and in-depth analysis. For example, the user enters incorrect instructions or passwords, or the error protocol packets received by other devices are detected.
5	Warning	The abnormal running of the device and the process likely to incur service interruption require full attention. This category contains the following situations: Users disable the routing process; BFD detects that packet loss occurs; error protocol packets are detected.
6	Notice	The information, which is key to operations, supports the normal running of the device. For example, users run the shutdown command on the interface. The neighbor discovery and the normal state change of the protocol state machine are also included.
7	informational	The operation information, which is of common usage, assists the normal running of the device. For example, users run the display command.
8	Debugging	The information, which displays the normal running of the device, requires no attention.

The information is filtered in terms of its severity. Only the information, whose severity level is equal to or lower than the configured threshold, can be output. In other words, only the information severer than the configured threshold can be output. For example, if the severity level threshold is configured 6, only the information whose severity level ranges from 1 to 6 can be output.

2.1.4 Information Channels and Output Directions

The information center supports up to 10 channels. By default, channels from 0 to 5 are labeled channel names, and the six information channels are respectively related to six output directions. **Table 2-2** shows the information channels and the output directions that the information center supports.

Table 2-2 Information channels and output directions

Channel No.	Default Channel Name	Default Output Direction	Description
0	console	console	Local console that receives logs, traps, and debugging information
1	monitor	monitor	Virtual Type Terminal (VTY) that receives logs, traps, and debugging information
2	loghost	loghost	Log host that receives logs
3	trapbuffer	trapbuffer	Trap buffer that receives traps
4	logbuffer	logbuffer	Log buffer that receives logs
5	snmpagent	snmpagent	Simple Network Management Protocol (SNMP) agent that receives traps
6	channel6	Unspecified	Reserved
7	channel7	Unspecified	Reserved
8	channel8	Unspecified	Reserved
9	channel9	Unspecified	Reserved

Information is sent to corresponding directions through specified channels. Users can change the information channel names or the corresponding relationship between the information channels and the output directions as required.

2.1.5 Format of a Log

The format of a log is as follows:

- Packet format:
`%timestamp sysname %%version module/level/descriptor digest:content`

Table 2-3 describes each field of a log in detail.

Table 2-3 Format of a log

Field Type	Description
Timestamp	Identifies the time at which a log is sent. It is expressed in the format "Mmm dd yyyy hh:mm:ss". <ul style="list-style-type: none"> • "Mmm" is the abbreviation of the month. It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec. • "dd" refers to the date. If the value is less than 10, one space should be kept before the value, for instance, " 7". • "yyyy" indicates the year. • "hh:mm:ss" refers to the local time. The value of "hh" ranges from 00 to 23. The values of both "mm" and "ss" range from 00 to 59.
Host name	Indicates the system name of the S-switch.
Module name	The software system of the S-switch consists of the protocol modules, the board driver, and the configuration modules. The module name identifies the module that generates the log. Table 2-4 shows the details on modules.
Level	Logs are classified into eight severity levels as shown in Table 2-1 .
Brief	Summaries a message in a phrase.
Log type	There are three types of logs, that is, d, l, t3, indicating debugging information, logs, and traps respectively.
Content	Indicates details of a log.

Table 2-4 lists the modules that the S-switch supports.

Table 2-4 Module name list

Module name	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List

Module name	Description
ACM	Access Control Module
ARP	Address Resolution Protocol
CFM	Configuration File Management
CHAT	Script configuration module of the modem
CMD	Command lines
L2IF	Layer 2 interface module of the S-switch
RRPP	Rapid Ring Protection Protocol (RRPP) module of the S-switch
DRV	Drive modules of cards
ENTEXT	Entity Extended Management Information Base (MIB)
ENTMIB	Entity MIB
ETH	Ethernet
FIB	Forwarding Information Base
FTPS	File Transfer Protocol (FTP) server
HGMP	Huawei Group Management Protocol
HWCM	Huawei Configuration Management
IFNET	Interface management
IP	Internet Protocol
IPC	Inter-Process Communication
L2IF	Layer 2 interface
MBUF	Memory Buffer
MCAST	Multicast
MEM	Memory Management
MODEM	Modulator-Demodulator
MSTP	Multi-Spanning Tree Protocol
QOS	Quality of Service
RDS	Module of Remote Authentication Dial In User Service
RMON	Remote Monitor
RRPP	Rapid Ring Protection Protocol
RSA	Revest-Shamir-Adleman Algorithm

Module name	Description
SHELL	User Interface
SNMP	Simple Network Management Protocol
SNPG	Internet Group Management Protocol (IGMP) Snooping
SOCKET	Socket
SRM	System Resource Management
SSH	Secure Shell
SYSMIB	System Management Information Base
TAC	Huawei Terminal Access Controller Access Control System
TELNET	Telnet module
TNLM	Tunnel management
TRUNK	Trunk interface
TUNNEL	Tunnel
UCM	User Control Management
VFS	Virtual File System
VLAN	Virtual Local Area Network
VOS	Virtual Operating System
VTY	Virtual Type Terminal

2.2 Configuring the Information Center

This section describes how to manage and configure the information center.

[2.2.1 Establishing the Configuration Task](#)

[2.2.2 Enabling the Information Center](#)

[2.2.3 \(Optional\) Naming the Information Channel](#)

[2.2.4 Defining the Information Channel](#)

[2.2.5 \(Optional\) Configuring the Timestamp for the Output Information](#)

[2.2.6 Checking the Configuration](#)

2.2.1 Establishing the Configuration Task

Applicable Environment

To collect debugging information, logs, and traps during the operation of the S-switch, and to send them to the terminal for display, or to the buffer or the host for storage, you need to configure the information center.

Pre-configuration Tasks

None.

Data Preparation

To manage the information center, you need the following data.

No.	Data
1	(Optional) Numbers and names of the information channels
2	(Optional) Format of the timestamp
3	(Optional) Severity level
4	(Optional) Language used in the logs and the address of the log host
5	(Optional) Size of the log buffer and the trap buffer

2.2.2 Enabling the Information Center

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 **info-center enable** command to enable the information center.



NOTE

The system sends the system information to the log host and the console only after the information center is enabled.

----End

2.2.3 (Optional) Naming the Information Channel

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 **info-center channel** *channel-number* **name** *channel-name* command to name the channels for sending debugging information, logs, and traps.
- End

2.2.4 Defining the Information Channel

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 **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **debug** | **log** | **trap** } { **state** { **off** | **on** } | **level** *severity* } *] command to specify a certain module or all modules to send debugging information, logs, or traps to the information channels.



NOTE

Run the **undo info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } command to disable the unnecessary modules and select one or more modules to send information to the information channels.

----End

2.2.5 (Optional) Configuring the Timestamp for the Output Information

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 **info-center timestamp** { **debugging** | **log** | **trap** } { **boot** | **date** | **none** | **short-date** } command to configure the format of the timestamp for sending debugging information, logs, or traps.
- End

2.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the configuration of the channel.	display channel [<i>channel-number</i> <i>channel-name</i>]
Check the information recorded by the information center.	display info-center [<i>statistics</i>]
Check the information in the log buffer of the memory.	display logbuffer [<i>level severity</i> <i>size value</i>]*[{ <i>exclude</i> <i>include</i> } <i>regular-expression</i>]
Check the summary of the information in the log buffer.	display logbuffer summary [<i>level severity</i>]
Check the information in the log buffer of Non-Volatile Random Access Memory (NVRAM).	display logbuffer permanent [<i>slave</i>]
Check the information in the trap buffer.	display trapbuffer [<i>size size</i>]

2.3 Sending Information of the Information Center

This section describes how to send information to the specified direction.

[2.3.1 Sending Information to the Console](#)

[2.3.2 Sending Information to the Telnet Terminal](#)

[2.3.3 Sending Information to the SNMP Agent](#)

[2.3.4 Sending Information to the Log Buffer](#)

[2.3.5 Sending Information to the Trap Buffer](#)

[2.3.6 Sending Information to the Log Host](#)

[2.3.7 Checking the Configuration](#)

2.3.1 Sending Information to the Console

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 **info-center console channel** { *channel-number* | *channel-name* } command to send information to the console.
- Step 3** Run the **quit** command to return to the user view.

Step 4 Run the **terminal monitor** command to enable the terminal display. By default, this function is enabled.

Step 5 Run the **terminal { debugging | logging | trapping }** command to enable the terminal to display debugging information, logs, and traps.



NOTE

Step 4 and **Step 5** are not listed in sequence.

----End

2.3.2 Sending Information to the Telnet Terminal

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 **info-center monitor channel { channel-number | channel-name }** command to send information to the telnet terminal.

Step 3 Run the **quit** command to return to the user view.

Step 4 Run the **terminal monitor** command to enable the terminal to display information.

Step 5 Run the **terminal { debugging | logging | trapping }** command to enable the terminal to display debugging information, logs, and traps.



NOTE

Step 4 and **Step 5** are not listed in sequence.

----End

2.3.3 Sending Information to the SNMP Agent

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 **info-center snmp channel { channel-number | channel-name }** command to send information to the SNMP agent.

Step 3 Run the **snmp-agent** command to enable the SNMP agent.

For details on configuring the SNMP agent, refer to the chapter "SNMP Configuration" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Network Management*.

----End

2.3.4 Sending Information to the Log Buffer

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 **info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffer-size*] * command to send information to the log buffer.
- End

2.3.5 Sending Information to the Trap Buffer

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 **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffer-size*] * command to send information to the trap buffer.
- End

2.3.6 Sending Information to the Log Host

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 **info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] * command to send information to the log host.
- Step 3** Run the **info-center loghost source** *interface-type interface-number* command to specify the source address for sending logs.
- End

2.3.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check statistics in the information center.	display info-center statistics

Run the preceding command. If the information center can send the statistics to the destination terminal, it means that the configuration succeeds.

2.4 Maintaining the Information Center

This section describes how to clear the statistics.



CAUTION

Statistics cannot be restored after being cleared. So, confirm the action before you run the command.

Action	Command
Clear the statistics in the information center.	reset info-center statistics
Clear the information in the log buffer.	reset logbuffer [permanent [slave]]
Clear the information in the trap buffer.	reset trapbuffer

2.5 Configuration Examples

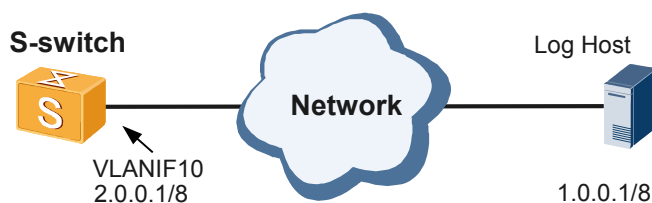
This section provides examples for configuring the information center.

2.5.1 Example for Configuring the Information Center

2.5.1 Example for Configuring the Information Center

Networking Requirements

Figure 2-2 Networking of sending logs to the log host



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the information center.
2. Configure the information channel to ensure that the S-switch can correctly send logs to the log host. Disable the sending of the traps and debugging information to the log host.
3. Configure the log host.

Data Preparation

To complete the configuration, you need the following data:

- The IP address of the log host is specified as 1.0.0.1/8.

Configuration Procedure

NOTE

In the example, only the commands related to monitoring are listed. For details on configuring the log host, see the help files on the log host.

1. Enable the information center.

Enable the information center. By default, the information center on the S-switch is enabled.

```
<Quidway> system-view
[Quidway] info-center enable
Info:Information center is enabled
```

2. Configure the information channel.

Send logs of severity levels 1 to 8 from all modules on the S-switch through the channel to the log host. Disable the sending of the debugging information and traps through the channel to the log host.

```
[Quidway] info-center source default channel loghost log level debugging state
on trap state off debug state off
```

Verify the configuration.

```
[Quidway] display channel loghost
channel number:2, channel name:loghost
MODU ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default   Y       debugging    N       debugging    N       debugging
```

3. Configure the log host.

Set the IP address of the log host to 1.0.0.1.

```
[Quidway] info-center loghost 1.0.0.1
```

Set VLANIF 10 as the interface for sending information to the log host on the S-switch.

```
[Quidway] vlan 10
[Quidway-vlan10] port ethernet 0/0/1
[Quidway-vlan10] quit
[Quidway] interface vlanif 10
[Quidway-vlanif10] ip address 2.0.0.1 255.0.0.0
[Quidway-vlanif10] quit
[Quidway] info-center loghost source vlanif 10
```

Verify the configuration.

```
[Quidway] display info-center
Information Center:enabled
Log host:
```

```
the interface name of the source address:vlanif 10
1.0.0.1, channel number 2, channel name loghost,
language english , host facility local7

Console:
channel number : 0, channel name : console
Monitor:
channel number : 1, channel name : monitor
SNMP Agent:
channel number : 5, channel name : snmpagent
Log buffer:
enabled,max buffer size 1024, current buffer size 512,
current messages 440, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 0
Trap buffer:
enabled,max buffer size 1024, current buffer size 256,
current messages 1, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
Information timestamp setting:
log - date, trap - date, debug - boot

Sent messages = 499, Received messages = 499

IO Reg messages = 0 IO Sent messages = 0
```

4. Enable the terminal display of the console.

Enable the terminal display of the console. Enable the corresponding terminal display to check the information type as required.

```
[Quidway] info-center console channel 0
[Quidway] quit
<Quidway> terminal monitor
Info:Current terminal monitor is on
<Quidway> terminal logging
Info:Current terminal logging is on
```

Configuration Files

```
#
info-center source default channel 2 log level debugging trap state off
info-center loghost source vlanif 10
info-center loghost 1.0.0.1
#
#
vlan batch 10
#
interface vlanif10
ip address 2.0.0.1 255.0.0.0
#
interface Ethernet0/0/1
port default vlan 10
#
return
```


3 Mirroring

About This Chapter

This chapter describes the principle of mirroring, and the procedures for configuring mirroring.

[3.1 Introduction](#)

This section describes the basics of mirroring.

[3.2 Configuring Interface-based Local SPAN](#)

This section describes how to configure interface-based local SPAN.

[3.3 Configuring Interface-based RSPAN](#)

This section describes how to configure interface-based RSPAN.

[3.4 Canceling Interface Mirroring](#)

This section describes how to cancel interface mirroring.

[3.5 Configuring VLAN-based RSPAN](#)

[3.6 Checking the Configuration](#)

[3.7 Configuring RSPAN Based on MAC Addresses](#)

This section describes how to configure RSPAN based on MAC addresses.

[3.8 Canceling Mirroring Based on MAC Addresses](#)

This section describes how to cancel mirroring based on MAC addresses.

[3.9 Configuring Flow-based Local SPAN](#)

This section describes how to configure flow-based local SPAN.

[3.10 Configuring Flow-based RSPAN](#)

This section describes how to configure flow-based RSPAN.

[3.11 Canceling Flow Mirroring](#)

This section describes how to cancel flow mirroring.

[3.12 Canceling an RSPAN VLAN](#)

This section describes how to cancel an RSPAN VLAN.

[3.13 Changing or Deleting an Observing Interface](#)

This section describes how to change or delete an observing interface.

[3.14 Configuring CPU Cache](#)

This section describes how to configure CPU cache.

[3.15 Configuring CPU Mirroring](#)

This section describes how to configure CPU mirroring.

[3.16 Maintaining Mirroring](#)

This section describes how to clear the statistics.

[3.17 Configuration Examples](#)

This section provides several configuration examples for mirroring.

3.1 Introduction

This section describes the basics of mirroring.

3.1.1 Mirroring Functions

3.1.2 Logical Relationships Between Configuration Tasks

3.1.3 Specifications

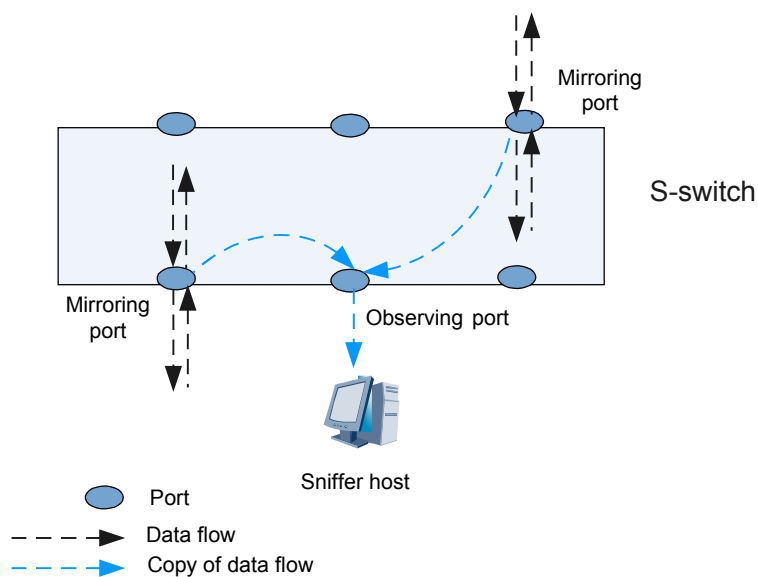
3.1.1 Mirroring Functions

Concepts

- Observing interface
An observing interface on the S-switch is connected to a monitoring host. It is used to export the traffic copied from a mirroring interface or a flow mirroring interface.
- Mirroring interface
A mirroring interface is the interface to be observed. Incoming traffic or outgoing traffic passing through a mirroring interface is copied to an observing interface.
- Flow mirroring interface
A flow mirroring interface is an interface to which traffic policies are applied. On such an interface, the incoming traffic that matches the traffic classifier in the traffic policy is copied to an observing interface.
- Mirroring flow
A mirroring flow is a flow that runs to a flow mirroring interface and is observed. When a flow becomes a mirroring flow, it is copied and sent to an observing interface.
- Mirroring VLAN
A mirroring VLAN is a VLAN to be observed. Incoming traffic or outgoing traffic passing through a mirroring VLAN is copied to an observing interface.
- MAC address of the packet to be mirrored
An MAC address of the packet to be mirrored is the source or destination MAC address of the packet to be mirrored. The S-switch copies the traffic matching this MAC address to an observing interface.
- RSPAN VLAN
An RSPAN VLAN is a Remote Switched Port Analyzer (RSPAN) VLAN. When the interface receiving mirroring packets is not located on the same S-switch as an observing interface, the S-switch broadcasts the mirroring packets if these mirroring packets need to pass through the RSPAN VLAN.

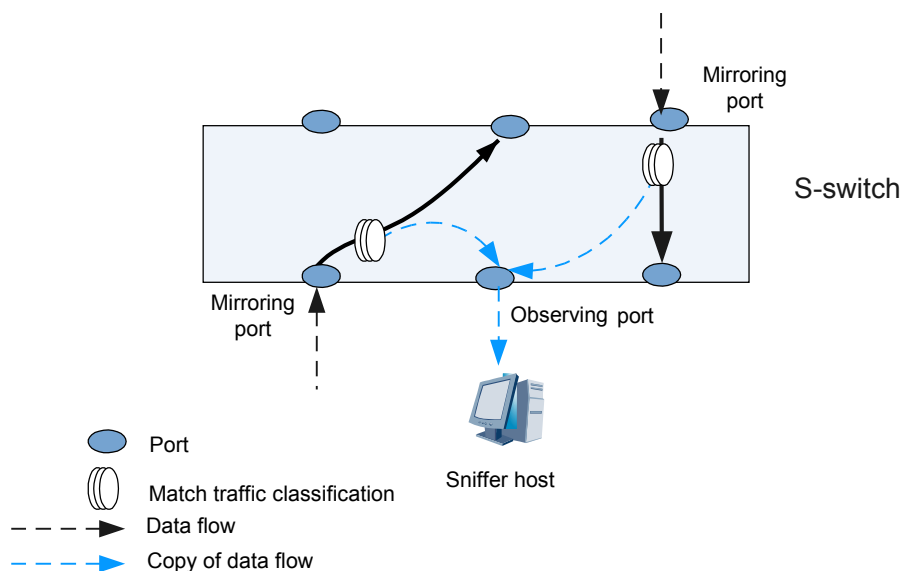
Interface Mirroring

In the process of interface mirroring, the S-switch copies the packets passing through a mirroring interface and then sends the copy to a specified observing interface. **Figure 3-1** shows the diagram of interface mirroring.

Figure 3-1 Schematic diagram of interface mirroring

Flow Mirroring

In the process of flow mirroring, the S-switch copies the mirroring flow passing one or more interfaces and sends the copy to an observing interface. **Figure 3-2** shows the diagram of flow mirroring.

Figure 3-2 Schematic diagram of flow mirroring

Flow mirroring is a type of action in traffic behaviors. When a traffic policy configured with flow mirroring is applied to an interface, the S-switch copies the incoming data flow on this interface that matches the traffic classifier and sends the copy to the observing interface.

VLAN Mirroring

In the process of VLAN mirroring, the S-switch mirrors the packets passing through all active interfaces in a specified VLAN to a specified observing interface. After VLAN mirroring is configured, all the packets received by all interfaces on the S-switch are mirrored to the observing interface. Compared with interface mirroring, VLAN mirroring provides more mirroring modes. You can monitor the packets from one or more VLANs.

Mirroring Based on MAC addresses

Mirroring based on MAC addresses allows you to monitor the packets received by or sent from a specified device on a network. The S-switch mirrors the packets matching a specified source or destination MAC address in a VLAN to a specified observing interface.

Local SPAN

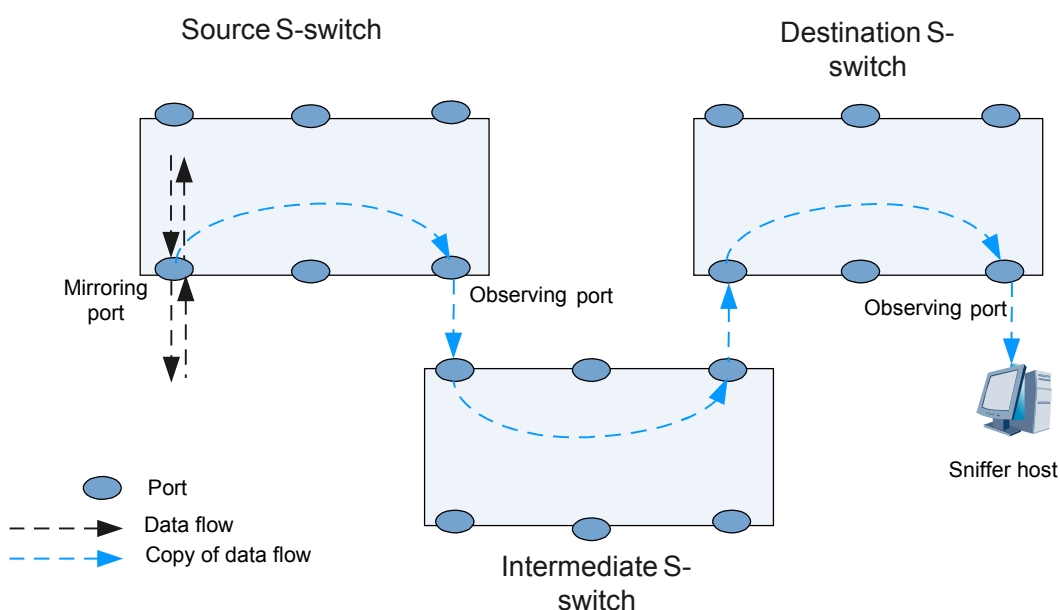
In the process of local Switched Port Analyzer (SPAN), the interface that mirroring traffic passes through is located on the same S-switch as an observing interface.

Local SPAN can forward the traffic to a specified observing interface according to interface mirroring, VLAN mirroring, mirroring based on MAC addresses, and flow mirroring.

RSPAN

In the process of interface mirroring, the S-switch copies the packets passing through a mirroring interface and then sends the copy to a specified observing interface. When the observing interface is not located on the same S-switch as the mirroring interface, RSPAN can be adopted to meet the demand.

Figure 3-3 Schematic diagram of RSPAN



As shown in **Figure 3-3**:

- **Source S-switch** indicates the S-switch where the mirroring interface is located.
- **Destination S-switch** indicates the S-switch where the observing interface is located.
- **Intermediate S-switch** indicates the intermediate S-switch connecting the source S-switch and the destination S-switch.

 **NOTE**

In the process of RSPAN, there is no intermediate S-switch if the source S-switch is directly connected to the destination S-switch.

RSPAN can broadcast mirroring packets from the source S-switch to the destination S-switch in the RSPAN VLAN. Ensure that all the interfaces connected with the source S-switch, the intermediate S-switch, and the destination S-switch belong to the RSPAN VLAN.

On the source S-switch, the observing interface is set as a Frame Relay (FR) interface. The mirroring packets are forwarded to the intermediate S-switch through the observing interface on the source S-switch, and then are broadcast to the observing interface on the destination S-switch.

On the destination S-switch, the observing interface is set as a remote interface and receives the remote mirroring packets.

RSPAN can forward packets to a specified observing interface according to interface mirroring, VLAN mirroring, mirroring based on MAC addresses, and flow mirroring.

CPU Cache

Central Processing Unit (CPU) cache is used to cache all the packets received by the CPU.

- If an Access Control List (ACL) rule is specified, the packets that match the ACL rule are cached.
- If no ACL rule is specified, all the packets received by the CPU are cached.

CPU Mirroring

CPU mirroring is used to mirror all the packets received by the CPU.

- If an ACL rule is specified, the packets that match the ACL rule are mirrored to a specified observing interface.
- If no ACL rule is specified, all the packets received by the CPU are mirrored to a specified observing interface.

CPU cache and CPU mirroring provide debugging, which facilitates users to debug and locate faults.

3.1.2 Logical Relationships Between Configuration Tasks

Before performing [3.13 Changing or Deleting an Observing Interface](#), complete [3.4 Canceling Interface Mirroring](#), [3.11 Canceling Flow Mirroring](#), [3.5.5 Canceling VLAN Mirroring](#) and [3.8 Canceling Mirroring Based on MAC Addresses](#).

3.1.3 Specifications

By configuring flow mirroring on an interface, you apply a traffic policy to that interface. The traffic policy binds the traffic classifiers and traffic behaviors.

3.2 Configuring Interface-based Local SPAN

This section describes how to configure interface-based local SPAN.

[3.2.1 Establishing the Configuration Task](#)

[3.2.2 Configuring Interface-based Local SPAN](#)

[3.2.3 Checking the Configuration](#)

3.2.1 Establishing the Configuration Task

Applicable Environment

When all incoming or outgoing packets passing through a specified interface of the S-switch need to be monitored, you can configure interface-based local SPAN if the mirroring interface is located on the same S-switch as the observing interface.

Pre-configuration Tasks

None.

Data Preparation

To configure interface-based local SPAN, you need the following data.

No.	Data
1	Type and number of an observing interface
2	Type and number of a mirroring interface

3.2.2 Configuring Interface-based Local SPAN

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 **observing-port o-index interface interface-type interface-number** command to configure an observing interface.
- Step 3** Run the **interface interface-type interface-number** command to enter the view of the mirroring interface.
- Step 4** Run the **port-mirroring to observe-port o-index { both | inbound | outbound }** command to configure interface mirroring on the mirroring interface.

You must specify the same value for *o-index* in [Step 2](#) and [Step 4](#). At present, the value of *o-index* ranges from 1 to 4.

You can repeatedly perform [Step 3](#) and [Step 4](#) to monitor the traffic passing through multiple interfaces.

----End

3.2.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	display port-mirroring

Run the preceding command. If the following information is displayed, it means that the configuration succeeds:

- The observing interface is configured properly.
- The mirroring interface and the mirroring direction are configured properly.

3.3 Configuring Interface-based RSPAN

This section describes how to configure interface-based RSPAN.

[3.3.1 Establishing the Configuration Task](#)

[3.3.2 Configuring Interface-based RSPAN](#)

This section describes how to configure interface-based RSPAN.

[3.3.3 Checking the Configuration](#)

3.3.1 Establishing the Configuration Task

Applicable Environment

When incoming or outgoing packets passing through a specified interface or some interfaces of the S-switch need to be monitored, you can configure interface-based RSPAN if the monitored interfaces are not located on the same S-switch as the observing interface.

Pre-configuration Tasks

None.

Data Preparation

To configure interface-based RSPAN, you need the following data.

No.	Data
1	Type and number of an observing interface
2	Number of a mirroring interface
3	ID of an RSPAN VLAN

3.3.2 Configuring Interface-based RSPAN

This section describes how to configure interface-based RSPAN.

Configuring a Remote Mirroring Interface and an RSPAN VLAN on the Source S-switch

Context

Do as follows on the source S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **observing-port o-index interface interface-type interface-number relay-type** command to set the observing interface as an FR interface.
- Step 3** Run the **vlan vlan-id** command to create a VLAN and enter the VLAN view.
- Step 4** Run the **rspan vlan enable** command to configure a VLAN as an RSPAN VLAN.
- Step 5** Run the **quit** command to return to the system view.
- Step 6** Run the **interface interface-type interface-number** command to enter the view of an observing interface.
- Step 7** Run the **port trunk allow-pass vlan vlan-id** command to add the interface to the **rspan vlan**.
- Step 8** Run the **quit** command to return to the system view.
- Step 9** Run the **interface interface-type interface-number** command to enter the view of the remote mirroring interface.
- Step 10** Run the **port-mirroring to observe-port o-index { both | inbound | outbound } [remote vlan-id]** command to configure interface-based RSPAN and specify an RSPAN VLAN.

You must specify the same value for *o-index* in [Step 2](#) and [Step 10](#). At present, the value of *o-index* ranges from 1 to 4.

You can repeatedly perform [Step 9](#) and [Step 10](#) to monitor the incoming and outgoing packets passing through multiple interfaces.

----End

Configuring an RSPAN VLAN and Attributes of Its Interfaces on an Intermediate S-switch

Context

Do as follows on an intermediate S-switch. The interface of the intermediate S-switch connected to the source S-switch must be configured the same as the interface connected to the destination S-switch. If there is no intermediate S-switch, this configuration procedure is not required.

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 **rspan vlan enable** command to configure a VLAN as an RSPAN VLAN.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **interface *interface-type interface-number*** command to enter the view of the interface of the intermediate S-switch connected to the source S-switch and destination S-switch.
- Step 6** Run the **port trunk allow-pass vlan *vlan-id*** command to add the interface to the **rspan vlan**.
- Step 7** Run the **quit** command to return to the system view.

----End

Configuring an Observing Interface for RSPAN on the Destination S-switch

Context

Do as follows on the destination S-switch.

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 **rspan vlan enable** command to configure a VLAN as an RSPAN VLAN.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **interface *interface-type interface-number*** command to enter the view of an observing interface.
- Step 6** Run the **port trunk allow-pass vlan *vlan-id*** command to add the observing interface to the RSPAN VLAN.
- Step 7** Run the **interface *interface-type interface-number*** command to enter the view of the interface of the intermediate S-switch connected to the destination S-switch.

NOTE

If there is no intermediate S-switch, run the **interface *interface-type interface-number*** command to enter the view of the interface connecting the source S-switch and the destination S-switch.

- Step 8** Run the **port trunk allow-pass vlan *vlan-id*** command to add the interface to the **rspan vlan**.

- Step 9** Run the **quit** command to return to the system view.
- Step 10** Run the **observing-port** *o-index* **interface** *interface-type* *interface-number* command to configure an observing interface.
- End

3.3.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	display port-mirroring

Run the preceding command. If the following information is displayed, it means that the configuration succeeds:

- The RSPAN VLAN is configured properly.
- The number of the observing interface is configured properly.
- The type of the observing interface is configured properly.
- The number of the mirroring interface and the mirroring direction are configured properly.

3.4 Canceling Interface Mirroring

This section describes how to cancel interface mirroring.

[3.4.1 Establishing the Configuration Task](#)

[3.4.2 Establishing the Configuration Task](#)

[3.4.3 Configuring VLAN-based RSPAN](#)

This section describes how to configure VLAN-based RSPAN.

[3.4.4 Establishing the Configuration Task](#)

3.4.1 Establishing the Configuration Task

Applicable Environment

When interface mirroring is enabled on an interface of the S-switch, and the incoming or outgoing packets passing through this interface do not need to be monitored, you can cancel interface mirroring on that interface. You must cancel interface mirroring on the bound observing interface before deleting this observing interface.

Pre-configuration Tasks

None.

Data Preparation

To cancel interface mirroring, you need the following data.

No.	Data
1	Type and number of an observing interface
2	Type and number of the mirroring interface to be deleted

[3.4.1.1 Canceling Interface Mirroring](#)

[3.4.1.2 Checking the Configuration](#)

[3.4.1.3 Configuring VLAN-based Local SPAN](#)

This section describes how to configure VLAN-based local SPAN.

Canceling Interface Mirroring

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 **interface** *interface-type interface-number* command to enter the view of the mirroring interface.
- Step 3** Run the **undo port-mirroring { both | inbound | outbound }** command to cancel interface mirroring.
- End

Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	display port-mirroring

Run the **display port-mirroring** command. If interface mirroring is cancelled properly, it means that the configuration succeeds.

Configuring VLAN-based Local SPAN

This section describes how to configure VLAN-based local SPAN.

3.4.2 Establishing the Configuration Task

Applicable Environment

When incoming packets passing through all active interfaces of the S-switch in a specified VLAN or some VLANs need to be monitored, you can configure VLAN-based local SPAN if all interfaces receiving these monitored incoming packets are located on the same S-switch as the observing interface.

Pre-configuration Tasks

Before configuring VLAN-based local SPAN, complete the following tasks:

- Creating a VLAN as the monitoring VLAN
- Adding physical interfaces to the monitoring VLAN

Data Preparation

To configure VLAN-based local SPAN, you need the following data.

No.	Data
1	Type and number of an observing interface
2	ID of a mirroring VLAN

[3.4.2.1 Configuring VLAN-based Local SPAN](#)

[3.4.2.2 Checking the Configuration](#)

Configuring VLAN-based Local SPAN

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 **observing-port o-index interface interface-type interface-number** command to configure an observing interface.
- Step 3** Run the **vlan vlan-id** command to enter the view of the mirroring VLAN.
- Step 4** Run the **mirroring to observe-port o-index { inbound }** command to configure VLAN mirroring.

You must specify the same value for *o-index* in [Step 2](#) and [Step 4](#). At present, the value of *o-index* ranges from 1 to 4.

You can repeatedly perform [Step 3](#) and [Step 4](#) to monitor the incoming packets from multiple VLANs.

----End

Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	display port-mirroring

Run the preceding command. If the following information is displayed, it means that the configuration succeeds:

- The type of the observing interface is configured properly.
- The number of the observing interface is configured properly.

3.4.3 Configuring VLAN-based RSPAN

This section describes how to configure VLAN-based RSPAN.

3.4.4 Establishing the Configuration Task

Applicable Environment

When incoming packets passing through any active interfaces of the S-switch in a specified VLAN or some VLANs need to be monitored, you can configure VLAN-based RSPAN if the interface added to the monitored VLAN is not located on the same S-switch as the observing interface.

Pre-configuration Tasks

Before configuring VLAN-based RSPAN, complete the following tasks:

- Creating a VLAN as the monitoring VLAN
- Adding physical interfaces to the monitoring VLAN

Data Preparation

To configure VLAN-based RSPAN, you need the following data.

No.	Data
1	Type and number of an observing interface
2	ID of a mirroring VLAN
3	ID of an RSPAN VLAN

3.5 Configuring VLAN-based RSPAN

[3.5.4 Checking the Configuration](#)

[3.5.5 Canceling VLAN Mirroring](#)

This section describes how to cancel VLAN-based local SPAN and RSPAN.

[3.5.6 Establishing the Configuration Task](#)

[3.5.7 Canceling VLAN Mirroring](#)

3.5.1 Configuring VLAN-based RSPAN on the Source S-switch

Context

Do as follows on the source S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **observing-port** *o-index* **interface** *interface-type interface-number* **relay-type** command to set the observing interface as an FR interface.
- Step 3** Run the **vlan** *vlan-id* command to create a VLAN and enter the VLAN view.
- Step 4** Run the **rspan vlan enable** command to configure a VLAN as an RSPAN VLAN.
- Step 5** Run the **quit** command to return to the system view.
- Step 6** Run the **interface** *interface-type interface-number* command to enter the view of an observing interface.
- Step 7** Run the **port trunk allow-pass vlan** *vlan-id* command to add the interface to the **rspan vlan**.
- Step 8** Run the **quit** command to return to the system view.
- Step 9** Run the **vlan** *vlan-id* command to enter the view of the mirroring VLAN.
- Step 10** Run the **mirroring to observe-port** *o-index* **inbound** [**remote** *vlan-id*] command to configure VLAN-based RSPAN.

You must specify the same value for *o-index* in [Step 2](#) and [Step 10](#). At present, the value of *o-index* ranges from 1 to 4.

You can repeatedly perform [Step 9](#) and [Step 10](#) to monitor the incoming packets from multiple VLANs.

----End

3.5.2 Configuring an RSPAN VLAN and Attributes of Its Interfaces on an Intermediate S-switch

Context

The configuration of an intermediate S-switch for VLAN-based RSPAN is the same as that for interface-based RSPAN. For detailed information, see [3.3.2 Configuring Interface-based RSPAN](#).

3.5.3 Configuring an Observing Interface for RSPAN on the Destination S-switch

Context

The configuration of the destination S-switch for VLAN-based RSPAN is the same as that for interface-based RSPAN. For detailed information, see [3.3.2 Configuring Interface-based RSPAN](#).

3.5.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	display port-mirroring

Run the preceding command. If the following information is displayed, it means that the configuration succeeds:

- The type of the observing interface is configured properly.
- The number of the observing interface is configured properly.

3.5.5 Canceling VLAN Mirroring

This section describes how to cancel VLAN-based local SPAN and RSPAN.

3.5.6 Establishing the Configuration Task

Applicable Environment

When VLAN mirroring is enabled in a specified VLAN and all incoming packets in this VLAN do not need to be monitored on the S-switch, or before deleting or changing the bound observing interface, you need to cancel VLAN mirroring.

Pre-configuration Tasks

None.

Data Preparation

To cancel VLAN mirroring, you need the following data.

No.	Data
1	ID of the mirrored VLAN to be deleted

3.5.7 Canceling VLAN Mirroring

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 **vlan *vlan-id*** command to enter the view of the monitored VLAN.
- Step 3** Run the **undo mirroring inbound** command to cancel VLAN mirroring.
- End

3.6 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	display port-mirroring

Run the preceding command. If VLAN mirroring is cancelled, it means that the operation succeeds.

[3.6.1 Configuring Local SPAN Based on MAC Addresses](#)

This section describes how to configure local SPAN based on MAC addresses.

[3.6.2 Establishing the Configuration Task](#)

[3.6.3 Configuring Local SPAN Based on MAC Addresses](#)

[3.6.4 Checking the Configuration](#)

3.6.1 Configuring Local SPAN Based on MAC Addresses

This section describes how to configure local SPAN based on MAC addresses.

3.6.2 Establishing the Configuration Task

Applicable Environment

When incoming packets with the specified source or destination MAC address in a VLAN need to be monitored on the S-switch, you can configure local SPAN based on MAC addresses if the monitoring interface receiving these incoming packets is located on the same S-switch as the observing interface.

Pre-configuration Tasks

None.

Data Preparation

To configure local SPAN based on MAC addresses, you need the following data.

No.	Data
1	Type and number of an observing interface
2	MAC address of the packet to be mirrored
3	ID of the VLAN that the packet with the MAC address to be mirrored belongs to

3.6.3 Configuring Local SPAN Based on MAC Addresses

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 **observing-port o-index interface interface-type interface-number** command to configure an observing interface.
- Step 3** Run the **vlan vlan-id** command to enter the VLAN view.
- Step 4** Run the **mac-mirroring mac-address to observe-port o-index { inbound }** command to configure local SPAN based on MAC addresses.

You must specify the same value for *o-index* in [Step 2](#) and [Step 4](#). At present, the value of *o-index* ranges from 1 to 4.

You can repeatedly perform [Step 3](#) and [Step 4](#) to monitor the incoming packets with multiple MAC addresses in multiple VLANs.

----End

3.6.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	display port-mirroring

Run the preceding command. If the following information is displayed, it means that the configuration succeeds:

- The type of the observing interface is configured properly.
- The number of the observing interface is configured properly.

3.7 Configuring RSPAN Based on MAC Addresses

This section describes how to configure RSPAN based on MAC addresses.

[3.7.1 Establishing the Configuration Task](#)

[3.7.2 Configuring RSPAN Based on MAC Addresses](#)

This section describes how to configure RSPAN based on MAC addresses.

[3.7.3 Checking the Configuration](#)

3.7.1 Establishing the Configuration Task

Applicable Environment

When incoming packets with the specified source or destination MAC address in a VLAN need to be monitored on the S-switch, you can configure RSPAN based on MAC addresses if the monitoring interface receiving these incoming packets is not located on the same S-switch as the observing interface.

Pre-configuration Tasks

None.

Data Preparation

To configure RSPAN based on MAC addresses, you need the following data.

No.	Data
1	Type and number of an observing interface
2	MAC address of the packet to be mirrored
3	ID of the VLAN that the packet with the MAC address to be mirrored belongs to

No.	Data
4	ID of an RSPAN VLAN

3.7.2 Configuring RSPAN Based on MAC Addresses

This section describes how to configure RSPAN based on MAC addresses.

Configuring RSPAN Based on MAC Addresses on the Source S-switch

Context

Do as follows on the source S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **observing-port o-index interface interface-type interface-number relay-type** command to set the observing interface as an FR interface.
- Step 3** Run the **vlan vlan-id** command to create a VLAN and enter the VLAN view.
- Step 4** Run the **rspan vlan enable** command to configure a VLAN as an RSPAN VLAN.
- Step 5** Run the **quit** command to return to the system view.
- Step 6** Run the **interface interface-type interface-number** command to enter the view of an observing interface.
- Step 7** Run the **port trunk allow-pass vlan vlan-id** command to add the interface to the **rspan vlan**.
- Step 8** Run the **quit** command to return to the system view.
- Step 9** Run the **vlan vlan-id** command to enter the view of the VLAN that the monitored MAC address belongs to.
- Step 10** Run the **mac-mirroring mac-address to observe-port o-index inbound [remote vlan-id]** command to configure RSPAN based on MAC addresses and specify an RSPAN VLAN.

You must specify the same value for *o-index* in [Step 2](#) and [Step 10](#). At present, the value of *o-index* ranges from 1 to 4.

You can repeatedly perform [Step 9](#) and [Step 10](#) to monitor the incoming packets with multiple specified source or destination MAC addresses.

----End

Configuring an RSPAN VLAN and Attributes of Its Interfaces on an Intermediate S-switch

Context

The configuration of an intermediate S-switch for RSPAN based on MAC addresses is the same as that for interface-based RSPAN. For detailed information, see [3.3.2 Configuring Interface-based RSPAN](#).

Configuring an Observing Interface for RSPAN on the Destination S-switch

Context

The configuration of the destination S-switch for RSPAN based on MAC addresses is the same as that for interface-based RSPAN. For detailed information, see [3.3.2 Configuring Interface-based RSPAN](#).

3.7.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring based on MAC addresses.	display port-mirroring

Run the preceding command. If the following information is displayed, it means that the configuration succeeds:

- The type of the observing interface is configured properly.
- The RSPAN VLAN is configured properly.
- The number of the observing interface is configured properly.

3.8 Canceling Mirroring Based on MAC Addresses

This section describes how to cancel mirroring based on MAC addresses.

[3.8.1 Establishing the Configuration Task](#)

[3.8.2 Canceling Mirroring Based on MAC Addresses](#)

[3.8.3 Checking the Configuration](#)

3.8.1 Establishing the Configuration Task

Applicable Environment

When mirroring based on MAC addresses is enabled and incoming packets with specified MAC addresses in this VLAN do not need to be monitored on the S-switch, or before deleting or changing the bound observing interface, you need to cancel mirroring based on MAC addresses.

Pre-configuration Tasks

None.

Data Preparation

To cancel mirroring based on MAC addresses, you need the following data.

No.	Data
1	MAC address of the mirrored packet to be deleted

3.8.2 Canceling Mirroring Based on MAC Addresses

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 **vlan *vlan-id*** command to enter the view of the VLAN that the packets with the monitored MAC address belong to.
- Step 3** Run the **undo mac-mirroring *mac-address* inbound** command to cancel mirroring based on MAC addresses.

----End

3.8.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about interface mirroring.	dis current-configuration

Run the preceding command. If mirroring based on MAC addresses on the VLAN interface is cancelled, it means that the operation succeeds.

3.9 Configuring Flow-based Local SPAN

This section describes how to configure flow-based local SPAN.

[3.9.1 Establishing the Configuration Task](#)

[3.9.2 Setting Traffic Classification Rules](#)

[3.9.3 Configuring Flow Mirroring](#)

[3.9.4 Creating and Applying a Traffic Policy](#)

[3.9.5 Checking the Configuration](#)

3.9.1 Establishing the Configuration Task

Applicable Environment

When incoming flows passing through the S-switch with the same attribute need to be monitored, you can configure flow-based local SPAN if the monitored interface receiving these incoming flows is located on the same S-switch as the observing interface.

Pre-configuration Tasks

None.

Data Preparation

To configure flow-based local SPAN, you need the following data.

No.	Data
1	Type and number of an observing interface
2	Type and number of a flow mirroring interface
3	Names of the traffic classifier, traffic behavior, and traffic policy

3.9.2 Setting Traffic Classification Rules

NOTE

In the traffic classifier view, there is no specified order among the matching rules. You can combine these rules.

Setting Simple Traffic Classification Rules

Do as follows on the S-switch that needs to be configured with flow mirroring.

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

2. Run the **traffic classifier** *class-name* command to create a traffic classifier and enter the traffic classifier view.
3. Run one of the following **if-match** commands as required to define a matching rule:
 - Run the **if-match 8021p 802.1p-precedence** command to define a rule to classify traffic based on the 802.1p priorities in VLAN frames.
 - Run the **if-match any** command to define a rule to classify all packets into a same class.
 - Run the **if-match cvlan-8021p** command to define a matching rule for classifying traffic based on the 802.1p priority contained in the inner tag of a QinQ packet.
 - Run the **if-match discard** command to define a matching rule for classifying traffic based on discarded packets.
 - Run the **if-match cvlan-id cvlan-id** command to define a rule to classify traffic based on the IDs of inner VLAN tags in QinQ frames.
 - Run the **if-match { destination-mac | source-mac } mac-address** command to define a rule to classify traffic based on the destination MAC address or source MAC address in frames.
 - Run the **if-match double-tag** command to define a rule to classify traffic based on QinQ frames.
 - Run the **if-match l2-protocol { arp | ip | mpls | rarp | protocol-value }** command to define a rule based on the protocol type field in the Ethernet frame header.
 - Run the **if-match outbound-interface interface-type interface-number** command to define a rule to classify traffic based on the outbound interface.
 - Run the **if-match vlan-id vlan-id** command to define a rule to classify traffic based on VLAN IDs in frames.

One traffic classifier can have several matching rules that can be applied together. When the matching rules are mutually exclusive, applying the traffic policy fails. Traffic classification rules are mutually exclusive in the following aspects:

- Traffic classification rules for different protocols at the same network layer are mutually exclusive, for example, Layer 3 protocols are exclusive.
- The matching rules defined by customized character strings are exclusive to other matching rules.

Setting Complex Traffic Classification Rules

Do as follows on the S-switch that needs to be configured with flow mirroring.

1. Run the **system-view** command to enter the system view.
2. Run the **acl [number] acl-number** command to create an Access Control List (ACL) and enter the ACL view.

For the output of the commands related to the ACL, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

3. Run the **rule** command to create a basic ACL rule or an advanced ACL rule.
 - Run the **rule [rule-id] { permit | deny } [fragment | source { source-address source-wildcard | any } | time-range time-name]*** command to create a basic ACL rule.
 - To create an advanced ACL rule, run the following command as required:
 - **rule [rule-id] { permit | deny } { protocol | gre | igmp | ip | ipinip | ospf } [destination { destination-address destination-wildcard | any } | dscp dscp |**

- ```
fragment | precedence precedence | source { source-address source-wildcard |
any } | time-range time-name | tos tos]*
```
- rule [ rule-id ] { permit | deny } { tcp | udp } [ destination { destination-address destination-wildcard | any } | destination-port operator port | fragment | precedence precedence | source { source-address source-wildcard | any } | source-port operator port | time-range time-name ]\*
  - rule [ rule-id ] { permit | deny } icmp [ destination { destination-address destination-wildcard | any } | fragment | icmp-type icmp-type icmp-code | precedence precedence | source { source-address source-wildcard | any } | time-range time-name ]\*

#### NOTE

When the S-switch classifies traffic based on ACL rules, the **rule** commands are used only to classify traffic. The S-switch does not filter packets based on **permit** or **deny** in the commands.

The parameters related to the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) of an ACL rule and the protocols such as the Address Resolution Protocol (ARP) and Reserve Address Resolution Protocol (RARP) involved in simple traffic classification are mutually exclusive.

4. Run the **quit** command to return to the system view.
5. Run the **traffic classifier class-name** command to create a traffic classifier and enter the traffic classifier view.
6. Run the **if-match acl acl-number** command to define an ACL rule.

## Setting Customized Traffic Classification Rules

It is recommended that you configure traffic classification rules according to the steps in [Setting Simple Traffic Classification Rules](#) and [Setting Complex Traffic Classification Rules](#) first. If the two types of rules yet cannot satisfy the needs, perform the following steps to set customized rules for traffic classification.

#### NOTE

The customized rules for traffic classification are exclusive to any other rule.

1. Run the **system-view** command to enter the system view.
2. Run the **traffic classifier class-name** command to create a traffic classifier and enter the traffic classifier view.
3. Run the **if-match rule-string { rule-string mask-string offset } <1-8>** command to define a rule to classify traffic based on customized rule string of packet headers.

## 3.9.3 Configuring Flow Mirroring

### Context

Do as follows on the S-switch that needs to be configured with flow mirroring.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **observing-port o-index interface interface-type interface-number** command to configure an observing interface.

- Step 3** Run the **traffic behavior** *behavior-name* command to create a traffic behavior and enter the traffic behavior view.
- Step 4** Run the **port-mirroring to observe-port** *o-index* command to configure flow mirroring based on traffic classification.
- End

## Postrequisite

After configuring flow mirroring in a traffic behavior, you need to bind the behavior to a traffic classifier in the traffic policy and then apply the policy to the interface. For detailed configuration procedures, see [3.9.4 Creating and Applying a Traffic Policy](#).

## 3.9.4 Creating and Applying a Traffic Policy

### Context

Do as follows on the S-switch that needs to be configured with flow mirroring.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **traffic policy** *policy-name* command to create a traffic policy and enter the policy view.
- Step 3** Run the **classifier** *class-name* **behavior** *behavior-name* command to configure a traffic behavior for a specified class in the traffic policy.

*class-name* in this step must be the same as the name of the traffic class created in [3.9.2 Setting Traffic Classification Rules](#).

In this step, *behavior-name* must be the same as that specified in [Step 3](#) when you configure the traffic behavior.

- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 6** Run the **traffic-policy** *policy-name* **inbound** command to apply the traffic policy that contains flow mirroring to the interface.

You can repeatedly perform [Step 5](#) and [Step 6](#) to monitor the incoming flows, with the same attributes, passing through multiple interfaces.

----End

## 3.9.5 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                             | Command                       |
|----------------------------------------------------|-------------------------------|
| Check the configuration of an observing interface. | <b>display port-mirroring</b> |

| Action                                                                        | Command                                                                                                      |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Check the flow mirroring configuration in the traffic policy on an interface. | <b>display traffic policy interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [ <b>inbound</b> ] |

Run the preceding commands. If the following information is displayed, it means that the configuration succeeds:

- The number of the observing interface is set properly.
- A proper traffic policy is applied to the interface where incoming flows need to be monitored.
- The applied traffic policy contains proper traffic classifier and traffic behavior and the traffic behavior contains flow mirroring.

## 3.10 Configuring Flow-based RSPAN

This section describes how to configure flow-based RSPAN.

### [3.10.1 Establishing the Configuration Task](#)

### [3.10.2 Setting Traffic Classification Rules](#)

### [3.10.3 Configuring Flow-based RSPAN](#)

### [3.10.4 Creating and Applying a Traffic Policy](#)

### [3.10.5 Checking the Configuration](#)

## 3.10.1 Establishing the Configuration Task

### Applicable Environment

When incoming flows passing through the S-switch with the same attribute need to be monitored, you can configure flow-based RSPAN if the monitored interface receiving these incoming flows is not located on the same S-switch as the observing interface.

### Pre-configuration Tasks

None.

### Data Preparation

To configure flow-based RSPAN, you need the following data.

| No. | Data                                          |
|-----|-----------------------------------------------|
| 1   | Type and number of an observing interface     |
| 2   | Type and number of a flow mirroring interface |

| No. | Data                                                                  |
|-----|-----------------------------------------------------------------------|
| 3   | Names of the traffic classifier, traffic behavior, and traffic policy |
| 4   | ID of an RSPAN VLAN                                                   |

## 3.10.2 Setting Traffic Classification Rules

### Context

For how to set traffic classification rules, see [3.9.2 Setting Traffic Classification Rules](#).

## 3.10.3 Configuring Flow-based RSPAN

### Configuring Flow-based RSPAN on the Source S-switch

### Context

Do as follows on the source S-switch.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **observing-port o-index interface interface-type interface-number relay-type** command to set the observing interface as an FR interface.
- Step 3** Run the **vlan vlan-id** command to create a VLAN and enter the VLAN view.
- Step 4** Run the **rspan vlan enable** command to configure a VLAN as an RSPAN VLAN.
- Step 5** Run the **quit** command to return to the system view.
- Step 6** Run the **interface interface-type interface-number** command to enter the view of an observing interface.
- Step 7** Run the **port trunk allow-pass vlan vlan-id** command to add the interface to the **rspan vlan**.
- Step 8** Run the **quit** command to return to the system view.
- Step 9** Run the **traffic behavior behavior-name** command to create a traffic behavior and enter the traffic behavior view.
- Step 10** Run the **port-mirroring to observe-port o-index [ remote vlan-id ]** command to configure flow-based RSPAN.

You must specify the same value for *o-index* in [Step 2](#) and [Step 10](#). At present, the value of *o-index* ranges from 1 to 4.

After configuring flow mirroring in a traffic behavior, you need to bind the behavior to a traffic classifier in the traffic policy and then apply the policy to the interface. For detailed configuration procedures, see [3.9.4 Creating and Applying a Traffic Policy](#).

----End

## Configuring an RSPAN VLAN and Attributes of Its Interfaces on an Intermediate S-switch

### Context

The configuration of an intermediate S-switch for flow-based RSPAN is the same as that for interface-based RSPAN. For detailed information, see [3.3.2 Configuring Interface-based RSPAN](#).

## Configuring an Observing Interface for RSPAN on the Destination S-switch

### Context

The configuration of the destination S-switch for flow-based RSPAN is the same as that for interface-based RSPAN. For detailed information, see [3.3.2 Configuring Interface-based RSPAN](#).

## 3.10.4 Creating and Applying a Traffic Policy

### Context

For how to setting traffic classification rules on the source S-switch, see [3.9.4 Creating and Applying a Traffic Policy](#).

## 3.10.5 Checking the Configuration

Run the following command to check the previous configuration.

| Action                                                                           | Command                                                                                                      |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Check the configuration of an observing interface.                               | <b>display port-mirroring</b>                                                                                |
| Check the configuration of flow mirroring in the traffic policy on an interface. | <b>display traffic policy interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [ <b>inbound</b> ] |

Run the preceding command. If the following information is displayed, it means that the configuration succeeds:

- The number of the observing interface is set properly.
- The type of the observing interface is configured properly.
- The RSPAN VLAN is configured properly.
- A proper traffic policy is applied to the interface where incoming flows need to be monitored.
- The applied traffic policy contains proper traffic classifier and traffic behavior, and the traffic behavior contains flow mirroring.

## 3.11 Canceling Flow Mirroring

This section describes how to cancel flow mirroring.

### [3.11.1 Establishing the Configuration Task](#)

### [3.11.2 Canceling Flow Mirroring](#)

### [3.11.3 Checking the Configuration](#)

## 3.11.1 Establishing the Configuration Task

### Applicable Environment

When flow mirroring is enabled and the flow, with the same attributes, passing through the S-switch does not need to be monitored, you can cancel flow mirroring.

### Pre-configuration Tasks

None.

### Data Preparation

To cancel flow mirroring, you need the following data.

| No. | Data                                                                        |
|-----|-----------------------------------------------------------------------------|
| 1   | Type and number of the interface where flow mirroring needs to be cancelled |
| 2   | Name of the traffic policy                                                  |

## 3.11.2 Canceling Flow Mirroring

### Context

Do as follows on the S-switch that needs to be configured with flow mirroring.

### Procedure

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

**Step 2** Run the **interface interface-type interface-number** command to enter the interface view.

**Step 3** Run the **undo traffic-policy inbound** command to cancel the created traffic policy and flow mirroring on the interface.

To cancel a traffic policy, you must cancel the traffic policy on all the interfaces where the traffic policy is applied, and then run the **undo traffic policy policy-name** command to cancel the traffic policy in the system view.

----End

### 3.11.3 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                                        | Command                                                                                                      |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Check the configuration of an observing interface.                            | <b>display port-mirroring</b>                                                                                |
| Check the flow mirroring configuration in the traffic policy on an interface. | <b>display traffic policy interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [ <b>inbound</b> ] |

Run the preceding commands. If the following information is displayed, it means that the configuration succeeds:

The traffic policy applied on an interface is cancelled.

## 3.12 Canceling an RSPAN VLAN

This section describes how to cancel an RSPAN VLAN.

[3.12.1 Establishing the Configuration Task](#)

[3.12.2 \(Optional\)Canceling an RSPAN VLAN](#)

[3.12.3 Verify the configuration.](#)

### 3.12.1 Establishing the Configuration Task

#### Applicable Environment

When traffic does not need to be monitored or an RSPAN VLAN needs to be changed, you can cancel the RSPAN VLAN.

#### Pre-configuration Tasks

Before canceling an RSPAN VLAN, complete the following tasks:

- [3.4.1.1 Canceling Interface Mirroring](#)
- [3.5.7 Canceling VLAN Mirroring](#)
- [3.8.2 Canceling Mirroring Based on MAC Addresses](#)
- [3.11.2 Canceling Flow Mirroring](#)

#### Data Preparation

To cancel an RSPAN VLAN, you need the following data.

| No. | Data                |
|-----|---------------------|
| 1   | ID of an RSPAN VLAN |

### 3.12.2 (Optional) Canceling an RSPAN VLAN

#### 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 **vlan *vlan-id*** command to enter the view of an RSPAN VLAN.
- Step 3** Run the **undo rspan vlan enable** command to cancel the RSPAN VLAN.

----End

#### Postrequisite

### 3.12.3 Verify the configuration.

Run the following command to check the previous configuration.

| Action                                       | Command                              |
|----------------------------------------------|--------------------------------------|
| Check information about interface mirroring. | <b>display current-configuration</b> |

Run the preceding command. If an RSPAN VLAN is canceled, it means that the operation succeeds.

## 3.13 Changing or Deleting an Observing Interface

This section describes how to change or delete an observing interface.

[3.13.1 Establishing the Configuration Task](#)

[3.13.2 \(Optional\) Deleting an Observing Interface](#)

[3.13.3 \(Optional\) Changing an Observing Interface](#)

[3.13.4 Checking the Configuration](#)

## 3.13.1 Establishing the Configuration Task

### Applicable Environment

When you do not need to monitor the flow passing through the S-switch, you can delete the current observing interface; when you need to specify another interface on the S-switch as an observing interface, you can change the current observing interface.

### Pre-configuration Tasks

Before changing or deleting an observing interface, complete the following tasks:

- [3.4 Canceling Interface Mirroring](#)
- [3.5.5 Canceling VLAN Mirroring](#)
- [3.8 Canceling Mirroring Based on MAC Addresses](#)
- [3.11 Canceling Flow Mirroring](#)

### Data Preparation

To change or delete an observing interface, you need the following data.

| No. | Data                                           |
|-----|------------------------------------------------|
| 1   | Type and number of the new observing interface |

## 3.13.2 (Optional) Deleting an Observing Interface

### Context

Do as follows on the S-switch where an observing interface needs to be deleted.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the view of the mirroring interface.
- Step 3** Run the **undo port-mirroring { both | inbound | outbound }** command to cancel interface mirroring.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **undo observing-port o-index** command to delete the observing interface.

----End

## 3.13.3 (Optional) Changing an Observing Interface

## Context

Do as follows on the S-switch where an observing interface needs to be deleted.

## Procedure

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

**Step 2** Run the **observing-port o-index interface interface-type interface-number** command to specify another interface as an observing interface.

----End

### 3.13.4 Checking the Configuration

Run the following command to check the previous configuration.

| Action                                             | Command                       |
|----------------------------------------------------|-------------------------------|
| Check the configuration of an observing interface. | <b>display port-mirroring</b> |

Run the **display port-mirroring** command. If an observing interface is deleted or a new observing interface is specified, it means that the configuration succeeds.

## 3.14 Configuring CPU Cache

This section describes how to configure CPU cache.

[3.14.1 Establishing the Configuration Task](#)

[3.14.2 \(Optional\) Setting an ACL Rule](#)

[3.14.3 Configuring CPU Cache](#)

[3.14.4 Checking the Configuration](#)

### 3.14.1 Establishing the Configuration Task

#### Applicable Environment

When debugging the S-switch, you can configure CPU cache, if you need to learn information about the packets received by the CPU.

#### Pre-configuration Tasks

None.

#### Data Preparation

To configure CPU cache, you need the following data.

| No. | Data                               |
|-----|------------------------------------|
| 1   | (Optional) ACL number and ACL rule |

## 3.14.2 (Optional) Setting an ACL Rule

### Context

Do as follows on the S-switch where CPU cache needs to be configured.

### Procedure

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

**Step 2** Run the **acl [ number ] acl-number** command to create an Access Control List (ACL) and enter the ACL view.

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

**Step 3** Run the **rule** command to create a basic ACL rule or an advanced ACL rule.

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

----End

## 3.14.3 Configuring CPU Cache

### Context

Do as follows on the S-switch where CPU cache needs to be configured.

### Procedure

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

**Step 2** Run the **cpu cache packet [ acl acl-number ]** command to configure CPU cache.

By default, CPU cache is not enabled.

----End

## 3.14.4 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                            | Command                  |
|-------------------------------------------------------------------|--------------------------|
| Check the packets received by the CPU in the cache of the device. | <b>display cpu cache</b> |

| Action                                                           | Command                      |
|------------------------------------------------------------------|------------------------------|
| Check the ACL number that match the packets received by the CPU. | <b>display cpu cache acl</b> |

After the configuration, run the **display cpu cache** command. If you can view the packets received by the CPU in the cache of the device, it means that the configuration succeeds.

```
<Quidway> display cpu cache

Port : Ethernet0/0/24 Vlan ID : 1
Date : 2008/01/02 Time : 02:47:29
DMAC : ffff-ffff-ffff
SMAC : 0018-8244-66b6
length : 64
DATA :
ff ff ff ff ff ff 00 18 82 44 66 b6 81 00 00 01
08 06 00 01 08 00 06 04 00 01 00 18 82 44 66 b6
c0 a8 00 71 00 00 00 00 00 00 c0 a8 d2 ff 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

After the configuration, run the **display cpu cache acl** command. If you can view the ACL number that matches the packets received by the CPU in the cache of the device, it means that the configuration succeeds.

```
<Quidway> display cpu cache acl
The number of CPU cache ACL is 2001.
```

## 3.15 Configuring CPU Mirroring

This section describes how to configure CPU mirroring.

### [3.15.1 Establishing the Configuration Task](#)

### [3.15.2 \(Optional\) Configuring an ACL Rule](#)

### [3.15.3 Configuring an Observing Interface](#)

### [3.15.4 Configuring CPU Mirroring](#)

### [3.15.5 Checking the Configuration](#)

## 3.15.1 Establishing the Configuration Task

### Applicable Environment

When debugging the S-switch, you can configure CPU mirroring, if you need to monitor the packets received by the CPU.

### Pre-configuration Tasks

None.

## Data Preparation

To configure CPU mirroring, you need the following data.

| No. | Data                                           |
|-----|------------------------------------------------|
| 1   | (Optional) ACL number and ACL rule             |
| 2   | Index, type, and ID of the observing interface |

### 3.15.2 (Optional) Configuring an ACL Rule

#### Context

Do as follows on the S-switch that needs to be configured with CPU mirroring.

#### Procedure

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

**Step 2** Run the **acl [ number ] acl-number** command to create an Access Control List (ACL) and enter the ACL view.

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

**Step 3** Run the **rule** command to create a basic or an advanced ACL rule.

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

----End

### 3.15.3 Configuring an Observing Interface

#### Context

Do as follows on the S-switch that needs to be configured with CPU mirroring.

#### Procedure

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

**Step 2** Run the **observing-port o-index interface interface-type interface-number** command to configure a global observing interface.

----End

### 3.15.4 Configuring CPU Mirroring

## Procedure

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

**Step 2** Run the **cpu mirror packet [ acl acl-number ] to observe-port o-index inbound** command to configure CPU mirroring.

By default, CPU mirroring is disabled.

----End

### 3.15.5 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                 | Command                   |
|----------------------------------------|---------------------------|
| Check information about CPU mirroring. | <b>display cpu mirror</b> |

Run the **display cpu mirror** command. If you can view the number of the Access Control List (ACL) that matches packets received by the CPU and the observing interface specified by mirroring, it means that the configuration succeeds.

```
<Quidway> display cpu mirror
The number of CPU Mirror ACL is 2001.
CPU mirror observe index 1 is set to interface Ethernet0/0/5.
```

## 3.16 Maintaining Mirroring

This section describes how to clear the statistics.

### 3.16.1 Clearing the Statistics on CPU Cache



#### CAUTION

The statistics on packets received by the CPU in the cache of the device cannot be restored after you clear them. So, confirm the action before you use the command.

To collect the statistics on the packets received by the CPU in the cache of the device, you can use the following command in the user view to clear the previous statistics.



#### NOTE

The device caches up to 100 packets. After the cache is full, the newly received packets override the previous ones.

| Action                                                                              | Command                |
|-------------------------------------------------------------------------------------|------------------------|
| Clear the statistics on the packets received by the CPU in the cache of the device. | <b>reset cpu cache</b> |

## 3.17 Configuration Examples

This section provides several configuration examples for mirroring.

[3.17.1 Example for Configuring Interface-based Local SPAN](#)

[3.17.2 Example for Configuring VLAN-based Local SPAN](#)

[3.17.3 Example for Configuring Local SPAN Based on MAC Addresses](#)

[3.17.4 Example for Configuring Flow-based Local SPAN](#)

[3.17.5 Example for Configuring Interface-based RSPAN](#)

[3.17.6 Example for Configuring CPU Cache](#)

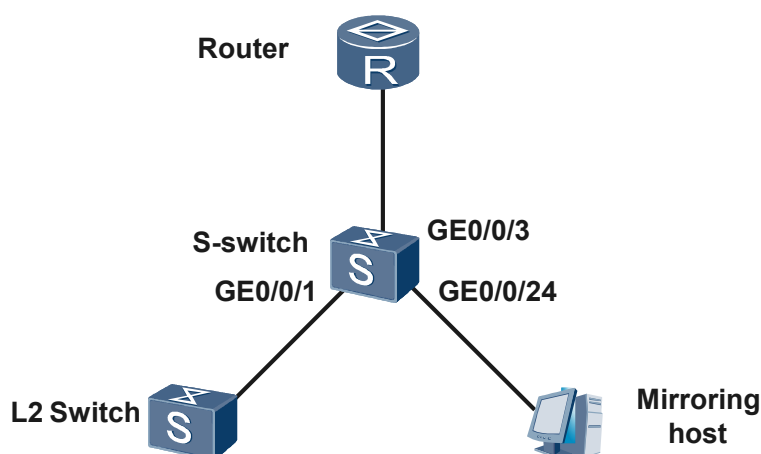
[3.17.7 Example for Changing an Observing Interface](#)

### 3.17.1 Example for Configuring Interface-based Local SPAN

#### Networking Requirements

As shown in [Figure 3-4](#), a Layer 2 (L2) switch is connected to GigabitEthernet 0/0/1 on the S-switch, and the incoming traffic on GigabitEthernet 0/0/1 needs to be monitored. In this case, you can configure interface-based local SPAN with GigabitEthernet 0/0/1 as a mirroring interface and GigabitEthernet 0/0/24 as an observing interface.

**Figure 3-4** Networking diagram of interface-based local SPAN



#### Configuration Roadmap

The configuration roadmap is as follows:

- Set GigabitEthernet 0/0/24 as an observing interface.
- Set GigabitEthernet 0/0/1 as a mirroring interface.

## Data Preparation

None.

## Configuration Procedure

1. Create a VLAN on the S-switch and add interfaces to the VLAN in trunk mode.  
# Add GigabitEthernet 0/0/1 and GigabitEthernet 0/0/3 to a same VLAN in trunk mode. The following takes the configuration of GigabitEthernet 0/0/1 as an example. The configuration of GigabitEthernet 0/0/3 is the same as the configuration of GigabitEthernet 0/0/1 and is not mentioned here.

```
<S-switch> system-view
[S-switch] vlan 1
[S-switch-vlan1] quit
[S-switch] interface GigabitEthernet 0/0/1
[S-switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 1
[S-switch-GigabitEthernet0/0/1] quit
```

2. Configure an observing interface.

# Set GigabitEthernet 0/0/24 as the observing interface.

```
<S-switch> system-view
[S-switch] observing-port 1 interface GigabitEthernet 0/0/24
```

3. Configure a mirroring interface.

# Set GigabitEthernet 0/0/1 as the mirroring interface.

```
[S-switch] interface GigabitEthernet 0/0/1
[S-switch-GigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
[S-switch-GigabitEthernet0/0/1] quit
```

4. Verify the configuration.

# Run the **display port-mirroring** command. You can check the configurations on the observing interface and mirroring interface.

```
[S-switch] display port-mirroring
Observe index 1 is set to interface GigabitEthernet0/0/24
 Observe Type: Local
 Interface GigabitEthernet0/0/1
 Mirrored to: Observe index 1
 Direction: inbound
Observe index 2 is not set to any interface
Observe index 3 is not set to any interface
Observe index 4 is not set to any interface
```

## Configuration Files

The following lists the configuration files of the S-switch.

```
#
sysname S-switch
#
observing-port 1 interface GigabitEthernet0/0/24
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1
port-mirroring to observe-port 1 inbound
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 1
```

.....  
return

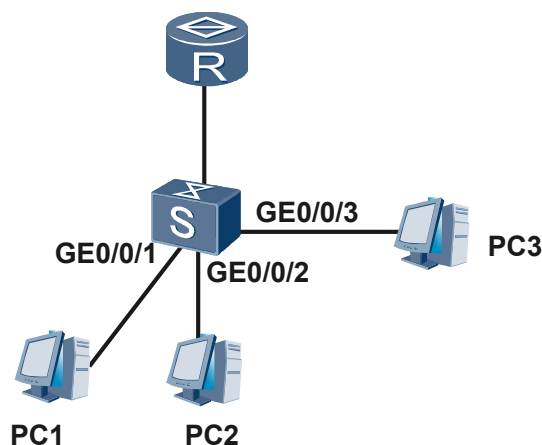
## 3.17.2 Example for Configuring VLAN-based Local SPAN

### Networking Requirements

As shown in **Figure 3-5**, GigabitEthernet 0/0/1 is connected to PC1; GigabitEthernet 0/0/2 is connected to PC2. PC1 and PC2 belong to VLAN 10. Now, incoming traffic of all active interfaces in VLAN 10 needs to be monitored. In this case, you can configure VLAN-based local SPAN.

GigabitEthernet 0/0/3 serves as an observing interface.

**Figure 3-5** Networking diagram of VLAN-based local SPAN



### Configuration Roadmap

The configuration roadmap is as follows:

- Set GigabitEthernet 0/0/3 as an observing interface.
- Set VLAN 10 as a mirroring VLAN.

### Data Preparation

None.

### Configuration Procedure

1. Configure an observing interface.  
# Set GigabitEthernet 0/0/3 as an observing interface.  

```
<S-switch> system-view
[S-switch] observing-port 1 interface GigabitEthernet 0/0/3
```
2. Configure a mirroring VLAN.  
# Set VLAN 10 as a mirroring VLAN.  

```
[S-switch] VLAN 10
[S-switch-VLAN10] mirroring to observe-port 1 inbound
```

```
[S-switch-VLAN10] quit
```

3. Verify the configuration.

# Run the **display port-mirroring** command. You can view the configuration of the observing interface.

```
[S-switch] display port-mirroring
Observe index 1 is set to interface GigabitEthernet0/0/3
Observe Type: Local
Observe index 2 is not set to any interface
Observe index 3 is not set to any interface
Observe index 4 is not set to any interface
```

## Configuration Files

The following lists the configuration files of the S-switch.

```
#
sysname S-switch
#
vlan batch 1 10
#
observing-port 1 interface GigabitEthernet0/0/3
#
cluster enable
ntdp enable
ntdp hop 16
ndp enable
#
vlan 10
mirroring to observe-port 1 inbound
#
interface GigabitEthernet0/0/1
port default vlan 10
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/2
port default vlan 10
bpdu enable
ntdp enable
ndp enable
#
#
return
```

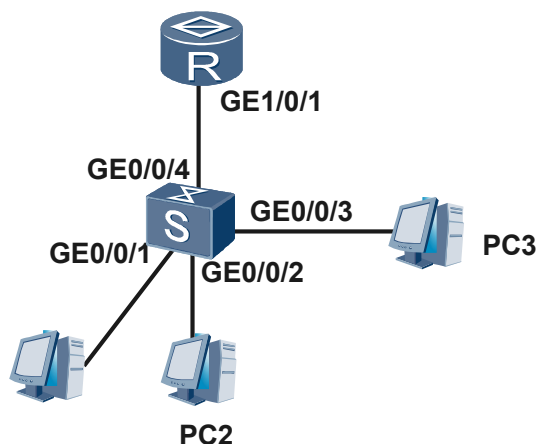
### 3.17.3 Example for Configuring Local SPAN Based on MAC Addresses

#### Networking Requirements

As shown in [Figure 3-6](#), GigabitEthernet 0/0/1 is connected to PC1; GigabitEthernet 0/0/2 is connected to PC2; GigabitEthernet 0/0/4 is connected to a router. GigabitEthernet 0/0/1, GigabitEthernet 0/0/2, and GigabitEthernet 0/0/4 belong to VLAN 10. Now, incoming traffic with the source or destination MAC as the MAC address of GigabitEthernet 1/0/1 on the router in VLAN 10 needs to be monitored. In this case, you can configure local SPAN based on MAC addresses on the S-switch.

GigabitEthernet 0/0/3 serves as an observing interface. The MAC address of GigabitEthernet 1/0/1 is 0001-0001-0001.

Figure 3-6 Networking diagram of local SPAN based on MAC addresses



## Configuration Roadmap

The configuration roadmap is as follows:

- Set GigabitEthernet 0/0/3 as an observing interface.
- Configure local SPAN based on MAC addresses in the view of VLAN 10.

## Data Preparation

None.

## Configuration Procedure

1. Configure VLAN 10 and then add GigabitEthernet 0/0/1, GigabitEthernet 0/0/2, and GigabitEthernet 0/0/4 to VLAN 10. The configuration procedure is not mentioned here.
2. # Set GigabitEthernet 0/0/3 as an observing interface.  

```
<S-switch> system-view
[S-switch] observing-port 1 interface GigabitEthernet 0/0/3
```
3. Configure a mirroring VLAN.  
# Configure local SPAN based on MAC addresses in the view of VLAN 10.  

```
[S-switch] VLAN 10
[S-switch-VLAN10] mac-mirroring 0001-0001-0001 to observe-port 1 inbound
[S-switch-VLAN10] quit
```
4. Verify the configuration.  
# Run the **display port-mirroring** command. You can view the configuration of the observing interface.  

```
[S-switch] display port-mirroring
Observe index 1 is set to interface GigabitEthernet0/0/3
Observe Type: Local
Observe index 2 is not set to any interface
Observe index 3 is not set to any interface
Observe index 4 is not set to any interface
```

## Configuration Files

The following lists the configuration files of the S-switch.

```
#
sysname S-switch
#
vlan batch 1 10
#
observing-port 1 interface GigabitEthernet0/0/3
#
cluster enable
ntdp enable
ntdp hop 16
ndp enable
#
vlan 10
mac-mirroring 0001-0001-0001 to observe-port 1 inbound
#
interface GigabitEthernet0/0/1
port default vlan 10
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/2
port default vlan 10
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/3
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/4
port default vlan 10
bpdu enable
ntdp enable
ndp enable
#
#
return
```

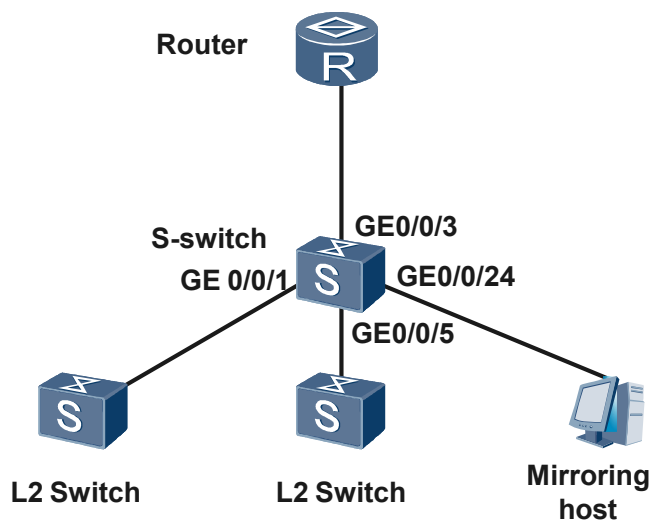
### 3.17.4 Example for Configuring Flow-based Local SPAN

#### Networking Requirements

As is shown in [Figure 3-7](#), the S-switch is connected to two L2 switches through GigabitEthernet 0/0/1 and GigabitEthernet 0/0/5. Packets with the same attributes received by GigabitEthernet 0/0/1 and GigabitEthernet 0/0/5 and transmitted from GigabitEthernet 0/0/3 need to be monitored. In this example, packets with the 802.1p priority as 6 need to be monitored.

GigabitEthernet 0/0/24 is set as an observing interface.

**Figure 3-7** Networking diagram of flow-based local SPAN



## Configuration Roadmap

The configuration roadmap is as follows:

- Set GigabitEthernet 0/0/24 as an observing interface.
- Create a traffic classifier and set the traffic classification rule that only the packets with the 802.1p priority as 6 can be matched.
- Create a traffic behavior and configure flow mirroring in the traffic behavior.
- Create a traffic policy and bind the traffic classifier to the traffic behavior.
- Apply the traffic policy to GigabitEthernet 0/0/1 and GigabitEthernet 0/0/5.
- Create a VLAN on the S-switch. Add GigabitEthernet 0/0/3, GigabitEthernet 0/0/1, and GigabitEthernet 0/0/5 to the same VLAN in trunk mode.

## Data Preparation

To complete the configuration, you need the following data:

- Name of the traffic classifier: c1
- Name of the traffic behavior: b1
- Name of the traffic policy: p1
- ID of the VLAN created on the S-switch: 1

## Configuration Procedure

1. Create a VLAN on the S-switch and add interfaces to the VLAN in trunk mode.  
# Add GigabitEthernet 0/0/1, GigabitEthernet 0/0/3, and GigabitEthernet 0/0/5 to the same VLAN in trunk mode. The following takes the configuration of GigabitEthernet 0/0/1 as an example. The configurations of GigabitEthernet 0/0/3 and GigabitEthernet 0/0/5 are the same as the configuration of GigabitEthernet 0/0/1 and are not mentioned here.

```
<S-switch> system-view
[S-switch] vlan 1
[S-switch-vlan1] quit
```

- ```
[S-switch] interface GigabitEthernet 0/0/1
[S-switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 1
[S-switch-GigabitEthernet0/0/1] quit
```
2. Configure an observing interface.
Set GigabitEthernet 0/0/24 as the observing interface.

```
[S-switch] observing-port 1 interface GigabitEthernet 0/0/24
```
 3. # Create a traffic classifier.
Create traffic classifier **c1** and set the traffic classification rule that only the packets with the 802.1p priority as 6 can be matched.

```
[S-switch] traffic classifier c1
[S-switch-classifier-c1] if-match 8021p 6
[S-switch-classifier-c1] quit
```
 4. # Create a traffic behavior.
Create traffic behavior **b1** and configure flow mirroring in the traffic behavior.

```
[S-switch] traffic behavior b1
[S-switch-behavior-b1] port-mirroring to observe-port 1
[S-switch-behavior-b1] quit
```
 5. Create a traffic policy.
Create a traffic policy and bind traffic classifier **c1** to traffic behavior **b1**.

```
[S-switch] traffic policy p1
[S-switch-trafficpolicy-p1] classifier c1 behavior b1
[S-switch-trafficpolicy-p1] quit
```
 6. Apply the traffic policy and enable the interface to trust the 802.1p priority of packets.
Apply traffic policy **p1** to GigabitEthernet 0/0/1 and GigabitEthernet 0/0/5, and enable GigabitEthernet 0/0/1 and GigabitEthernet 0/0/5 to trust the 802.1p priority of packets.

```
[S-switch] interface GigabitEthernet 0/0/1
[S-switch-GigabitEthernet0/0/1] traffic-policy p1 inbound
[S-switch-GigabitEthernet0/0/1] trust 8021p
[S-switch-GigabitEthernet0/0/1] quit
[S-switch] interface GigabitEthernet 0/0/5
[S-switch-GigabitEthernet0/0/5] traffic-policy p1 inbound
[S-switch-GigabitEthernet0/0/5] trust 8021p
[S-switch-GigabitEthernet0/0/5] quit
```
 7. Verify the configuration.
Run the **display port-mirroring** command. You can check the observing interface.

```
[S-switch] display port-mirroring
Observe index 1 is set to interface GigabitEthernet0/0/24
  Observe Type: Local
Interface GigabitEthernet0/0/1
  Mirrored to: Observe index 1
    Direction: inbound
Observe index 2 is not set to any interface
Observe index 3 is not set to any interface
Observe index 4 is not set to any interface
```


Run the **display traffic policy interface** command. You can check the traffic policy applied to GigabitEthernet 0/0/1 and GigabitEthernet 0/0/5.

```
[S-switch] display traffic policy interface
Interface: GigabitEthernet0/0/1
Direction: Inbound
Policy: p1
Classifier: c1
  Rule(s) : if-match 8021p 6
Behavior: b1
  Port-mirroring to observe-port 1

Interface: GigabitEthernet0/0/5
Direction: Inbound
```

```
Policy: p1
Classifier: c1
Rule(s) : if-match 8021p 6
Behavior: b1
Port-mirroring to observe-port 1
```

Configuration Files

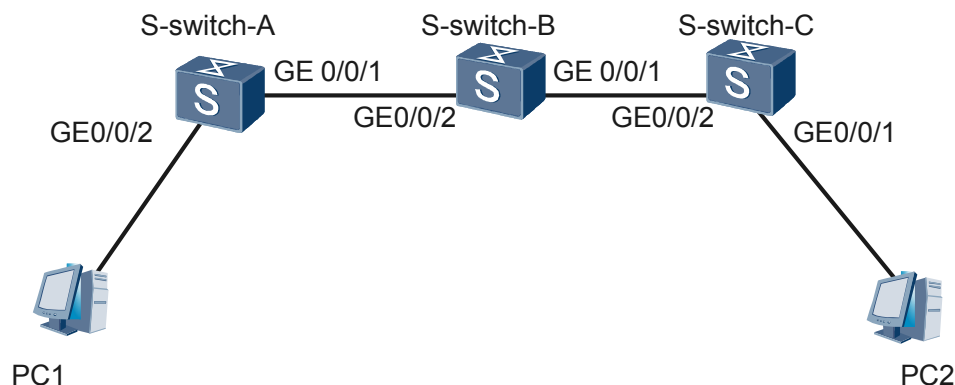
The following lists the configuration files of the S-switch.

```
#
sysname S-switch
#
vlan batch 1
#
observing-port 1 interface GigabitEthernet0/0/24
#
traffic classifier c1
if-match 8021p 6
#
traffic behavior b1
port-mirroring to observe-port 1
#
traffic policy p1
classifier c1 behavior b1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1
traffic-policy p1 inbound
trust 8021p
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 1
#
interface GigabitEthernet0/0/5
port trunk allow-pass vlan 1
trust 8021p
.....
interface GigabitEthernet0/0/24
#
return
```

3.17.5 Example for Configuring Interface-based RSPAN

Networking Requirements

As shown in [Figure 3-8](#), S-switch-A is connected to PC1; S-switch-C is connected to PC2. Now, incoming traffic of GigabitEthernet 0/0/2 on S-switch-A needs to be monitored on PC2. In this case, you can configure interface-based RSPAN on S-switch-A.

Figure 3-8 Networking diagram of interface-based RSPAN

Configuration Roadmap

The configuration roadmap is as follows:

- Set GigabitEthernet 0/0/1 of S-switch-A as an observing interface, and set the observing interface as an FR interface.
- Set GigabitEthernet 0/0/2 of S-switch-A as a mirroring interface.
- Set GigabitEthernet 0/0/1 of S-switch-C as an observing interface.

Data Preparation

To complete the configuration, you need the following data:

- Index number of the observing interface on S-switch-A: 1
- ID of the RSPAN VLAN on S-switch-A, S-switch-B, and S-switch-C: 2
- Index number of the observing interface on S-switch-C: 1

Configuration Procedure

1. Do as follows on S-switch-A:

- Set GigabitEthernet 0/0/1 as an observing interface, and set the observing interface as an FR interface.
- Create an RSPAN VLAN.
- Add GigabitEthernet 0/0/1 to the RSPAN VLAN in trunk mode.
- Configure interface-based RSPAN and specify the RSPAN VLAN on GigabitEthernet 0/0/2 for incoming traffic.

Set GigabitEthernet 0/0/1 as an observing interface, and set the observing interface as an FR interface.

```
<S-switch-A> system-view
[S-switch-A] observing-port 1 interface GigabitEthernet 0/0/1 relay-type
```

Create an RSPAN VLAN.

```
[S-switch-A] vlan 2
[S-switch-A-vlan2] rspan vlan enable
[S-switch-A-vlan2] quit
```

Add GigabitEthernet 0/0/1 to an RSPAN VLAN in trunk mode.

```
[S-switch-A] interface GigabitEthernet 0/0/1
```

```
[S-switch-A-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[S-switch-A-GigabitEthernet0/0/1] quit
```

Configure interface-based RSPAN and specify the RSPAN VLAN on GigabitEthernet 0/0/2 for incoming traffic.

```
[S-switch-A] interface GigabitEthernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] port-mirroring to observe-port 1 inbound
remote 2
[S-switch-A-GigabitEthernet0/0/2] quit
```

2. Do as follows on S-switch-B:

- Create an RSPAN VLAN.
- Add GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 to the RSPAN VLAN in trunk mode.

Create an RSPAN VLAN.

```
<S-switch-B> system-view
[S-switch-B] vlan 2
[S-switch-B-vlan2] rspan vlan enable
[S-switch-B-vlan2] quit
```

Add GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 to the RSPAN VLAN in trunk mode.

```
[S-switch-B] interface GigabitEthernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface GigabitEthernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[S-switch-B-GigabitEthernet0/0/2] quit
```

3. Do as follows on S-switch-C:

- Create an RSPAN VLAN.
- Add GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 to the RSPAN VLAN in trunk mode.
- Set GigabitEthernet 0/0/1 as an observing interface, and set the observing interface as a remote interface.

Create an RSPAN VLAN.

```
<S-switch-C> system-view
[S-switch-C] vlan 2
[S-switch-C-vlan2] rspan vlan enable
[S-switch-C-vlan2] quit
```

Add GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 to the RSPAN VLAN in trunk mode.

```
[S-switch-C] interface GigabitEthernet 0/0/2
[S-switch-C-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[S-switch-C-GigabitEthernet0/0/2] quit
[S-switch-C] interface GigabitEthernet 0/0/1
[S-switch-C-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[S-switch-C-GigabitEthernet0/0/1] quit
```

Set GigabitEthernet 0/0/1 as an observing interface, and set the observing interface as a remote interface.

```
[S-switch-C] observing-port 1 interface GigabitEthernet 0/0/1 remote-type
```

Configuration Files

The following lists the configuration files of the S-switch.

Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 1 to 2
#
observing-port 1 interface GigabitEthernet0/0/1 relay-type
#
cluster enable
ntdp enable
ntdp hop 16
ndp enable
#
vlan 2
rspan vlan enable
#
interface GigabitEthernet0/0/1

port trunk allow-pass vlan 2
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/2
port-mirroring to observe-port 1 inbound remote 2
bpdu enable
ntdp enable
ndp enable
#

#
return
```

Configuration file of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 1 to 2
#
cluster enable
ntdp enable
ntdp hop 16
ndp enable
#
vlan 2
rspan vlan enable
#
interface GigabitEthernet0/0/1

port trunk allow-pass vlan 2
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/2

port trunk allow-pass vlan 2
bpdu enable
ntdp enable
ndp enable
#

#
return
```

Configuration file of S-switch-C

```
#
sysname S-switch-C
```

```
#
vlan batch 1 to 2
#
observing-port 1 interface GigabitEthernet 0/0/1 remote-type
#
cluster enable
ntdp enable
ntdp hop 16
ndp enable
#
vlan 2
rspan vlan enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/2

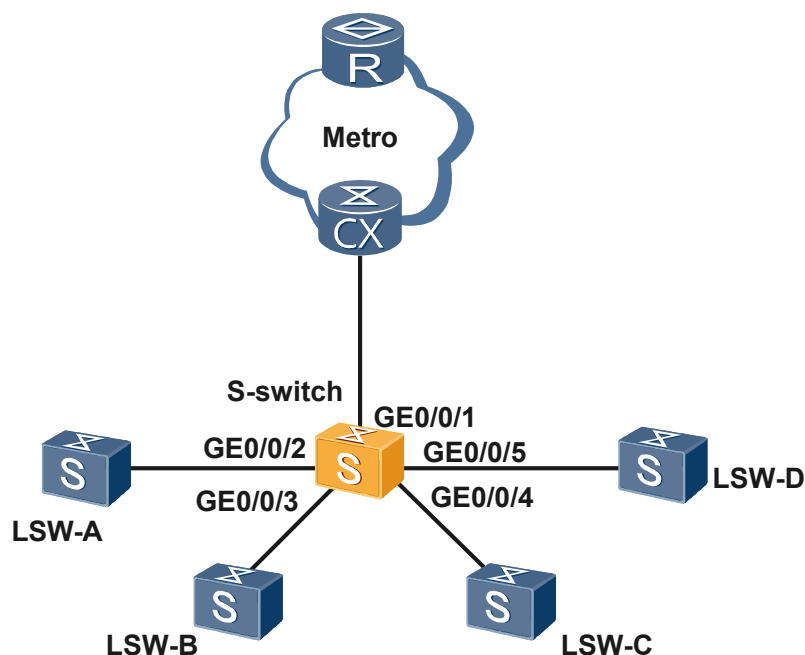
port trunk allow-pass vlan 2
bpdu enable
ntdp enable
ndp enable
#

#
return
```

3.17.6 Example for Configuring CPU Cache

Networking Requirements

As shown in [Figure 3-9](#), on the S-switch, GigabitEthernet0/0/1 is connected to the network; GigabitEthernet0/0/2, Eth 0/0/3, GigabitEthernet0/0/4, and GigabitEthernet0/0/5 are connected to LSW-A, LSW-B, LSW-C, and LSW-D respectively. When a device connected to the S-switch sends a large number of attack packets, the S-switch and the network may be disconnected. To find out the source device that sends attack packets, you need to configure CPU cache on the S-switch. Then, you can find out the device that sends attack packets by checking the packets sent to the CPU and the interface that receives the packets.

Figure 3-9 Networking for configuring CPU cache

Configuration Roadmap

The configuration roadmap is as follows:

- Configure CPU cache on the S-switch to check the type and source of attack packets.

Data Preparation

None.

Configuration Procedure

1. Configure CPU cache.

Configure the S-switch to cache all the packets received by the CPU.

```
[Quidway] cpu cache packet
```

2. Verify the configuration.

Run the **display cpu cache** command. You can view the packets received by the CPU in the cache of the device.

```
[Quidway] display cpu cache
```

```
-----
Port   : GigabitEthernet0/0/4          Vlan ID : 10
Date   : 2008/01/01                  Time    : 04:51:45
DMAC   : 0180-c200-0000
SMAC   : 0001-0001-0001
length : 124
DATA   :
01 80 c2 00 00 00 00 01 00 01 00 01 81 00 00 0a
00 6e 42 42 03 00 00 03 02 2c 80 00 00 01 00 01
00 01 00 00 00 00 80 00 00 01 00 01 00 01 80 45
00 00 0a 00 02 00 0f 00 00 00 00 40 52 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 01 ac 36
```

```

17 7f 50 28 3c d4 b8 38 21 d8 ab 26 de 62 80 00
00 01 00 01 00 01 00 00 00 00 00 14 00

-----
Port      : GigabitEthernet0/0/4          Vlan ID : 10
Date      : 2008/01/01                    Time   : 04:51:45
DMAC      : 0180-c200-0000
SMAC      : 0001-0001-0001
length    : 124
DATA      :
01 80 c2 00 00 00 00 01 00 01 00 01 81 00 00 0a
00 6e 42 42 03 00 00 03 02 2c 80 00 00 01 00 01
00 01 00 00 00 00 80 00 00 01 00 01 00 01 80 45
00 00 0a 00 02 00 0f 00 00 00 00 40 52 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 ac 36
17 7f 50 28 3c d4 b8 38 21 d8 ab 26 de 62 80 00
00 01 00 01 00 01 00 00 00 00 00 14 00

-----
Port      : GigabitEthernet0/0/4          Vlan ID : 10
Date      : 2008/01/01                    Time   : 04:51:45
DMAC      : 0180-c200-0000
SMAC      : 0001-0001-0001
length    : 124
DATA      :
01 80 c2 00 00 00 00 01 00 01 00 01 81 00 00 0a
00 6e 42 42 03 00 00 03 02 2c 80 00 00 01 00 01
00 01 00 00 00 00 80 00 00 01 00 01 00 01 80 45
00 00 0a 00 02 00 0f 00 00 00 00 40 52 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 ac 36
17 7f 50 28 3c d4 b8 38 21 d8 ab 26 de 62 80 00
00 01 00 01 00 01 00 00 00 00 00 14 00

-----
Port      : GigabitEthernet0/0/4          Vlan ID : 10
Date      : 2008/01/01                    Time   : 04:51:45
DMAC      : 0180-c200-0000
SMAC      : 0001-0001-0001
length    : 124
DATA      :
01 80 c2 00 00 00 00 01 00 01 00 01 81 00 00 0a
00 6e 42 42 03 00 00 03 02 2c 80 00 00 01 00 01
00 01 00 00 00 00 80 00 00 01 00 01 00 01 80 45
00 00 0a 00 02 00 0f 00 00 00 00 40 52 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 ac 36
17 7f 50 28 3c d4 b8 38 21 d8 ab 26 de 62 80 00
00 01 00 01 00 01 00 00 00 00 00 14 00

```

From the preceding result, you can find that GigabitEthernet0/0/4 on LSW-C sends a large number of STP packets to the S-switch. As a result, the CPU is busy and fails to process other normal packets.

Configuration Files

None

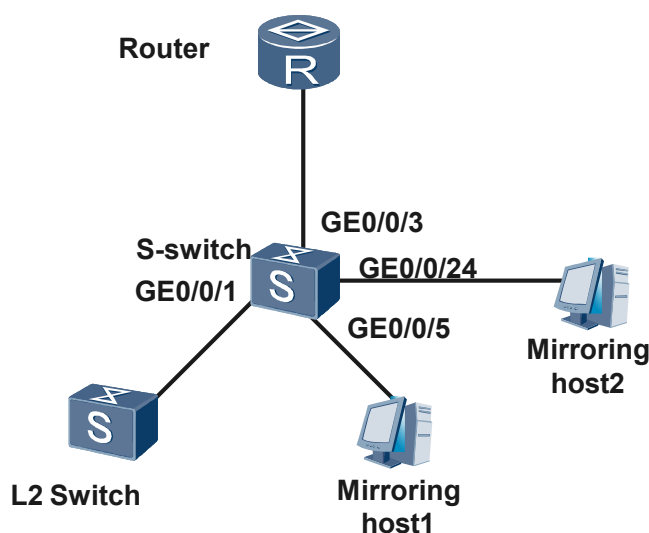
3.17.7 Example for Changing an Observing Interface

Networking Requirements

As shown in [Figure 3-10](#), an L2 switch is connected to GigabitEthernet 0/0/1 on the S-switch. To monitor the incoming traffic on GigabitEthernet 0/0/1, interface mirroring is configured on the S-switch, with GigabitEthernet 0/0/1 as a mirroring interface and GigabitEthernet 0/0/24 connected to host 1 as an observing interface.

Here, the incoming traffic on GigabitEthernet 0/0/1 of the S-switch needs to be monitored from host 2. Host 2, however, is connected to GigabitEthernet 0/0/5 of the S-switch, so the observing interface needs to be changed.

Figure 3-10 Networking for changing the observing interface



Configuration Roadmap

The configuration roadmap is as follows:

- Delete the mirroring interface GigabitEthernet 0/0/1.
- Set GigabitEthernet 0/0/5 instead of GigabitEthernet 0/0/24 as the observing interface.
- Reset GigabitEthernet 0/0/1 as the mirroring interface.

Data Preparation

To complete the configuration, you need the following data:

- Type and number of the new observing interface, that is, GigabitEthernet 0/0/5

Configuration Procedure

1. Check the configurations on the current observing interface and mirroring interface.
Run the **display port-mirroring** command to check the configurations on the current observing interface and mirroring interface.
`<S-switch> display port-mirroring`
2. Observe index 1 is set to interface GigabitEthernet0/0/24
Observe Type: Local
Interface GigabitEthernet0/0/1
Mirrored to: Observe index 1
Direction: inbound
Observe index 2 is not set to any interface
Observe index 3 is not set to any interface
Observe index 4 is not set to any interface
3. Delete the mirroring interface.
Delete the mirroring interface GigabitEthernet 0/0/1.

- ```
<S-switch> system-view
[S-switch] interface GigabitEthernet 0/0/1
[S-switch-GigabitEthernet0/0/1] undo port-mirroring inbound
```
4. Change the observing interface.  
# Change the observing interface to GigabitEthernet 0/0/5.  

```
[S-switch] observing-port 1 interface GigabitEthernet 0/0/5
```
  5. Configure a mirroring interface.  
# Reset GigabitEthernet 0/0/1 as the mirroring interface.  

```
[S-switch] interface GigabitEthernet 0/0/1
[S-switch-GigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
[S-switch-GigabitEthernet0/0/1] quit
```
  6. Verify the configuration.  
# Run the **display port-mirroring** command. You can check the configurations on the current observing interface and mirroring interface.  

```
[S-switch] display port-mirroring
Observe index 1 is set to interface GigabitEthernet0/0/5
 Observe Type: Local
Interface GigabitEthernet0/0/1
 Mirrored to: Observe index 1
 Direction: inbound
Observe index 2 is not set to any interface
Observe index 3 is not set to any interface
Observe index 4 is not set to any interface
```

## Configuration Files

The following lists the configuration files of the S-switch.

```
#
sysname S-switch
#
observing-port 1 interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/1
 port-mirroring to observe-port 1 inbound
#
return
```



# 4 Debugging and Diagnosis

---

## About This Chapter

This chapter describes the basics of debugging and the common commands for fault diagnosis.

### [4.1 Introduction](#)

This section describes the principle of the debugging function on the S-switch.

### [4.2 Debugging the S-switch](#)

This section describes how to debug the S-switch.

### [4.3 Using the ping Command](#)

This section describes how to diagnose faults and maintain the S-switch by using the **ping** command.

### [4.4 Running the tracert Command](#)

This section describes how to diagnose faults or maintain the S-switch by using the **tracert** command.

### [4.5 Maintaining the S-switch](#)

This section describes how to locate faults through ICMP packets.

### [4.6 Configuration Examples](#)

This section provides several examples for configuring diagnosis and debugging.

## 4.1 Introduction

This section describes the principle of the debugging function on the S-switch.

## 4.2 Debugging the S-switch

This section describes how to debug the S-switch.

### 4.2.1 Precautions on Debugging the S-switch

#### 4.2.2 Enabling Debugging

#### 4.2.3 Disabling Debugging

#### 4.2.4 Sending Debugging Information to the Console and VTY

### 4.2.1 Precautions on Debugging the S-switch

Debugging affects the performance of the system. So, run the **debugging all** command with caution. Before debugging, run the **display debugging** command to display the enabled debuggings and minimize the items to be debugged. To determine whether to enable debugging, you can run the **display cpu-usage** command to display the current CPU usage. After debugging, run the **undo debugging** command to disable it immediately.

### 4.2.2 Enabling Debugging

#### Context

#### Procedure

- Step 1** Run the **terminal monitor** command to enable the terminal display.
- Step 2** Run the **terminal debugging** command to enable the terminal to display debugging information.
- Step 3** Run the **debugging type** command to enable debugging. You can set debugging options according to different values of *type*.
- If the value is set as **all [ timeout timeout ]**, all debuggings are enabled and the duration of debugging is set.
  - If the value is set as **module-name [ debug-option1 ] [ debug-option2 ]...**, the debugging for a module is enabled.

In this step, the default value of *timeout* is 1 minute.

----End

### 4.2.3 Disabling Debugging

## Context

Do as follows on the S-switch.

## Procedure

Run the **undo debugging** *type* command to disable debugging. Set the debugging option according to different values of *type*.

- If the value is set as **all**, all debuggings are disabled.
- If the value is set as *module-name* [ *debug-option1* ] [ *debug-option2* ]..., the debugging for a module is disabled.

----End

## 4.2.4 Sending Debugging Information to the Console and VTY

### Context

Do as follows on the S-switch that is enabled with debugging to send debugging information to the terminals.

### Procedure

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

**Step 2** Run the **info-center { console channel | monitor channel } { channel-number | channel-name }** command to send information to the console and Virtual Type Terminal (VTY).

**Step 3** Run the **quit** command to return to the user view.

**Step 4** Run the **terminal monitor** command to enable the terminal display.

By default, terminal display on the console is enabled.

**Step 5** Run the **terminal debugging** command to enable the terminal to display debugging information.

[Step 4](#) and [Step 5](#) are not listed in sequence.

----End

## 4.3 Using the ping Command

This section describes how to diagnose faults and maintain the S-switch by using the **ping** command.

### [4.3.1 Introduction](#)

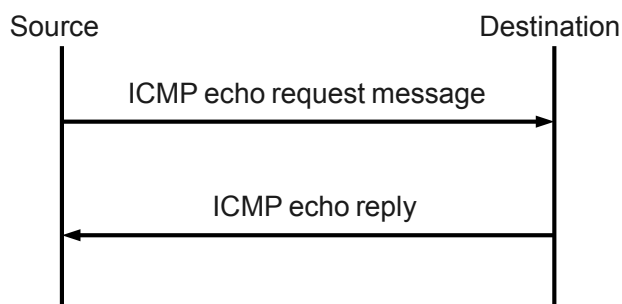
### [4.3.2 Usage of the ping Command](#)

### 4.3.1 Introduction

The word "ping", originating from the Sonar operation, indicates the pulse signals from the Sonar equipment.

As shown in [Figure 4-1](#), run the **ping** command to send an Internet Control Message Protocol (ICMP) echo request packet to the destination. The destination sends back an ICMP echo reply packet immediately when receiving the ICMP echo request packet.

**Figure 4-1** Principle of the **ping** command



Run the **ping** command to check whether an ICMP echo reply packet is sent back, and to determine the interval between sending an ICMP echo request packet and receiving an ICMP echo reply packet. Thus, you can detect the reachability between the source and the destination and the link status between the two ends.

**Figure 4-2** Format of ICMP echo request and echo reply packets

|            |   |      |                 |    |
|------------|---|------|-----------------|----|
| 0          | 7 | 15   | 23              | 31 |
| Type       |   | Code | Checksum        |    |
| Identifier |   |      | Sequence Number |    |
| Data       |   |      |                 |    |

[Figure 4-2](#) shows the format of ICMP echo request and echo reply packets. The Data field of a packet is variable in length. You can run the **ping** command to specify the length of the Data field.

## 4.3.2 Usage of the ping Command

### Context

Based on ICMP, the S-switch can detect the network connectivity and reachability of the host through the **ping** command. For the description of parameters of the **ping** command, refer to the *Quidway S5300 Series Ethernet Switches - Command Reference*.

## 4.4 Running the tracert Command

This section describes how to diagnose faults or maintain the S-switch by using the **tracert** command.

### 4.4.1 Introduction to the tracert Command

### 4.4.2 Usage of the tracert Command

## 4.4.1 Introduction to the tracert Command

The word "tracert" is short for "trace route". It is mainly used to detect the IP addresses and the number of gateways between the source and the destination.

Figure 4-3 Principle of the trace route command

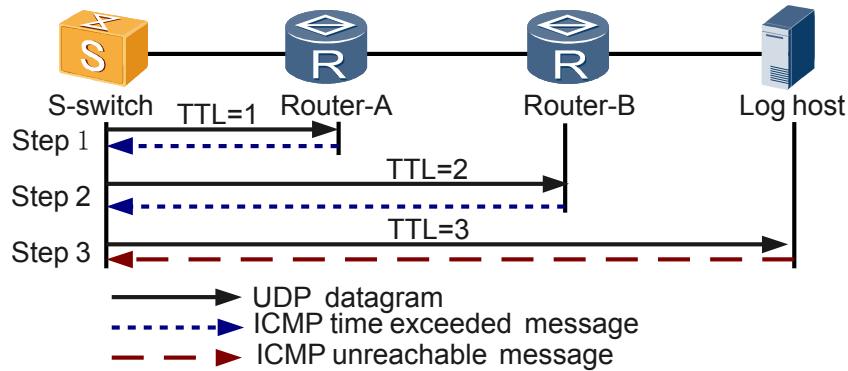


Figure 4-3 describes how to run the **tracert** command on the S-switch. Run the **tracert** command on the S-switch. By default, the IP address of the log host is specified as that of the destination.

1. The S-switch sends a User Datagram Protocol (UDP) packet to the log host, with the Time to Live (TTL) field being 1 and the destination UDP interface number being 33434.
  2. After receiving the UDP packet, Router-A determines whether the destination is itself. Then, the TTL value is deducted by 1. When the TTL value reaches 0, Router-A sends an ICMP Time Exceeded packet to the S-switch.
  3. After receiving the ICMP time exceeded packet, the S-switch adds to the TTL field value and the UDP interface number by 1, and then sends out the UDP packet again.
  4. Repeat Step 2 and Step 3 until the log host receives the UDP packet from the S-switch.
  5. After receiving the UDP packet from the S-switch, the log host finds the destination is itself and then begins to process this packet. The log host tries to find the corresponding upper layer protocol but fails. In most cases, the interfaces whose numbers are greater than 30000 are not occupied. Then, the log host sends an ICMP destination unreachable packet to the S-switch, which indicates that the destination interface is unreachable.
  6. After receiving the ICMP destination unreachable packet from the log host, the S-switch ensures that the UDP packet has reached the destination and stops the tracert program.
- The source learns IP addresses of the gateways between the source and the destination through the ICMP time exceeded packet.

## 4.4.2 Usage of the tracert Command

### Context

Based on ICMP, the S-switch records the gateways between the source and the destination, detect the network connectivity, and locate faults through the **tracert** command. For the description of parameters of the **tracert** command, refer to the *Qidway S5300 Series Ethernet Switches - Command Reference*.

To detect the gateways between the source and the destination, do as follows on the S-switch.

## Procedure

Run the **tracert** [ **-a** *source-ip-address* | **-f** *first-TTL* | **-m** *max-TTL* | **-p** *port* | **-q** *number* | **-w** *timeout* ] *\*host* command to detect the gateways between the source and the destination.

----End

## 4.5 Maintaining the S-switch

This section describes how to locate faults through ICMP packets.



### CAUTION

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

If you run the **ping** or the **tracert** command to detect the disconnectivity between two S-switches but the physical connection is normal, you can run the following command respectively on the two S-switches to further locate the fault.

| Action                                | Command                  |
|---------------------------------------|--------------------------|
| Enable the debugging of ICMP packets. | <b>debugging ip icmp</b> |

Run the preceding command. You can check the transmitting and receiving of ICMP packets during the running of the **ping** or the **tracert** command and thus determine which device fails.

## 4.6 Configuration Examples

This section provides several examples for configuring diagnosis and debugging.

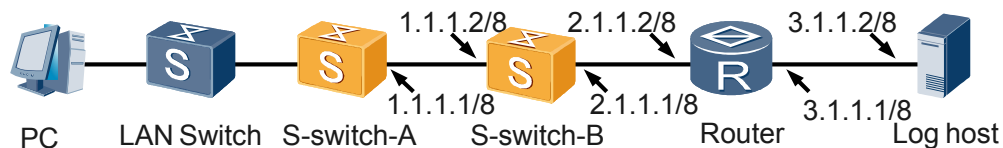
### 4.6.1 Example for Running the ping Command and the tracert Command

#### 4.6.1 Example for Running the ping Command and the tracert Command

### Networking Requirements

As shown in [Figure 4-4](#), you need to check the connectivity of the link between S-switch-A and the log host after configuring S-switch-A. There are other network devices between S-switch-A and the log host. If the link is detected unavailable, you need to locate which link fails.

**Figure 4-4** Networking diagram of running the **ping** command and the **tracert** command



## Configuration Roadmap

The configuration roadmap is as follows:

- Run the **ping** command on S-switch-A to detect the connectivity between S-switch-A and the log host.
- Run the **tracert** command to locate the fault when the link is detected faulty.

## Data Preparation

To complete the configuration, you need the following data.

- The IP address of S-switch-B is specified as 1.1.1.2/8 and 2.1.1.1/8.
- The IP address of the router is specified as 2.1.1.2/8 and 3.1.1.1/8.
- The IP address of the log host is specified as 3.1.1.2/8.

## Configuration Procedure

1. Run the **ping** command.

# Run the **ping** command on S-switch-A to detect the connectivity between S-switch-A and the log host.

```

<Quidway> ping 3.1.1.2
 PING 3.1.1.2: 56 data bytes, press CTRL_C to break
 Request time out
 Request time out
 Request time out
 Request time out
 Request time out

 --- 3.1.1.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
 100.00% packet loss

```

S-switch-A displays that the log host cannot be pinged, which indicates that a fault occurs on a link between S-switch-A and the log host.

2. Run the **tracert** command.

# Run the **tracert** command on S-switch-A to locate the fault.

```

<Quidway> tracert 3.1.1.2
 traceroute to 3.1.1.2(3.1.1.2) 30 hops max, 40 bytes packet
 1 1.1.1.2 4 ms 5 ms 5 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 ...

```

The displayed information indicates that the packet passes through S-switch-B but fails to reach the router. The link between S-switch-B and the Router is thus detected faulty.

## Configuration Files

None.

# 5 Restarting and Resetting

---

## About This Chapter

This chapter introduces the basics of the BootROM software and the Versatile Routing Platform (VRP) system software, and describes how to restart the S-switch.

### [5.1 Introduction](#)

This section introduces the required knowledge in restarting and resetting the S-switch.

### [5.2 Restarting the S-switch Immediately](#)

This section describes how to restart the S-switch immediately.

### [5.3 Restarting the S-switch at a Fixed Time](#)

This section describes how to restart the S-switch at a fixed time.

## 5.1 Introduction

This section introduces the required knowledge in restarting and resetting the S-switch.

### 5.1.1 Process of Starting the S-switch

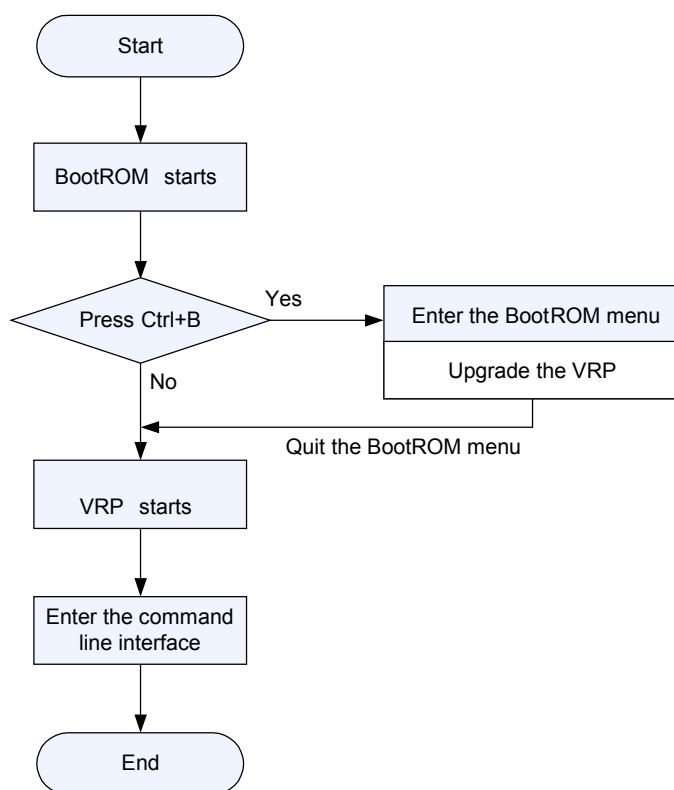
#### 5.1.2 Process of Starting the BootROM

#### 5.1.3 Logical Relationships Between Configuration Tasks

### 5.1.1 Process of Starting the S-switch

S-switchThe software of the S-switch consists of the BootROM and the VRP. After the S-switch is powered on, the BootROM and the VRP start the system in turn as shown in [Figure 5-1](#).

**Figure 5-1** Process of starting the S-switch



The advanced BootROM starts the VRP.

### 5.1.2 Process of Starting the BootROM

The advanced BootROM initializes the hardware of the S-switch and the terminal displays parameters of the hardware. The displayed information is as follows:

\*\*\*\*\*

```

*
* S5300 Bootrom, Ver001.04 *
*

Copyright (c) 2007-2008 HUAWEI TECH CO., LTD.
Creation date: Nov 22 2007, 19:32:20

CPU Type : BCM56024
CPU L2 Cache : 32KB
CPU Clock Speed : 266MHz
Bus Clock Speed : 133MHz
Memory Size : 128MB
Press Ctrl+B to enter Boot Menu... 0

```

Press **Ctrl+B** within two seconds. The system prompts you to enter the password of the advanced BootROM menu as follows:

```

password:
 BOOTROM MENU

1. Boot with default mode
2. Enter serial submenu
3. Enter startup submenu
4. Display flash files
5. Modify BOOTROM password
6. Reboot

```

Enter your choice(1-6):

In the advanced BootROM menu, you can choose to upgrade the VRP or specify the VRP version to be loaded when the S-switch is started.

The BootROM initializes the serial interface and the console interface, decompresses the logical files on the logical chip and the VRP, and then starts the VRP. The terminal displays information as follows:

```

Decompressing VRP software...done

Initialize switch chip Initialize DOPRA root Initialize hardware Initialize VOS VFS
Initialize VOS monitor Initialize CFM

Switch chip loopback test pass

Initialize device link Create VRP task Initialize VRP task Register command lines
Awake task Recover configuration....done

Console 0 is available Press ENTER to start

```

When the terminal displays the preceding information, it indicates that the starting of the VRP is complete. Press **Enter** to enter a Command Line Interface (CLI).

### 5.1.3 Logical Relationships Between Configuration Tasks

There is no logical relationship among restarting the S-switch immediately, restarting the S-switch at a fixed time, and resetting cards.

## 5.2 Restarting the S-switch Immediately

This section describes how to restart the S-switch immediately.

### 5.2.1 Restarting the S-switch Immediately Through Command Lines

### 5.2.2 Restarting the S-switch Through the Power Button on the S-switch

## 5.2.1 Restarting the S-switch Immediately Through Command Lines

### Context



#### CAUTION

The **reboot** command can paralyze the network for a while. Therefore, run the **reboot** command with caution.

Before restarting the S-switch, check whether to save the configuration file and whether the file contents are correct. For details on saving the configuration file, refer to the *Quidway S5300 Series Ethernet Switches Configuration Guide - Basic Configuration*.

---

### Procedure

Run the **reboot** command to restart the S-switch immediately.

By default, this command can only be run by users at the management level.

----End

## 5.2.2 Restarting the S-switch Through the Power Button on the S-switch

### Context



#### CAUTION

The action can paralyze the network for a while. Therefore, perform this action with caution.

Before restarting the S-switch, check whether to save the configuration file and whether the file contents are correct. For details on saving the configuration file, refer to the *Quidway S5300 Series Ethernet Switches Configuration Guide - Basic Configuration*.

---

### Procedure

**Step 1** Press the power button on the S-switch to power off the running S-switch.

**Step 2** Press the power button on the S-switch again to restart the S-switch.

----End

## 5.3 Restarting the S-switch at a Fixed Time

This section describes how to restart the S-switch at a fixed time.

## Context

## Procedure

Run the **schedule reboot** *type* command to enable the function of restarting the S-switch at a fixed time. *type* specifies the time for restarting the S-switch.

- **at** *time*: sets the restarting time.
- **delay** *interval*: specifies the period of time before the S-switch is restarted.

By default, this command can only be run by users at the management level. The S-switch does not support the function of restarting the S-switch at a fixed time by default.

You can run the **display schedule reboot** command to view the configurations of restarting of the S-switch at a fixed time. For details on the procedure, refer to the *Quidway S5300 Series Ethernet Switches - Command Reference*.

----**End**



# 6 Auto-Config Configuration

---

## About This Chapter

This chapter describes basic concepts and configuration procedures of Auto-Config.

### [6.1 Introduction](#)

This section describes the Auto-Config function and its applications.

### [6.2 Specifying the Configuration File for the Next Startup](#)

This section describes how to specify the configuration file for the next startup by using Auto-Config.

## 6.1 Introduction

This section describes the Auto-Config function and its applications.

### [6.1.1 Auto-Config Overview](#)

### [6.1.2 Auto-Config Supported by the S-switch](#)

### [6.1.3 Logical Relationships Between Configuration Tasks](#)

### [6.1.4 History](#)

## 6.1.1 Auto-Config Overview

Auto-Config is a function used by the S-switch to automatically specify the configuration file for the next startup in case of no configuration file for the next startup.

By default, Auto-Config is enabled on the S-switch.

## 6.1.2 Auto-Config Supported by the S-switch

This section describes the applications of Auto-Config on the S-switch.

After the configuration file for the next startup is deleted, the S-switch logs anonymously in to the File Transfer Protocol (FTP) server to obtain the first configuration file and uses this configuration file to start the system.

## 6.1.3 Logical Relationships Between Configuration Tasks

| If You Want to...                                                 | Perform the Task of...                                                     |
|-------------------------------------------------------------------|----------------------------------------------------------------------------|
| Use Auto-Config                                                   | <a href="#">6.2.2 Enabling Auto-Config</a>                                 |
| Clear the configuration file for the next startup on the S-switch | <a href="#">6.2.3 Deleting the Configuration File for the Next Startup</a> |
| Check the configuration of Auto-Config                            | <a href="#">6.2.4 Restarting the S-switch</a>                              |

## 6.1.4 History

| Version         | Revision                   |
|-----------------|----------------------------|
| V200R002C01B010 | This is the first release. |

## 6.2 Specifying the Configuration File for the Next Startup

This section describes how to specify the configuration file for the next startup by using Auto-Config.

[6.2.1 Establishing the Configuration Task](#)

[6.2.2 Enabling Auto-Config](#)

[6.2.3 Deleting the Configuration File for the Next Startup](#)

[6.2.4 Restarting the S-switch](#)

[6.2.5 Checking the Configuration](#)

## 6.2.1 Establishing the Configuration Task

### Applicable Environment

If the S-switch fails to find the configuration file for the next startup, the S-switch can use Auto-Config.

### Pre-configuration Tasks

Before using Auto-Config, complete the following tasks:

- Setting up the Dynamic Host Configuration Protocol (DHCP) server
- Setting up the TFTP server

#### NOTE

For details on setting up the DHCP server and TFTP server, refer to the *Ethernet Switches Basic Configurations*.

The name of the configuration file of Auto-Config cannot be mere numbers or cannot contain special characters such as **1.cfg** or **S#.file**.

## 6.2.2 Enabling Auto-Config

### Prerequisite

Do as follows on the S-switch.

### Context

### Procedure

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

**Step 2** Run the **autoconfig enable** command to enable Auto-Config.

By default, Auto-Config is enabled on the S-switch.

----End

## 6.2.3 Deleting the Configuration File for the Next Startup

### Context

Do as follows on the S-switch.

## Procedure

Run the **undo startup saved-configuration** command to delete the configuration file for the next startup.

----End

## 6.2.4 Restarting the S-switch

### Context

Do as follows on the S-switch.

### Procedure

Run the **reboot** command to restart the S-switch.

----End

## 6.2.5 Checking the Configuration