

**CloudEngine 9800, 8800, 6800 and 5800
V200R023C00SPC500**

Plug-in Operation Guide - Remote Mirroring

Issue	01
Date	2023-09-28



Copyright © Huawei Technologies Co., Ltd. 2023. 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 trademarks of Huawei Technologies Co., Ltd.

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <https://e.huawei.com>

About This Document

Intended Audience

This document is intended for:

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

Symbol Conventions

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

Symbol	Description
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

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

Convention	Description
Boldface	The keywords of a command line are in boldface .
<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.

Interface Numbering Conventions

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

Security Conventions

- Password setting
 - When configuring a password, the cipher text is recommended. To ensure device security, change the password periodically.
 - When you configure a password in plain text that starts and ends with %^%#.....%^%# (the password can be decrypted by the device), the password is displayed in the same manner as the configured one in the configuration file. Do not use this setting. After the system master key is set using the **set master-key** command, do not start and end the key with %@%# because the string starting and ending with %@%# is considered as a valid cipher-text key.
 - When you configure a password in cipher text, different features cannot use the same cipher-text password. For example, the cipher-text password set for the AAA feature cannot be used for other features.

- After the system software is downgraded and the switch restarts with the configuration of the higher version, AAA, VTY, serial interface login, and SNMP user passwords become invalid. As a result, users fail to log in to the switch using the passwords and the switch is disconnected from the network management system.

To address this problem, take the following measures:

- i. If no password is configured for the console port, log in to the device through the console port, and reconfigure AAA and password for users such as VTY and SNMP users. For security purposes, the console port password is recommended.
 - ii. If a password is configured for login through the console port, the password becomes invalid after the downgrade and you cannot log in to the switch through the console port. In this case, contact Huawei technical support engineers for assistance.
- Encryption algorithm
Currently, the device uses the following encryption algorithms: DES, 3DES, AES, DSA, RSA, DH, ECDH, HMAC, SHA1, SHA2, PBKDF2, scrypt, and MD5. The encryption algorithm depends on the applicable scenario. Use the recommended encryption algorithm; otherwise, security defense requirements may be not met.
 - For the symmetrical encryption algorithm, use AES with the key of 256 bits or more.
 - When you need to use an asymmetric cryptography, RSA (3072-bit or longer key) is recommended. In addition, use different key pairs for encryption and signature.
 - For the digital signature, RSA (3072-bit or longer key) or DSA (2048-bit or longer key) is recommended.
 - For key negotiation, DH (2048-bit or longer key) or ECDH (256-bit or longer key) is recommended.
 - For the hash algorithm, use SHA with the key of 256 bits or more.
 - For the HMAC algorithm, use HMAC-SHA2.
 - DES, 3DES, RSA and AES are reversible encryption algorithm. If protocols are used for interconnection, the locally stored password must be reversible.
 - SHA1, SHA2, and MD5 are irreversible encryption algorithm. When configuring a password for local administrator, it is recommended that you use the SHA2 irreversible encryption algorithm.
 - To prevent brute force cracking of the user password, the iteration algorithm is added to the password on the basis of salts. The iteration algorithm uses PBKDF2 or scrypt key export algorithm.
 - The ECB mode has a poor capability of defending against plaintext playback attacks, so ECB is not recommended for password encryption.
 - In SSH2.0, the symmetric cryptography using the CBC mode may undergo the plaintext-recovery attack to cause a data leak. Therefore, the CBC mode is not recommended for SSH2.0.
 - Data
Some data (such as MAC or IP addresses of terminals) may be obtained or used during operation or fault location of your purchased products, services,

features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect data.

- The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this manual are mentioned only to describe the product's function of communication error or failure detection, and do not involve collection or processing of any personal information or communication data of users.

Declaration

- This manual is only a reference for you to configure your devices. The contents in the manual, such as command line syntax, and command outputs, are based on the device conditions in the lab. The manual provides instructions for general scenarios, but do not cover all usage scenarios of all product models. The contents in the manual may be different from your actual device situations due to the differences in software versions, models, and configuration files. The manual will not list every possible difference. You should configure your devices according to actual situations.
- The specifications provided in this manual are tested in lab environment (for example, the tested device has been configured with a certain type of cards or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values with multiple functions enabled on the device.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.

Mapping Between Product Software and Related Products

For details about the mapping between product software and related products, see [CloudEngine Switches Software Versions](#). Select the correct matching version. Otherwise, functions may be unavailable.

Contents

About This Document.....	ii
1 Document Overview.....	1
1.1 Basic Information.....	1
1.2 Antivirus Scan Report.....	2
2 Plug-In Installation Guide.....	3
2.1 Precautions for Plug-In Installation.....	3
2.2 Preparations.....	4
2.2.1 Preparing the Plug-in.....	4
2.2.2 Verifying the Running System Software Version.....	6
2.2.3 Checking Available Space in the Flash Memory.....	6
2.3 Plug-in Installation Procedure.....	7
2.3.1 Uploading/Downloading the Plug-in to the Device.....	8
2.3.1.1 Uploading the Plug-In to the Switch Functioning as an FTP Server.....	8
2.3.1.2 Downloading the Plug-In to the Switch Functioning as an FTP Client.....	9
2.3.1.3 Downloading the Plug-In to the Switch Functioning as an SFTP Client.....	11
2.3.2 Installing the Plug-in.....	12
2.3.3 Verifying the Installation.....	13
2.4 Uninstalling the Plug-in.....	13
3 Remote Mirroring Operation Guide.....	15
3.1 Remote Mirroring Configuration.....	15
3.1.1 Understanding Remote Mirroring.....	15
3.1.2 Licensing Requirements and Limitations for Remote Mirroring.....	18
3.1.3 Configuring Remote Mirroring.....	24
3.1.3.1 Configuring Remote Port Mirroring.....	24
3.1.3.2 Configuring Remote Traffic Mirroring.....	28
3.1.3.3 Configuring Remote VLAN Mirroring.....	36
3.1.3.4 Verifying the Remote Mirroring Configuration.....	39
3.1.4 Configuration Examples for Remote Mirroring.....	39
3.1.4.1 Example for Configuring Layer 2 Remote Port Mirroring.....	40
3.1.4.2 Example for Configuring Layer 3 Remote Port Mirroring (Through a Layer 3 Network).....	43
3.1.4.3 Example for Configuring Layer 3 Remote Port Mirroring (Through a GRE Tunnel).....	45
3.1.4.4 Example for Configuring Remote Truncated Mirroring (Through a Layer 3 Network).....	48

3.2 Mirroring Configuration Commands.....	51
3.2.1 display observe-port.....	51
3.2.2 display port-mirroring.....	53
3.2.3 display traffic-mirroring.....	55
3.2.4 mirroring observe-port.....	57
3.2.5 mirroring observe-port (VLAN view).....	59
3.2.6 observe-port (remote observing port).....	61
3.2.7 observe-port filter enable.....	68
3.2.8 port-mirroring observe-port.....	69
3.2.9 traffic-mirroring (interface view).....	71
3.2.10 traffic-mirroring (system view).....	73
3.3 FAQ.....	76
3.3.1 Why Does MAC Address Learning Need to Be Disabled When Layer 2 Remote Port Mirroring Is Configured in Some Scenarios?.....	76
4 Remote Mirroring Personal Data Description.....	84

1 Document Overview

- 1.1 Basic Information
- 1.2 Antivirus Scan Report

1.1 Basic Information

Table 1-1 describes the basic information about plug-ins of CloudEngine 9800, 8800, 6800, and 5800 series switches.

Table 1-1 Basic information about plug-ins

Applicable Product	Plug-in Name	Applicable Software Version
CE9860EI	CE9800_V200R023C00SPC500_ERSPAN_MOD001.MOD	V200R023C00SPC500
CE8850EI	CE8850EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE8861EI	CE8861EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE8868EI	CE8868EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6881/ CE6820/ CE6863/ CE6863E/ CE6881K/ CE6863K/ CE6881E	CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6856HI	CE6856HI_V200R023C00SPC500_ERSPAN_MOD001.MOD	

Applicable Product	Plug-in Name	Applicable Software Version
CE6857EI	CE6857EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6857E	CE6857E_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6857F	CE6857F_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6865EI	CE6865EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6865E, CE8850E-32 CQ-EI	CE6865E_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6870-48S 6CQ-EI	CE6870S- EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6870-48T 6CQ-EI	CE6870T- EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE5882	CE5882_V200R023C00SPC500_ERSPAN_MOD001.mod	
CE5881	CE5800_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE5855E	CE5855E_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE5855F	CE5855F_V200R023C00SPC500_ERSPAN_MOD001.MOD	

1.2 Antivirus Scan Report

This software package has been scanned by antivirus software and no virus is found. For detailed scanning information, see "Virus Scan Report" of the corresponding device model.

2 Plug-In Installation Guide

This document describes the precautions, preparations, and procedure for plug-in installation, as well as plug-in uninstallation.

NOTE

This document describes how to install the plug-in on a CE6881 switch.

[2.1 Precautions for Plug-In Installation](#)

[2.2 Preparations](#)

[2.3 Plug-in Installation Procedure](#)

[2.4 Uninstalling the Plug-in](#)

2.1 Precautions for Plug-In Installation

Before installing the plug-in, read the precautions carefully.

- Starting from V200R001C00, the switch supports only local mirroring by default and does not support remote mirroring (including Layer 2 and Layer 3 remote mirroring). After the switch is upgraded from a version earlier than V200R001C00 to V200R001C00 or a later version, the remote mirroring configuration is lost. To use this function, download and install the required plug-in first. For details, see the appropriate plug-in operation guide.

If there is the remote mirroring configuration before the upgrade, run the **install-module *file-name* next-startup** command before the upgrade to specify the mirroring plug-in to be installed at the next startup. After the upgrade is complete, the remote mirroring configuration is automatically loaded. If there is no remote mirroring configuration before the upgrade but remote mirroring needs to be configured after the upgrade, you can still run this command before the upgrade to specify the mirroring plug-in to be installed at the next startup, and configure remote mirroring after the upgrade is complete.

To obtain the plug-in and operation guide, contact technical support personnel or log in to <https://support.huawei.com/enterprise> or <https://support.huawei.com>.

- The remote mirroring function is excluded from the system software and delivered as a plug-in since V200R001C00. To use this function, see this document.
- The plug-in should be uploaded or downloaded to the **\$_install_mod** directory of the device. In a stack, if an active/standby switchover is required or may occur, you are advised to upload or download the plug-in to the **\$_install_mod** directories of all the devices.
- The version of the remote mirroring plug-in to be installed must match the software version.
- In different scenarios, you are advised to install the plug-in according to the following procedure.

Table 2-1 Procedure of installing the plug-in in different scenarios

Scenario	Procedure
Only the plug-in needs to be installed, and the device does not need to be upgraded. Alternatively, the plug-in needs to be installed after the device is upgraded.	1. Upload or download the plug-in to the switch. 2. Configure the plug-in to take effect immediately.
The device needs to be upgraded and the plug-in needs to be installed. Ensure that the functions supported by the plug-in are enabled before the upgrade and can still take effect after the upgrade.	1. Upload or download the plug-in to the switch. 2. Configure the plug-in to take effect upon the next startup. 3. Upgrade the device.

2.2 Preparations

2.2.1 Preparing the Plug-in

Procedure

- Step 1** Log in to <https://support.huawei.com/enterprise> or <https://support.huawei.com>, and search for and download the required plug-in by referring to [Table 2-2](#).

Table 2-2 Basic information about plug-ins

Applicable Product	Plug-in Name	Applicable Software Version
CE9860EI	CE9800_V200R023C00SPC500_ERSPAN_MOD001.MOD	V200R023C00SPC500
CE8850EI	CE8850EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	

Applicable Product	Plug-in Name	Applicable Software Version
CE8861EI	CE8861EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE8868EI	CE8868EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6881/ CE6820/ CE6863/ CE6863E/ CE6881K/ CE6863K/ CE6881E	CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6856HI	CE6856HI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6857EI	CE6857EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6857E	CE6857E_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6857F	CE6857F_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6865EI	CE6865EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6865E, CE8850E-32 CQ-EI	CE6865E_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6870-48S 6CQ-EI	CE6870S-EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE6870-48T 6CQ-EI	CE6870T-EI_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE5882	CE5882_V200R023C00SPC500_ERSPAN_MOD001.mod	
CE5881	CE5800_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE5855E	CE5855E_V200R023C00SPC500_ERSPAN_MOD001.MOD	
CE5855F	CE5855F_V200R023C00SPC500_ERSPAN_MOD001.MOD	

----End

2.2.2 Verifying the Running System Software Version

Procedure

Step 1 Verify the running system software version of the switch.

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.200 (CE6881 V200R023C00SPC500)
...
```

Step 2 Check whether the switch has plug-ins installed.

```
<HUAWEI> display module-information
Module Information
-----
Module      Version      InstallTime      PackageName
-----
-           -           -               -
-----
Total = 0
```

If there are running plug-ins on the switch, the names and versions of the plug-ins will be displayed.

----End

2.2.3 Checking Available Space in the Flash Memory

Prerequisites

The available space in the flash memory of a device must be larger than the size of the plug-in software to be uploaded or downloaded to the device.

Procedure

Step 1 Check the available space in the flash memory.

Run the **dir** command in the user view to check the available space in the flash memory of the device.

- Run the **dir** or **dir flash:/** command to check the storage space in the flash memory of the device. In a stack, the two commands display the storage space in the flash memory of the master device.
- Run the **dir slot-id#flash:/** command to check the storage space in the flash memories of all devices except the master device in a stack.

```
<HUAWEI> dir
Directory of flash:/

Idx Attr  Size(Byte) Date      Time      FileName
0  drwx    -   Mar 09 2019 01:48:16  $_backuphome
1  dr-x    -   Jun 21 2019 11:22:32  $_checkpoint
2  dr-x    -   Jun 20 2019 08:41:56  $_install_mod
.....
674,928 KB total (178,120 KB free)
```

Step 2 (Optional) Delete unneeded files.

If the available space in the flash memory is less than the size of the plug-in software to be uploaded or downloaded to the device, delete unneeded files.

NOTE

Before deleting the .cc system software package, .cfg, .zip, or .dat configuration file, .dat or .zip license file, or .pat patch file, ensure that it is not in use.

- A file deleted using the **delete filename** command is placed into the recycle bin but still occupies space in the flash memory. To permanently delete files from the recycle bin, run the **reset recycle-bin** command.
- A file deleted using the **delete /unreserved filename** command is permanently deleted without being placed into the recycle bin. This command is equivalent to running the **delete filename** command first and then the **reset recycle-bin** command.

Permanently delete the unneeded file **test.txt** from the device.

```
<HUAWEI> delete /unreserved flash:/test.txt
```

In a stack, permanently delete the unneeded file **test.txt** from the device with the stack ID 2.

```
<HUAWEI> delete /unreserved 2#flash:/test.txt
```

----End

2.3 Plug-in Installation Procedure

In different scenarios, you are advised to install the plug-in according to the following procedure.

Table 2-3 Procedure of installing the plug-in in different scenarios

Scenario	Procedure
Only the plug-in needs to be installed, and the device does not need to be upgraded. Alternatively, the plug-in needs to be installed after the device is upgraded.	1. Upload or download the plug-in to the switch. 2. Configure the plug-in to take effect immediately.
The device needs to be upgraded and the plug-in needs to be installed. Ensure that the functions supported by the plug-in are enabled before the upgrade and can still take effect after the upgrade.	1. Upload or download the plug-in to the switch. 2. Configure the plug-in to take effect upon the next startup. 3. Upgrade the device.

2.3.1 Uploading/Downloading the Plug-in to the Device

You can use one of the following methods to upload/download the plug-in to the device based on the actual conditions.

2.3.1.1 Uploading the Plug-In to the Switch Functioning as an FTP Server

Pre-configuration Tasks

Before uploading the plug-in from a PC to the switch that functions as an FTP server, you have completed the following tasks:

- Ensure that there are reachable routes between the PC and switch.
- Ensure that the PC supports the FTP client software.

The following example uses the switch as an FTP server. In this example, the FTP user name is **ftpuser**, the password is **Huawei@123**, the switch IP address is **10.1.1.1/24**, the PC IP address is **10.1.1.2/24**, and the FTP working directory is **flash:/\$_install_mod/**. You can change the settings according to the live-network plan.

NOTE

The FTP protocol has security risks; therefore, SFTP is recommended for file management.

Procedure

Step 1 Configure the switch as an FTP server.

Enable the FTP service on the switch, and set the FTP user name to **ftpuser** and password to **Huawei@123**.

```
<HUAWEI> system-view
[~HUAWEI] ftp server enable
[*HUAWEI] commit
[~HUAWEI] aaa
[~HUAWEI-aaa] local-user ftpuser password irreversible-cipher Huawei@123
[*HUAWEI-aaa] local-user ftpuser service-type ftp
[*HUAWEI-aaa] local-user ftpuser level 3
[*HUAWEI-aaa] local-user ftpuser ftp-directory flash:/$_install_mod/
[*HUAWEI-aaa] commit
[~HUAWEI-aaa] return
```

NOTE

The user privilege level must be set to 3 or higher, so that FTP connections can be successfully established.

Step 2 Connect to the FTP server from the PC.

NOTE

This example assumes that the PC runs a Windows operating system.

Save the plug-in to the specified directory (for example, **D:**) on the PC. Choose **Start > Run**. Enter **cmd** and press **Enter**. Enter **ftp 10.1.1.1**. Enter the user name and password as prompted, and press **Enter**. Set the file transfer mode to **binary**.

```
C:\Documents and Settings\Administrator>ftp 10.1.1.1
Connected to 10.1.1.1.
```

```
220 FTP service ready.
User (10.1.1.2:(none)): ftpusher //Enter the FTP user name.
331 Password required for ftpusher.
Password: //Enter the FTP password.
230 User logged in.
ftp> binary //Set the file transfer mode to binary.
200 Type set to I.
```

Step 3 Upload the plug-in software to the switch from the PC.

Run the **put local-filename [remote-filename]** command to upload the plug-in software from the PC to the **flash:/\$_install_mod** directory on the switch. After the plug-in software is uploaded, run the **bye** command to terminate the FTP connection.

```
ftp> put D:\CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
200 Port command okay.
150 Opening BINARY mode data connection for CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD.
226 Transfer complete.
ftp: 109144 bytes sent in 0.05sSeconds 2322.21Kbytes/sec.
ftp> bye
221 Server closing.

C:\Documents and Settings\Administrator>
```

Step 4 Check for the plug-in software on the switch.

Run the **cd** command on the switch to enter the **\$_install_mod** directory and run the **dir** command to check whether the plug-in software is uploaded to this directory.

```
<HUAWEI> cd flash:/$_install_mod
<HUAWEI> dir
Directory of flash:/$_install_mod/

  Idx  Attr   Size(Byte)  Date      Time      FileName
   0  -rw-    80,362  Jun 20 2019 18:56:58  CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD

674,928 KB total (178,152 KB free)
```

----End

2.3.1.2 Downloading the Plug-In to the Switch Functioning as an FTP Client

Pre-configuration Tasks

Before downloading the plug-in from a PC to the switch that functions as an FTP client, you have completed the following tasks:

- Ensure that there are reachable routes between the PC and switch.
- Ensure that the FTP server program is installed on the PC.

In the following example, the switch is used as the FTP client and the PC is used as the FTP server. The FTP user name is **ftpusher**, the password is **Huawei@123**, the PC IP address is **10.1.1.1/24**, and the switch IP address is **10.1.1.2/24**. You can change the settings according to the live-network plan.

NOTE

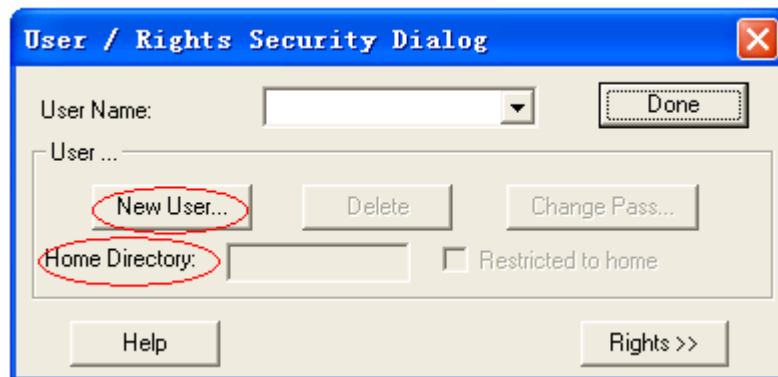
The FTP protocol has security risks; therefore, SFTP is recommended for file management.

Procedure

Step 1 Configure the PC as an FTP server.

Run the FTP server program (for example, wftpd32) on the PC. Choose **Security > Users/rights**.

Figure 2-1 Configuring the FTP server



Click **New User** in the displayed dialog box, and set the user name to **ftpuser** and password to **Huawei@123**. Enter the FTP working directory in the **Home Directory** text box on the PC. In this example, the working directory is **D:\ftp**. Click **Done** to close the dialog box. Do not close the FTP server program when the plug-in is being downloaded.

Step 2 Connect to the FTP server from the switch.

```
<HUAWEI> cd flash:/install_mod //Set the current working directory of the switch.
<HUAWEI> ftp 10.1.1.1
Trying ftp 10.1.1.1 ...
Press CTRL + K to abort
Connected to ftp 10.1.1.1.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(ftp 10.1.1.1:(none)):ftpuser //Enter the FTP user name.
331 Give me your password, please
Enter password: //Enter the FTP password.
230 Logged in successfully
[ftp] binary //Set the file transfer mode to binary.
200 Type is Image (Binary)
```

Step 3 Download the plug-in software.

Run the **get local-filename [remote-filename]** command on the switch to download the plug-in software from the FTP server (PC). After the software is downloaded, run the **bye** command to terminate the FTP connection.

```
[ftp] get CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
500 Unidentified command SIZE CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
200 PORT command okay
150 "D:\FTP\CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD" file ready to send (109144 bytes) in
IMAGE / Binary mode
..
226 Transfer finished successfully.

FTP: 109144 byte(s) received in 1.533 second(s) 69.527Kbyte(s)/sec.
[ftp] bye
```

Step 4 Check for the plug-in software on the switch.

Run the **cd** command on the switch to enter the **\$_install_mod** directory and run the **dir** command to check whether the plug-in software is uploaded to this directory.

```
<HUAWEI> cd flash:/$_install_mod
<HUAWEI> dir
Directory of flash:/$_install_mod/

Idx Attr   Size(Byte) Date      Time      FileName
 0 -rw-      80,362 Jun 20 2019 18:56:58 CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD

674,928 KB total (178,152 KB free)
```

----End

2.3.1.3 Downloading the Plug-In to the Switch Functioning as an SFTP Client

Pre-configuration Tasks

Before downloading the plug-in from a PC to the switch that functions as an SFTP client, you have completed the following tasks:

- Ensure that there are reachable routes between the PC and switch.
- Ensure that the SFTP server program is installed on the PC.

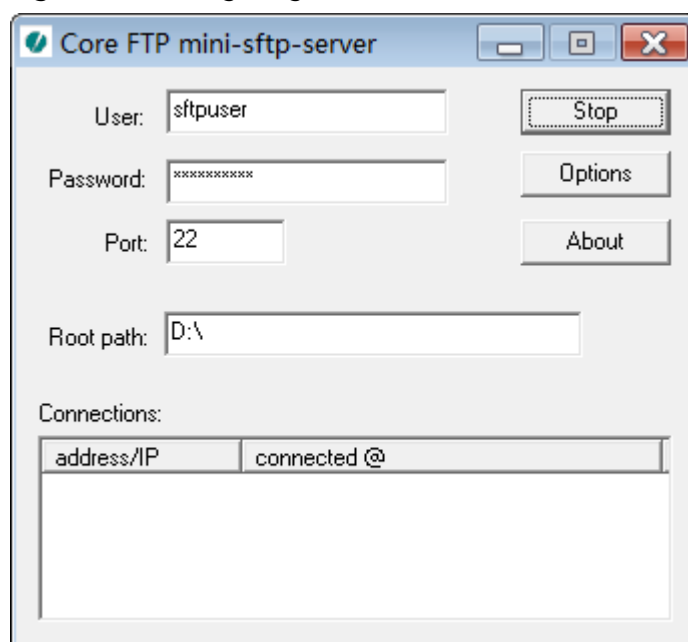
In the following example, the switch is used as the SFTP client and the PC is used as the SFTP server. The SFTP user name is **sftpuser**, the password is **Huawei@123**, the switch IP address is **10.1.1.2/24**, and the PC IP address is **10.1.1.1/24**. You can change the settings according to the live-network plan.

Procedure

Step 1 Configure the PC as an SFTP server.

Run the SFTP server program (for example, Core FTP mini-sftp-server) on the PC.

Figure 2-2 Configuring the SFTP server



In the displayed dialog box, set **User** to **sftpuser** and **Password** to **Huawei@123**. Set **Root path** to the SFTP working directory on the PC, for example, **D:**. Do not close the SFTP server program when the plug-in is being downloaded.

Step 2 Connect to the SFTP server from the switch.

```
<HUAWEI> cd flash:/$_install_mod/ //Set the current working directory of the switch.
<HUAWEI> system-view
[~HUAWEI] ssh client first-time enable
[*HUAWEI] commit
[~HUAWEI] sftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it? [Y/N]: y
Save the server's public key? [Y/N]: n

Please input the username: sftpuser //Enter the SFTP user name.
Enter password: //Enter the SFTP password.
sftp-client>
```

Step 3 Download the plug-in software.

Run the **get local-filename [remote-filename]** command on the switch to download the plug-in software from the SFTP server (PC). After the software is downloaded, run the **quit** command to terminate the SFTP connection.

```
sftp-client> get CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
Remote file: / CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD ---> Local file:
CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
Downloading the file. Please wait.../
Downloading file successfully ended.
File download is completed in 1 seconds.
sftp-client> quit
```

Step 4 Check for the plug-in software on the switch.

Run the **cd** command on the switch to enter the **\$_install_mod** directory and run the **dir** command to check whether the plug-in software is uploaded to this directory.

```
<HUAWEI> cd flash:/$_install_mod
<HUAWEI> dir
Directory of flash:/$_install_mod/

  Idx  Attr   Size(Byte)  Date       Time       FileName
   0   -rw-    80,362   Jun 20 2019 18:56:58  CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD

674,928 KB total (178,152 KB free)
```

----End

2.3.2 Installing the Plug-in

Two methods are available to install the plug-in. Select a method according to [2.1 Precautions for Plug-In Installation](#).

 NOTE

In a stack, before loading the plug-in, you are advised to run the **copy file-name all#flash:/\$_install_mod/** command to copy the plug-in to the **\$_install_mod** directories of all devices.

- Configure the device to install the plug-in immediately.

```
<HUAWEI> install-module CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
```
- Configure the device to install the plug-in upon the next startup.

```
<HUAWEI> install-module CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD next-startup
```

2.3.3 Verifying the Installation

- Run the **display module-information verbose** command to check whether the plug-in is successfully installed.
If no information about the plug-in is displayed, the plug-in fails to be installed.
- Run the **display module-information next-startup** command to check the plug-in to be installed upon the next startup.

```
<HUAWEI> display module-information next-startup
Next startup module packages

-----
No.  PackageName
-----
1    flash:/$_install_mod/CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
-----
Total = 1
```

If no information about the plug-in is displayed, the plug-in to be installed upon the next startup fails to be configured.

2.4 Uninstalling the Plug-in

Context

Select an uninstallation method that suits your need.

NOTE

Before uninstalling the plug-in, delete the configurations of features related to this plug-in. Exercise caution when uninstalling the plug-in.

Procedure

Step 1 Configure the device to uninstall the plug-in immediately.

```
<HUAWEI> uninstall-module CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD
This will uninstall the module. Are you sure? [Y/N]: y
```

To check whether the plug-in has been uninstalled after the **uninstall-module file-name** command is executed, run the **display module-information** command.

```
<HUAWEI> display module-information
Module Information
-----
Module  Version      InstallTime      PackageName
-----
-        -            -                -                //No plug-in is installed on the switch.
-----
Total = 0
```

Step 2 Configure the device to uninstall the plug-in upon the next startup.

```
<HUAWEI> uninstall-module CE6800_V200R023C00SPC500_ERSPAN_MOD001.MOD next-startup
```

To check whether the configuration is successful after the **uninstall-module file-name next-startup** command is executed, run the **display module-information next-startup** command.

```
<HUAWEI> display module-information next-startup
Next startup module packages
-----
No.   PackageName
-----
-     --                //No plug-in will be automatically installed upon the next startup.
-----
Total = 0

----End
```

3 Remote Mirroring Operation Guide

NOTE

Remote mirroring is mainly used for network monitoring and fault management and may use user communication information. Huawei will not collect or save user communication information independently. You must use this function in compliance with applicable laws and regulations. Ensure that your customers' privacy is protected when you are using or saving communication information.

[3.1 Remote Mirroring Configuration](#)

[3.2 Mirroring Configuration Commands](#)

[3.3 FAQ](#)

3.1 Remote Mirroring Configuration

3.1.1 Understanding Remote Mirroring

In remote mirroring, mirrored packets are sent to specified observing ports, which then send the packets to monitoring devices across a Layer 2 or Layer 3 network for analysis and monitoring.

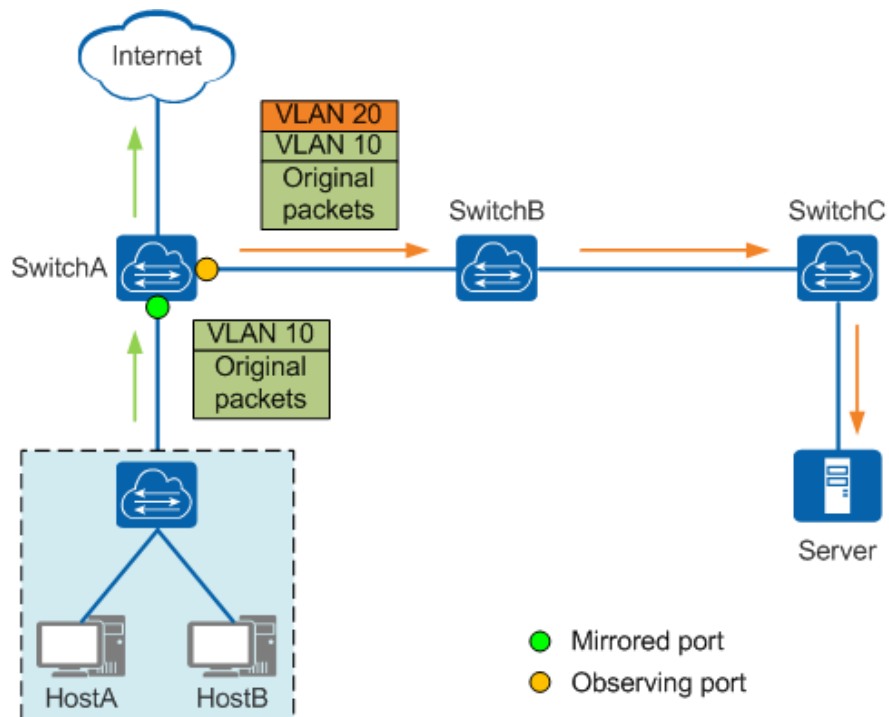
Remote mirroring includes Layer 2 remote mirroring and Layer 3 remote mirroring.

- **Layer 2 remote mirroring (RSPAN)**

In Layer 2 remote mirroring, mirrored packets are encapsulated with a VLAN tag and then forwarded to monitoring devices across a Layer 2 network.

In [Figure 3-1](#), SwitchA copies packets passing through a mirrored port to a remote observing port, which then adds an outer remote mirrored VLAN tag to the mirrored packets and forwards these packets to a Layer 2 network. To ensure that the mirrored packets can be forwarded to the monitoring device (Server), configure ports that connect the intermediate Layer 2 device to the remote observing port and monitoring device to permit packets of the remote mirrored VLAN.

Figure 3-1 Networking of Layer 2 remote port mirroring

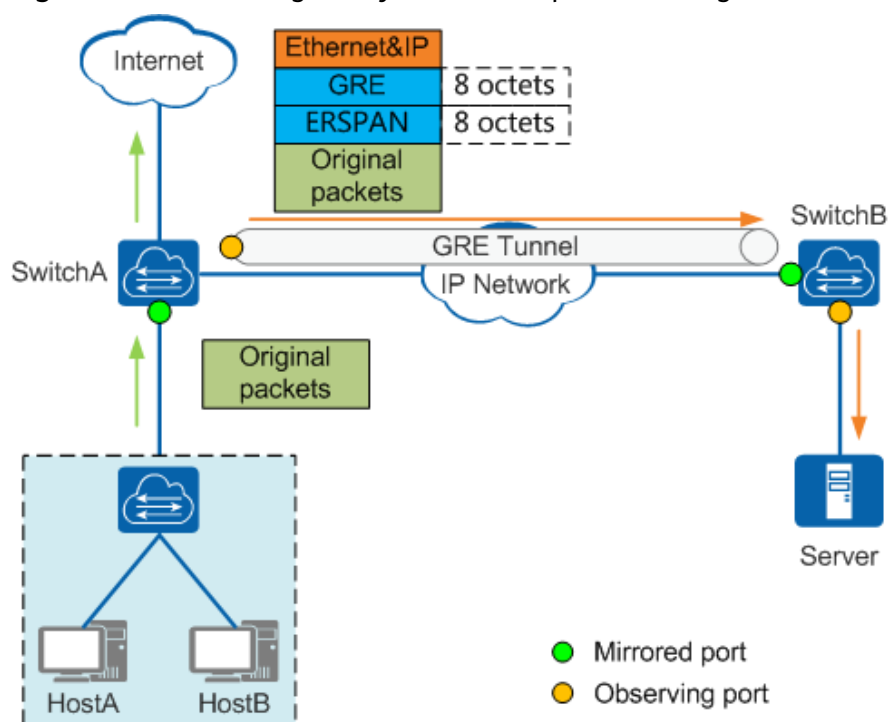


- **Layer 3 remote mirroring (ERSPAN)**

In Layer 3 remote mirroring, mirrored packets are encapsulated with a GRE header and then forwarded to monitoring devices across a Layer 3 IP network. Mirrored packets can be forwarded over a GRE tunnel or through a Layer 3 IP network.

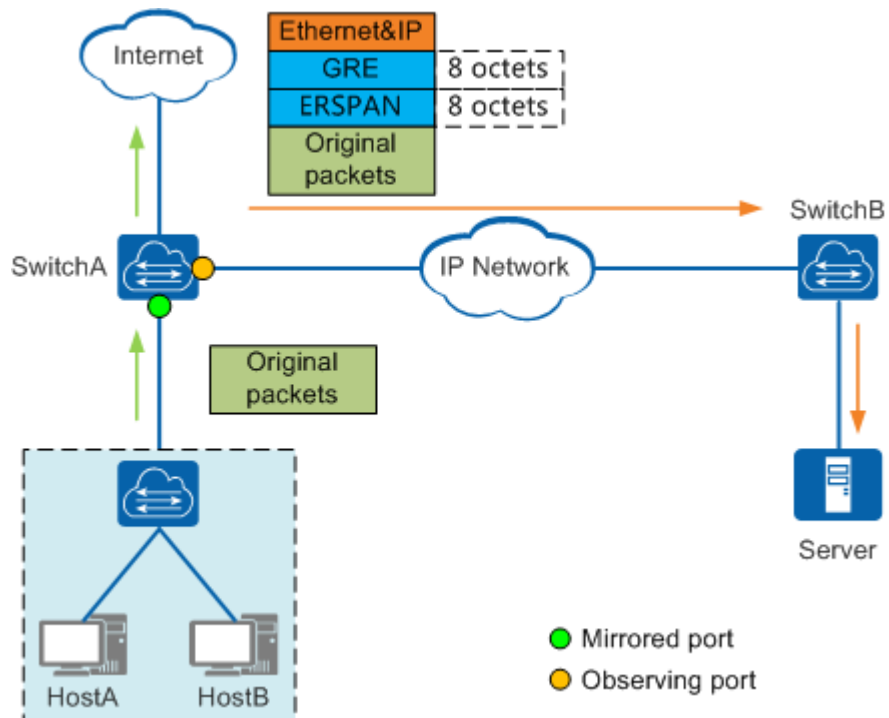
- In [Figure 3-2](#), SwitchA copies packets passing through a mirrored port to a remote observing port (Tunnel interface). The remote observing port encapsulates the packets with a GRE header and then forwards the packets to SwitchB through a GRE tunnel. The mirrored packets are forwarded to SwitchB. To ensure that these packets are forwarded to the monitoring device (Server), SwitchB also needs to perform local port mirroring. It needs to copy the mirrored packets received by the physical port of the tunnel interface to the port connected to the monitoring device, and finally this port forwards the mirrored packets to the monitoring device.

Figure 3-2 Networking of Layer 3 remote port mirroring



- In [Figure 3-3](#), SwitchA copies packets passing through a mirrored port to a remote observing port, which then encapsulates the packets with a GRE header and forwards the packets to the monitoring device (Server) across a Layer 3 IP network. The source and destination IP addresses in the IP header encapsulated in GRE packets are manually configured. To ensure that mirrored packets can reach the monitoring device, specify the monitoring device's IP address and SwitchA's interface IP address as the destination and source IP addresses respectively.

Figure 3-3 Networking of Layer 3 remote port mirroring



3.1.2 Licensing Requirements and Limitations for Remote Mirroring

Mirroring Specifications

- **Observing Port Specifications**

In V100R006C00 and earlier versions, the switch can have a maximum of eight observing ports configured but can use at most two of them at a time. Each observing port can be used to copy both inbound and outbound traffic.

In V200R001C00 and later versions, A switch can have a maximum of eight observing ports configured. A CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, and CE6881E switch can use at most eight observing ports at a time, while other switch models can use at most four observing ports at a time. On the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, and CE6881E, each observing port can be used to copy both inbound and outbound traffic. On a switch except the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, and CE6881E, the maximum numbers of available observing ports for inbound and outbound traffic are calculated separately. For example, when the same observing port is specified for both inbound and outbound traffic, the number of available observing ports for inbound and outbound traffic is 2, not 3.

- **1:N Mirroring Specifications**

In 1:N mirroring, packets on one mirrored port are copied to N observing ports.

In port mirroring, the switch supports 1:N mirroring, in which N indicates the number of available observing ports on the switch.

Only the CE6870EI, CE6863, CE6863E, CE6863K, CE6881E, CE6881, CE5881, CE6881K, CE6820 support 1:N VLAN mirroring.

Only the CE6870EI support 1:N traffic mirroring.

The CE5855E, CE5855F does not support 1:N MQC-based traffic mirroring.

In versions earlier than V200R021C00, the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, and CE6881E do not support 1:N MQC-based traffic mirroring. In V200R021C00 and later versions, the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, and CE6881E support 1:N MQC-based traffic mirroring. For the CE9860EI, supports 1:N MQC-based traffic mirroring.

Packets in the same direction of a mirrored port can only be copied to either an observing port or an observing port group.

Packets in the same direction of a mirrored port can be copied to only one observing port group.

- **N:1 Mirroring Specifications**

In N:1 mirroring, packets on N mirrored ports are copied to one observing port.

The switch supports N:1 mirroring.

- **M:N Mirroring Specifications**

In M:N mirroring, packets on M mirrored ports are copied to N observing ports. An M:N mirroring rule is equivalent to multiple 1:N mirroring rules.

The switch supports M:N mirroring.

Feature Limitations

- Since V200R001C00, by default, the switch supports only local mirroring and does not support remote mirroring (including Layer 2 remote mirroring RSPAN and Layer 3 remote mirroring ERSPAN). If you want to enable remote mirroring on the switch, the switch must have the plug-in of the required version installed.

After the switch is upgraded from a version earlier than V200R001C00 to V200R001C00 or later, the remote mirroring configuration will be lost on the switch.

Since V200R001C00, the remote mirroring function cannot be used with ISSU. The remote mirroring function needs to be deleted from the switch in either of the following situations: The switch needs to be upgraded from a version earlier than V200R001C00 to V200R001C00 or later using ISSU. The switch needs to be upgraded from V200R001C00 or later using ISSU.

- ERSPAN packets passing through a GRE tunnel are mirrored packets encapsulated with a GRE header, and will not participate in GRE traffic statistics collection.
- When configuring an observing port for ERSPAN, if you also configure both the outbound interface and destination IP address:

When the command is run, the system prompts you to ensure that the configured outbound interface is the same as the outbound interface of the route corresponding to the configured destination IP address. If they are different, traffic forwarding may be affected.

After the configuration is committed, the system prompts you with a risk of abnormal traffic forwarding if the configured outbound interface is different

from the outbound interface queried in the routing table based on the destination IP address. This risk message is displayed only after the configuration is committed, and will not be displayed in other scenarios, such as route change scenarios.

- Mirroring traffic occupies the forwarding bandwidth of the switch. During full-load traffic forwarding on cards, enabling the mirroring function may cause packet loss due to insufficient forwarding capability.
- The forwarding traffic and the mirrored traffic cannot exceed the chip forwarding bandwidth. The mirrored traffic across the board needs to occupy the bandwidth of the stack interface.
- For the CE6863, CE6863E, CE6863K, CE6881E, CE6881K, CE6881, and CE5881, mirror traffic cross-chip forwarding will occupy the bandwidth of the inline port. It will impact the service traffic cross-chip forwarding, so avoid cross-chip mirroring.
- When Layer 3 remote mirroring ERSPAN is used, the mirrored packets can be forwarded only at common Layer 2 and Layer 3 modes, and cannot be forwarded over VXLAN or MPLS tunnels. In addition, the mirrored packets cannot be sent to VBDIF interfaces.
- An interface bound to a local VPN cannot be used as an observing port for remote mirroring.
- When Layer 3 remote mirroring (ERSPAN) is used, ECMP-based load balancing is not supported for mirrored packets.
- For the CE8868EI, CE8861EI, CE8850-64CQ-EI, CE6857EI, and CE6865EI, CE6865E, CE8850E-32CQ-EI, observing ports in enhanced mode can be specified only during the configuration of simplified traffic mirroring.
- To prevent information from being lost during mirroring, you are advised to configure ports of the same type as observing and mirrored ports and set the same bandwidth for the observing and mirrored ports. If the bandwidth of an observing port is smaller than that of a mirrored port, information may be lost on the observing port during mirroring.
- To prevent other services from conflicting with mirroring services, do not configure other services on observing ports.
- In a stack system, the observing and mirrored ports can be configured on different devices. However, physical stack member ports do not support inter-device mirroring; the observing ports and physical stack member ports that function as mirrored ports must be configured on the same device.
- When configuring Layer 2 remote port mirroring, do not use a remote mirroring VLAN to transmit other service packets. You are advised to run the **mac-address learning disable** command in the VLAN view on the device that forwards mirrored packets to disable MAC address learning of the remote mirroring VLAN.
- A port cannot be configured as both a mirrored port and an observing port. An Ethernet or Eth-Trunk port can be configured as a mirrored port. An Eth-Trunk member interface cannot be configured as an observing port.
- If an Eth-Trunk is configured as a mirrored port, its member interfaces cannot be configured as mirrored ports.

If a member interface of an Eth-Trunk is configured as a mirrored port, the Eth-Trunk cannot be configured as a mirrored port.

- For CE9860EI, CE8850EI, CE8861EI, CE8868EI, CE6856HI, CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, and CE5855E, CE5855F series switches, if the mirrored port is an access port, the outbound packets mirrored to an observing port carry VLAN tags, and are different from original packets.
- For CE9860EI, CE8850EI, CE8861EI, CE8868EI, CE6856HI, CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, and CE5855E, CE5855F series switches, the following configurations in the outbound direction of a mirrored port do not take effect for mirrored traffic:
 - Configure an ACL in which the rule is deny.
 - Configure traffic policing.
 - Configure WRED profiles.
 - Configure the traffic shaping rate.
 - Configure the queue scheduling mode.

Outbound packets discarded on the mirrored port are still mirrored to the observing port.

- If an MQC-based traffic policy or an ACL-based simplified traffic policy is applied to the outbound direction on the CE6863, CE6863E, CE6863K, CE6881E, CE6881, CE5881, CE6881K, or CE6820, the traffic policy cannot match mirrored traffic.
- For the CE6857EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8850EI, CE8861EI, and CE8868EI, in a distributed VXLAN gateway scenario, when the enhanced mode of the VXLAN gateway is loopback and MQC-based traffic mirroring is applied globally, an observing port will receive multiple copies of mirrored packets.
- If port mirroring is configured on a port of the CE6870EI and traffic statistics are collected in the inbound direction of the VLAN to which this port is added, traffic statistics of this port are twice the actual values.
- NetStream and port mirroring can be configured on the same interface, and NetStream does not conflict with MQC-based traffic mirroring, simplified traffic mirroring, or VLAN mirroring.

On the CE6870EI:

- When inbound NetStream sampling is configured to use snoop resources, port mirroring and inbound NetStream can be configured on the same interface.

Since V200R005C00, sFlow, NetStream, and port mirroring can be configured together in the inbound direction.

- When inbound NetStream sampling is not configured to use snoop resources:

In versions earlier than V200R019C00, port mirroring and NetStream cannot be configured on the same interface. In V200R019C00 and later versions, inbound port mirroring and inbound NetStream cannot be configured together on the same interface, and outbound port mirroring and outbound NetStream also cannot be configured together on the same interface.

NetStream conflicts with MQC-based traffic mirroring, simplified traffic mirroring, and VLAN mirroring. After NetStream is configured on an interface, do not configure any MQC-based traffic mirroring, simplified traffic mirroring, or VLAN mirroring to contain this interface. If

NetStream and a mirroring function (MQC-based traffic mirroring, simplified traffic mirroring, or VLAN mirroring) are configured on the same interface, NetStream does not sample the mirrored packets.

Since V200R005C00, sFlow, NetStream, and port mirroring cannot be configured together in the same direction on an interface or in the same direction on both an Eth-Trunk and its member interfaces.

On other models:

- In versions earlier than V200R019C00, port mirroring and NetStream cannot be configured together on the same interface. Port mirroring and NetStream can be configured together on the same interface in V200R019C00 and later versions.
- In V200R005C20, port mirroring and NetStream can be configured together on the same interface.
- The mirrored packets sent by an observing port cannot be sampled.
- If NetStream or sFlow has been configured on an Eth-Trunk, port mirroring cannot be configured on the member interfaces of the Eth-Trunk. If port mirroring has been configured on member interfaces of an Eth-Trunk, NetStream or sFlow cannot be configured on the Eth-Trunk.
- Port mirroring, VLAN mirroring, MQC-based traffic mirroring, and simplified traffic mirroring may conflict with each other. The details are as follows:
 - For the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, port mirroring, VLAN mirroring, MQC-based traffic mirroring, and simplified traffic mirroring cannot be configured together on the same port. If port mirroring, VLAN mirroring, MQC-based traffic mirroring, and simplified traffic mirroring are configured together on the same port, only one of them takes effect.
 - For switches excluding the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, if port mirroring, VLAN mirroring, MQC-based traffic mirroring, and simplified traffic mirroring are configured together on the same port, and the observing ports of these mirroring functions are different, these mirroring functions can take effect simultaneously. If the observing ports of these mirroring functions are the same, only one among them can take effect.
- For switches excluding the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, the inbound VLAN mirroring function cannot mirror packets terminated by tunnels (such as GRE tunnels).
- For CE series switches except the CE6870EI, when outbound mirroring is performed on TRILL unicast packets sent from the user side to the network side, the source MAC address, destination MAC address, and VLAN ID encapsulated in the packets received by the observing port are all 0s, but service data is correct.
- For switches excluding the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, the **DSCP**, **IP Precedence**, **802.1p**, and **MPLS EXP** fields in mirrored outbound packets are the values of the corresponding fields in the original packets.
- When outbound encapsulated VXLAN packets on VXLAN tunnel encapsulation devices (CE series switches except the CE6870EI) are mirrored, the following situations occur: The mirrored multicast, broadcast, and unknown unicast packets are not encapsulated; the destination MAC address, source MAC

address, and VLAN ID encapsulated in the mirrored known unicast packets are all 0s, and original packets are correct. The problem does not occur when VXLAN packets are forwarded across VNIs at Layer through a loopback interface.

- When outbound traffic on a VXLAN tunnel endpoint (a switch except the CE6870EI) is mirrored, inbound multicast traffic and unknown unicast traffic are also mirrored. To prevent this problem, you are advised to mirror inbound traffic on the other end of the tunnel. This operation ensures that only outbound traffic on switch is mirrored.
- When Layer 3 remote mirroring is configured on a port of the CE6870EI, do not mirror outbound traffic on another port to this port. Otherwise, the traffic will be looped, affecting traffic forwarding.
- For switches excluding the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, when outbound mirroring is performed on Layer 3 main interfaces, mirrored packets will carry the VLAN ID, which is the reserved VLAN ID and defaults to 4064.
- On the CE6870EI:
 - When inbound flow sampling is configured to use snoop resources:
Port mirroring and inbound sFlow sampling can be configured on the same interface. Inbound sFlow sampling conflicts with VLAN mirroring. As a result, sFlow cannot sample packets to be mirrored by VLAN mirroring.
Since V200R005C00, sFlow, NetStream, and port mirroring can be configured together in the inbound direction.
 - When inbound flow sampling is not configured to use snoop resources:
In versions earlier than V200R019C00, port mirroring and sFlow sampling cannot be configured on the same interface. In V200R019C00 and later versions, inbound sFlow sampling and inbound port mirroring cannot be configured on the same interface, and outbound sFlow sampling and outbound port mirroring also cannot be configured on the same interface.
sFlow sampling conflicts with MQC-based traffic mirroring, simplified traffic mirroring, and VLAN mirroring. After sFlow sampling is configured on an interface, do not configure any MQC-based traffic mirroring, simplified traffic mirroring, or VLAN mirroring to contain this interface. If the sFlow and mirroring functions (MQC-based traffic mirroring, simplified traffic mirroring, or VLAN mirroring) are configured on the same interface, sFlow cannot sample the packets to be mirrored.
Since V200R005C00, sFlow, NetStream, and port mirroring cannot be configured together in the same direction on an interface or in the same direction on both an Eth-Trunk and its member interfaces.
- On other models:
 - In versions earlier than V200R019C00, port mirroring and sFlow sampling cannot be configured on the same interface. In V200R019C00 and later versions, port mirroring and sFlow sampling can be configured on the same interface.
 - The mirrored packets sent by an observing port cannot be sampled.
- Unknown TRILL unicast packets are mirrored on the device that decapsulates TRILL packets.

- For CE series switches except the CE6870EI, outbound port mirroring cannot mirror packets sent by hosts.
- For CE series switches, outbound port mirroring cannot mirror packets sent by hosts.
- When Layer 3 remote mirroring is configured in the inbound direction of a main interface on a CE series switch except the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, and CE6881E, original packets of mirrored packets carry the reserved VLAN tag.
- For CE6870EI series switches running versions earlier than V200R003C00, if the **total length** field in Layer 3 remote mirrored packets is incorrectly encapsulated, an exception may occur when the analyzer or other network devices parse the Layer 3 remote mirrored packets.
- When a CE series switch except the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E mirrors reassembled fragmented packets, fragmented packets sent from ports are mirrored in port mirroring and reassembled packets are mirrored in traffic mirroring.
- For CE series switches except the CE6870EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, when outbound mirroring is configured on a port and broadcast, multicast, and unknown unicast packets are sent, only one copy of the packets can be mirrored.
- To perform inbound VLAN mirroring for packets that require VLAN mapping, configure inbound VLAN mirroring in the VLAN view after performing VLAN mapping. Mirrored packets are original packets before VLAN mapping.
- For the CE8868EI, CE8861EI, CE8850EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, and CE6857EI, CE6857E, CE6857F series switches, mirrored packets sent from an observing port occupy the priority queue of the forwarded packets. For other CE series switches, mirrored packets sent from an observing port always occupy queue 0.
- When the CE6870EI is an intermediate node of a VXLAN tunnel and simplified traffic mirroring is configured for VXLAN packets, the VXLAN packets cannot be mirrored if the inner VXLAN packets carry VLAN tags.
- In enhanced Layer 3 remote mirroring mode, when the CE8868EI, CE8861EI, CE8850-64CQ-EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, or CE6857EI functions as a VXLAN tunnel termination device and mirrors incoming traffic on tunnel interfaces, the switch will add a VLAN tag to the mirrored packets if the VXLAN packets to be mirrored have no outer VLAN tag and need to be forwarded across VBDIF interfaces.
 - On the CE8850-64CQ-EI, the added VLAN tag is a reserved VLAN.
 - On the CE8868EI, CE8861EI, CE6865EI, CE6865E, CE8850E-32CQ-EI and CE6857EI, CE6857E, CE6857F, the added VLAN tag is VLAN 0.
- For the CE6870EI switch, when simplified traffic mirroring with an observing port in enhanced mode is configured in the interface view and intelligent traffic analysis is also configured, the simplified traffic mirroring function takes precedence.

3.1.3 Configuring Remote Mirroring

3.1.3.1 Configuring Remote Port Mirroring

Context

In remote port mirroring, packets that pass through a mirrored port are copied to observing ports, which then send the packets to monitoring devices across a Layer 2 or Layer 3 network.

Pre-configuration Tasks

Before configuring Layer 3 remote mirroring, configure a GRE tunnel between the observing port and monitoring device so that mirrored packet packets can be forwarded through the GRE tunnel. If no GRE tunnel is configured between the observing port and the monitoring device, mirrored packet packets are forwarded across a Layer 3 network.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Configure a remote observing port.

NOTE

For the CE8868EI, CE8861EI, CE8850-64CQ-EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857E, CE6857F, and CE6857EI, parameters **interface** and **enhanced-mode** cannot be configured together.

- For Layer 2 remote mirroring:
 - (On the CE9860EI, CE5855E, CE5855F, CE8868EI, CE8861EI, CE8850EI, CE6870EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857EI, CE6857E, CE6857F, and CE6856HI) Run **observe-port** [*observe-port-index*] **interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id*
 - (On the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E) Run **observe-port** [*observe-port-index*] **interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id* [*cir cir-value* [**kbps** | **mbps** | **gbps**]] [**truncate packet** *packet-length*]
- For Layer 3 remote mirroring:
 - On the CE6857EI, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8861EI, and CE8868EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**truncate** | **enhanced-mode** [**length** *packet-length*]].
 - If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate** | **enhanced-mode** [**length** *packet-length*]].
 - If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-**

instance *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate** | **enhanced-mode** [**length** *packet-length*]].

- On the CE6857E:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**truncate**].
 - If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate**].
 - If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate**].
- On the CE6870EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**erspan-id** *erspan-id*].
 - If mirrored packets need to be forwarded through a Layer 3 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value*] [**erspan-id** *erspan-id*].
- On the CE9860EI, CE6856HI, CE5855E, CE5855F:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id*.
 - (CE9860EI, CE6856HI, CE5855E, CE5855F) If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *.
 - (CE9860EI) If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *.
- On the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id*

[**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbps** | **mbps** | **gbps**]] [**truncate packet** *packet-length*].

- If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbps** | **mbps** | **gbps**]] [**truncate packet** *packet-length*].
- If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbps** | **mbps** | **gbps**]] [**truncate packet** *packet-length*].
- On the CE8850-64CQ-EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**enhanced-mode** [**length** *packet-length*]].
 - If mirrored packets need to be forwarded through a Layer 3 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type* *interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**enhanced-mode** [**length** *packet-length*]].

By default, no remote observing port is configured.

Step 3 (Optional) Run **observe-port filter enable**

Basic forwarding validity check on an observing port is enabled.

By default, the basic forwarding validity check function is disabled on an observing port.

NOTE

This function is supported only by the CE6870EI.

Step 4 Run **interface** *interface-type interface-number*

The interface view is displayed.

Step 5 Run **port-mirroring observe-port** *observe-port-index* { **both** | **inbound** | **outbound** } [**session-id** *session-id*]

Traffic on the interface is mirrored to the observing port.

NOTE

The **session-id** *session-id* parameter is supported only by the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E.

Step 6 Run **commit**

The configuration is committed.

----End

3.1.3.2 Configuring Remote Traffic Mirroring

Context

In remote traffic mirroring, packets of a specified service flow that passes through a mirrored port are copied to observing ports, which then send the packets to monitoring devices across a Layer 2 or Layer 3 network.

Pre-configuration Tasks

Before configuring Layer 3 remote mirroring, configure a GRE tunnel between the observing port and monitoring device so that mirrored packet packets can be forwarded through the GRE tunnel. If no GRE tunnel is configured between the observing port and the monitoring device, mirrored packet packets are forwarded across a Layer 3 network.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Configure a remote observing port.

NOTE

For the CE8868EI, CE8861EI, CE8850-64CQ-EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857E, CE6857F, and CE6857EI, parameters **interface** and **enhanced-mode** cannot be configured together.

- For Layer 2 remote mirroring:
 - (On the CE9860EI, CE5855E, CE5855F, CE8868EI, CE8861EI, CE8850EI, CE6870EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857EI, CE6857E, CE6857F, and CE6856HI) Run **observe-port** [*observe-port-index*] **interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id*
 - (On the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E) Run **observe-port** [*observe-port-index*] **interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id* [**cir** *cir-value* [**kbps** | **mbps** | **gbps**]] [**truncate packet** *packet-length*]
- For Layer 3 remote mirroring:
 - On the CE6857EI, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8861EI, and CE8868EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**truncate** | **enhanced-mode** [*length packet-length*]].

- If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate** | **enhanced-mode** [**length** *packet-length*]].
- If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate** | **enhanced-mode** [**length** *packet-length*]].
- On the CE6857E:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**truncate**].
 - If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate**].
 - If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate**].
- On the CE6870EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**erspan-id** *erspan-id*].
 - If mirrored packets need to be forwarded through a Layer 3 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value*] [**erspan-id** *erspan-id*].
- On the CE9860EI, CE6856HI, CE5855E, CE5855F:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id*.
 - (CE9860EI, CE6856HI, CE5855E, CE5855F) If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *.

- (CE9860EI) If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *.
- On the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbits** | **mbits** | **gbits**]] [**truncate packet** *packet-length*].
 - If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbits** | **mbits** | **gbits**]] [**truncate packet** *packet-length*].
 - If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbits** | **mbits** | **gbits**]] [**truncate packet** *packet-length*].
- On the CE8850-64CQ-EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**enhanced-mode** [**length** *packet-length*]].
 - If mirrored packets need to be forwarded through a Layer 3 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**enhanced-mode** [**length** *packet-length*]].

By default, no remote observing port is configured.

Step 3 (Optional) Run **observe-port filter enable**

Basic forwarding validity check on an observing port is enabled.

By default, the basic forwarding validity check function is disabled on an observing port.

NOTE

This function is supported only by the CE6870EI.

Step 4 Configure a mirrored port and packet matching rules.

Two methods are available: simplified traffic mirroring and MQC-based traffic mirroring. Simplified traffic mirroring is easy to configure and applies to configuration delivery and management in FabricInsight. MQC-based traffic mirroring is complex to configure but has rich and detailed packet matching rules.

Simplified traffic mirroring

- Configure simplified traffic mirroring globally.

- a. Configure packet matching rules.

Run **traffic-mirroring** [**vxlan** [**tag-format** { **none** | **single** }]] [**ipv6**]
{ **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * } **observe-port** *observe-port-index* &<1-8> **inbound** [**slot** *slot-id*]

Simplified traffic mirroring is configured globally.

By default, simplified traffic mirroring is not configured globally.

NOTE

You can specify 1 to 8 *observe-port-index* parameters simultaneously only on the CE6870EI.

For the CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8850-64CQ-EI, CE8868EI, and CE8861EI, observing ports in enhanced mode can be specified only when you configure simplified traffic mirroring.

Only the CE6863, CE6863E, CE6863K, CE6881E, CE6820, CE6881K, CE6881, and CE5881 support the **ipv6** parameter.

- b. Run **commit**

The configuration is committed.

- Configure simplified traffic mirroring on an interface.

- a. Run **interface** *interface-type interface-number*

The interface view is displayed.

- b. Configure packet matching rules.

Run **traffic-mirroring** [**vxlan** [**tag-format** { **none** | **single** }]] { **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * } **observe-port** *observe-port-index* &<1-8> **inbound**

Simplified traffic mirroring is configured on the specified interface.

By default, simplified traffic mirroring is not configured on an interface.

NOTE

You can specify 1 to 8 *observe-port-index* parameters simultaneously only on the CE6870EI.

For the CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8850-64CQ-EI, CE8868EI, and CE8861EI, observing ports in enhanced mode can be specified only when you configure simplified traffic mirroring.

The CE6863, CE6863E, CE6863K, CE6881E, CE6820, CE6881K, CE6881, and CE5881 do not support this command.

Simplified traffic mirroring cannot be configured in the port group view.

If simplified traffic mirroring is configured in both the system view and interface view, the configuration in the interface view takes effect.

- c. Run **commit**

The configuration is committed.

MQC-based traffic mirroring

1. Configure a traffic classifier.

- a. Run **traffic classifier** *classifier-name* [**type** { **and** | **or** }]

A traffic classifier is created and the traffic classifier view is displayed, or the view of an existing traffic classifier is displayed.

and is the logical operator between rules in a traffic classifier, which means that:

- If a traffic classifier contains ACL rules, packets match the traffic classifier only if they match one ACL rule and all the non-ACL rules.
- If a traffic classifier does not contain any ACL rules, packets match the traffic classifier only if they match all the rules in the classifier.

The logical operator **or** means that packets match a traffic classifier if they match one or more rules in the classifier.

By default, the relationship between rules in a traffic classifier is **or**.

- b. Run **if-match**

Matching rules are defined for the traffic classifier. For details about matching rules in a traffic classifier, see "Configuring a Traffic Classifier" in "MQC Configuration" of the *CloudEngine 9800, 8800, 6800, 5800 Series Switches Configuration Guide - QoS Configuration Guide*.

- c. Run **commit**

The configuration is committed.

- d. Run **quit**

Exit from the traffic classifier view.

2. Configure a traffic behavior.

- a. Run **traffic behavior** *behavior-name*

A traffic behavior is created and the traffic behavior view is displayed, or the view of an existing traffic behavior is displayed.

- b. (On the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E) Run **mirroring observe-port** *observe-port-index* &<1-4> [**session-id** *session-id*]

The traffic matching the rules is mirrored to the specified observing port.

- c. (On the CE6870EI) Run **mirroring observe-port** *observe-port-index* &<1-8> [**random-packets** *random-packets*]

The traffic matching the rules is mirrored to the specified observing port.

- d. (On the CE5855E, CE5855F) Run **mirroring observe-port** *observe-port-index*

The traffic matching the rules is mirrored to the specified observing port.

- e. (On switches except the CE6870EI, CE5855E, CE5855F, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E) Run **mirroring observe-port** *observe-port-index* &<1-4>

The traffic matching the rules is mirrored to the specified observing port.

- f. Run **commit**

The configuration is committed.

- g. Run **quit**
Exit from the traffic behavior view.
3. Configure a traffic policy.
 - a. Run **traffic policy** *policy-name*
A traffic policy is created and the traffic policy view is displayed, or the view of an existing traffic policy is displayed.
 - b. Run **classifier** *classifier-name* **behavior** *behavior-name* [**precedence** *precedence-value*]
A traffic behavior is bound to a traffic classifier in the traffic policy.
 - c. Run **commit**
The configuration is committed.
 - d. Run **quit**
Exit from the traffic policy view.
 - e. Run **quit**
Exit from the system view.
4. (On switches except the CE6870EI) Apply the traffic policy.

 NOTE

- Only on the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E, a traffic policy containing the mirroring action can be applied to the outbound direction.
- Only on the CE6881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E outbound mirroring can be configured on a VBDIF or VLANIF interface where a traffic policy has been applied.
- Outbound mirroring is not supported by a Layer 2 sub-interface where a traffic policy has been applied.
- IPv6 packets cannot be mirrored when a traffic policy is applied to a Layer 3 sub-interface.
- For details about the configuration guidelines of applying traffic policies in different views on the CE switches excluding CE6870EI, see Licensing Requirements and Limitations for MQC (CE Switches Excluding the CE6870EI).
- Applying a traffic policy to an interface
 - i. Run **system-view**
The system view is displayed.
 - ii. Run **interface** *interface-type interface-number*
The interface view is displayed.
 - iii. Run **traffic-policy** *policy-name* { **inbound** | **outbound** }
A traffic policy is applied to the interface.
 - iv. Run **commit**
The configuration is committed.
- Applying a traffic policy to a VLAN
 - i. Run **system-view**
The system view is displayed.
 - ii. Run **vlan** *vlan-id*
The VLAN view is displayed.

- iii. Run **traffic-policy** *policy-name* { **inbound** | **outbound** }
A traffic policy is applied to the VLAN.
The system applies traffic policing to the packets that belong to the VLAN and match traffic classification rules in the inbound or outbound direction.
- iv. Run **commit**
The configuration is committed.
- Applying a traffic policy to the system
 - i. Run **system-view**
The system view is displayed.
 - ii. Run **traffic-policy** *policy-name* **global** [*slot slot-id*] { **inbound** | **outbound** }
A traffic policy is applied to the system.
 - iii. Run **commit**
The configuration is committed.
- Applying a traffic policy to a QoS group
 - i. Run **system-view**
The system view is displayed.
 - ii. Run **qos group** *group-name*
The QoS group view is displayed.
 - iii. Run the following commands as required:
 - o Run the **group-member interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-8> command to add interfaces to the QoS group.
 - o Run the **group-member vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-8> command to add VLANs to the QoS group.
 - o (For CE switches excluding the CE6870EI) Run the **group-member ip source** *ip-address* { *mask* | *mask-length* } command to add source IP addresses to the QoS group.
 - o (For CE6881, CE5881, CE6881K, CE6863, CE6863E, CE6863K, CE6881E) Run the **group-member bridge-domain** { *bd-id1* [**to** *bd-id2*] } &<1-8> command to add BDs to the QoS group.
 - iv. Run **traffic-policy** *policy-name* { **inbound** | **outbound** }
A traffic policy is applied to the QoS group.
 - v. Run **commit**
The configuration is committed.
- Applying a traffic policy to a BD

 NOTE

This function is only supported on the CE8868EI, CE8861EI, CE8850EI, CE8850E-32CQ-EI, CE6881, CE6881K, CE6881E, CE6870EI, CE6865EI, CE6865E, CE6863K, CE6863E, CE6863, CE6857EI, CE6857E, CE6857F, CE6856HI, and CE5881.

- i. Run **system-view**
The system view is displayed.

- ii. Run **bridge-domain** *bd-id*
The BD view is displayed.
 - iii. Run **traffic-policy** *policy-name* { **inbound** | **outbound** }
A traffic policy is applied to the BD.
 - iv. Run **commit**
The configuration is committed.
5. (On the CE6870EI) Apply the traffic policy.

 NOTE

- IPv6 packets cannot be mirrored when a traffic policy is applied to a Layer 3 sub-interface.
- For details about the configuration guidelines of applying traffic policies in different views on the CE6870EI, see Licensing Requirements and Limitations for MQC (CE6870EI).
- Applying a traffic policy to an interface
 - i. Run **system-view**
The system view is displayed.
 - ii. Run **interface** *interface-type interface-number*
The interface view is displayed.
 - iii. Run **traffic-policy** *policy-name* { **inbound** | **outbound** }
A traffic policy is applied to the interface.
 - iv. Run **commit**
The configuration is committed.
- Applying a traffic policy to a VLAN
 - i. Run **system-view**
The system view is displayed.
 - ii. Run **vlan** *vlan-id*
The VLAN view is displayed.
 - iii. Run **traffic-policy** *policy-name* { **inbound** | **outbound** }
A traffic policy is applied to the VLAN.
The system applies traffic policing to the packets that belong to the VLAN and match traffic classification rules in the inbound or outbound direction.
 - iv. Run **commit**
The configuration is committed.
- Applying a traffic policy to the system
 - i. Run **system-view**
The system view is displayed.
 - ii. Run **traffic-policy** *policy-name* **global** [**slot** *slot-id*] { **inbound** | **outbound** }
A traffic policy is applied to the system.
 - iii. Run **commit**
The configuration is committed.

- Applying a traffic policy to a BD

 NOTE

This function is only supported on the CE8868EI, CE8861EI, CE8850EI, CE8850E-32CQ-EI, CE6881, CE6881K, CE6881E, CE6870EI, CE6865EI, CE6865E, CE6863K, CE6863E, CE6863, CE6857EI, CE6857E, CE6857F, CE6856HI, and CE5881.

- Run **system-view**
The system view is displayed.
- Run **bridge-domain** *bd-id*
The BD view is displayed.
- Run **traffic-policy** *policy-name* { **inbound** | **outbound** }
A traffic policy is applied to the BD.
- Run **commit**
The configuration is committed.

----End

3.1.3.3 Configuring Remote VLAN Mirroring

Context

In remote VLAN mirroring, packets on all active ports in a specified VLAN are copied to observing ports, which then send the packets to monitoring devices across a Layer 2 or Layer 3 network.

Pre-configuration Tasks

Before configuring Layer 3 remote mirroring, configure a GRE tunnel between the observing port and monitoring device so that mirrored packet packets can be forwarded through the GRE tunnel. If no GRE tunnel is configured between the observing port and the monitoring device, mirrored packet packets are forwarded across a Layer 3 network.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Configure a remote observing port.

 NOTE

For the CE8868EI, CE8861EI, CE8850-64CQ-EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857E, CE6857F, and CE6857EI, parameters **interface** and **enhanced-mode** cannot be configured together.

- For Layer 2 remote mirroring:
 - (On the CE9860EI, CE5855E, CE5855F, CE8868EI, CE8861EI, CE8850EI, CE6870EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857EI, CE6857E, CE6857F, and CE6856HI) Run **observe-port** [*observe-port-index*]

- interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id*
- (On the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E) Run **observe-port** [*observe-port-index*] **interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id* [*cir cir-value* [**kbps** | **mbps** | **gbps**]] [**truncate packet** *packet-length*]
 - For Layer 3 remote mirroring:
 - On the CE6857EI, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8861EI, and CE8868EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**truncate** | **enhanced-mode** [**length** *packet-length*]].
 - If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate** | **enhanced-mode** [**length** *packet-length*]].
 - If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate** | **enhanced-mode** [**length** *packet-length*]].
 - On the CE6857E:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**truncate**].
 - If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate**].
 - If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate**].
 - On the CE6870EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**erspan-id** *erspan-id*].
 - If mirrored packets need to be forwarded through a Layer 3 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*]

- destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value*] [**erspan-id** *erspan-id*].
- On the CE9860EI, CE6856HI, CE5855E, CE5855F:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id*.
 - (CE9860EI, CE6856HI, CE5855E, CE5855F) If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *.
 - (CE9860EI) If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *.
 - On the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbits** | **mbits** | **gbits**]] [**truncate packet** *packet-length*].
 - If mirrored packets need to be forwarded through a Layer 3 IPv4 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbits** | **mbits** | **gbits**]] [**truncate packet** *packet-length*].
 - If mirrored packets need to be forwarded through a Layer 3 IPv6 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**erspan-id** *erspan-id*] [**enhanced-mode**] [**cir** *cir-value* [**kbits** | **mbits** | **gbits**]] [**truncate packet** *packet-length*].
 - On the CE8850-64CQ-EI:
 - If mirrored packets need to be forwarded over a GRE tunnel, run **observe-port** [*observe-port-index*] **interface tunnel** *tunnel-id* [**enhanced-mode** [**length** *packet-length*]].
 - If mirrored packets need to be forwarded through a Layer 3 network, run **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**enhanced-mode** [**length** *packet-length*]].

By default, no remote observing port is configured.

Step 3 (Optional) Run **observe-port filter enable**

Basic forwarding validity check on an observing port is enabled.

By default, the basic forwarding validity check function is disabled on an observing port.

 NOTE

This function is supported only by the CE6870EI.

Step 4 Run **vlan *vlan-id***

The VLAN view is displayed.

Step 5 Run **mirroring observe-port *observe-port-index* { inbound | outbound | both } [session-id *session-id*]**

VLAN traffic is mirrored to a specified observing port.

 NOTE

Only the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E support **session-id *session-id***, **outbound** and **both** parameter.

Step 6 Run **commit**

The configuration is committed.

----End

3.1.3.4 Verifying the Remote Mirroring Configuration

Procedure

- Run the **display observe-port** command to check the observing port configuration.
- Run the **display port-mirroring** command to check the port mirroring configuration.
- Run the **display traffic-mirroring [verbose]** command to display the simplified traffic mirroring configuration.
- Run the **display traffic behavior [*behavior-name*]** command to check the traffic behavior configuration.
- Run the **display traffic classifier [*classifier-name*]** command to check the traffic classifier configuration.
- Run the **display traffic policy [*policy-name* [classifier *classifier-name*]]** command to check the traffic policy configuration.
- Run the **display traffic-policy applied-record [*policy-name*]** command to check the application record of a specified mirroring policy.

----End

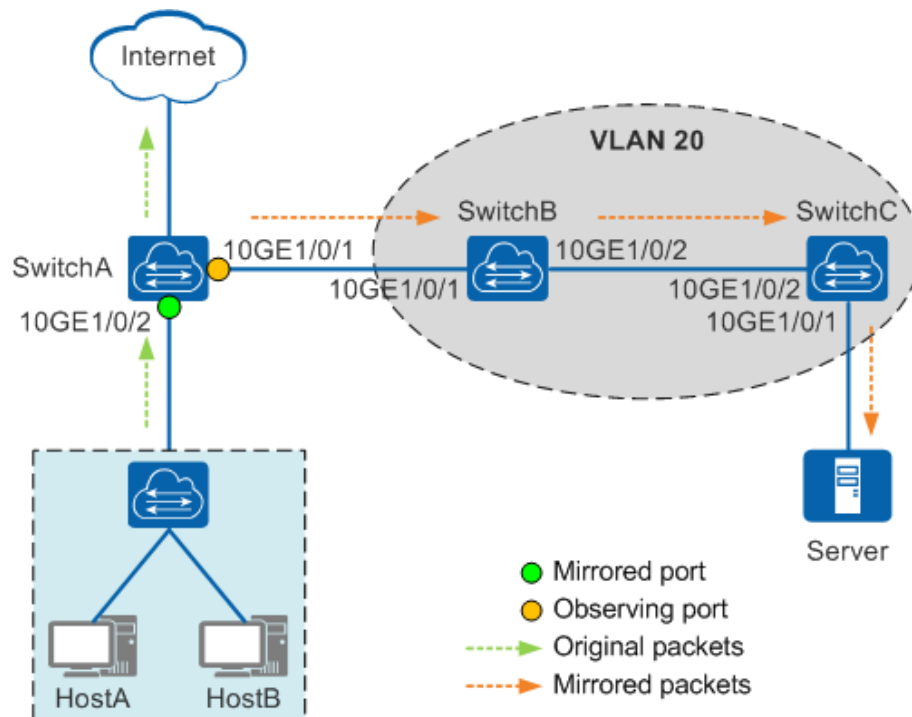
3.1.4 Configuration Examples for Remote Mirroring

3.1.4.1 Example for Configuring Layer 2 Remote Port Mirroring

Networking Requirements

In [Figure 3-4](#), a department of a company accesses the Internet through SwitchA, and the monitoring device Server is connected to SwitchC through a Layer 2 network. Internet access traffic of this department needs to be monitored through the Server.

Figure 3-4 Networking diagram of Layer 2 remote port mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure 10GE1/0/1 of SwitchA as a Layer 2 remote observing port to forward mirrored packets to the Layer 2 network.
2. Configure 10GE1/0/2 of SwitchA as a mirrored port to copy Internet access traffic of the department to the observing port.
3. Create a VLAN on SwitchB and SwitchC, and add ports to the VLAN to forward the mirrored packets sent from the observing port to the Server.

NOTE

When configuring Layer 2 remote port mirroring, do not use a remote mirroring VLAN to transmit other service packets. You are advised to run the **mac-address learning disable** command in the VLAN view on the device that forwards mirrored packets to disable MAC address learning of the remote mirroring VLAN.

Procedure

Step 1 Configure a Layer 2 remote observing port.

Configure 10GE1/0/1 of SwitchA as a Layer 2 remote observing port and configure VLAN 20 as a remote mirroring VLAN.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] observe-port 1 interface 10ge 1/0/1 vlan 20
[*SwitchA] commit
```

After the configuration is complete, the observing port forwards mirrored packets to VLAN 20, removing the need to add this observing port to VLAN 20.

Step 2 Configure a mirrored port.

Configure 10GE1/0/2 of SwitchA as a mirrored port to copy incoming traffic of this port to the Layer 2 remote observing port.

```
[~SwitchA] interface 10ge 1/0/2
[~SwitchA-10GE1/0/2] port-mirroring observe-port 1 inbound
[*SwitchA-10GE1/0/2] quit
[*SwitchA] commit
[~SwitchA] quit
```

Step 3 Configure the Layer 2 network.

Create VLAN 20 on SwitchB and add 10GE1/0/1 and 10GE1/0/2 to VLAN 20.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchB
[*HUAWEI] commit
[~SwitchB] vlan 20
[*SwitchB-vlan20] mac-address learning disable
[*SwitchB-vlan20] quit
[*SwitchB] interface 10ge 1/0/1
[*SwitchB-10GE1/0/1] port link-type trunk
[*SwitchB-10GE1/0/1] port trunk allow-pass vlan 20
[*SwitchB-10GE1/0/1] quit
[*SwitchB] interface 10ge 1/0/2
[*SwitchB-10GE1/0/2] port link-type trunk
[*SwitchB-10GE1/0/2] port trunk allow-pass vlan 20
[*SwitchB-10GE1/0/2] quit
[*SwitchB] commit
```

Create VLAN 20 on SwitchC and add 10GE1/0/1 and 10GE1/0/2 to VLAN 20.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchC
[*HUAWEI] commit
[~SwitchC] vlan 20
[*SwitchC-vlan20] mac-address learning disable
[*SwitchC-vlan20] quit
[*SwitchC] interface 10ge 1/0/1
[*SwitchC-10GE1/0/1] port default vlan 20
[*SwitchC-10GE1/0/1] quit
[*SwitchC] interface 10ge 1/0/2
[*SwitchC-10GE1/0/2] port link-type trunk
[*SwitchC-10GE1/0/2] port trunk allow-pass vlan 20
[*SwitchC-10GE1/0/2] quit
[*SwitchC] commit
```

Step 4 Verify the configurations.

Check the observing port configuration.

```
<SwitchA> display observe-port
```

```
-----  
Index   : 1  
Slot: 1  
  Interface: 10GE1/0/1  
  Vlan    : 20  
-----
```

Check the mirrored port configuration.

```
<SwitchA> display port-mirroring
```

```
Observe port mirroring:
```

```
-----  
MirroringPort   Direction   ObservePort  
-----  
10GE1/0/2       Inbound      1  
-----
```

----End

Configuration Files

- Configuration file of SwitchA

```
#  
sysname SwitchA  
#  
observe-port 1 interface 10GE1/0/1 vlan 20  
#  
interface 10GE1/0/2  
  port-mirroring observe-port 1 inbound  
#  
return
```

- Configuration file of SwitchB

```
#  
sysname SwitchB  
#  
vlan batch 20  
  mac-address learning disable  
#  
interface 10GE1/0/1  
  port link-type trunk  
  port trunk allow-pass vlan 20  
#  
interface 10GE1/0/2  
  port link-type trunk  
  port trunk allow-pass vlan 20  
#  
return
```

- Configuration file of SwitchC

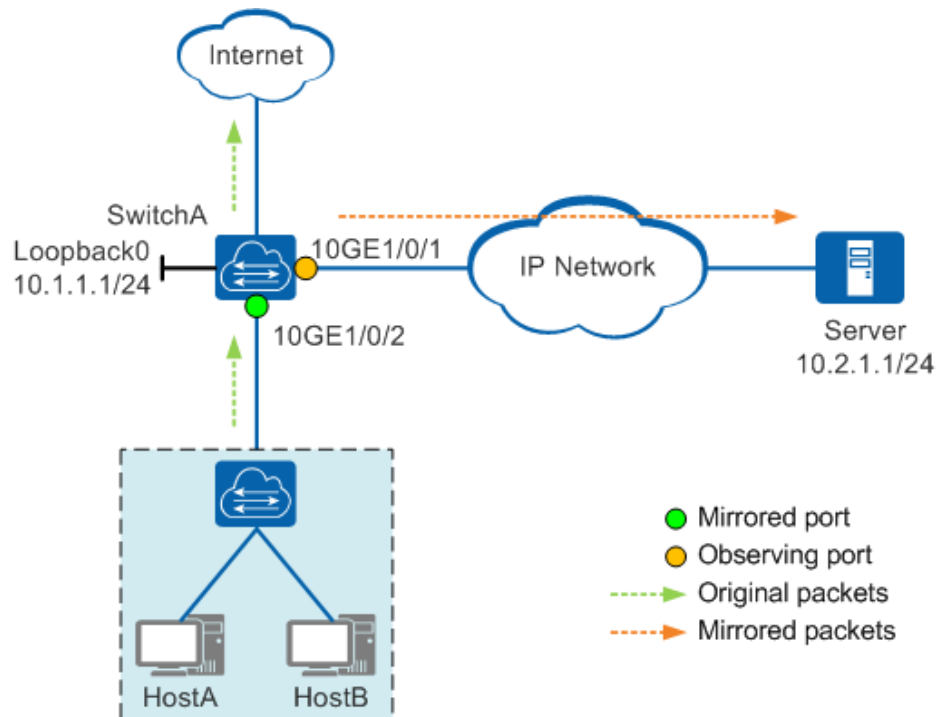
```
#  
sysname SwitchC  
#  
vlan batch 20  
  mac-address learning disable  
#  
interface 10GE1/0/1  
  port default vlan 20  
#  
interface 10GE1/0/2  
  port link-type trunk  
  port trunk allow-pass vlan 20  
#  
return
```

3.1.4.2 Example for Configuring Layer 3 Remote Port Mirroring (Through a Layer 3 Network)

Networking Requirements

In [Figure 3-5](#), a department of a company accesses the Internet through SwitchA. The monitoring device Server is connected to SwitchA through a Layer 3 network and has a reachable route to SwitchA. Internet access traffic of this department needs to be monitored through the Server.

Figure 3-5 Networking diagram of Layer 3 remote port mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure 10GE1/0/1 of SwitchA as a Layer 3 remote observing port, and specify the Server's IP address and SwitchA's interface IP address as the destination and source addresses respectively to be encapsulated in mirrored packets.
2. Configure 10GE1/0/2 of SwitchA as a mirrored port to copy Internet access traffic of the department to the observing port.

Procedure

Step 1 Configure a Layer 3 remote observing port.

Create a loopback interface on SwitchA and configure an IP address 10.1.1.1 for it as the source address to be encapsulated in mirrored packets. You can also specify the IP address of another interface on SwitchA as the source address.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] interface loopback 0
[*SwitchA-LoopBack0] ip address 10.1.1.1 24
[*SwitchA-LoopBack0] quit
[*SwitchA] commit
```

Configure 10GE1/0/1 of SwitchA as a Layer 3 remote observing port, and specify the destination and source addresses to be encapsulated in mirrored packets as 10.2.1.1 and 10.1.1.1.

```
[~SwitchA] observe-port 1 interface 10ge 1/0/1 destination-ip 10.2.1.1 source-ip 10.1.1.1
[*SwitchA] commit
```

Ensure that the specified source and destination IP addresses are reachable at Layer 3.

Step 2 Configure a mirrored port.

Configure 10GE1/0/2 of SwitchA as a mirrored port to copy incoming traffic of this port to the Layer 3 remote observing port.

```
[~SwitchA] interface 10ge 1/0/2
[~SwitchA-10GE1/0/2] port-mirroring observe-port 1 inbound
[*SwitchA-10GE1/0/2] commit
[~SwitchA-10GE1/0/2] return
```

Step 3 Verify the configurations.

Check the observing port configuration.

```
<SwitchA> display observe-port
-----
Index   : 1
Src-Ip   : 10.1.1.1
Dst-Ip   : 10.2.1.1
Dscp     : 0
Slot: 1
  Interface: 10GE1/0/1
  Vlan     : --
  Src-Mac  : 00-25-9e-37-ee-a5
  Dst-Mac  : ff-ff-ff-ff-ff-ff
-----
```

Check the mirrored port configuration.

```
<SwitchA> display port-mirroring
Observe port mirroring:
-----
MirroringPort  Direction  ObservePort
-----
10GE1/0/2      Inbound    1
-----
```

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
observe-port 1 interface 10GE1/0/1 destination-ip 10.2.1.1 source-ip 10.1.1.1
#
interface 10GE1/0/2
```

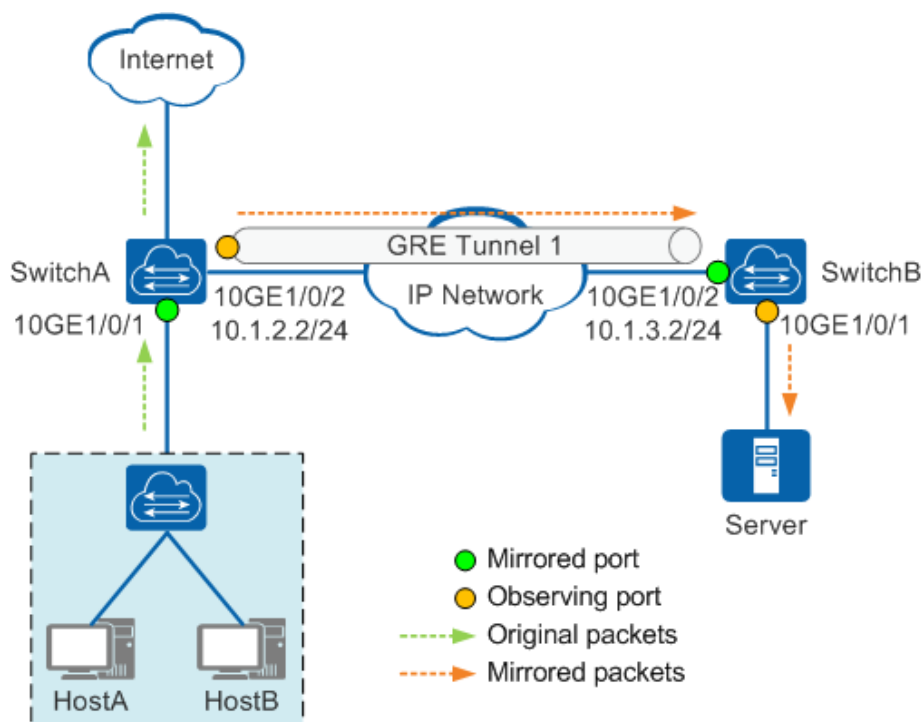
```
port-mirroring observe-port 1 inbound
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
return
```

3.1.4.3 Example for Configuring Layer 3 Remote Port Mirroring (Through a GRE Tunnel)

Networking Requirements

As shown in [Figure 3-6](#), a department of a company accesses the Internet through SwitchA. SwitchB is connected to SwitchA through a Layer 3 network and has a reachable route to SwitchA. The monitoring device Server is directly connected to SwitchB. Internet access traffic of this department needs to be monitored through the Server.

Figure 3-6 Networking diagram of Layer 3 remote port mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a GRE tunnel between SwitchA and SwitchB.
2. Configure the GRE tunnel interface on SwitchA as a Layer 3 remote observing port and 10GE1/0/1 as a mirrored port to copy Internet access traffic of the department to this observing port and forward the traffic to SwitchB.
3. Configure local port mirroring on SwitchB to copy mirrored packets received by 10GE1/0/2 to 10GE1/0/1.

Procedure

Step 1 # Configure a GRE tunnel.

Configure IP addresses and routes for the Layer 3 network between SwitchA and SwitchB so that the two switches have reachable routes to each other. The configuration details are not provided here.

Set the tunnel mode of SwitchA and SwitchB to GRE (this configuration is required only on the CE6870EI).

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] ip tunnel mode gre
[*SwitchA] commit
<HUAWEI> system-view
[~HUAWEI] sysname SwitchB
[*HUAWEI] commit
[~SwitchB] ip tunnel mode gre
[*SwitchB] commit
```

NOTE

The tunnel mode configured on a switch takes effect after you save the configuration and restart the switch. You can restart the switch immediately or after you complete all the configurations.

Configure a GRE tunnel between SwitchA and SwitchB.

```
[~SwitchA] interface tunnel 1
[*SwitchA-Tunnel1] tunnel-protocol gre
[*SwitchA-Tunnel1] ip address 10.1.4.1 24
[*SwitchA-Tunnel1] source 10.1.2.2
[*SwitchA-Tunnel1] destination 10.1.3.2
[*SwitchA-Tunnel1] quit
[*SwitchA] commit
[~SwitchB] interface tunnel 1
[*SwitchB-Tunnel1] tunnel-protocol gre
[*SwitchB-Tunnel1] ip address 10.1.4.2 24
[*SwitchB-Tunnel1] source 10.1.3.2
[*SwitchB-Tunnel1] destination 10.1.2.2
[*SwitchB-Tunnel1] quit
[*SwitchB] commit
```

Step 2 Configure Layer 3 remote mirroring on SwitchA.

On SwitchA, configure Tunnel 1 as a Layer 3 remote observing port and 10GE1/0/1 as a mirrored port to copy incoming traffic of 10GE1/0/1 to Tunnel 1.

```
[~SwitchA] observe-port 1 interface tunnel 1
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port-mirroring observe-port 1 inbound
[*SwitchA-10GE1/0/1] commit
[~SwitchA-10GE1/0/1] return
```

Step 3 Configure local port mirroring on SwitchB.

On SwitchB, configure 10GE1/0/1 as a local observing port and 10GE1/0/2 as a mirrored port to copy the mirrored packets received by 10GE1/0/2 to 10GE1/0/1 connected to the Server.

```
[~SwitchB] observe-port 1 interface 10ge 1/0/1
[*SwitchB] interface 10ge 1/0/2
[*SwitchB-10GE1/0/2] port-mirroring observe-port 1 inbound
[*SwitchB-10GE1/0/2] commit
[~SwitchB-10GE1/0/2] return
```

Step 4 Verify the configuration.

Check the observing port configuration.

```
<SwitchA> display observe-port
-----
Index   : 1
Slot: 1
  Interface: Tunnel1
-----
<SwitchB> display observe-port
-----
Index   : 1
Slot: 1
  Interface: 10GE1/0/1
-----
```

Check the mirrored port configuration.

```
<SwitchA> display port-mirroring
Observe port mirroring:
-----
MirroringPort  Direction  ObservePort
-----
10GE1/0/1      Inbound    1
-----
<SwitchB> display port-mirroring
Observe port mirroring:
-----
MirroringPort  Direction  ObservePort
-----
10GE1/0/2      Inbound    1
-----
```

----End

Configuration Files

- SwitchA configuration file

```
#
sysname SwitchA
#
ip tunnel mode gre
#
observe-port 1 interface Tunnel1
#
interface 10GE1/0/1
  port-mirroring observe-port 1 inbound
#
interface Tunnel1
  ip address 10.1.4.1 255.255.255.0
  tunnel-protocol gre
  source 10.1.2.2
  destination 10.1.3.2
#
return
```

- SwitchB configuration file

```
#
sysname SwitchB
#
ip tunnel mode gre
#
observe-port 1 interface 10GE1/0/1
#
interface 10GE1/0/2
  port-mirroring observe-port 1 inbound
#
```

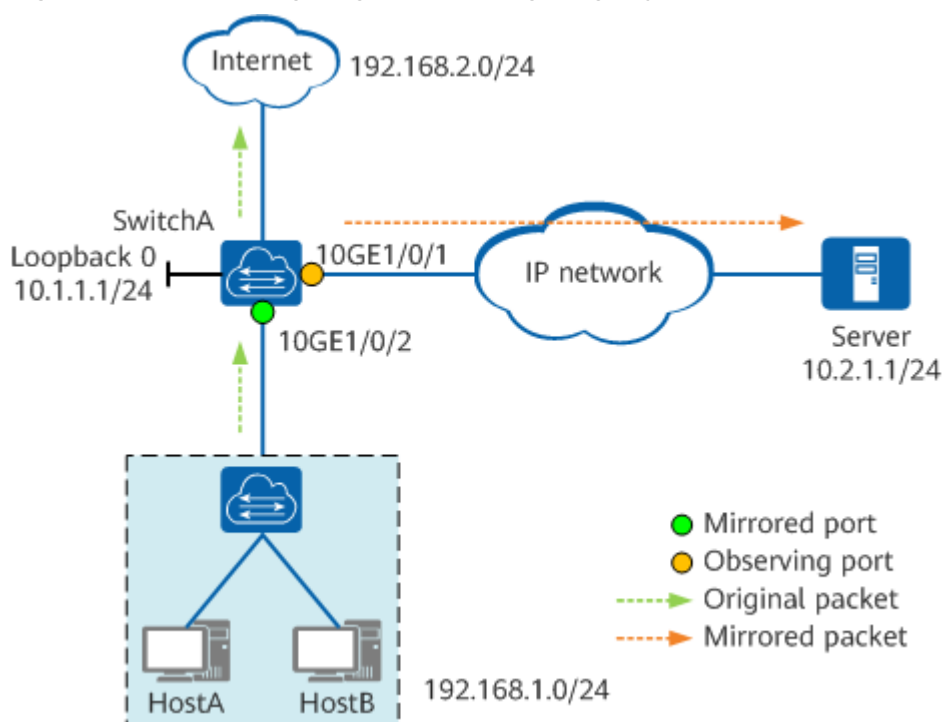
```
interface Tunnel1
ip address 10.1.4.2 255.255.255.0
tunnel-protocol gre
source 10.1.3.2
destination 10.1.2.2
#
return
```

3.1.4.4 Example for Configuring Remote Truncated Mirroring (Through a Layer 3 Network)

Networking Requirements

On the network shown in [Figure 3-7](#), users access the Internet through SwitchA, and the monitoring device (Server) is connected to SwitchA through a Layer 3 network. SwitchA and Server have reachable routes to each other. There is a heavy traffic volume between users and the Internet. To facilitate monitoring of Internet access traffic on Server, configure remote truncated mirroring on SwitchA to mirror only a part of packets.

Figure 3-7 Networking diagram of configuring Layer 3 remote truncated mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure 10GE1/0/1 of SwitchA as a Layer 3 remote observing port. Configure remote truncated mirroring. The destination IP address of mirrored packets is the monitoring device address, and the source IP address is an interface address of SwitchA. Ensure that the destination and source IP addresses are reachable at Layer 3.

 NOTE

After Layer 3 remote truncated mirroring is configured, mirrored packets carry the ERSPAN header.

In V200R019C10 and later versions, truncated mirroring is supported on the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863.

2. Configure a traffic classifier to match packets with the source address being the user address and the destination address being an Internet address.
3. Configure a traffic behavior and configure the traffic mirroring action in the traffic behavior view.
4. Configure a traffic policy, bind the traffic classifier and traffic behavior to the traffic policy, and apply the traffic policy to the inbound direction of 10GE1/0/1 to truncate and mirror Internet access packets to the observing port.

Procedure

Step 1 Configure a Layer 3 remote observing port.

Create a loopback interface on SwitchA, and configure the IP address 10.1.1.1 for the interface. This IP address is used as the source address to be encapsulated in mirrored packets. You can also specify the IP address of a non-loopback interface on SwitchA as the source address of mirrored packets.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] interface loopback 0
[*SwitchA-LoopBack0] ip address 10.1.1.1 24
[*SwitchA-LoopBack0] quit
[*SwitchA] commit
```

Configure 10GE1/0/1 of SwitchA as a Layer 3 remote observing port, and specify 10.2.1.1 (IP address of Server) and 10.1.1.1 as the destination and source addresses to be encapsulated in mirrored packets, respectively.

```
[~SwitchA] observe-port 1 interface 10ge 1/0/1 destination-ip 10.2.1.1 source-ip 10.1.1.1 truncate
packet 128
[*SwitchA] commit
```

 NOTE

The **truncate packet** parameter specifies the length of truncated packets to be mirrored. The value ranges from 64 to 256, in bytes.

Ensure that there are reachable routes between the specified source and destination IP addresses.

Step 2 Configure traffic classifier c1.

On SwitchA, create traffic classifier **c1** and configure a rule to match packets with the source address 192.168.1.0/24 and destination address 192.168.2.0/24.

```
[~SwitchA] acl number 3000
[*SwitchA-acl4-advance-3000] rule permit ip source 192.168.1.0 24 destination 192.168.2.0 24
[*SwitchA-acl4-advance-3000] quit
[*SwitchA] traffic classifier c1
[*SwitchA-classifier-c1] if-match acl 3000
[*SwitchA-classifier-c1] quit
[*SwitchA] commit
```

Step 3 Configure traffic behavior **b1**.

On SwitchA, create traffic behavior **b1** and configure the mirroring action.

```
[~SwitchA] traffic behavior b1
[*SwitchA-behavior-b1] mirroring observe-port 1
[*SwitchA-behavior-b1] quit
[*SwitchA] commit
```

Step 4 # Configure traffic policy **p1** and apply it.

On SwitchA, configure traffic policy **p1**, bind the traffic behavior and traffic classifier to the traffic policy, and apply the traffic policy to the inbound direction of 10GE1/0/2 to monitor packets sent from users to the Internet.

```
[~SwitchA] traffic policy p1
[*SwitchA-trafficpolicy-p1] classifier c1 behavior b1
[*SwitchA-trafficpolicy-p1] quit
[*SwitchA] interface 10ge 1/0/2
[*SwitchA-10GE1/0/2] traffic-policy p1 inbound
[*SwitchA-10GE1/0/2] quit
[*SwitchA] commit
```

Step 5 Verify the configuration.

Check the observing port configuration.

```
<SwitchA> display observe-port
-----
Index   : 1
Src-Ip   : 10.1.1.1
Dst-Ip   : 10.2.1.1
Dscp     : 0
Slot: 1
  Interface: 10GE1/0/1
  Vlan     : --
  Src-Mac  : 00-25-9e-37-ee-a5
  Dst-Mac  : ff-ff-ff-ff-ff-ff
-----
```

Check the mirrored port configuration.

```
<SwitchA> display port-mirroring
Observe port mirroring:
-----
MirroringPort   Direction   ObservePort
-----
10GE1/0/2       Inbound     1
-----
```

----End

Configuration Files

- SwitchA configuration file (CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863)

```
#
sysname SwitchA
#
observe-port 1 interface 10GE1/0/1 destination-ip 10.2.1.1 source-ip 10.1.1.1 truncate packet 128
#
acl number 3000
rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
traffic classifier c1 type or
if-match acl 3000
#
```

```
traffic behavior b1
  mirroring observe-port 1
#
traffic policy p1
  classifier c1 behavior b1 precedence 5
#
interface 10GE1/0/2
  traffic-policy p1 inbound
#
interface LoopBack0
  ip address 10.1.1.1 255.255.255.0
#
return
```

3.2 Mirroring Configuration Commands

3.2.1 display observe-port

Function

The **display observe-port** command displays the observing port configuration.

Format

display observe-port [*index*]

Parameters

Parameter	Description	Value
<i>index</i>	Index of the observing port.	The value is an integer that ranges from 1 to 8.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

```
# Display the observing port configuration (CE Switches Excluding CE9860EI,
CE6863, CE6863E, CE6863K, CE6881E, CE6881K, CE6881, and CE5881).
<HUAWEI> display observe-port 2
-----
Index   : 2
Src-Ip  : 10.2.2.2
Dst-Ip  : 10.1.1.1
```

```
Dscp    : 0
Slot: 1
  Interface: 10GE1/0/23
  Vlan     : 134
  Src-Mac  : 00-25-22-66-11-0a
  Dst-Mac  : 00-00-31-46-53-33
Slot: 2
  Interface: 10GE1/0/23
  Vlan     : 134
  Src-Mac  : 00-25-22-66-11-0a
  Dst-Mac  : 00-00-31-46-53-33
-----
```

Display the observing port configuration (CE9860EI).

<HUAWEI> **display observe-port 2**

```
-----
Index   : 1
Src-Ip   : 10.2.2.2
Dst-Ip   : 10.1.1.1
Dscp     : 0
Slot: 1
  Interface: 100GE1/1/1
  Vlan     : 134
  Src-Mac  : 00-25-22-66-11-0a
  Dst-Mac  : 00-00-31-46-53-33
-----
```

Display the observing port configuration (CE6863, CE6863E, CE6863K, CE6881E, CE6881K, CE6881, and CE5881).

<HUAWEI> **display observe-port 2**

```
-----
Index   : 2
Src-Ip   : 10.2.2.2
Dst-Ip   : 10.1.1.1
Dscp     : 0
Erspan-Id: 0
CIR(kbps): 3072
Slot: 1
  Chip: 0
    Interface: 10GE1/0/23
    Vlan     : 134
    Src-Mac  : 00-25-22-66-11-0a
    Dst-Mac  : 00-00-31-46-53-33
  Chip: 1
    Interface: 10GE1/0/48
    Vlan     : 134
    Src-Mac  : 00-25-22-66-11-0a
    Dst-Mac  : 00-00-31-46-53-33
Slot: 2
  Chip: 0
    Interface: 10GE1/0/23
    Vlan     : 134
    Src-Mac  : 00-25-22-66-11-0a
    Dst-Mac  : 00-00-31-46-53-33
  Chip: 1
    Interface: 10GE1/0/23
    Vlan     : 134
    Src-Mac  : 00-25-22-66-11-0a
    Dst-Mac  : 00-00-31-46-53-33
-----
```

NOTE

The command output provided here is used for reference only. The actual output information depends on the situation.

Table 3-1 Description of the **display observe-port** command output

Item	Description
Index	Index of the observing port.
Src-Ip	Source IP address of GRE packets.
Dst-Ip	Destination IP address of GRE packets.
Dscp	Priority of GRE packets.
Ersan-Id	ERSAN ID. NOTE Only the CE6820, CE6863, CE6863E, CE6863K, CE6881E, CE6881K, CE6881, and CE5881 support this parameter.
CIR(kbps)	Committed information rate. NOTE Only the CE6820, CE6863, CE6863E, CE6863K, CE6881E, CE6881K, CE6881, and CE5881 support this parameter.
Slot	Indicates the slot number of the observing port.
Chip	Indicates the ID of the chip where the observing port resides.
Interface	Observing port.
Vlan	In Layer 2 remote mirroring, the value is the VLAN ID that the observing port belongs to. In Layer 3 remote mirroring, the value is the VLAN ID encapsulated into GRE packets.
Src-Mac	Source MAC address of GRE packets.
Dst-Mac	Destination MAC address of GRE packets.

3.2.2 display port-mirroring

Function

The **display port-mirroring** command displays the mirroring configuration on the device.

Format

display port-mirroring

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

```
# Display the packet mirroring configuration.
<HUAWEI> display port-mirroring
Observe port mirroring:
-----
MirroringPort      Direction      ObservePort
-----
10GE1/0/1          Inbound        1
-----
Traffic mirroring:
-----
TrafficBehavior      ObservePort
-----
b1                    1
-----
```

Table 3-2 Description of the **display port-mirroring** command output

Item	Description
MirroringPort	Mirrored ports.
Direction	Direction of mirrored packets. The value can be: - Inbound: indicates incoming packets. - Outbound: indicates outgoing packets.
ObservePort	Observing port that mirrored packets send to.
TrafficBehavior	Traffic behavior of traffic mirroring.

3.2.3 display traffic-mirroring

Function

The **display traffic-mirroring** command displays the simplified traffic mirroring configuration.

Format

display traffic-mirroring [verbose]

Parameters

Parameter	Description	Value
verbose	Displays detailed configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the simplified traffic mirroring configuration.

```
<HUAWEI> display traffic-mirroring
Observe traffic mirroring:
-----
MirroringPort      Slot  Direction  ObservePort
-----
IPv4 10GE2/0/45    -   Inbound    1
-----
```

Table 3-3 Description of the **display traffic-mirroring** command output

Item	Description
Observe traffic mirroring	Simplified traffic mirroring configurations.
MirroringPort	Mirrored port. NOTE If the simplified traffic mirroring function is configured in the system view, this field displays IPv4 Global or IPv6 Global .

Item	Description
Slot	device to which simplified traffic mirroring is applied.
Direction	Direction of mirrored packets. Inbound: inbound direction
ObservePort	Observing port to which mirrored packets are sent.

Display detailed configuration of simplified traffic mirroring.

<HUAWEI> **display traffic-mirroring verbose**

```

-----
MirroringPort  : IPv4 10GE2/0/45
Slot           : -
Direction      : Inbound
ObservePort    : 1
VxlanFlag      : -
TcpFlag        : ack
Status         : Success
-----

```

Table 3-4 Description of the **display traffic-mirroring verbose** command output

Item	Description
MirroringPort	Mirrored port. NOTE If the simplified traffic mirroring function is configured in the system view, this field displays IPv4 Global or IPv6 Global .
Slot	device to which simplified traffic mirroring is applied.
Direction	Direction of mirrored packets. Inbound: inbound direction
ObservePort	Index of an observing port.
VxlanFlag	Whether to match VXLAN packets: - vxlan: Match VXLAN packets. -: Do not match VXLAN packets.
TcpFlag	TCP flag used to match TCP packets.
Status	Simplified flow mirroring configuration delivery status: - Success: The configuration is successfully delivered. - Failed: The configuration fails to be delivered.

3.2.4 mirroring observe-port

Function

The **mirroring observe-port** command mirrors the traffic matching certain rules to an observing port.

The **undo mirroring** command disables traffic mirroring that mirrors the traffic matching certain rules to an observing port.

By default, traffic mirroring that mirrors the traffic matching certain rules to an observing port is disabled.

Format

For the CE6870EI:

mirroring observe-port *observe-port-index* <1-8> [**random-packets** *random-packets*]

undo mirroring [**observe-port** *observe-port-index* <1-8> [**random-packets** *random-packets*]]

For the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E:

mirroring observe-port *observe-port-index* <1-4> [**session-id** *session-id*]

undo mirroring [**observe-port** *observe-port-index* <1-4> [**session-id** *session-id*]]

For the CE5855E, CE5855F:

mirroring observe-port *observe-port-index*

undo mirroring [**observe-port** *observe-port-index*]

For other switches:

mirroring observe-port *observe-port-index* <1-4>

undo mirroring [**observe-port** *observe-port-index* <1-4>]

Parameters

Parameter	Description	Value
<i>observe-port-index</i>	Specifies the index of an observing port.	The value is an integer that ranges from 1 to 8.

Parameter	Description	Value
session-id <i>session-id</i>	Specifies a mirroring ID. The <i>session-id</i> parameter is encapsulated in mirrored packets to differentiate different mirrored packets. NOTE - Only the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E support this parameter. - This parameter takes effect only for Layer 3 remote mirroring. - When both this parameter and the erspan-id <i>erspan-id</i> parameter used in the observe-port command are configured, this parameter takes effect first.	The value is an integer that ranges from 0 to 1023.
random-packets <i>random-packets</i>	Specifies the interval for collecting mirrored packets. By default, all mirrored packets are copied to observing ports. NOTE A larger interval causes more differences between actual and expected mirrored packets.	The value is an integer that ranges from 1 to 65535.

Views

Traffic behavior view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **mirroring observe-port** command to mirror the traffic matching certain rules to an observing port.

Prerequisites

An observing port has been configured using the **observe-port** command.

Example

Mirror the traffic matching certain rules to observing port 1.

```
<HUAWEI> system-view
[~HUAWEI] observe-port 1 interface 10ge 1/0/1 vlan 10
[*HUAWEI] traffic behavior tb1
[*HUAWEI-behavior-tb1] mirroring observe-port 1
```

3.2.5 mirroring observe-port (VLAN view)

Function

The **mirroring observe-port** command configures VLAN mirroring.

The **undo mirroring** command deletes VLAN mirroring configuration.

By default, VLAN mirroring is not configured.

Format

mirroring observe-port *observe-port-index* { **inbound** | **outbound** | **both** }
[**session-id** *session-id*]

undo mirroring [**observe-port** *observe-port-index*] { **inbound** | **outbound** | **both** }

Parameters

Parameter	Description	Value
<i>observe-port-index</i>	Specifies the index of the observing port.	The value is an integer that ranges from 1 to 8.
inbound	Indicates that mirroring is configured for the incoming traffic in the VLAN.	-
outbound	Indicates that mirroring is configured for the outgoing traffic in the VLAN. NOTE Only the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E support this parameter.	-
both	Indicates that mirroring is configured for the incoming and outgoing traffic in the VLAN. NOTE Only the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E support this parameter.	-

Parameter	Description	Value
session-id <i>session-id</i>	Specifies a mirroring ID. The <i>session-id</i> parameter is encapsulated in mirrored packets to differentiate different mirrored packets. NOTE • Only the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E support this parameter. • This parameter takes effect only for Layer 3 remote mirroring. • When both this parameter and the erspan-id <i>erspan-id</i> parameter used in the observe-port command are configured, this parameter takes effect first.	The value is an integer that ranges from 0 to 1023.

Views

VLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Users can use the **mirroring observe-port** command to mirror the traffic on all active ports in a specified VLAN to an observing port.

Prerequisites

An observing port has been configured using the **observe-port** command.

Precautions

VLAN mirroring can be simultaneously configured in a maximum of 128 VLANs.

Example

Mirror incoming packets on active ports in VLAN 10 to observing port 1.

```
<HUAWEI> system-view
[~HUAWEI] observe-port 1 interface 10ge 1/0/1 vlan 111
[*HUAWEI] vlan 10
[*HUAWEI-vlan10] mirroring observe-port 1 inbound
```

3.2.6 observe-port (remote observing port)

Function

The **observe-port** command configures a remote observing port.

The **undo observe-port** command deletes a remote observing port.

By default, no remote observing port is configured.

Format

Layer 2 remote mirroring:

On the :

observe-port [*observe-port-index*] **interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id*

On the CE6820, CE6863, CE6863E, CE6863K, CE6881E, CE6881K, CE6881, and CE5881:

observe-port [*observe-port-index*] **interface** { *interface-type interface-number* | *interface-name* } **vlan** *vlan-id* [*cir cir-value* [*kbps* | *mbps* | *gbps*]] [**truncate packet** *packet-length*]

undo observe-port *observe-port-index*

Layer 3 remote mirroring:

On the CE9860EI, CE6856HI, CE5855E, CE5855F:

observe-port [*observe-port-index*] **interface tunnel** *tunnel-id*

observe-port [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *

(Only CE9860EI) **observe-port** [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **ipv6 destination-ip** *dest-ipv6-address* **source-ip** *source-ipv6-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] *

On the CE6857EI, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8861EI, and CE8868EI:

observe-port [*observe-port-index*] **interface tunnel** *tunnel-id* [**truncate** | **enhanced-mode** [**length** *packet-length*]]

observe-port [*observe-port-index*] [**interface** { *interface-type interface-number* | *interface-name* }] [**vpn-instance** *vpn-name*] **destination-ip** *dest-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id*] * [**truncate** | **enhanced-mode** [**length** *packet-length*]]

```
observe-port [ observe-port-index ] [ interface { interface-type interface-number | interface-name } ] [ vpn-instance vpn-name ] ipv6 destination-ip dest-ipv6-address source-ip source-ipv6-address [ dscp dscp-value | vlan vlan-id ] *  
[ truncate | enhanced-mode [ length packet-length ] ]
```

On the CE6857E:

```
observe-port [ observe-port-index ] interface tunnel tunnel-id [ truncate ]
```

```
observe-port [ observe-port-index ] [ interface { interface-type interface-number | interface-name } ] [ vpn-instance vpn-name ] destination-ip dest-ip-address  
source-ip source-ip-address [ dscp dscp-value | vlan vlan-id ] * [ truncate ]
```

```
observe-port [ observe-port-index ] [ interface { interface-type interface-number | interface-name } ] [ vpn-instance vpn-name ] ipv6 destination-ip dest-ipv6-address source-ip source-ipv6-address [ dscp dscp-value | vlan vlan-id ] *  
[ truncate ]
```

On the CE6870EI:

```
observe-port [ observe-port-index ] interface tunnel tunnel-id [ erspan-id erspan-id ]
```

```
observe-port [ observe-port-index ] [ interface { interface-type interface-number | interface-name } ] [ vpn-instance vpn-name ] destination-ip dest-ip-address  
source-ip source-ip-address [ dscp dscp-value ] [ erspan-id erspan-id ]
```

On the CE6820, CE6863, CE6863E, CE6863K, CE6881, CE5881, CE6881E, and CE6881K:

```
observe-port [ observe-port-index ] interface tunnel tunnel-id [ erspan-id erspan-id ] [ enhanced-mode ] [ cir cir-value [ kbits | mbits | gbits ] ] [ truncate packet packet-length ]
```

```
observe-port [ observe-port-index ] [ interface { interface-type interface-number | interface-name } ] [ vpn-instance vpn-name ] destination-ip dest-ip-address  
source-ip source-ip-address [ dscp dscp-value | vlan vlan-id ] * [ erspan-id erspan-id ] [ enhanced-mode ] [ cir cir-value [ kbits | mbits | gbits ] ] [ truncate packet packet-length ]
```

```
observe-port [ observe-port-index ] [ interface { interface-type interface-number | interface-name } ] [ vpn-instance vpn-name ] ipv6 destination-ip dest-ipv6-address source-ip source-ipv6-address [ dscp dscp-value | vlan vlan-id ] *  
[ erspan-id erspan-id ] [ enhanced-mode ] [ cir cir-value [ kbits | mbits | gbits ] ] [ truncate packet packet-length ]
```

On the CE8850-64CQ-EI:

```
observe-port [ observe-port-index ] interface tunnel tunnel-id [ enhanced-mode [ length packet-length ] ]
```

```
observe-port [ observe-port-index ] [ interface { interface-type interface-number | interface-name } ] [ vpn-instance vpn-name ] destination-ip dest-ip-address  
source-ip source-ip-address [ dscp dscp-value | vlan vlan-id ] * [ enhanced-mode [ length packet-length ] ]
```

```
undo observe-port observe-port-index
```

Parameters

Parameter	Description	Value
<i>observe-port-index</i>	Specifies the index of an observing port.	The value is an integer in the range from 1 to 8. If no observing port index is specified, the system assigns unused indexes in the range from 1 to 8 to observing ports in sequence.
interface { <i>interface-type</i> <i>interface-number</i> <i>interface-name</i> }	Specifies the type and number of the observing port. <i>interface-type</i> specifies the interface type. <i>interface-number</i> specifies the interface number. <i>interface-name</i> specifies the interface name.	The interface type can be Ethernet or Eth-Trunk. NOTE On the CE9860EI, an Eth-Trunk cannot be configured as an observing port.
vpn-instance <i>vpn-name</i>	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value <code>_public_</code> is reserved and cannot be used as the VPN instance name.
vlan <i>vlan-id</i>	In Layer 2 remote mirroring, <i>vlan-id</i> specifies the VLAN ID encapsulated into mirrored packets.	The value is an integer in the range from 1 to 4094, excluding reserved VLAN IDs, which can be configured using the vlan reserved <i>vlan-id</i> command.
destination-ip <i>dest-ip-address</i>	Specifies the destination IP address of mirrored packets.	The value is in dotted decimal notation.
ipv6 destination-ip <i>dest-ipv6-address</i>	Specifies the destination IPv6 address of mirrored packets.	The value is in dotted decimal notation.
source-ip <i>source-ip-address</i>	Specifies the source IP address of mirrored packets.	The value is in dotted decimal notation.

Parameter	Description	Value
source-ip <i>source-ipv6-address</i>	Specifies the source IPv6 address of mirrored packets.	The value is in dotted decimal notation.
dscp <i>dscp-value</i>	Specifies the priority of mirrored packets.	The value is an integer in the range from 0 to 63. The default value is 0.
tunnel <i>tunnel-id</i>	Specifies the ID of a GRE tunnel interface.	The value is an integer and must be the ID of a tunnel interface that has been created. The tunnel interface has been created using the interface tunnel tunnel-id command.
erspan-id <i>erspan-id</i>	Specifies the ERSPAN ID. The <i>erspan-id</i> parameter is encapsulated in mirrored packets to differentiate mirrored packets.	The value is an integer in the range from 0 to 1023.
enhanced-mode	Specifies the remote observing port in enhanced mode.	-
cir <i>cir-value</i>	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer. The value range varies depending on the rate unit. The default unit is kbit/s. - When the specified rate unit is kbit/s, the value ranges from 24 to 100000000. - When the specified rate unit is Mbit/s, the value ranges from 1 to 100000. - When the specified rate unit is Gbit/s, the value ranges from 1 to 100.
kbps	Specifies the rate unit as kbit/s.	-
mbps	Specifies the rate unit as Mbit/s.	-

Parameter	Description	Value
gbps	Specifies the rate unit as Gbit/s.	-
truncate	Mirrors a specified length of packets. For the CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8861EI, and CE8868EI, only the first 188 bytes of packets can be mirrored and this length cannot be configured. For the CE6881, CE5881, CE6881K, CE6881E, CE6863, CE6863E, CE6863K, and CE6820, you can set the packet packet-length parameter to specify the length of packets to be mirrored.	-
length <i>packet-length</i>	Specifies the length of packets to be mirrored.	The value is an integer in the range from 64 to 256, in bytes.
packet <i>packet-length</i>	Specifies the length of packets to be mirrored.	The value is an integer in the range from 64 to 256, in bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In remote mirroring, the monitoring device and the observing port are connected over a Layer 2 or Layer 3 network. There are Layer 2 remote mirroring and Layer 3 remote mirroring.

- Layer 2 remote mirroring: Mirrored packets are encapsulated with a specified VLAN ID and then forwarded to a remote monitoring device across a Layer 2 network.
- Layer 3 remote mirroring: Mirrored packets are encapsulated with a GRE header and then forwarded to a remote monitoring device across a Layer 3 network.

If the **enhanced-mode** parameter is specified on the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, and CE6863, CE6863E, you can configure a remote observing port in enhanced mode to enable mirrored packets to carry information about the packet receiving port and time. Based on the information, an external system (such as FabricInsight) can identify the packet forwarding path and network delay.

For the CE8850-64CQ-EI and CE6865EI, if PTP is enabled in enhanced mode, mirrored packets carry 1588v2 timestamps.

If traffic of mirrored ports is copied to observing ports and exceeds the bandwidth of observing ports, congestion will occur or a large number of packets will be dropped, affecting the device forwarding performance. You can configure rate limiting on observing ports so that they send packets evenly.

Precautions

- When you configure **observe-port** to remotely mirror an observing port, the system prompts you to check whether the bandwidth of the observe port is sufficient to prevent network congestion.
- If you configure multiple observing ports without specifying *observe-port-index*, the system selects the smallest unused indexes from 1 to 8 and assigns the indexes to the observing ports in sequence.
- These indexes cannot conflict with the existing configured indexes.
- The device applies **cir** to interfaces of the same chip resource uniformly and applies **cir** to interfaces on different chip resources separately. When the **observe-port** command is applied to an Eth-Trunk, the system, or a VLAN, if interfaces of the object to which the observing port is applied belong to N chip resources, the actual committed information rate is N times as large as the **cir** value.

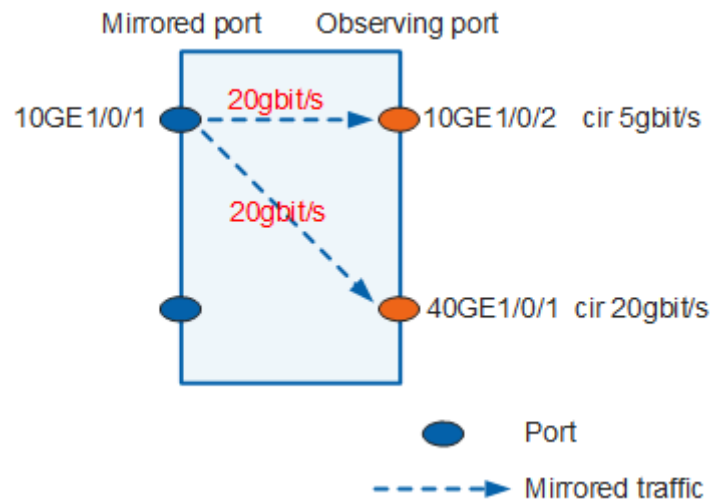
Assume that 10GE1/0/1 and 10GE1/0/2 belong to chip resource 0 and 10GE1/0/25 and 10GE1/0/26 belong to chip resource 1. If 10GE1/0/1, 10GE1/0/2, 10GE1/0/25, and 10GE1/0/26 join VLAN 10 and the **observe-port** configuration containing the rate limit of 1 Mbit/s is applied to VLAN 10, the rate limit of 10GE1/0/1 and 10GE1/0/2 is 1 Mbit/s and the rate limit of 10GE1/0/25 and 10GE1/0/26 is also 1 Mbit/s. That is, the rate limit is 2 Mbit/s after the **observe-port** configuration is applied to VLAN 10.

You can query the relationship between ports and chip resources using a [tool](#).

- On the CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, CE6863, CE6863E, CE8868EI, CE8861EI, CE8850-64CQ-EI, CE6857EI, CE6857E, CE6857F you can configure only one remote observing port in enhanced mode.
- For the CE8868EI, CE8861EI, CE8850-64CQ-EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, and CE6857EI, CE6857E, CE6857F, parameters **interface** and **enhanced-mode** cannot be configured together.
- In the same view, traffic cannot be mirrored to observing ports both in non-enhanced mode and enhanced mode.
- For the CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8850-64CQ-EI, CE8861EI, and CE8868EI, observing ports in enhanced mode can be specified only when you configure simplified traffic mirroring.
- If **observer-port** specifies an observing port in enhanced mode, only incoming traffic mirroring is supported.

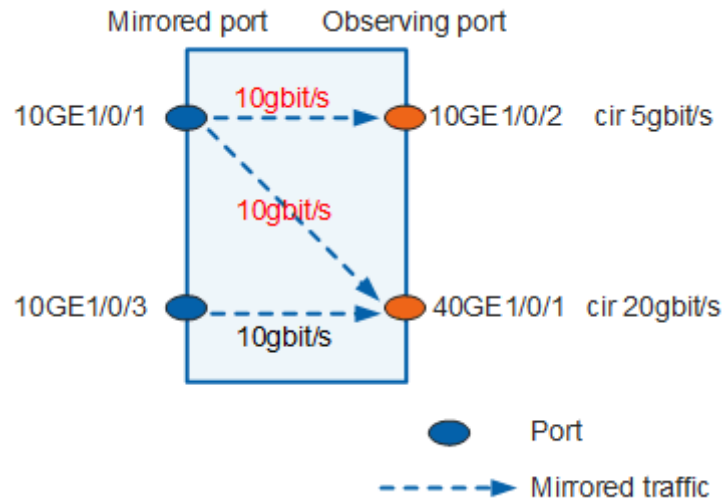
- Rate limiting configured on an observing port takes effect on all the mirrored traffic (including inbound and outbound mirrored traffic) received on the observing port.
- In the 1:N mirroring scenario, if rate limiting is configured on multiple observing ports, the maximum rate limit is used as the bandwidth limit of each observing port. In [Figure 3-8](#), 1:2 port mirroring is configured on the device, and 10GE1/0/1 is the mirrored port. 10GE1/0/2 and 40GE1/0/1 are two observing ports and have the traffic rate limits configured as 5 Gbit/s and 20 Gbit/s respectively. In this situation, the device uses 20 Gbit/s as the bandwidth limit of the two observing ports.

Figure 3-8 Observing ports sharing the maximum bandwidth limit



- In the 1:N mirroring scenario, among N observing ports, if the port with the configured maximum rate limit also functions as an observing port of another mirroring function, the actual bandwidth limit of this observing port in 1:N mirroring will be less than this maximum rate limit. This is because other mirrored packets copied to this observing port will occupy a certain amount of bandwidth. As a result, the bandwidth limit of other observing ports in 1:N mirroring is also less than this maximum rate limit. In [Figure 3-9](#), 1:2 port mirroring is configured on the device, and 10GE1/0/1 is the mirrored port. 10GE1/0/2 and 40GE1/0/1 are two observing ports and have the traffic rate limits configured as 5 Gbit/s and 20 Gbit/s respectively. In this situation, the device uses 20 Gbit/s as the bandwidth limit of the two observing ports. If 40GE1/0/1 is also configured as an observing port in 1:1 port mirroring and mirrored traffic of this port will occupy 10 Gbit/s bandwidth, the actual rate limit of 40GE1/0/1 is 10 Gbit/s in 1:2 port mirroring, and the device uses 10 Gbit/s as the bandwidth limit of the two observing ports (10GE1/0/2 and 40GE1/0/1).

Figure 3-9 Actual bandwidth limit of an observing port being less than the configured maximum rate limit



Example

Configure 10GE1/0/2 as an observing port for Layer 2 remote mirroring, with the VLAN ID set to 2.

```
<HUAWEI> system-view
[~HUAWEI] observe-port 1 interface 10ge 1/0/2 vlan 2
```

Configure 10GE1/0/1 as an observing port for Layer 3 remote mirroring, set the CIR to 20000 kbit/s, and set the destination IP address to 10.1.1.1 and the source IP address to 10.2.2.2.

```
<HUAWEI> system-view
[~HUAWEI] observe-port 2 interface 10ge 1/0/1 destination-ip 10.1.1.1 source-ip 10.2.2.2 cir 20000 kbps
```

Configure Tunnel 1 as an observing port for Layer 3 remote port mirroring.

```
<HUAWEI> system-view
[~HUAWEI] observe-port 2 interface tunnel 1
```

3.2.7 observe-port filter enable

Function

The **observe-port filter enable** command enables the observing port filter.

The **undo observe-port filter enable** command disables the observing port filter.

By default, after a port is configured as an observing port, the port filter is disabled.

NOTE

Only the CE6870EI support this command.

Format

observe-port filter enable
undo observe-port filter enable

Parameters

None

Views

System view

Default Level

3: Configuration level

Usage Guidelines

If packet matching rules are configured on a port, the port filter will filter packets based on the configured rules. If the port filter is disabled, the port will not perform any check on packets and will forward all packets. If broadcast packets even invalid packets exist on the network, data transmission will be affected.

Generally, after a port is configured as an observing port, the port filter is disabled. In this situation, to prevent other services from conflicting with the mirroring service, you are advised not to configure other services on the observing port. If you need to configure other services on the observing port, run the **observe-port filter enable** command to enable the observing port filter. Then service packets to be forwarded by the observing port need to match the rules configured on the port. Otherwise, these packets will be discarded.

Example

Enable the observing port filter.

```
<HUAWEI> system-view  
[~HUAWEI] observe-port filter enable
```

3.2.8 port-mirroring observe-port

Function

The **port-mirroring observe-port** command configures port mirroring on a port.

The **undo port-mirroring** command disables port mirroring on a port.

By default, port mirroring is not configured on a port.

Format

port-mirroring observe-port *observe-port-index* { **both** | **inbound** | **outbound** }
[**session-id** *session-id*]

undo port-mirroring [**observe-port** *observe-port-index*] { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
<i>observe-port-index</i>	Specifies the index of the observing port.	The value is an integer ranging from 1 to 8.
both	Mirrors incoming and outgoing packets on a port.	-
inbound	Mirrors only incoming packets on a port.	-
outbound	Mirrors only outgoing packets on a port.	-
session-id <i>session-id</i>	Specifies a mirroring ID. The <i>session-id</i> parameter is encapsulated in mirrored packets to differentiate different mirrored packets. NOTE - Only the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E support this parameter. - This parameter takes effect only for Layer 3 remote mirroring. - When both this parameter and the erspan-id <i>erspan-id</i> parameter used in the observe-port command are configured, this parameter takes effect first.	The value is an integer that ranges from 0 to 1023.

Views

GE interface view, 10GE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, FC interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In port mirroring, you can run the **port-mirroring observe-port** command to mirror traffic to a specified observing port.

Prerequisites

An observing port has been configured using the **observe-port** command.

Precautions

To ensure that all mirrored packets are transmitted to the observing port, configure the same link type and bandwidth for the mirrored and observing ports.

Example

Mirror incoming packets on 10GE1/0/1 to remote observing port 10GE1/0/2.

```
<HUAWEI> system-view
[~HUAWEI] observe-port 1 interface 10ge 1/0/2 vlan 111
[*HUAWEI] interface 10ge 1/0/1
[*HUAWEI-10GE1/0/1] port-mirroring observe-port 1 inbound
```

3.2.9 traffic-mirroring (interface view)

Function

The **traffic-mirroring** command configures simplified traffic mirroring on an interface.

The **undo traffic-mirroring** command cancels simplified traffic mirroring on an interface.

By default, simplified traffic mirroring is not configured on an interface.

NOTE

The CE6863, CE6863E, CE6863K, CE6881E, CE6820, CE6881K, CE6881, and CE5881 do not support this command.

Format

traffic-mirroring [vxlan [tag-format { none | single }]] { tcp-flag { ack | fin | psh | rst | syn | urg } * } observe-port *observe-port-index* &<1-8> inbound

undo traffic-mirroring [vxlan [tag-format { none | single }]] [tcp-flag { ack | fin | psh | rst | syn | urg } *] [observe-port *observe-port-index* &<1-8>] inbound

Parameters

Parameter	Description	Value
vxlan	Matches VXLAN packets.	-
tag-format	Matches tagged VXLAN packets.	-
none	Matches packets without the inner VLAN tag.	-

Parameter	Description	Value
single	Matches packets with a single layer of inner VLAN tag. NOTE The CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8861EI, and CE8868EI do not support this parameters.	-
tcp-flag	Matches packets based on the TCP flag in a TCP packet header.	-
ack	Matches TCP packets with the TCP flag as ACK (010000).	-
fin	Matches TCP packets with the TCP flag as FIN (000001).	-
psh	Matches TCP packets with the TCP flag as PSH (001000).	-
rst	Matches TCP packets with the TCP flag as RST (000100).	-
syn	Matches TCP packets with the TCP flag as SYN (000010).	-
urg	Matches TCP packets with the TCP flag as URG (100000).	-
observe-port <i>observe-port-index</i>	Specifies the index of an observing port. NOTE You can specify 1 to 8 <i>observe-port-index</i> parameters simultaneously only on the CE6870EI.	The value is an integer that ranges from 1 to 8.
inbound	Mirrors incoming packets on an interface.	-

Views

100GE interface view, 10GE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a Fabric Insight solution, traditional MQC-based traffic mirroring is complex to configure, requiring an observing port, and then a traffic classifier, traffic behavior, and traffic policy to be configured. This mode does not apply to configuration delivery and management in Fabric Insight. Simplified traffic mirroring can facilitate configuration delivery and management.

After simplified traffic mirroring is configured on an interface using the **traffic-mirroring** command, matched incoming packets on this interface are mirrored to observing ports.

Prerequisites

An observing port has been configured using the **observe-port** command.

Precautions

- When the functions as a VXLAN tunnel termination device, and the **traffic-mirroring vxlan tag-format { none | single }** command is executed on the tunnel outbound interface, VXLAN inner packets will be mirrored regardless of whether the packets are tagged.
- Only ordinary IPv4 packets or IPv4 VXLAN-encapsulated inner IPv4 packets can be matched.
- If multiple parameters among **tcp-flag { ack | fin | psh | rst | syn | urg } *** have been specified, the relationship between these parameters is logical OR.
- If simplified traffic mirroring is configured in both the system view and interface view, the configuration in the interface view takes effect.
- When the CE6870EI is an intermediate node of a VXLAN tunnel and simplified traffic mirroring is configured for VXLAN packets, the VXLAN packets cannot be mirrored if the inner packets carry VLAN tags.

Example

Configure simplified traffic mirroring on an interface to mirror incoming packets with the TCP flag as SYN on 10GE1/0/1 to the observing port 1.

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] traffic-mirroring tcp-flag syn observe-port 1 inbound
```

3.2.10 traffic-mirroring (system view)

Function

The **traffic-mirroring** command configures simplified traffic mirroring globally.

The **undo traffic-mirroring** command cancels simplified traffic mirroring globally.

By default, simplified traffic mirroring is not configured globally.

Format

```
traffic-mirroring [ vxlan [ tag-format { none | single } ] ] [ ipv6 ] { tcp-flag  
{ ack | fin | psh | rst | syn | urg } * } observe-port observe-port-index &<1-8>  
inbound [ slot slot-id ]
```

undo traffic-mirroring [**vlan** [**tag-format** { **none** | **single** }]] [**ipv6**] { **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * } **observe-port** *observe-port-index* &<1-8> **inbound** [**slot** *slot-id*]

 NOTE

Only the CE6863, CE6863E, CE6863K, CE6881E, CE6820, CE6881K, CE6881, and CE5881 support the **ipv6** parameter.

tag-format { **none** | **single** } is not supported by the CE6863, CE6863E, CE6863K, CE6881E, CE6820, CE6881K, CE6881, and CE5881.

Parameters

Parameter	Description	Value
vlan	Matches VXLAN packets.	-
tag-format	Matches tagged VXLAN packets.	-
none	Matches packets without the inner VLAN tag.	-
single	Matches packets with a single layer of inner VLAN tag. NOTE The CE6857EI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE8861EI, and CE8868EI do not support this parameters.	-
ipv6	Matches IPv6 packets.	-
tcp-flag	Matches packets based on the TCP flag in a TCP packet header.	-
ack	Matches TCP packets with the TCP flag as ACK (010000).	-
fin	Matches TCP packets with the TCP flag as FIN (000001).	-
psh	Matches TCP packets with the TCP flag as PSH (001000).	-
rst	Matches TCP packets with the TCP flag as RST (000100).	-
syn	Matches TCP packets with the TCP flag as SYN (000010).	-

Parameter	Description	Value
urg	Matches TCP packets with the TCP flag as URG (100000).	-
observe-port <i>observe-port-index</i>	Specifies the index of an observing port. NOTE You can specify 1 to 8 <i>observe-port-index</i> parameters simultaneously only on the CE6870EI.	The value is an integer that ranges from 1 to 8.
inbound	Mirrors incoming packets on an interface.	-
slot <i>slot-id</i>	Specifies the device to which simplified traffic mirroring is applied. <i>slot-id</i> specifies the stack ID of the device.	The value is an integer. You can enter a question mark (?) and select a value from the displayed value range.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a Fabric Insight solution, traditional MQC-based traffic mirroring is complex to configure, requiring an observing port, and then a traffic classifier, traffic behavior, and traffic policy to be configured. This mode does not apply to configuration delivery and management in Fabric Insight. Simplified traffic mirroring can facilitate configuration delivery and management.

After simplified traffic mirroring is configured globally using the **traffic-mirroring** command, matched incoming packets on all interfaces or interfaces in a specified device to an observing port.

Prerequisites

An observing port has been configured using the **observe-port** command.

Precautions

- When the CE6865EI, CE6865E, CE8850E-32CQ-EI and CE6857EI, CE6857E, CE6857F functions as a VXLAN tunnel termination device, and the **traffic-mirroring vxlan tag-format { none | single }** command is executed on the tunnel outbound interface, VXLAN inner packets will be mirrored regardless of whether the packets are tagged.

- Only ordinary IPv4 packets or IPv4 VXLAN-encapsulated inner IPv4 packets can be matched.
- If multiple parameters among **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * have been specified, the relationship between these parameters is logical OR.
- If simplified traffic mirroring is configured in both the system view and interface view, the configuration in the interface view takes effect.
- When the CE6870EI is an intermediate node of a VXLAN tunnel and simplified traffic mirroring is configured for VXLAN packets, the VXLAN packets cannot be mirrored if the inner packets carry VLAN tags.

Example

Configure simplified traffic mirroring globally to mirror incoming packets with the TCP flag as SYN on all interfaces to the observing port 1.

```
<HUAWEI> system-view  
[~HUAWEI] traffic-mirroring tcp-flag syn observe-port 1 inbound
```

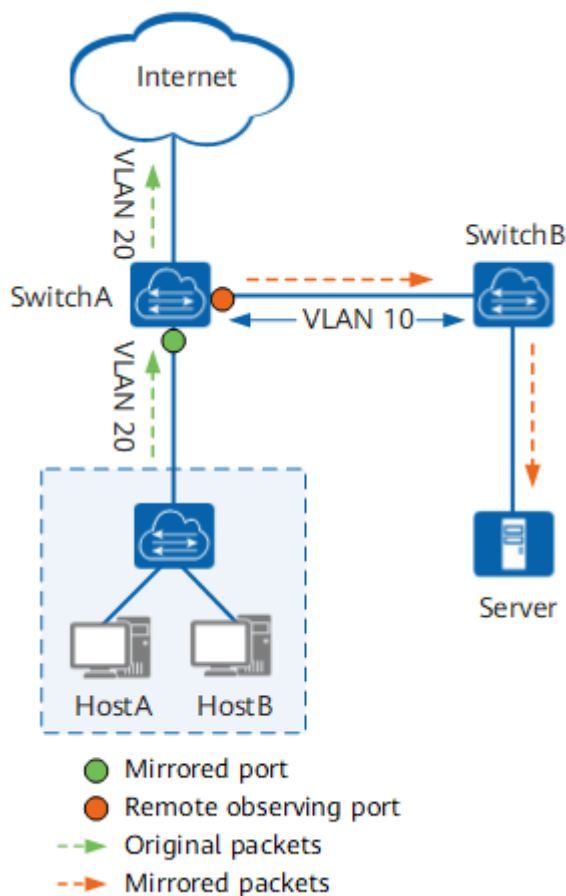
3.3 FAQ

3.3.1 Why Does MAC Address Learning Need to Be Disabled When Layer 2 Remote Port Mirroring Is Configured in Some Scenarios?

First, you need to understand how mirrored packets are forwarded to the monitoring device after Layer 2 remote port mirroring is configured.

As shown in [Figure 3-10](#), in Layer 2 remote port mirroring, the remote observing port receives the mirrored packets from the mirrored port, adds another VLAN tag (VLAN 10) to the packets tagged with VLAN 20, and then forwards the mirrored packets to the server by following the Layer 2 forwarding process. The destination MAC address of mirrored packets is the same as that of the original packets, but not the server's MAC address. To reach the server, the mirrored packets must be treated as unknown unicast packets and forwarded in broadcast mode. The mirrored packets can be forwarded to the server in broadcast mode as long as the MAC address table of VLAN 10 contains no entry matching the destination MAC address of the mirrored packets.

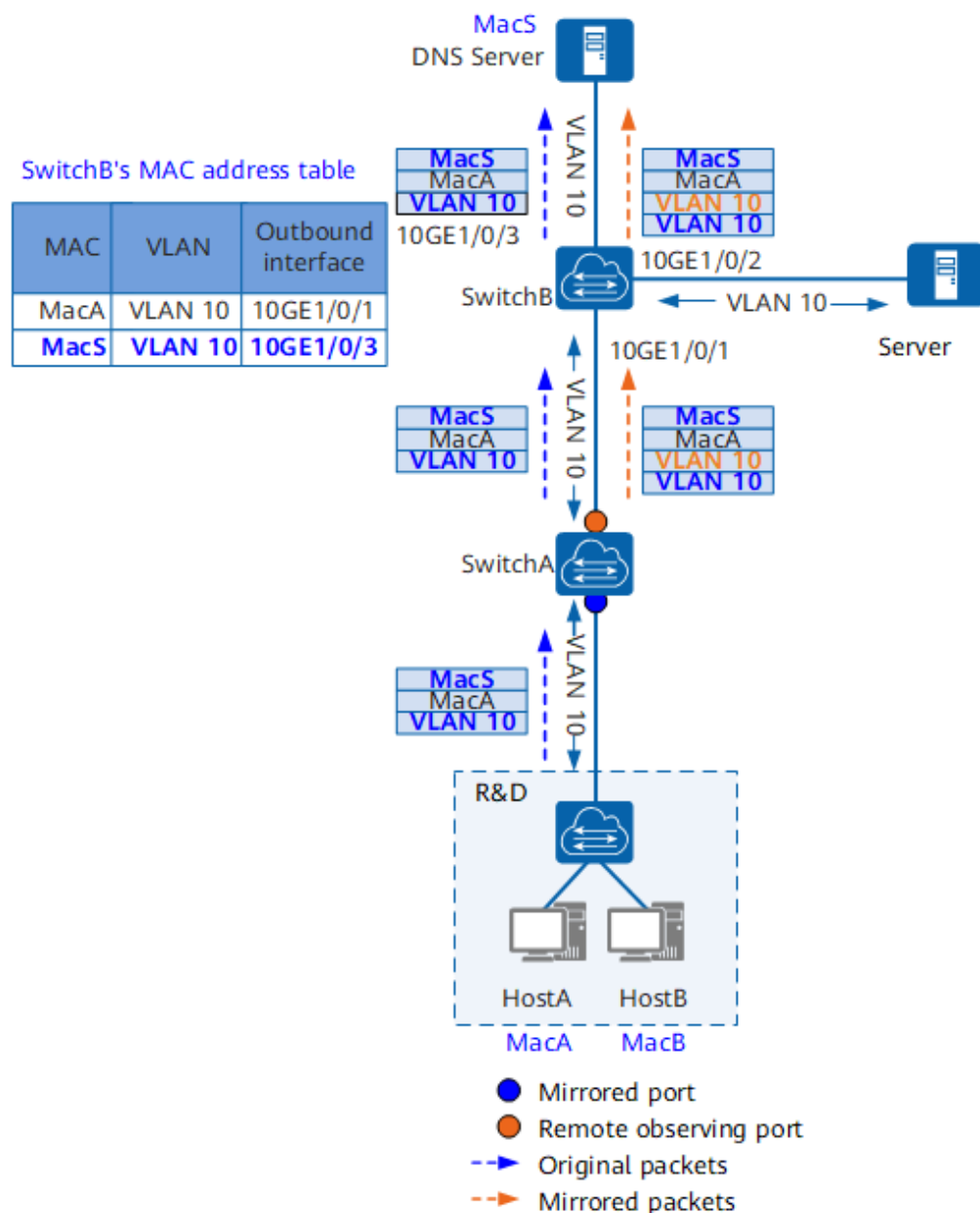
Figure 3-10 Mirrored packet forwarding in a Layer 2 remote port mirroring scenario



In most Layer 2 remote mirroring scenarios, intermediate devices will not learn destination MAC addresses of mirrored packets in the corresponding VLANs. This means that mirrored packets can be forwarded to the monitoring devices in broadcast mode. In the following scenarios, however, Layer 2 remote port mirroring will fail because destination MAC addresses of mirrored packets can be learned in the corresponding VLANs.

- **The original service traffic and mirrored traffic are forwarded in the same VLAN.**

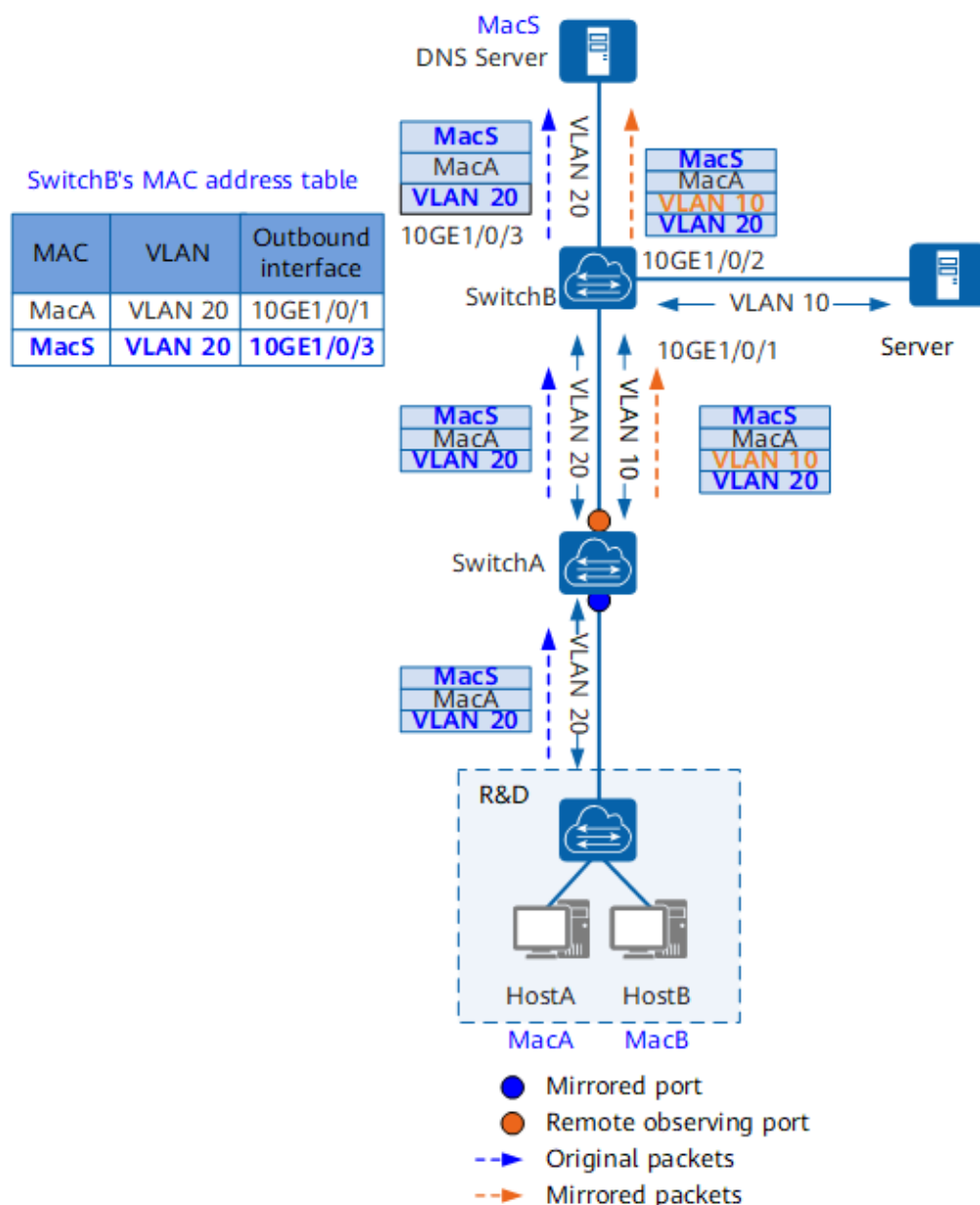
Figure 3-11 Layer 2 remote port mirroring fails when the original service traffic and mirrored traffic are forwarded in the same VLAN



As shown in **Figure 3-11**, a company configures Layer 2 remote port mirroring on SwitchA to monitor the traffic sent from employees in the R&D department to the DNS server. The original traffic and mirrored traffic are both forwarded through VLAN 10. When SwitchA receives the packets sent from HostA to the DNS server, it copies the packets and forwards the mirrored packets in VLAN 10. The mirrored packets and original packets all use the MAC address of the DNS server as the destination MAC address. SwitchB between HostA and the DNS server learns the MAC address entry matching the DNS server. Therefore, SwitchB forwards the mirrored packets with the destination MAC address set to the DNS server MAC address according to the learned MAC address entry in VLAN 10. As a result, Layer 2 remote port monitoring fails.

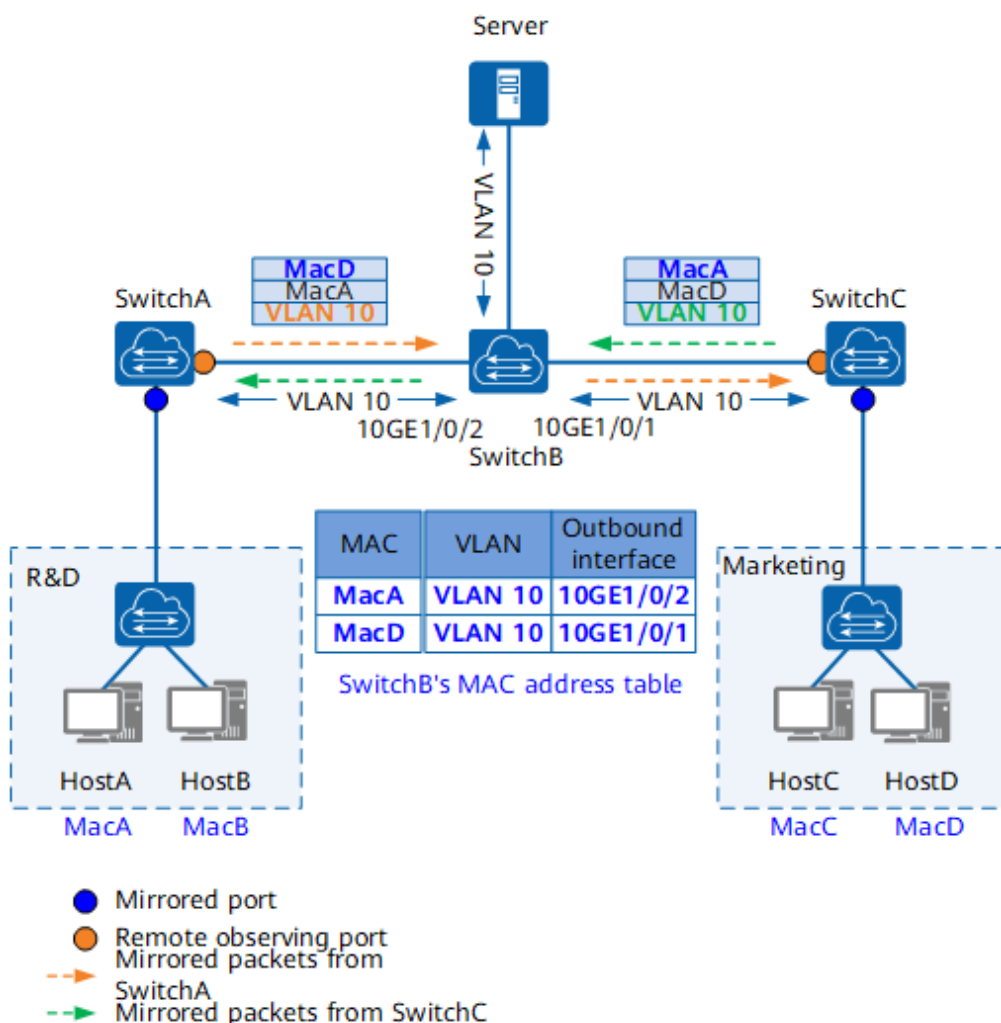
To resolve this problem, use different VLANs to forward the original service traffic and mirrored traffic, as shown in **Figure 3-12**. If the original service traffic and mirrored traffic need to be forwarded in the same VLAN, run the **mac-address learning disable** command on the intermediate devices to disable MAC address learning in this VLAN. However, disabling MAC address learning will cause a waste of link bandwidth.

Figure 3-12 Original service traffic and mirrored traffic are forwarded in different VLANs



- Mirrored packets from different source MAC addresses are forwarded in the same VLAN.

Figure 3-13 Layer 2 remote port mirroring fails when mirrored packets from different source MAC addresses are forwarded in the same VLAN

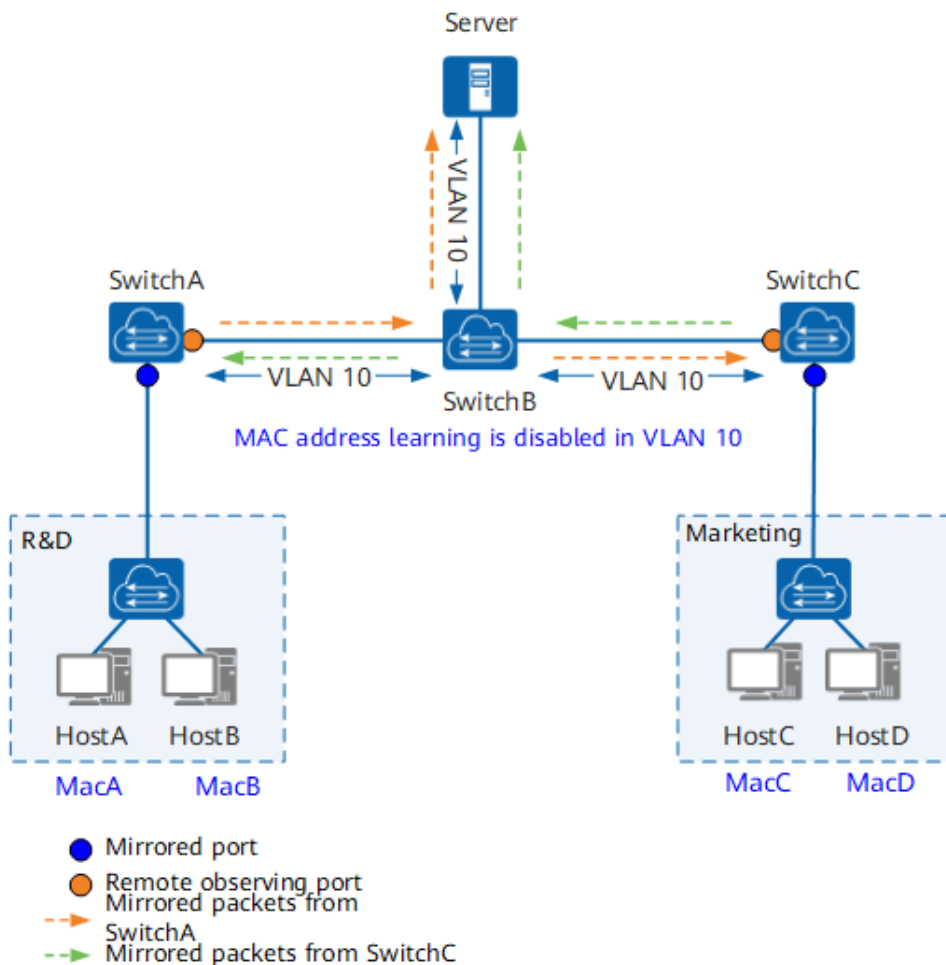


As shown in [Figure 3-13](#), a company configures Layer 2 remote port mirroring on SwitchA and SwitchC to monitor communication traffic between the R&D and marketing departments. All mirrored packets are forwarded in VLAN 10, and the original communication traffic between the two departments is forwarded in another VLAN. When packets sent from downstream hosts arrive at the mirrored port on SwitchA and SwitchC, SwitchA and SwitchC copy the packets and forward the mirrored packets in VLAN 10. Source MAC addresses of the mirrored packets are MAC addresses of sender hosts, which can be learned in the MAC address table of SwitchB. Because destination MAC addresses of the mirrored packets are MAC addresses of destination hosts, SwitchB forwards the mirrored packets according to the matching entries found in its MAC address table. Layer 2 remote port mirroring fails.

Use any of the following methods to solve the preceding problem:

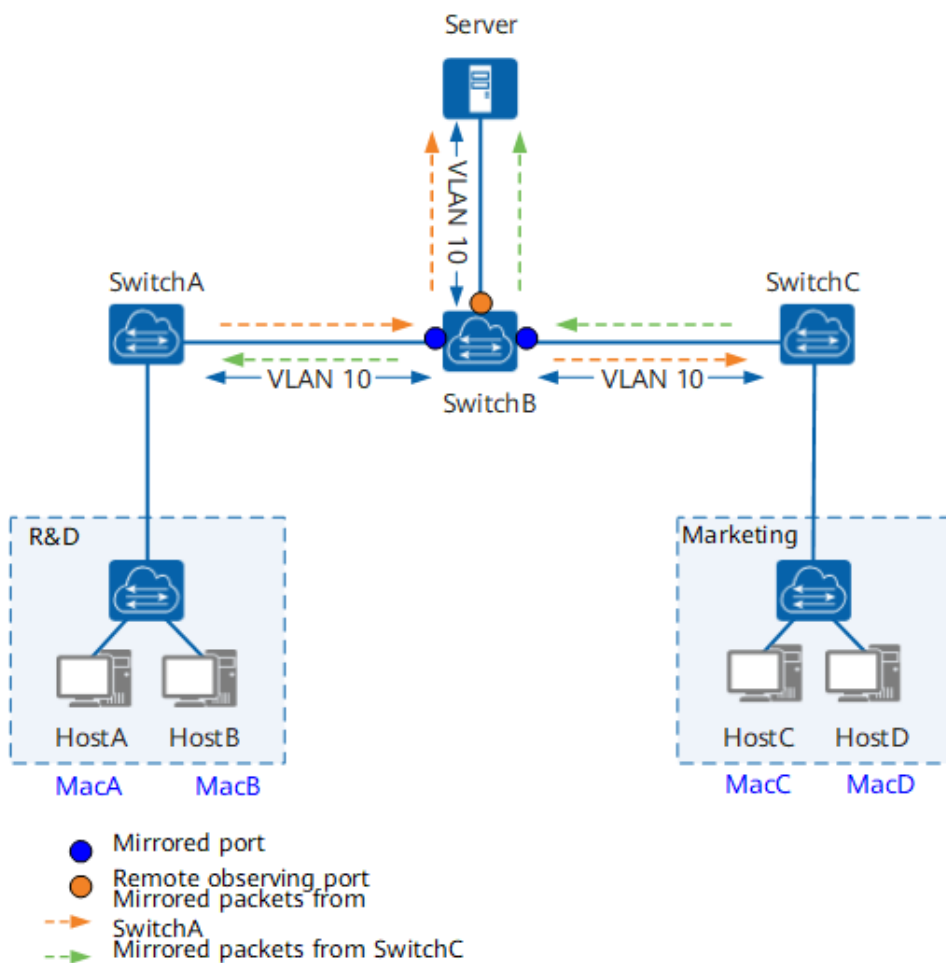
- Run the **mac-address learning disable** command on SwitchB to disable MAC address learning in VLAN 10. [Figure 3-14](#) shows the packet flows after MAC address learning is disabled in VLAN 10.

Figure 3-14 MAC address learning is disabled in VLAN 10



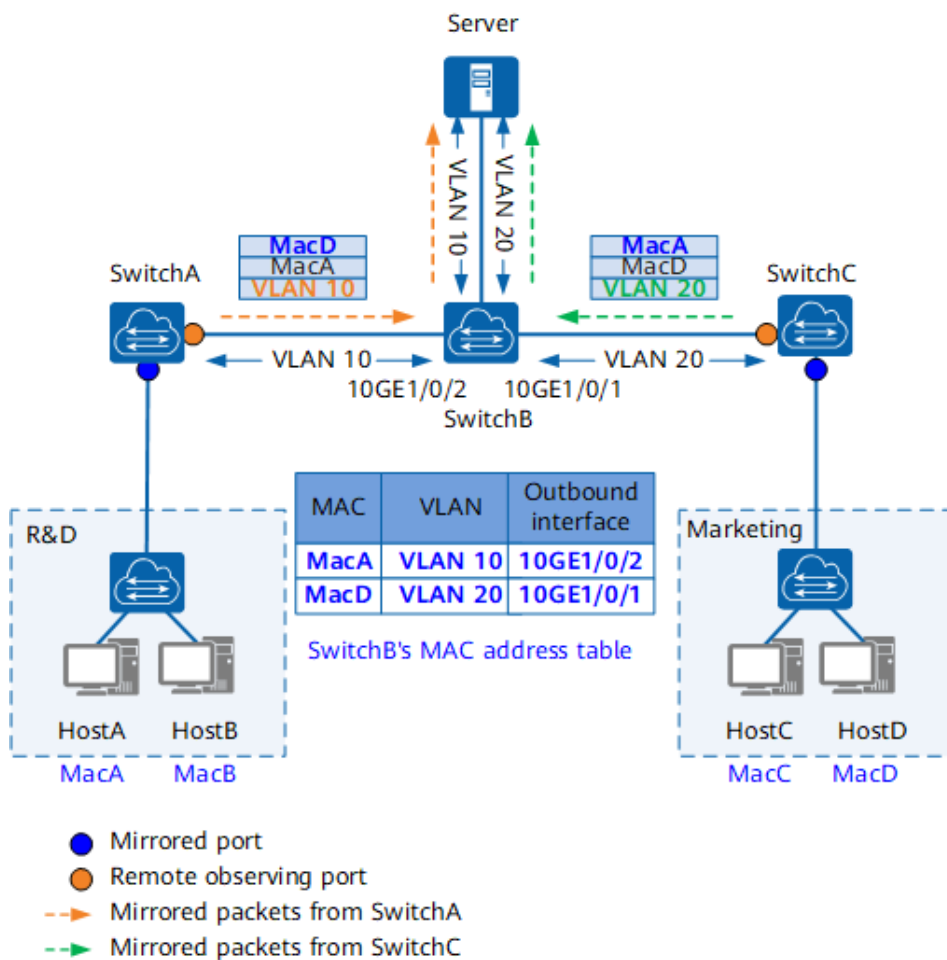
- Configure port mirroring on SwitchB: configure the ports connected to SwitchA and SwitchC as mirrored ports, and configure the port connected to the monitoring server as a local observing port. [Figure 3-15](#) shows the packet flow after port mirroring is configured on SwitchB.

Figure 3-15 Local port mirroring is configured on SwitchB



- Use different VLANs to forward the mirrored packets in different directions, as shown in [Figure 3-16](#).

Figure 3-16 Mirrored packets in different directions are forwarded in different VLANs



4

Remote Mirroring Personal Data
Description

Us ag e Sce nar io	Col lec ted Per son al Da ta	Data Source and Collection Method	Purpose and Security Measure	Data Retenti on Period and Policy	Data Deletio n Metho d	Export Metho d (Interf aces or Comm ands) and Imple menta tion Schem e (Anon ymizat ion or Pseud onymi zation)	Data Expo rt Guid e

Re mo te mir ror ing	Sou rce and des tin ati on IP add ress es Sou rce and des tin ati on MA C add ress es Pac ket dat a	The data comes from the network traffic passing through the device. The administrator can configure a remote observing port to copy network traffic to the observing port. The device does not collect data.	Mainly used for network detection and fault management. The device sends mirrored packets to monitoring devices for analysis. Only the administrator has the permission to perform this operation.	The device does not retain data.	The device does not retain data.	The device does not retain data.	The device does not retain data.
-------------------------------------	---	---	---	----------------------------------	----------------------------------	----------------------------------	----------------------------------