

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

Plug-in Operation Guide - Packet Capture

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>

Contents

1 About This Document.....	1
2 Document Overview.....	5
2.1 Basic Information.....	5
2.2 Antivirus Scan Report.....	6
3 Plug-In Installation Guide.....	7
3.1 Precautions for Plug-In Installation.....	7
3.2 Preparations.....	8
3.2.1 Preparing the Plug-in.....	8
3.2.2 Verifying the Running System Software Version.....	10
3.2.3 Checking Available Space in the Flash Memory.....	10
3.3 Plug-in Installation Procedure.....	11
3.3.1 Uploading/Downloading the Plug-in to the Device.....	12
3.3.1.1 Uploading the Plug-In to the Switch Functioning as an FTP Server.....	12
3.3.1.2 Downloading the Plug-In to the Switch Functioning as an FTP Client.....	13
3.3.1.3 Downloading the Plug-In to the Switch Functioning as an SFTP Client.....	15
3.3.2 Installing the Plug-in.....	16
3.3.3 Verifying the Installation.....	17
3.4 Uninstalling the Plug-in.....	17
4 Packet Capture Operation Guide.....	19
4.1 Packet Capture Configuration.....	19
4.1.1 Overview of Packet Capture.....	19
4.1.2 Licensing Requirements and Limitations for Packet Capture.....	20
4.1.3 Configuring the Device to Capture Forwarded Packets.....	22
4.1.4 Configuring the Device to Capture Packets Sent to the CPU.....	24
4.1.5 Configuration Examples for Packet Capture.....	25
4.1.5.1 Example for Configuring Packet Capture Function.....	25
4.2 Packet Capture Configuration Command.....	27
4.2.1 capture-packet file limit.....	27
4.2.2 capture-packet interface.....	28
4.2.3 capture-packet local-host.....	34
4.2.4 display capture-packet config-state.....	38
4.2.5 display capture-packet file.....	39

5 Packet Capture Personal Data Description..... 43

1 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
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

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

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

2 Document Overview

- 2.1 Basic Information
- 2.2 Antivirus Scan Report

2.1 Basic Information

Table 2-1 describes the basic information about plug-ins of CloudEngine 9800, 8800, 6800, and 5800 series switches.

Table 2-1 Basic information about plug-ins

Applicable Product	Plug-in Name	Applicable Software Version
CE9860EI	CE9800_V200R023C00SPC500_CAPTURE_MOD001.MOD	V200R023C00SPC500
CE8850EI	CE8850EI_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE8861EI	CE8861EI_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE8868EI	CE8868EI_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE6881/ CE6820/ CE6863/ CE6863E/ CE6881K/ CE6863K/ CE6881E	CE6800_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE6856HI	CE6856HI_V200R023C00SPC500_CAPTURE_MOD001.MOD	

Applicable Product	Plug-in Name	Applicable Software Version
CE6857EI	CE6857EI_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE6857E	CE6857E_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE6857F	CE6857F_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE6865EI	CE6865EI_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE6865E, CE8850E-32 CQ-EI	CE6865E_V200R023C00SPC500_CAPTURE_MOD001.MOD	
CE6870-48S 6CQ-EI	CE6870S- EI_V200R023C00SPC500_CAPTURE_M OD001.MOD	
CE6870-48T 6CQ-EI	CE6870T- EI_V200R023C00SPC500_CAPTURE_M OD001.MOD	
CE5882	CE5882_V200R023C00SPC500_CAPTU RE_MOD001.mod	
CE5881	CE5800_V200R023C00SPC500_CAPTU RE_MOD001.MOD	
CE5855E	CE5855E_V200R023C00SPC500_CAPT URE_MOD001.MOD	
CE5855F	CE5855F_V200R023C00SPC500_CAPT URE_MOD001.MOD	

2.2 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.

3 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.

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

[3.2 Preparations](#)

[3.3 Plug-in Installation Procedure](#)

[3.4 Uninstalling the Plug-in](#)

3.1 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 3-1 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.

3.2 Preparations

3.2.1 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 3-2](#).

Table 3-2 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

3.2.2 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

3.2.3 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

3.3 Plug-in Installation Procedure

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

Table 3-3 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.

3.3.1 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.

3.3.1.1 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)): ftpuser //Enter the FTP user name.
331 Password required for ftpuser.
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

3.3.1.2 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 **ftpuser**, 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

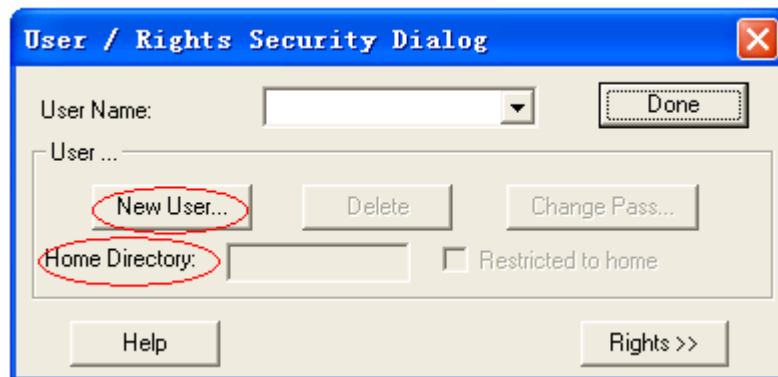
The FTP protocol has security risks; therefore, SFTP is recommended for file management.

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 3-1 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

3.3.1.3 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.

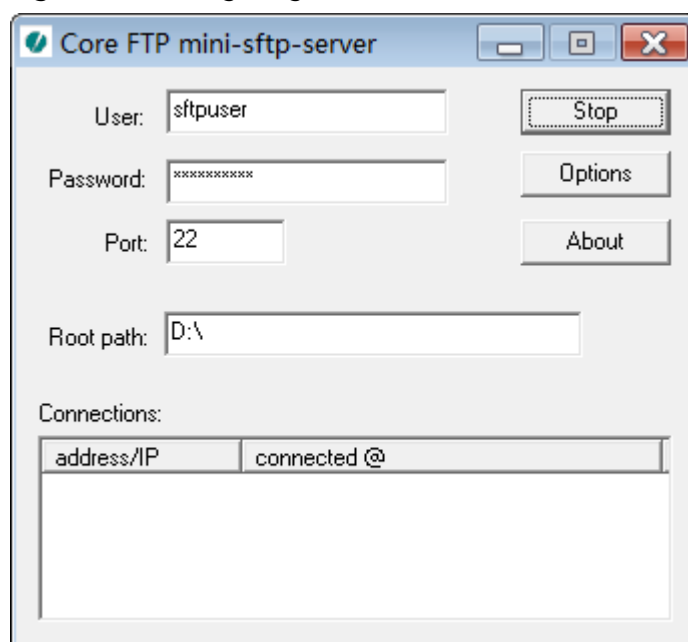
In the following example, the switch is used as the SFTP client and the PC is used as the SFTP server. The SFTP user name is **sftpuser**, the password is **Huawei@123**, the switch IP address is **10.1.1.2/24**, and the PC IP address is **10.1.1.1/24**. You can change the settings according to the live-network 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 3-2 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

3.3.2 Installing the Plug-in

Two methods are available to install the plug-in. Select a method according to [3.1 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
```

3.3.3 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.

3.4 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
```

4 Packet Capture Operation Guide

[4.1 Packet Capture Configuration](#)

This chapter describes how to configure packet capture and provides a configuration example.

[4.2 Packet Capture Configuration Command](#)

4.1 Packet Capture Configuration

This chapter describes how to configure packet capture and provides a configuration example.

NOTE

The device supports the packet header obtaining function, which is mainly used to detect transmission faults and errors. Huawei cannot collect or store user communication information without permission. Therefore, you must ensure that this function is used for legitimate purposes and within the boundaries defined by applicable laws and regulations. During the collection and storage of user communication information, measures must be taken to protect user communication information.

4.1.1 Overview of Packet Capture

This function improves network maintenance efficiency and reduces maintenance costs. As Internet develops, devices on a network transmit various services, and network administrators often need to capture packets on devices to locate faults. The packet capturing function allows devices to capture received packets for fault location. This function simplifies the configurations of packet analysis device and network monitoring device.

After the packet capturing function is enabled, the devices capture the packets matching certain conditions. The maintenance personnel can run commands to view information about captured packets or save the captured packets to the local storage media as *.cap files. The saved files can be downloaded for fault analysis. This function greatly improves maintenance efficiency and reduces maintenance costs.

The CloudEngine 9800, 8800, 6800, and 5800 series switches can capture the following two types of packets:

- Forwarded packets: If the device fails to forward traffic correctly, for example, the traffic does not match the traffic model, configure the packet capture function to capture forwarded packets for analysis. This allows the device to process invalid packets in time, ensuring that network data can be transmitted correctly.
- Packets sent to the CPU: When a CPU fault occurs, such as the CPU usage is high, configure the packet capture function to capture packets sent to the CPU for analysis. This allows the device to process invalid packets in time, ensuring that the CPU works properly.

4.1.2 Licensing Requirements and Limitations for Packet Capture

Involved Network Elements

Other network elements are not required.

Licensing Requirements

Packet capture is a basic function of switches, and as such is controlled by the license for basic software functions. This license has been loaded and activated before delivery. You do not need to manually activate it.

Version Requirements

Table 4-1 Products and minimum version supporting packet capture

Product Model	Minimum Version Required
CE9860EI	V200R020C00
CE8868EI/CE8861EI	V200R005C10
CE8850-32CQ-EI	V200R002C50
CE8850-64CQ-EI	V200R005C00
CE6857EI	V200R005C10
CE6857E	V200R020C10
CE6857F	V200R021C00
CE6870-48S6CQ-EI	V200R001C00
CE6870-48S6CQ-EI-A	V200R022C00
CE6856HI/CE6870-48T6CQ-EI	V200R002C50
CE6881/CE6820/CE6863	V200R005C20
CE6863E	V200R021C00
CE5881	V200R020C00

Product Model	Minimum Version Required
CE6881K	V200R019C10
CE6863K	V200R019C10
CE6881E	V200R019C10
CE6865EI	V200R005C00
CE6865E	V200R021C00
CE8850E-32CQ-EI	V200R021C10
CE5855E	V200R020C10
CE5855F	V200R021C00

NOTE

For details about the mapping between software versions and switch models, see the [Hardware Query Tool](#).

Software version evolution:

- For switches excluding the CE9860EI, CE6881, CE6881E, CE6881K, CE6863, CE6863K, CE6820, CE5881
V100R001C00 -> V100R002C00 -> V100R003C00 -> V100R003C10 -> V100R005C00 -> V100R005C10 -> V100R006C00 -> V200R001C00 -> V200R002C50 -> V200R003C00 -> V200R005C00 -> V200R005C10 -> V200R019C00 -> V200R019C10 -> V200R020C10 -> V200R021C00 -> V200R021C10 -> V200R022C00 -> V200R022C10 -> V200R023C00
- For the CE9860EI, CE6881, CE6881E, CE6881K, CE6863, CE6863K, CE6820, CE5881
V200R005C20 -> V200R019C10 -> V200R020C00 -> V200R020C10 -> V200R021C00 -> V200R021C10 -> V200R022C00 -> V200R022C10 -> V200R023C00

Feature Limitations

Captured packets are cached in .cap files in the flash card. When the remaining space of the flash card is less than or equal to 10 MB, there is insufficient space for capturing data. In this case, the capture function cannot be used normally.

If traffic control is triggered by a large amount of delivered configuration data or telemetry data collection, the packet capture function is unavailable.

Restriction of capturing forwarded packets

- Packet capture is supported in both inbound and outbound directions on the CE6881, CE5881, CE6881K, CE6863, CE6863E, CE6863K, CE6881E, and CE6820, and only one packet capture instance is supported.
- The CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, and CE6870EI cannot capture packets on stack member ports or logical stack ports. Other stack-capable switches can capture packets on stack member ports, but not logical stack ports.
- When the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, or CE6870EI captures packets without VLAN information, no VLAN

information is displayed. When other switches capture packets without VLAN information, the default VLAN of interfaces is displayed.

- The CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, and CE6870EI can capture packets on Eth-Trunks, but not specified Eth-Trunk member interfaces. Other switches can capture packets on both Eth-Trunks and Eth-Trunk member interfaces.
- The packet capture function of the device conflicts with other functions (such as the function of sending protocol packets to the CPU and mirroring function). When the packet capture function is configured together with the function of sending protocol packets to the CPU or the mirroring function, only one function takes effect.
- For the CE6881, CE5881, CE6881K, CE6820, CE6863E, CE6863K, CE6881E, and CE6863, the **protocol** field in an IPv6 ACL supports only TCP, UDP, ICMPv6, OSPF, and GRE.
- If a CE6870EI switch is configured to capture packets with matching VLAN information, the packets forwarded by sub-interfaces cannot be captured.
- When the CE9860EI, CE8850EI, CE8861EI, CE8868EI, CE6856HI, CE6857E, CE6857F, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE5855E, CE5855F or CE6857EI functions as a VXLAN termination node, only packets terminated at the tunnel side can be matched, and passerby packets transparently transmitted on VXLAN cannot be matched.
- When both intelligent traffic analysis and inbound forwarded packet capture are configured, intelligent traffic analysis takes effect.

Restriction of capturing packets sent to the CPU

- The device supports a maximum of eight packet capture instances.
- When the CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, or CE6870EI captures packets without VLAN information, no VLAN information is displayed. When other switches capture packets without VLAN information, the default VLAN of interfaces is displayed.
- The device cannot capture packets on logical stack interfaces or stack member interfaces of stack members.
- The device can capture packets on Eth-Trunks, but not on Eth-Trunk member interfaces.

4.1.3 Configuring the Device to Capture Forwarded Packets

If the device fails to forward traffic correctly, you can configure the packet capture function to capture forwarded packets for analysis, so that you can process invalid packets in time and ensure correct transmission of network data.

Precautions

Pay attention to the following when configuring the device to capture forwarded packets:

- The device supports only one packet capture instance.
- You can set the timeout period specified by *time* and the number of packets to be captured specified by *number* for a packet capture instance. If the

timeout period expires or the specified number of packets are captured, the system stops capturing packets.

- You can set packet capture parameters based on the number of packets on the interface. If a large number of packets are forwarded on an interface, set the *time* parameter to a small value and the *number* parameter to a large value. If a small number of packets are forwarded on an interface, set the *time* parameter to a large value and the *number* parameter to a small value.
- If resources on the device are insufficient, the system displays a message "Failed to capture packet on slot [slot], because the resource is not enough to use." In this case, the packet capture function is unavailable. It is recommended that you capture packets using other methods such as mirroring.

Procedure

Step 1 Run **capture-packet interface** { *interface-type interface-number* } &<1-4> [**vlan** [*vni vni-id*] [**tag-format** { **none** | **single** }] [**acl** *acl-number*] [**vlan** *vlan-id* | **inner-vlan** *inner-vlan-id* | **acl** { *acl-number* | **ipv6** *acl6-number* }] *] [**clear payload**] [**inbound** | **outbound** | **both**] **destination** { **terminal** | **file** *file-name* } * [**time-out** *time* | **packet-num** *number* | **packet-len** *length*] *

An instance for capturing forwarded packets is configured.

- If an ACL is specified for matching the inner packets encapsulated in VXLAN packets to be captured, the ACL rules can contain only the source MAC address, Ethernet frame type, destination IP address, source IP address, destination port number, and source port number. If the ACL rules specify other options, VXLAN packets cannot be captured.
- If an ACL is specified for matching Layer 2 packets, the ACL rules can contain only the outer VLAN tag, inner VLAN tag, source MAC address, destination MAC address, Ethernet II encapsulation format, and 802.1p priority. If the ACL rules specify other options, Layer 2 packets cannot be captured.
- If an ACL is specified for matching Layer 3 packets, the ACL rules can contain only the source IP address, destination IP address, protocol type, source port number, destination port number, ICMP type, ICMP code, TCP flag, fragment type, and ToS. If the ACL rules specify other options, Layer 3 packets cannot be captured.
- If you configure the device to match VXLAN packets without inner VLAN tags and also configure a Layer 2 ACL to match packets, tagged packets will be captured.

When the **clear payload** parameter is specified, the switch sets the data content in the captured TCP and UDP packets to 0.

NOTE

Only the CE8868EI, CE8861EI, CE8850EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, CE6870EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857EI, CE6857E, CE6857F, CE6856HI can capture VXLAN packets when the original Ethernet frame information in the VXLAN packets matching the specified conditions.

The CE9860EI and CE6870EI do not support the **inner-vlan** *inner-vlan-id* parameter.

Step 2 (Optional) Run **capture-packet file limit** *limit-value*

The maximum number of packet capture files (.cap files) that can be stored in a directory is configured.

By default, a maximum of 10 packet capture files can be stored in a directory.

----End

4.1.4 Configuring the Device to Capture Packets Sent to the CPU

When the CPU of a device is abnormal, you are advised to capture packets sent to the CPU for analysis, so that you can process invalid packets in time and ensure stable running of the CPU.

Precautions

Pay attention to the following when configuring the device to capture packets sent to the CPU:

- You can set the timeout period specified by *time* and the number of packets to be captured specified by *number* for a packet capture instance. If the timeout period expires or the specified number of packets are captured, the system stops capturing packets.
- You can set packet capture parameters based on the number of packets on the interface. If a large number of packets are forwarded on an interface, set the *time* parameter to a small value and the *number* parameter to a large value. If a small number of packets are forwarded on an interface, set the *time* parameter to a large value and the *number* parameter to a small value.
- The device supports a maximum of eight capture instances.
- The device can capture packets on the Eth-Trunk interface but cannot capture packets on a specified Eth-Trunk member interface.
- In a packet capturing instance, the packets on a maximum of four interfaces can be captured. If you delete any interface from the instance or an interface goes Down, the entire instance is deleted.
- If the ACL and VLAN parameters as well as the specified interfaces in an instance you want to configure are the same as those in an existing instance, the device considers that this instance has been enabled.
- The device can capture packets of various protocols sent to the CPU.
- The device cannot capture packets on stack ports or physical ports of stack members.

Procedure

Step 1 Run **capture-packet local-host** [**interface** { *interface-type interface-number* } &<1-4>] [**acl** { { *acl-number* | **name** *acl-name* } | **ipv6** { *acl6-number* | **name** *acl6-name* } } | **vlan** *vlan-id* | **inner-vlan** *inner-vlan-id*] * **destination** { **terminal** | **file** *file-name* } * [**time-out** *time* | **packet-num** *number* | **packet-len** *length*] *

The device is configured to capture packets sent to the CPU.

Step 2 (Optional) Run **capture-packet file limit** *limit-value*

The maximum number of packet capture files (.cap files) that can be stored in a directory is configured.

By default, a maximum of 10 packet capture files can be stored in a directory.

----End

4.1.5 Configuration Examples for Packet Capture

This section only provides configuration examples for individual features. For details about multi-feature configuration examples, feature-specific configuration examples, interoperation examples, protocol or hardware replacement examples, and industry application examples, see the *Typical Configuration Examples*.

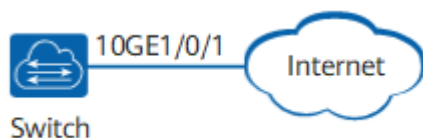
4.1.5.1 Example for Configuring Packet Capture Function

Networking Requirements

As shown in [Figure 4-1](#), the switch connects to the network through 10GE1/0/1.

A fault occurs on the [Figure 4-1](#), for example, the CPU or traffic forwarding process is abnormal. The network administrator wants to capture the packets sent to the CPU or forwarded to other devices through 10GE1/0/1, and display information about captured packets on the screen so that the administrator can process invalid packets in a timely manner. This ensures stable running of the CPU and correct network data transmission.

Figure 4-1 Networking diagram for configuring the packet capture function



Configuration Roadmap

The configuration roadmap is as follows:

1. Capture all packets to be forwarded and display information about these packets on a terminal.
2. Capture packets sent to the CPU and display captured packet information on the terminal.

Procedure

- Step 1** Capture packet to be forwarded on 10GE1/0/1 and display information about these packets on a terminal.

```
<HUAWEI> capture-packet interface 10GE 1/0/1 destination terminal packet-num 1 packet-len 64
Warning: Capture-packet will be shown on terminal.
<HUAWEI>
Packet: 0 Interface: 10GE1/0/1
```

```
-----
00 25 9e 95 7c 4e 00 25 9e 95 7c 3e 81 00 20 de
08 06 00 01 08 00 06 04 00 02 00 25 9e 95 7c 3e
c0 a8 27 01 00 25 9e 95 7c 4e c0 a8 27 02 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----
```

-----capture report-----

```
Capture-Packet Index 1
Type      : forwarding
Interface : 10GE1/0/1
Direction : inbound
Time-out  : 60 seconds
Packet-num : 1
Packet-len : 64
BufferOnly : disabled
-----
```

Step 2 Capture packets sent to the CPU and display captured packet information on the terminal.

```
<HUAWEI> capture-packet local-host interface 10GE 1/0/1 destination terminal packet-num 3 time-out 10
```

Info: Capture-packet will be shown on terminal.

```
<HUAWEI>
```

```
Packet: 0 Interface: 10GE1/0/1
```

```
-----
00 25 9e 95 7c 40 00 19 21 db 25 a3 08 00 45 00
00 28 fb df
-----
```

```
Packet: 1 Interface: 10GE1/0/1
```

```
-----
00 25 9e 95 7c 40 00 19 21 db 25 a3 08 00 45 00
00 28 fb e4
-----
```

```
Packet: 2 Interface: 10GE1/0/1
```

```
-----
00 25 9e 95 7c 40 00 19 21 db 25 a3 08 00 45 00
00 28 fb e8
-----
```

-----capture report-----

```
Capture-Packet Index 8
Type      : local-host
LinkType  : ethernet
Interface : 10GE1/0/1
Time-out  : 10 seconds
Packet-num : 3
```

```
Packet-len : 20
BufferOnly : disabled
-----
```

----End

Configuration Files

None

4.2 Packet Capture Configuration Command

NOTE

The device supports the packet header obtaining function, which is mainly used to detect transmission faults and errors. Huawei cannot collect or store user communication information without permission. Therefore, you must ensure that this function is used for legitimate purposes and within the boundaries defined by applicable laws and regulations. During the collection and storage of user communication information, measures must be taken to protect user communication information.

4.2.1 capture-packet file limit

Function

The **capture-packet file limit** command configures the maximum number of packet capture files (.cap files) that can be stored in a directory.

The **undo capture-packet file limit** command restores the default maximum number of packet capture files that can be stored in a directory.

By default, a maximum of 10 packet capture files can be stored in a directory.

Format

capture-packet file limit *limit-value*

undo capture-packet file limit [*limit-value*]

Parameters

Parameter	Description	Value
<i>limit-value</i>	Specifies the maximum number of packet capture files that can be stored in a directory.	The value is an integer that ranges from 1 to 50.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure the maximum number of packet capture files that can be stored in a directory to save storage space on the device and ensure that new packet capture files can be stored.

Precautions

After the **capture-packet file limit** command is run, if the number of packet capture files in the directory exceeds the upper limit, the system does not delete excess files immediately. Instead, the system deletes the earliest one or more files when new packet capture files are created next time.

Example

Set the maximum number of packet capture files that can be stored in a directory to 20.

```
<HUAWEI> system-view  
[~HUAWEI] capture-packet file limit 20
```

4.2.2 capture-packet interface

Function

The **capture-packet interface** command configures an instance for capturing forwarded packets.

The **undo capture-packet** command deletes the configured packet capture instance.

By default, no instance is configured for capturing forwarded packets.

Format

capture-packet interface { *interface-type interface-number* } &<1-4> [**vlan** [**vni** *vni-id*] [**acl** *acl-number* | **tag-format** { **none** | **single** } **acl** *acl-number*] | [**vlan** *vlan-id* | **inner-vlan** *inner-vlan-id* | **acl** { *acl-number* | **ipv6** *acl6-number* }] *] [**clear payload**] [**inbound** | **outbound** | **both**] **destination** { **terminal** | **file** *file-name* } * [**time-out** *time* | **packet-num** *number* | **packet-len** *length*] *

undo capture-packet [*capture-index*]

NOTE

Only the CE8868EI, CE8861EI, CE8850EI, CE6881, CE5881, CE6881K, CE6820, CE6863, CE6863E, CE6863K, CE6881E, CE6870EI, CE6865EI, CE6865E, CE8850E-32CQ-EI, CE6857EI, CE6857E, CE6857F, CE6856HI can capture VXLAN packets when the original Ethernet frame information in the VXLAN packets matching the specified conditions.

The CE9860EI and CE6870EI do not support the **inner-vlan** *inner-vlan-id* parameter.

Parameters

Parameter	Description	Value
<i>interface-type interface-number</i>	Captures packets on a specified interface. <i>interface-type</i> specifies the interface type. <i>interface-number</i> specifies the interface number.	-
vxlan	Captures the VXLAN packets in which the original Ethernet frame information matches the specified conditions.	-
vni <i>vni-id</i>	Captures the VXLAN packets matching the specified VNI.	The value is an integer ranging from 1 to 16000000.
tag-format { none single }	Indicates whether to capture the VXLAN packets in which the original Ethernet frames contain tags. none: captures the VXLAN packets in which the original Ethernet frames do not contain tag. single: captures the VXLAN packets in which the original Ethernet frames contain a single tag. NOTE If the vxlan parameter is specified but the tag-format parameter is not specified, VXLAN packets without any inner VLAN tag are matched.	-

Parameter	Description	Value
acl <i>acl-number</i>	Captures the VXLAN packets in which the original Ethernet frames match the specified ACL rules. The ACL rule can specify only the source MAC address, Ethernet frame type, destination IP address, source IP address, destination port number, and source port number. If the ACL rules specify other options, VXLAN packets cannot be captured.	The value is an integer that ranges from 2000 to 4999.
vlan <i>vlan-id</i>	Captures packets from a specified VLAN.	The value of <i>vlan-id</i> is an integer that ranges from 1 to 4094.
inner-vlan <i>inner-vlan-id</i>	Captures packets with a specified inner VLAN ID.	The value of <i>vlan-id</i> is an integer that ranges from 1 to 4094.
acl	Configures an ACL.	-
<i>acl-number</i>	Captures packets matching a specified ACL.	The value is an integer that ranges from 2000 to 4999.
ipv6	Configures an ACL6.	-
<i>acl6-number</i>	Captures packets matching a specified ACL6.	The value is an integer that ranges from 2000 to 3999.
clear payload	Sets the data content in captured packets to 0. NOTE The data content of only the TCP and UDP packets can be set to 0.	-
inbound outbound both	Specifies the direction of packets to be captured. NOTE This parameter is supported only by the CE6881, CE5881, CE6881K, CE6863, CE6863E, CE6863K, CE6881E, and CE6820.	The default value is inbound . That is, only incoming packets on an interface are captured by default.

Parameter	Description	Value
destination	Indicates the destination to which captured packet information is sent.	-
terminal	Displays captured packet information on a terminal.	-
file <i>file-name</i>	Saves captured packet information to a file. The file name extension must be .cap .	The value is a string of 5 to 64 characters without spaces.
time-out <i>time</i>	Specifies the timeout period for capturing packets. The system stops capturing packets after the specified timeout period expires.	The value is an integer that ranges from 1 to 300, in seconds. By default, the timeout period is 60s.
packet-num <i>number</i>	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	The value is an integer that ranges from 1 to 1000. The default value is 100.
packet-len <i>length</i>	Specifies the length of captured packets that can be displayed on the terminal or stored on the storage medium.	The value is an integer that ranges from 20 to 64, in bytes. The default value is 20 bytes. For a VXLAN-encapsulated packet, this parameter specifies the length of the inner packet to be obtained. The length of a packet displayed on the terminal is the sum of the length of the outer packet header, length of the VXLAN header, and specified length of the inner packet.
<i>capture-index</i>	Deletes the packet capture instance with a specified index.	The value is an integer that ranges from 1 to 8. To view the index of a packet capture instance, run the display capture-packet config-state command.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the device fails to forward traffic correctly, for example, the traffic does not match the traffic model, configure the packet capture function to capture forwarded packets for analysis. This allows the device to process invalid packets in time, ensuring that network data can be transmitted correctly.

You can set packet capture parameters based on the number of packets on the interface. If a large number of packets are forwarded on an interface, set the *time* parameter to a small value and the *number* parameter to a large value. If a small number of packets are forwarded on an interface, set the *time* parameter to a large value and the *number* parameter to a small value.

Precautions

- After the packet capture function is enabled, performance of the device may be affected. Exercise caution when you configure this function.
- The device supports only one instance for capturing packets on an interface.
- The CE6881, CE5881, CE6881K, CE6820, CE6863K, CE6881E, CE6870EI, and CE6863, CE6863E switches cannot capture packets on stack member interfaces or logical stack interfaces.
- The device cannot capture packets on a fabric port or its member ports.
- You can set the timeout period specified by *time* and the number of packets to be captured specified by *number* for a packet capture instance. If the timeout period expires or the specified number of packets are captured, the system stops capturing packets.
- If you configure the device to match VXLAN packets without inner VLAN tags and also configure a Layer 2 ACL to match packets, tagged packets will be captured. If the device is configured to match VXLAN packets with one inner VLAN tag and also to match Layer 2 ACL fields, packets with multiple VLAN tags are captured.
- When the CE6856HI, CE6865EI, CE6865E, CE6857EI, CE6857E, CE6857F, CE8850EI, CE8850E-32CQ-EI, CE8861EI, and CE8868EI functions as a VXLAN tunnel termination device and is configured to capture packets, only inner packets of VXLAN packets can be matched regardless of whether the **vxlan** parameter is specified.
- Only a maximum of 16 ACLs can be matched using this command.

Example

Capture packets on 10GE1/0/1 matching ACL 2000 and save captured packet information in the **capture.cap** file.

```
<HUAWEI> capture-packet interface 10ge 1/0/1 acl 2000 destination file capture.cap
```

Capture packets on 10GE1/0/1 and 10GE1/0/2 and display packet information on the terminal.

```
<HUAWEI> capture-packet interface 10ge 1/0/1 10ge 1/0/2 destination terminal packet-len 64
```

Warning: Capture-packet will be shown on terminal.

```
<HUAWEI>
```

```
-----  
Packet: 1 Interface: 10GE1/0/1
```

```
-----  
04 f9 38 8d e6 82 30 6b 20 79 22 02 08 00 45 00  
00 54 10 01 00 00 fe 01 8e a2 0e 02 01 02 0e 01  
01 01 00 00 ed 1e 12 e0 00 01 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
-----
```

```
Packet: 2 Interface: 10GE1/0/2
```

```
-----  
04 f9 38 8d e6 82 00 19 74 59 33 02 08 00 45 00  
00 54 10 02 00 00 ff 01 8d a1 0e 01 01 01 0e 02  
01 02 08 00 e5 1d 12 e0 00 02 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
-----
```

```
-----capture report-----
```

```
Capture-Packet Index 1  
Type      : forwarding  
Interface : 10GE1/0/1  
Interface : 10GE1/0/2  
Direction : inbound  
Time-out  : 60 seconds  
Packet-num : 100  
Packet-len : 64  
BufferOnly : disabled  
-----
```

Table 4-2 Description of the **capture-packet interface** command output

Item	Description
Capture-Packet Index	Index of a packet capture instance.
Type	Type of packet capture. forwarding indicates that forwarded packets are captured.

Item	Description
Interface	Interface name.
Direction	Direction of forwarded packets that are captured. The device can capture the forwarded packets only in the inbound direction.
Time-out	Packet capture timeout.
Packet-num	Number of packets that can be captured.
Packet-len	Length of each captured packet.
BufferOnly	Whether to save the captured packets in buffer. - disabled: not save. - enabled: save.

4.2.3 capture-packet local-host

Function

The **capture-packet local-host** command configures an instance for capturing packets sent to the CPU.

The **undo capture-packet** command deletes the configured instance.

By default, no instance is configured for capturing packets sent to the CPU.

Format

```
capture-packet local-host [ interface { interface-type interface-number }
&<1-4> ] [ acl { { acl-number | name acl-name } | ipv6 { acl6-number | name
acl6-name } } | vlan vlan-id | inner-vlan inner-vlan-id ] * destination { terminal |
file file-name } * [ time-out time | packet-num number | packet-len length ] *
undo capture-packet [ capture-index ]
```

Parameters

Parameter	Description	Value
interface <i>interface-type</i> <i>interface-number</i>	Captures packets on a specified interface. <i>interface-type</i> specifies the interface type. <i>interface-number</i> specifies the interface number.	-
acl	Configures an ACL.	-
<i>acl-number</i>	Captures packets matching a specified ACL.	The value is an integer that ranges from 2000 to 4999. - The value of a basic ACL ranges from 2000 to 2999. - The value of an advanced ACL ranges from 3000 to 3999. - The value of a Layer 2 ACL ranges from 4000 to 4999.
name <i>acl-name</i>	Captures packets matching a specified ACL.	The value is a string of 1 to 32 case-sensitive characters except spaces. The value must start with a letter or digit, and cannot contain only digits.
ipv6	Configures an ACL6.	-
<i>acl6-number</i>	Captures packets matching a specified ACL6.	The value is an integer that ranges from 2000 to 3999. - The value of a basic ACL ranges from 2000 to 2999. - The value of an advanced ACL ranges from 3000 to 3999.

Parameter	Description	Value
name <i>acl6-name</i>	Captures packets matching a specified ACL6.	The value is a string of 1 to 32 case-sensitive characters except spaces. The value must start with a letter or digit, and cannot contain only digits.
vlan <i>vlan-id</i>	Captures packets from a specified VLAN ID.	The value is an integer ranging from 1 to 4094, except reserved VLAN IDs, which can be configured using the vlan reserved command.
inner-vlan <i>inner-vlan-id</i>	Captures packets with a specified outer VLAN ID.	The value is an integer ranging from 1 to 4094.
destination	Indicates the destination to which captured packet information is sent.	-
terminal	Displays captured packet information on a terminal.	-
file <i>file-name</i>	Saves captured packet information to a file. The file name extension must be .cap .	The value is a string of 5 to 64 characters without spaces.
time-out <i>time</i>	Specifies the timeout period for capturing packets. The system stops capturing packets after the specified timeout period expires.	The value is an integer that ranges from 1 to 3600, in seconds. By default, the timeout period is 15s.
packet-num <i>number</i>	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	The value is an integer that ranges from 1 to 6000. The default value is 10.
packet-len <i>length</i>	Specifies the length of captured packets that can be displayed on the terminal or stored on the storage medium.	The value is an integer that ranges from 20 to 64, in bytes. The default value is 20 bytes.

Parameter	Description	Value
<i>capture-index</i>	Deletes capture instance with a specified index.	The value is an integer that ranges from 1 to 8. To view the index of a packet capture instance, run the display capture-packet config-state command.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Devices on a network transmit various services, and network administrators often need to capture packets on devices to locate faults. The device does not support remote packet capture; therefore, administrators need to capture packets onsite by connecting a PC to the switch. If packets need to be captured on an optical interface, an optical-to-electrical converter must be installed on the interface, reducing maintenance efficiency. Running the **capture-packet local-host** command can remotely capture the packets to be sent to the CPU and analyze the captured packets, to greatly improve maintenance efficiency and reduce maintenance cost.

Precautions

Capturing forwarded packets and capturing packets sent to the CPU are independent of each other. The following are constraints on capturing packets to be sent to the CPU:

- The device supports a maximum of eight capture instances.
- The device can capture packets on the Eth-Trunk interface but cannot capture packets on a specified Eth-Trunk member interface.
- In a packet capturing instance, the packets on a maximum of four interfaces can be captured. If you delete any interface from the instance or an interface goes Down, the entire instance is deleted.
- If the ACL and VLAN parameters as well as the specified interfaces in an instance you want to configure are the same as those in an existing instance, the device considers that this instance has been enabled.

When configuring a capture instance, note the following two points:

- The device can capture packets of various protocols sent to the CPU.

- You can set the timeout period specified by *time*, number of captured packets specified by *number*, and number of capture instances. If the timeout period for capturing packets expires, the specified number of packets are captured, or the configured capture instance exceeds the limit, the system stops capturing packets.

Example

Capture packets sent to the CPU on 10GE1/0/1, set the timeout period to 360s and number of packets to be captured to 100.

```
<HUAWEI> capture-packet local-host interface 10ge 1/0/1 destination file capture1.cap time-out 360 packet-num 100
```

Info: Capture-packet data will be saved to flash:/logfile/capture1.cap.

4.2.4 display capture-packet config-state

Function

The **display capture-packet config-state** command displays packet capture information.

Format

display capture-packet config-state

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the device is configured to capture the packets to be sent to the CPU or forwarded, you can run this command to view packet capturing status, parameters, and name of the saved packet capturing file during packet capturing.

Example

Display packet capture information.

```
<HUAWEI> display capture-packet config-state
Capture-Packet Index 1
Type      : local-host
LinkType  : ethernet
Interface : 10GE1/0/1
ACL       : 2001
File Name : flash:/logfile/capture_host_all_GigabitEthernet_2012-05-03-14-44-01.cap
Time-out  : 3600 seconds
```

```
Packet-num : 1000
Packet-len : 64

Capture-Packet Index 2
Type      : forwarding
Interface : 10GE1/0/2
Direction : inbound
ACL       : 2001
File Name  : flash:/logfile/capture_fwd_GigabitEthernet3.0.0_2012-05-03-14-44-54.cap
Time-out   : 3600 seconds
Packet-num : 900
Packet-len : 62
```

Table 4-3 Description of the **display capture-packet config-state** command output

Item	Description
Capture-Packet Index	Index of a packet capture instance.
Type	Type of captured packets: • local-host: packets that are destined for the local device • forwarding: packets that are destined for a device other than the local one
LinkType	Link type.
Interface	Interface name.
Direction	Direction of forwarded packets.
ACL	ACL number.
File Name	Name of a file saving an instance.
Time-out	Timeout time before the system stops capturing packets.
Packet-num	Number of captured packets in a file.
Packet-len	Length of each packet in a file.

4.2.5 display capture-packet file

Function

The **display capture-packet file** command displays the content of a specified packet capture file.

Format

display capture-packet file *file-name* [**verbose**]

Parameters

Parameter	Description	Value
<i>file-name</i>	Specifies the name of the packet capture file.	The file-name must already exist, in the format of flash:/path name/file name.
verbose	Specifies to display the detail information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After the device is configured to remotely obtain packets, you can analyze the captured packets to check whether the data is correct and locate data problems. You do not need to download the packet capture files. Instead, you can run this command to view the content of the files.

The content of the packet header obtaining file is displayed in the command output as a hexadecimal character string. You can convert the content into a binary file and use packet analysis tool to view the packet information.

Example

Display information about the capture instance named **capture_host_GE3.1.8_2013-05-09-10-45-57.cap**.

```
<HUAWEI> display capture-packet file flash:/logfile/capture_host_GE3.1.8_2013-05-09-10-45-57.cap
a1 b2 c3 d4 00 02 00 04 00 00 00 00 00 00 00 00
00 00 ff ff 00 00 00 09 4d 10 36 db 00 0a d5 81
00 00 00 0c 00 00 00 0c ff 03 c0 21 09 9d 00 08
8a 8c bc c3 4d 10 36 db 00 0a d6 ae
```

View details about a packet capture instance and set the packet capture file name to **pingcapture.cap**.

```
<HUAWEI> display capture-packet file flash:/logfile/pingcapture.cap verbose
packet NO      : 1
packet length is : 64
capture-time   : 2015-09-01 03:45:32
  L2 Type: Ethernet
    Source mac  : f84a-bff0-cac2
    Dest mac    : 0019-7459-3302
    Ethernet type/length: 0x0800

  L3 Type: IPv4
    Protocol Num : 1
    Source Ip    : 10.1.1.2
    Dest Ip      : 10.1.1.1
```

```

L4 Type: ICMP
Source Port : -
Dest Port   : -

00 19 74 59 33 02 f8 4a bf f0 ca c2 08 00 45 00
00 54 08 01 00 00 ff 01 9d a3 0a 01 01 02 0a 01
01 01 08 00 f3 be 04 40 00 01 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

packet NO      : 2
packet length is : 64
capture-time   : 2015-09-01 03:45:32
L2 Type: Ethernet
Source mac    : f84a-bff0-cac2
Dest mac     : 0019-7459-3302
Ethernet type/length: 0x0800

L3 Type: IPv4
Protocol Num : 1
Source Ip   : 10.1.1.2
Dest Ip    : 10.1.1.1

L4 Type: ICMP
Source Port : -
Dest Port   : -

00 19 74 59 33 02 f8 4a bf f0 ca c2 08 00 45 00
00 54 08 02 00 00 ff 01 9d a2 0a 01 01 02 0a 01
01 01 08 00 f3 bd 04 40 00 02 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Table 4-4 Description of the **display capture-packet file flash:/logfile/pingcapture.cap verbose** command output

Item	Description
packet NO	Packet sequence number in the packet capture file.
packet length is	Length of each packet in the packet capture file.
capture-time	Time when the packet with the specified sequence number is captured.
L2 Type	Layer 2 protocol type.
Source mac	Source MAC address.
Dest mac	Destination MAC address.
Ethernet type/ length	Ethernet type.
L3 Type	Layer 3 protocol type.
Protocol Num	Protocol number.

Item	Description
Source Ip	Source IP address.
Dest Ip	Destination IP address.
L4 Type	Layer 4 protocol type.
Source Port	Source port number.
Dest Port	Destination port number.

5

Packet Capture 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
-----------------------------------	---	---	---------------------------------------	--	------------------------------------	--	---------------------------------

Ob tai nin g pac ket s	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 packet header obtaining based on ACLs, interfaces, VLANs, or packet loss causes.	The data is used for troubleshooting. 1. By default, 64 bytes are obtained. The number of bytes to be obtained can be configured in the range from 20 to 9500. 2. A whitelist of processes that can read the packet header obtaining file can be configured. 3. Only authorized administrators can view and export the data.	The data is saved as a file and can be deleted by the administrator.	The administrator deletes files using commands.	The administrator exports files through SFTP, FTP, or TFTP.	Data export through SFTP is recommended.
--	---	---	---	--	---	---	--