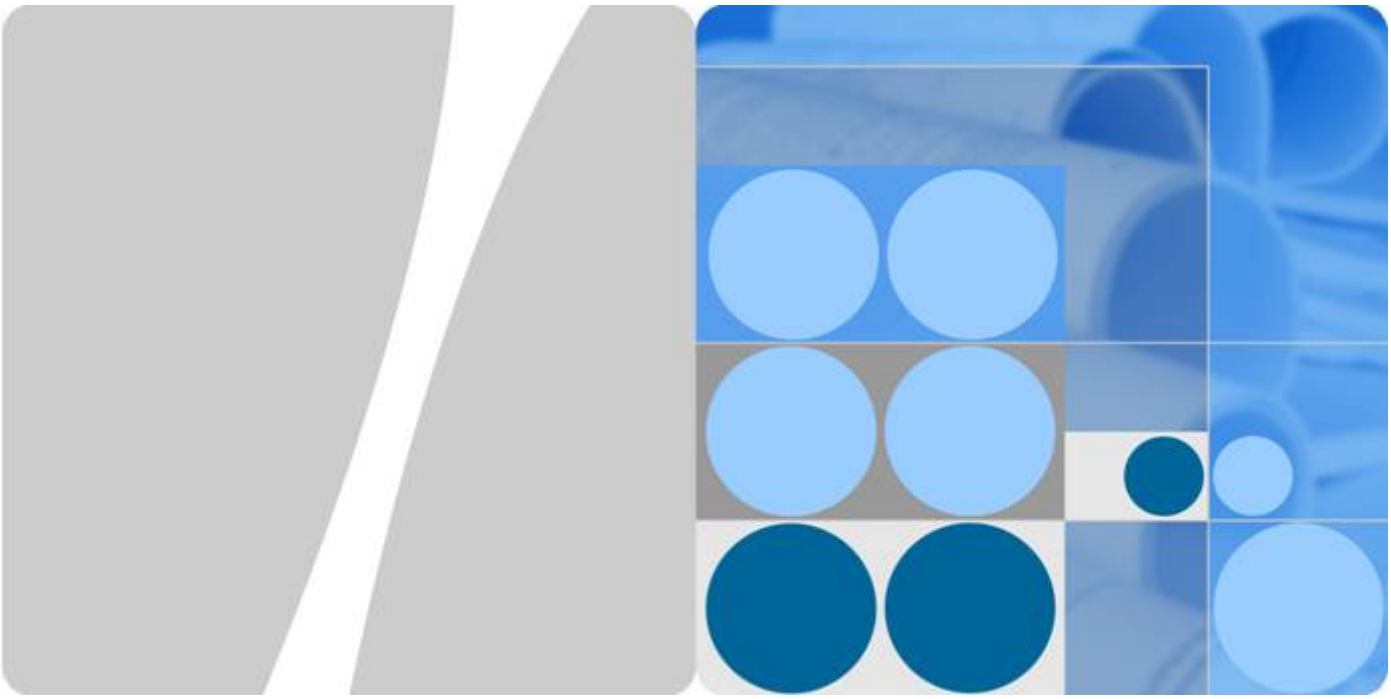


Huawei Wireless Access Points

# Troubleshooting

Issue 02

Date 2014-01-15

HUAWEI TECHNOLOGIES CO., LTD.

### Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

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

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

## Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

# About This Document

## Intended Audience

This document describes common troubleshooting procedure and methods.

This document is intended for:

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

## Symbol Conventions

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

| Symbol | Description |
| --- | --- |
|  DANGER | Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. |
|  WARNING | Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. |
|  CAUTION | Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. |
|  NOTICE | Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.<br>NOTICE is used to address practices not related to personal injury. |

| Symbol | Description |
| --- | --- |
| NOTE | Calls attention to important information, best practices and tips.<br>NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration. |

# Command Conventions

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

| Convention | Description |
| --- | --- |
| **Boldface** | The keywords of a command line are in **boldface**. |
| *Italic* | Command arguments are in *italics*. |
| [ ] | Items (keywords or arguments) in brackets [ ] are optional. |
| { x \| y \| ... } | Optional items are grouped in braces and separated by vertical bars. One item is selected. |
| [ x \| y \| ... ] | Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected. |
| { x \| y \| ... }* | Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected. |
| [ x \| y \| ... ]* | Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected. |
| &<1-n> | The parameter before the & sign can be repeated 1 to n times. |
| # | A line starting with the # sign is comments. |

# Interface Numbering Conventions

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

# Security Conventions

- Password setting

When configuring a password in plain text, the password is saved in the configuration file in plain text. The plain text has high security risks, so the cipher text is recommended. To ensure device security, change the password periodically.

When you configure a password in cipher text that starts and ends with %@%@.....%@%@ or @%@%.....@%@% (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.

- Encryption algorithm

  Currently, the device uses the following encryption algorithms: DES, 3DES, AES, RSA, SHA1, SHA-2, MD5 and SMS4. 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 128 bits or more.
  - For the asymmetrical encryption algorithm, use RSA with the key of 2048 bits or more.
  - For the hash algorithm, use SHA with the key of 256 bits or more.
  - For the HMAC algorithm, use HMAC-SHA2.

- Personal data

  Some personal data 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 personal data.

# Change History

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

## Changes in Issue 02 (2014-01-25)

This version has the following updates:

The following information is modified:

- **2.1 Recovering the Console Port Password**

## Changes in Issue 01 (2013-09-30)

Initial commercial release.

# Contents

**About This Document** ..... ii

**1 Instructions for Maintenance Engineers** ..... 1

1.1 Precautions ..... 2

1.2 Backing Up Data ..... 2

1.3 Troubleshooting Process ..... 2

1.4 Ask for Help ..... 2

1.4.1 Huawei Enterprise Website ..... 3

1.4.2 Hotline&Email ..... 3

**2 Forgetting Passwords** ..... 4

2.1 Recovering the Console Port Password ..... 5

2.2 Recovering the Telnet Login Password ..... 7

2.3 Recovering the Uboot Password ..... 7

**3 Information Collection** ..... 9

3.1 Overview ..... 10

3.2 Collecting Diagnostic Information ..... 10

3.3 Collecting Log Information ..... 11

**4 System Maintenance Methods** ..... 12

4.1 Using the RESET Button to Restore Factory Settings ..... 13

4.2 Using the Configuration File to Restore Device Configurations ..... 13

4.3 Restarting a Device ..... 13

4.4 Upgrading the Device ..... 14

4.5 Transferring Files Using FTP/TFTP ..... 14

**5 Startup Failures** ..... 18

5.1 Terminal Does Not Display Anything Or Displays Garbled Characters ..... 19

5.2 Device Restarts Unexpectedly ..... 19

**6 Hardware Failures** ..... 21

6.1 Power Supply Failures ..... 22

6.1.1 An device Fails to Be Powered On ..... 22

6.2 Interface Faults ..... 22

6.2.1 An Optical Interface Cannot Turn Up ..... 22

**7 Memory Failures.....24**

**8 Common Fault Diagnostic Commands.....26**

8.1 display Commands.....27
8.1.1 Overview.....27
8.1.2 Regular Expression in display Commands.....27
8.1.3 Common display Commands.....31
8.2 reset Commands.....32
8.2.1 Overview.....33
8.2.2 reset Commands Clearing Packet Statistics.....33
8.2.3 Using reset Commands.....33
8.3 Ping and Tracert.....34
8.4 Alarms.....37
8.5 Logs.....38
8.6 Packet Capturing.....38

**9 List of Indicators.....41**

# 1 Instructions for Maintenance Engineers

## About This Chapter

This section describes troubleshooting notes and provides the flowchart and procedure for key data backup and fault troubleshooting.

1.1 Precautions

1.2 Backing Up Data

1.3 Troubleshooting Process

1.4 Ask for Help

# 1.1 Precautions

If you are a maintenance engineer, read the following precautions before doing your work:

- Confirm whether the fault is an emergency fault. If it is an emergency fault, recover the faulty module by using the pre-defined troubleshooting methods immediately, and then restore services.
- Strictly conform to operation rules and industrial safety standards, ensuring human and device safety.
- Wear the ESD wrist strap when touching device components.
- Record original information about the problems occurring during troubleshooting.
- Record all the operations you have performed, especially the key operations such as restarting device and clearing database. Before performing the key operations, confirm the operation feasibility, back up data, and prepare the emergency and security measures. Only qualified personnel can perform key operations.

# 1.2 Backing Up Data

Some faults cause resource or money loss for customers. Therefore, maintenance engineers should focus on preventing faults and quickly restoring faults. Data backup helps you quickly locate and recover faults. After a network is set up and operates normally, you should back up important data as soon as possible.

Important data includes:

- Complete network topology, including device models, versions, and networking diagram
- Configuration files
- System software and patch files
- (Optional) Logs

# 1.3 Troubleshooting Process

Systematic troubleshooting is to find fault causes step by step, and finally recover the fault.

Generally, troubleshooting steps include observing fault symptom, collecting information, analyzing problem, and finding the root cause. The possible causes of all faults can be grouped into multiple cause sets, which make troubleshooting easier.

# 1.4 Ask for Help

At http://support.huawei.com/enterprise, you can:

- Search troubleshooting cases to find a way to fix your problem.
- Post your question on BBS and wait for answers from online technical experts.
- Contact Huawei technical support personnel that click **Contact Us** in the lower area of the page, and select the country to obtain contact information about Huawei local office.

## 1.4.1 Huawei Enterprise Website

At http://support.huawei.com/enterprise, you can:

- Search troubleshooting cases to find a way to fix your problem.
- Post your question on BBS and wait for answers from online technical experts.

## 1.4.2 Hotline&Email

If you cannot recover the fault, you can:

- Contact the agent.
- Visit http://support.huawei.com/enterprise.
- Send a mail to support@huawei.com.

**NOTICE**

Provide device and fault information to technical support personnel.

# 2 Forgetting Passwords

## About This Chapter

This section describes how to recover the console port, Telnet, and uBoot passwords. You are advised to keep passwords secure and change them regularly.

2.1 Recovering the Console Port Password

2.2 Recovering the Telnet Login Password

2.3 Recovering the Uboot Password

# 2.1 Recovering the Console Port Password

You can use either of the following methods to recover the console port password.

- Method 1: Log in to the device using Telnet and change the console port password.
- Method 2: Clear the console port password in Uboot view and change the console port password.

**NOTE**

Method 1 is preferred. Use method 2 if you forget the Telnet login password.

## Logging In to the Device Using Telnet and Changing the Console Port Password

If you have a Telnet account and user rights of level 3 or higher, log in to the device using Telnet, change the console port password, and save the configuration.

1. Log in to the device using Telnet. Ensure that your user right is level 3 or higher.

   Run the **display users** command to display all the users that have logged into the device. The item marked with + indicates your user account, which corresponds to VTY0.

   ```
   <Huawei> display users
     User-Intf    Delay    Type   Network Address     AuthenStatus
   AuthorcmdFlag
     0   CON 0   00:00:56                                pass
     Username : Unspecified

   + 5   VTY 0   00:00:00  TEL    172.168.254.206          pass
     Username : huawei123
   ```

   Run the **display user-interface** command to display user rights of all users. VTY0 corresponds to the user right level 15; therefore, you have the rights to change the console port password.

   ```
   <Huawei> display user-interface
     Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
     0    CON 0    9600       -     15    -           P     -
   + 5    VTY 0               -     15    15          A     -
     6    VTY 1               -     15    -           A
   -
     7    VTY 2               -     15    -           A
   -
     8    VTY 3               -     15    -           A
   -
     9    VTY 4               -     15    -           A
   -
   ```

2. Change the console port password. In this example, the authentication mode is set to password authentication and the password is changed to **huawei@123**.

   ```
   <Huawei> system-view
   [Huawei] user-interface console 0
   [Huawei-ui-console0] authentication-mode password
   [Huawei-ui-console0] set authentication password cipher
   Enter Password(<6-16>):
   Confirm Password:
   [Huawei-ui-console0] return
   ```

3. Save the configuration to prevent configuration loss after a restart.

   ```
   <Huawei> save
     The current configuration will be written to the device.
   ```

```
  Are you sure to continue? (y/n)[n]:y
  It will take several minutes to save configuration file, please
wait.........
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

## Clearing the Console Port Password in Uboot View and Change the Console Port Password

If the device is started in Uboot view, it does not check the password when you log in through the console port. However, all other configurations are loaded normally. After the device is started, change the console port password and save the configurations.

**NOTICE**

- You must restart the device to enter the Uboot view, which results in service interruption. Back up services and perform this operation in off-peak hours.
- After clearing the console port password, configure a new password immediately after you log in to the device. Otherwise, the login time expires or the device restarts, and you must clear the password and log in to the device again.
- Do not power off the device during the operation.

1. Connect a PC to the device with a serial cable and restart the device. When the message "Press f or F to stop Auto-Boot ……" is displayed, press **f** and enter the password (**admin@huawei.com** by default) to enter the Uboot view.
2. Run the **defaultuser** command to clear the console port password.

   ```
   ar7240> defaultuser
   Start setting whether to Change Password.....
   Current Bootup Change PW is N
   Do you Want To Change The Default password, Y or N : Y

   ar7240>
   ```

3. Run the **reset** command to restart the device.

   ```
   ar7240> reset
   Resetting...
   ```

4. Log in to the device through the console port. Authentication is not required when you log in. Change the console port password. In this example, the authentication mode is set to password authentication and the password is set to **huawei@123**.

   ```
   <Huawei> system-view
   [Huawei] user-interface console 0
   [Huawei-ui-console0] authentication-mode password
   [Huawei-ui-console0] set authentication password cipher
   Enter Password(<6-16>):
   Confirm Password:
   [Huawei-ui-console0] return
   ```

5. Save the configuration to prevent configuration loss after a restart.

   ```
   <Huawei> save
     The current configuration will be written to the device.
     Are you sure to continue? (y/n)[n]:y
     It will take several minutes to save configuration file, please
   wait.........
   ```

```
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

# 2.2 Recovering the Telnet Login Password

You can use Telnet to remotely maintain and manage a device. If you forget the Telnet login password, log in to the device using the console port and set a new password.

Currently, the device supports two authentication modes for Telnet login.

- AAA authentication: To log in to the device, you must have a user name and a password.
- Password authentication: To log in to the device, you must have a password.

In this example, the configurations for VTY0 to VTY4 are the same.

**NOTE**

After you log in to the device, run the **display current-configuration configuration user-interface** command to view the authentication mode of the VTY user. You can change the password without changing the authentication mode or configure a new authentication mode.

## AAA Authentication

```
<Huawei> system-view
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode aaa
[Huawei-ui-vty0-4] quit
[Huawei] aaa
[Huawei-aaa] local-user huawei password cipher huawei@123
[Huawei-aaa] local-user huawei service-type telnet
[Huawei-aaa] local-user huawei privilege level 15
```

After the configuration is complete, you can use the user name **huawei** and password **huawei@123** to log in to the device.

## Password Authentication

In this example, the Telnet login password is set to **huawei@123**.

```
<Huawei> system-view
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode password
[Huawei-ui-vty0-4] set authentication password cipher
Enter Password(<6-16>):    //The message displayed depends on device models.
Confirm Password:
[Huawei-ui-vty0-4] return
```

After the configuration is complete, you can use the password **huawei@123** to log in to the device.

# 2.3 Recovering the Uboot Password

Loss of the Uboot password may cause threats to your device security; therefore, you must keep your password safe. If you forget your Uboot password, you can restore the default password and then configure a new password.

Connect a PC to the device using the serial cable.

1. Restore the default Uboot password and restart the device.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] reset boot password
The password used to enter the BootROM menu by clicking ctrl+B will be
restored
to the factory setting, continue? [Y/N] y
Info: Succeeded in setting password of boot to default.
[Huawei-diagnose] return
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup
configuration.
Continue ? [y/n]:y
  It will take several minutes to save configuration file, please
wait..........
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

2. Change the Uboot password in Uboot view.

   During device restart, when the message "Press f or F to stop Auto-Boot ……" is displayed, press **f** and enter the password (**admin@huawei.com** by default) to enter the Uboot view.

```
ar7240> passwd
Start modify boot password.....
Confirm old password :

The password must be '0'~'9' , 'a'~'z' , 'A'~'Z' , or '@'!
Please enter new password :
Please confirm new password :

The password is changed successfully.
```

# 3 Information Collection

## About This Chapter

This section describes how to collect fault information.

This chapter describes the information collection method. You must collect detailed fault information as soon as possible no matter whether you locate faults by yourself or ask help from agent or Huawei technical support personnel.

NOTE

If you provide fault information to agents or Huawei technical support personnel, you can delete the security information, such as network configurations.

3.1 Overview
After a device fault occurs, collect fault information immediately. This helps you locate the fault accurately.

3.2 Collecting Diagnostic Information
The **display diagnostic-information** command displays debugging information outputs of multiple display commands. You can use this command to collect device diagnostic information.

3.3 Collecting Log Information
When a device is faulty, collect the log information on the device immediately. The log information helps you know what had happened during device operation and where the fault occurred.

# 3.1 Overview

After a device fault occurs, collect fault information immediately. This helps you locate the fault accurately.

If you cannot locate the fault by yourself, provide the following information to agents or Huawei technical support personnel:

- Fault occurrence time, network topology, operations triggering the fault, fault symptom, measures that you have taken and results, and affected services
- Name, version, current configurations, interfaces of the faulty device. For the method of obtaining these information, see **3.2 Collecting Diagnostic Information** and **8.1.3 Common display Commands**.
- Logs generated when the fault occurs. For the method of obtaining the log information, see **3.3 Collecting Log Information**.

# 3.2 Collecting Diagnostic Information

The **display diagnostic-information** command displays debugging information outputs of multiple display commands. You can use this command to collect device diagnostic information.

The **display diagnostic-information** [ *file-name* ] command displays the device diagnostic information on screen or outputs the information to a .txt file. The device diagnostic information includes startup configuration, current configurations, interface information, time, and system version. The following is an example:

```
<Huawei> display diagnostic-information dia-info.txt
  This operation will take several minutes, please wait.....................
.........................................................................
...
Info: The diagnostic information was saved to the device successfully.
```

By default, the diagnostic information is saved to the root directory of the default storage device (flash:/). You can run the **dir** command in the user view to check whether the file is correctly generated.

After a device becomes faulty, provide the device diagnostic information to agents or Huawei technical support personnel immediately for fast fault location. For the method of transmitting the diagnostic information from the device to your computer, see **4.5 Transferring Files Using FTP/TFTP**.

**NOTE**

- Executing this command requires a long time. You can press **Ctrl+C** to pause diagnosis information display on screen.
- When a large amount of diagnostic information is displayed, the CPU usage may be high in a short period.

# 3.3 Collecting Log Information

When a device is faulty, collect the log information on the device immediately. The log information helps you know what had happened during device operation and where the fault occurred.

Logs, including user logs and diagnostic logs, record user operations, system faults, and system security.

```
<Huawei> save logfile
Info: It may take several seconds,please wait...
Save log file successfully.
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] save diag-logfile
Save diagnostic log file successfully.
[Huawei-diagnose] info-center create logbook flash:/logfile/logbook.xml
Info: It may take several seconds,please wait...
Info: Succeeded in creating a data dictionary.
```

After the preceding configurations are complete, upload all files in flash:/logfile/ to your computer through FTP or TFTP. For details, see **4.5 Transferring Files Using FTP/TFTP**.

# 4 System Maintenance Methods

## About This Chapter

This section describes how to restore default settings, restart a device, and transfer files.

4.1 Using the RESET Button to Restore Factory Settings

4.2 Using the Configuration File to Restore Device Configurations

4.3 Restarting a Device

4.4 Upgrading the Device

4.5 Transferring Files Using FTP/TFTP

# 4.1 Using the RESET Button to Restore Factory Settings

When a fault, such as a device login failure, occurs due to incorrect configurations, hold down the RESET button to enable the device to restart using the factory settings.

Method to restore factory settings: After the device is started, hold down the RESET button for more than 5s. The device then uses the factory settings for a restart.

**NOTICE**

- If you hold down the RESET button for less than 5s, the device restarts without saving the current configurations and uses the original configuration file for the next startup. Therefore, save your configurations before you hold down the RESET button.
- After the factory settings are restored, the original configuration file still exists. You can run the **startup saved-configuration** command to change the startup configuration file; otherwise, the device uses the factory settings for the next startup.
- During your operations, do not power off the device.

# 4.2 Using the Configuration File to Restore Device Configurations

After a device is powered on, it initializes configurations by reading configuration information from the specified startup configuration file. If no configuration file is available in the storage directory, the device uses factory settings for initialization. You must restart the device to make the recovered device configurations take effect.

- Restore the configuration file through the FTP/TFTP server.

  For details, see **Using FTP/TFTP to Transfer Files** and download the default configuration file to the device.
- Run the **startup saved-configuration** command to specify the default configuration file for the next startup and restore default system configurations.

```
<Huawei> startup saved-configuration vrpcfg.cfg
<Huawei> reboot fast
```

**NOTE**

You can also run the **reset factory-configuration** command to restart the device and restore the factory settings.

# 4.3 Restarting a Device

You can rectify a network fault by restarting a device. This section describes how to restart a device.

You can restart a device using any of the methods in the following table.

**Table 4-1** Device restart methods

| Method | Description |
| --- | --- |
| Cold restart | To perform a cold restart, you need to power off and then power on the device again. Cold restart has limitations and is used by onsite maintenance personnel.<br>Current configurations will not be saved during a cold restart. Therefore, save configurations before performing a cold restart. |
| Hot restart (device restart using command lines): you can run the **reboot** command in the user view to restart the device. | Hot restart is performed using command lines, which is used by maintenance personnel who remotely manage the device.<br>During a hot restart, the system asks whether to save the configuration, which effectively prevents configuration loss. |
| Holding down the RESET button in less than 5s | If you hold down the RESET button for less than 5s, the device restarts using the current startup configuration file.<br>**NOTE**<br>If you hold down the RESET button for more than 5s, the device uses the factory settings for a restart.<br>Current configurations will not be saved during the restart. Therefore, save configurations before restarting the device. |

# 4.4 Upgrading the Device

The upgrade of a device is closely related to the released software versions. The corresponding upgrade guide is released with each new version and you can upgrade the device according to the guide. To obtain the upgrade guides, visit **http://support.huawei.com/enterprise**, choose **Software** > **Product Software** > **Enterprise Networking** > **WLAN** > **AP**, and download the upgrade guide based on the product name and version.

# 4.5 Transferring Files Using FTP/TFTP

During system maintenance such as software upgrade and configuration file backup, files must be transferred between a PC and the device. FTP/TFTP is used to transfer files.

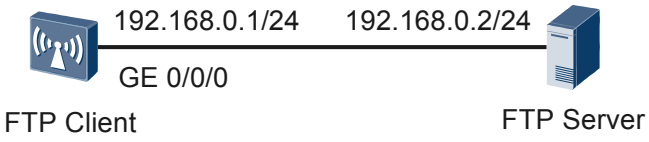
When transferring files using FTP/TFTP, the roles of PC and device vary in different methods:

- PC functioning as an FTP server: You must install the FTP server software on your PC.
- PC functioning as a TFTP server: You must install the TFTP server software on your PC. TFTP is easy to configure but this method has low security and transmission speed.

- Device functioning as an FTP server: You can perform configurations on the device without installing any software. When there are a large number of devices on a network, the first two methods are recommended.

## PC Functioning as an FTP Server

**Figure 4-1** Networking diagram




1. Run the FTP server software on the FTP server and configure the FTP service. For details, see relevant help documentation.
2. Connect the device and the FTP server. (The IP addresses are used as an example.)
   a. Connect the FTP server to GE0/0/0 of the device using a network cable.
   b. Configure an IP address 192.168.0.1/24 for GE0/0/0.
   c. Configure an IP address 192.168.0.2/24 for the FTP server. (Configure an IP address for the network adapter of the PC. The configuration details are omitted.)

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.0.1 24
[Huawei-GigabitEthernet0/0/0] ping 192.168.0.2
  PING 192.168.0.2: 56 data bytes, press CTRL_C to break
    Reply from 192.168.0.2: bytes=56 Sequence=1 ttl=128 time=4 ms
    Reply from 192.168.0.2: bytes=56 Sequence=2 ttl=128 time=3 ms
    Reply from 192.168.0.2: bytes=56 Sequence=3 ttl=128 time=18 ms
    Reply from 192.168.0.2: bytes=56 Sequence=4 ttl=128 time=3 ms
    Reply from 192.168.0.2: bytes=56 Sequence=5 ttl=128 time=3 ms

  --- 192.168.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/6/18 ms

[Huawei-GigabitEthernet0/0/0] return
```

**NOTE**

- In this example, the FTP server and the device are directly connected. If they are not directly connected, you must ensure that they have reachable routes to each other.
- After the configuration is complete, run the **ping** command to test the connectivity between the FTP server and device.

3. Log in to the FTP server using FTP.

```
<Huawei> ftp 192.168.0.2
Trying 192.168.0.2 ...
Press CTRL+K to abort
Connected to 192.168.0.2.
220 FTP Server ready.
User(192.168.0.2:(none)):ftpuser
331 Password required for ftpuser.
Enter password:
230 User logged in.
```

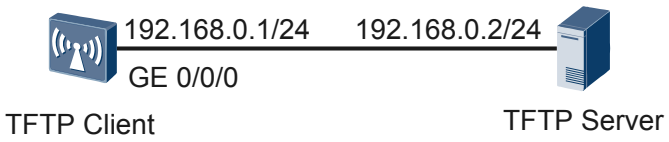
```
[Huawei-ftp]
```

4. Run the **put** command to upload files to the FTP server or run the **get** command to download files from the FTP server to the device.

```
[Huawei-ftp] put vrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.zip.
226 Transfer complete.
FTP: 8174 byte(s) sent in 0.099 second(s) 82.56Kbyte(s)/sec.

[Huawei-ftp] binary
200 Type set to I.

[Huawei-ftp] get devicesoft.cc
200 Port command okay.
150 Opening ASCII mode data connection for devicesoft.cc.
226 Transfer complete.
FTP: 141952 byte(s) received in 6.796 second(s) 20.88Kbyte(s)/sec.

[Huawei-ftp]
```

## PC Functioning as a TFTP Server

**Figure 4-2** Networking diagram

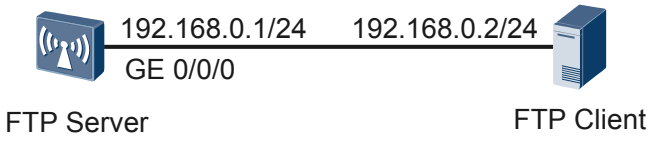



1. Run the TFTP server software on the TFTP server (PC) and configure the TFTP service. For details, see relevant help documentation.
2. Connect the TFTP server and the device and configure IP addresses for them. For details, see **PC Functioning as an FTP Server**.
3. Run the **tftp put** command to upload files to the TFTP server or run the **tftp get** command to download files from the TFTP server to the device.

```
<Huawei> tftp 192.168.0.2 get vrpcfg.zip vrpcfg1.zip
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...\
TFTP: Downloading the file successfully.
    8174 bytes received in 1 second.

<Huawei> tftp 192.168.0.2 put vrpcfg.zip vrpcfg2.zip
Info: Transfer file in binary mode.
Uploading the file to the remote TFTP server. Please wait...|
TFTP: Uploading the file successfully.
    8174 bytes send in 1 second.

<Huawei>
```

## Device Functioning as an FTP Server

**Figure 4-3** Networking diagram



1. Connect the PC and the device and configure IP addresses for them. For details, see **PC Functioning as an FTP Server**.
2. Enable FTP on the device, and create a user name, password, and FTP path.

   You must set the user level to level 3 or above to establish an FTP connection.

   ```
   <Huawei> system-view
   [Huawei] ftp server enable
   [Huawei] aaa
   [Huawei-aaa] local-user huawei password cipher huawei@123
   [Huawei-aaa] local-user huawei service-type ftp
   [Huawei-aaa] local-user huawei ftp-directory flash:
   [Huawei-aaa] local-user huawei privilege level 15
   [Huawei-aaa] quit
   [Huawei] quit
   ```

3. Log in to the device by running the **ftp** command on the PC. Run the **get** command to download files from the device to the PC or run the **put** command to upload files to the device.

   For example, on an FTP server with the Windows operating system, choose **Start** > **Run**, enter **cmd**, and click **OK**.

   ```
   C:\Documents and Settings\Administrator> ftp 192.168.0.1
   Connected to 192.168.0.1.
   220 FTP service ready.
   User (192.168.0.1:(none)): huawei
   331 Password required for huawei.
   Password:
   230 User logged in.
   ftp> get vrpcfg.zip
   200 Port command okay.
   150 Opening ASCII mode data connection for vrpcfg.zip.
   226 Transfer complete.
   ftp: receive 5203 bytes in 0.01 seconds 346.87Kbytes/sec.
   ftp> lcd
   Local directory now C:\Documents and Settings\Administrator.
   ftp> put vrpcfg.zip
   200 Port command okay.
   150 Opening ASCII mode data connection for vrpcfg.zip.
   226 Transfer complete.
   ftp: send 5203 bytes in 0.01 seconds 346.00Kbytes/sec.
   ```

   **NOTE**

   If you use the user name **Administrator** to log in to the PC, the output differs from the above.

   You can run the **lcd** command to view the path where backup configuration files are saved.

   The commands vary with the operating system. For details, see relevant help documentation of each operating system.

# 5 Startup Failures

## About This Chapter

This section describes how to troubleshoot device startup failures.

5.1 Terminal Does Not Display Anything Or Displays Garbled Characters

5.2 Device Restarts Unexpectedly

# 5.1 Terminal Does Not Display Anything Or Displays Garbled Characters

## Fault Description

After a terminal connecting to the device, it cannot display anything or displays garbled characters.

## Possible Cause

- The power module of the device is faulty or the device is not powered on.
- The serial interface connecting to the device is incorrectly configured.
- The cable between the terminal and device is faulty or not firmly connected to the serial interface.

## Troubleshooting Roadmap

- Check the power indicator on the device's front panel to ensure that the power module is working properly.
- Ensure that the serial interface is correctly configured.
- Install the cable firmly or replace the cable.

## Troubleshooting Procedure

1. Check indicators on the device. If the LED indicator is on, the power module is working properly; if not, the device is not powered on. In this case, see **Power Supply Fault** for details.
2. Check whether the correct combo interface is selected and whether the physical attributes of the PC are consistent with those of the serial interface. The default parameters are as follows:
   - Baud rate: 9600
   - Data bit: 8
   - Stop bit: 1
   - Parity check: None
   - Flow control: None
3. Ensure that the cable is firmly connected to the serial interface. You can replace it with a new cable to verify whether the cable is faulty.

# 5.2 Device Restarts Unexpectedly

## Fault Description

The device restarts unexpectedly or repeatedly.

## Possible Cause

- The hardware is faulty or the software has a bug.
- Other errors occur on the device.

## Troubleshooting Procedure

1. Check the causes of a device reset.

   Run the **display reset-reason** command to check the causes of a device reset.

   - If "Reset for power off" is displayed, the device restarts due to a power-off.
   - If "Reset for unknown reason" is displayed, the device restarts due to an unknown error.
   - If "Reset for update version success" is displayed, the device restarts due to a successful upgrade.
   - If "Reset for update version failed" is displayed, the device restarts due to an upgrade failure.
   - If "Reset for kernel panic" is displayed, the device restarts due to a kernel error.
   - If "reset for unknown reason" is displayed, the device restarts because the watchdog resets or SOC hardware restarts.
   - If "Reset for mfpi detect fwd abnormal" is displayed, the device restarts due to a forwarding kernel error.
   - If "Reset for memory use out" is displayed, the device restarts due to insufficient memory.
   - If "Reset for exception" is displayed, the device restarts due to a VOS error.

2. If the fault is not caused by the preceding reasons, a hardware fault occurs or the software has bugs. Contact the Huawei technical support personnel.

   Perform the following operations to collect related information and provide the information to the technical support personnel.

   **NOTICE**

   Do not power off the device before information is collected.

   a. Collect information according to **Information Collection**.

   b. Run the following commands to collect related information.

```
<Huawei> display reset-reason
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] display inspect black-box record 8 0 0 0
[Huawei-diagnose] display inspect black-box record 10 0 0 0
[Huawei-diagnose] display inspect black-box record 12 0 0 0
[Huawei-diagnose] display inspect black-box record 13 0 0 0
[Huawei-diagnose] set kernel-monitor irq
[Huawei-diagnose] display kernel-monitor irq level 1
[Huawei-diagnose] display kernel-monitor irq level 2
[Huawei-diagnose] display kernel-monitor irq level 3
[Huawei-diagnose] display lastwords all
```

# 6 Hardware Failures

## About This Chapter

This section describes common methods for troubleshooting typical hardware faults.

6.1 Power Supply Failures

6.2 Interface Faults

# 6.1 Power Supply Failures

## 6.1.1 An device Fails to Be Powered On

### Fault Description

The SYS indicators of an device is off.

### Possible Causes

- The power switch on the device is turned off.
- The power cable is not securely connected to the device.
- The power supply unit has failed.
  - If the device connects to an external power source, its power adapter may fail.
  - If the device has a built-in power supply, the device itself may be faulty.

### Troubleshooting Procedure

1. Check that the power switch is on.
2. Check that the power cable is securely connected to the device.
3. Check whether the power supply is normal.
   - If the device uses a power adapter, replace the power adapter with a normal one. If the device is powered on, the original power adapter is faulty. Contact Huawei technical support or Huawei agent through **1.4.2 Hotline&Email** and ask them to replace the power adapter.
4. If the device still cannot be powered on, the device itself is faulty. Contact Huawei technical support or Huawei agent through **1.4.2 Hotline&Email** and ask them to replace the device.

# 6.2 Interface Faults

## 6.2.1 An Optical Interface Cannot Turn Up

### Fault Description

After an optical interface is connected to a remote device through an optical fiber, its LINK indicator is off.

NOTE

GE0/0/0 on the AP6610DN-AGN is a combo interface.

### Possible Causes

- The optical fiber is faulty.
- The optical module on the optical interface cannot meet the requirements.

## Troubleshooting Procedure

1. Replace the optical fiber and optical module and check whether the optical interface can turn Up. Ensure that the optical module meets the following requirements.
2. Determine optical module attributes.
   - The optical module has passed Huawei certification.
   - The transmission speed of the optical module is the same as the interface speed.
   - The wavelength of the optical module is the same as that of the remote optical module.
   - The transmission distance of the optical module is suitable for the actual distance between the two devices.

     **NOTE**

     - The transmission distance of an optical module is 10 km, 15 km, 20 km, 40 km, or 80 km. The optical modules with a longer transmission distance have a higher transmit power. If an optical module with a long transmission distance is used for short-distance transmission, the optical interface cannot turn Up because the transmit power is too high. The high transmit power may even burn the receiver of the remote optical module. To reduce the transmit power in this situation, use an optical attenuator between the optical module and optical fiber.
     - Optical modules with different speeds are available, for example, 155 Mbit/s, 622 Mbit/s, and 1.25 Gbit/s. It is recommended that you use an optical module with the same speed as the optical interface to ensure efficient optical transmission.
3. If the interface remains Down, contact Huawei technical support through **1.4.2 Hotline&Email**.

# 7 Memory Failures

Memory usage refers to the ratio of occupied memory space to the total memory space. Memory usage is an important indicator to evaluate device performance.

## Fault Description

After running the **display memory-usage** command, you find that the memory usage is high. By default,

- If the device memory is smaller than 128 MB, a level 1 alarm is generated when the memory usage exceeds 83% and a level 2 alarm is generated when the memory usage exceeds 88%.
- If the device memory is larger than or equal to 128 MB, a level 1 alarm is generated when the memory usage exceeds 90% and a level 2 alarm is generated when the memory usage exceeds 95%.

**NOTE**

Level 1 and level 2 alarms trigger the same trap message **ENTITYTRAP_1.3.6.1.4.1.2011.5.25.219.2.15.1 hwMemUtilizationRising**. Their differences lie in that after a level 2 alarm is generated, the device also restarts. If the memory usage keeps increasing, the system is automatically reset and services are interrupted.

## Possible Causes

If the memory usage keeps increasing, a memory leak may occur.

**NOTE**

Memory leak indicates that applications occupy memory space for a long time. If the applications do not release memory, the memory usage increases until the system memory is exhausted.

## Procedure

Collect the memory usage, memory block size of partition 1, memory usage of the specified memory block, each PID, and specified PID, and provide the collected information to Huawei.

1. Display the memory usage.

   ```
   <Huawei> display memory-usage
   ```

2. Configure memory block size of partition 1 to be displayed every day in three days.

   ```
   <Huawei> system-view
   [Huawei] diagnose
   [Huawei-diagnose] display inspect mem-debug-info 13 1 0 0
   ```

**NOTE**

The meanings of *record-number* in the **display inspect mem-debug-info** *record-number mid-hex hex-string hex-value* command are displayed as follows:

```
[Huawei-diagnose] display inspect mem-debug-info ?

INTEGER<0-26>
                 0 help; 1 utilization; 2 contents; 3 memory by
address;
                 4 memory by time; 5 memory by PID; 6 memory by
SID;
                 7 memory by SID&PID; 8 block size; 9 memory by used
size;
                 11 shortage; 12 tracing; 13 show
partition;
                 14 show information; 15 show Size; 16 pid by
size;
                 17 show PID; 18 show all; 19 show
PID&SID;
                 20 alloc free times; 21 block PID by SID; 22 memory
piece;
                 23 alloc failed; 24 PID peak value; 25 partition; 26
partition
               used by PIDSID
```

# 8 Common Fault Diagnostic Commands

## About This Chapter

The common fault diagnostic commands include **display**, **reset**, **ping**, and **tracert** commands. Additionally, alarms, logs, and packet capturing are effective methods to locate faults.

8.1 display Commands
Using **display** commands and understanding command functions are essential skills of maintenance engineers.

8.2 reset Commands
**reset** commands are used to clear statistics. These commands help you quickly locate faults.

8.3 Ping and Tracert
This section describes how to use **Ping** and **Tracert** commands to check network connectivity and locate network faults. The **Ping** command checks network connectivity and host reachability and the **Tracert** command tracks the gateways that packets pass through from the source host to the destination host.

8.4 Alarms

8.5 Logs

8.6 Packet Capturing
Packet capturing is used to obtain packet headers. The device copies packet headers from the mirrored port to an observing port or server. The captured packet headers help you locate faults.

# 8.1 display Commands

Using **display** commands and understanding command functions are essential skills of maintenance engineers.

## 8.1.1 Overview

The **display** commands provide the following information:

- Current device status
- Neighbor device information
- Overall network information
- Network fault location

The **display** commands can be executed in any view.

The following is an example of **display** commands:

```
<Huawei> display ?
  aaa                       AAA
  access-user               User access
  accounting-scheme         Accounting scheme
  acl                       <Group> acl command group
  actual                    Current actual
  alarm                     Alarm
  antenna                   Current antenna that outputting radio
  anti-attack               Specify anti-attack configurations
  ap                        <Group> ap command group
 ---- More ----
```

**NOTE**

- After you enter **display ?**, the system displays all the keywords behind **display**. More keywords can be added behind these displayed keywords.
- Different device models or versions support different features. The keywords actually displayed may be different from the preceding example.

This section involves only commonly used **display** commands. For more **display** commands, see the Huawei Wireless Access Points Command Reference.

## 8.1.2 Regular Expression in display Commands

### Regular Expressions

A regular expression is a mode matching tool. It consists of common characters (such as letters from a to z) and special characters (called meta-characters). The regular expression is a template according to which you can search for the required string.

A regular expression provides the following functions:

- Searches for and obtains a sub-string that matches a rule in the string.
- Substitutes a string based on a certain matching rule.

The regular expression consists of common characters and special characters.

- Common characters

  Common characters are used to match themselves in a string, including all upper-case and lower-case letters, digits, punctuations, and special symbols. For example, a matches the letter "a" in "abc", 202 matches the digit "202" in "202.113.25.155", and @ matches the symbol "@" in "xxx@xxx.com".

- Special characters

  Special characters are used together with common characters to match the complex or special string combination. **Table 8-1** describes special characters and their syntax.

**Table 8-1** Description of special characters

| Special Characters | Function | Example |
| --- | --- | --- |
| \ | Defines an escape character, which is used to mark the next character (common or special) as the common character. | * matches "*". |
| ^ | Matches the starting position of the string. | ^10 matches "10.10.10.1" instead of "20.10.10.1". |
| $ | Matches the ending position of the string. | 1$ matches "10.10.10.1" instead of "10.10.10.2". |
| * | Matches the preceding element zero or more times. | 10* matches "1", "10", "100", "1000", and so on.<br>(10)* matches "null", "10", "1010", "101010", and so on. |
| + | Matches the preceding element one or more times. | 10+ matches "10", "100", "1000", and so on.<br>(10)+ matches "10", "1010", "101010", and so on. |
| ? | Matches the preceding element zero or one time.<br>**NOTE**<br>Huawei datacom devices do not support regular expressions with ?. When regular expressions with ? are entered on Huawei datacom devices, helpful information is provided. | 10? matches "1" or "10".<br>(10)? matches "null" or "10". |
| . | Matches any single character. | 0.0 matches "0x0", "020", and so on.<br>.oo. matches "book", "look", "tool", and so on. |
| () | Defines a subexpression, which can be null. Both the expression and the subexpression should be matched. | 100(200)+ matches "100200", "100200200", and so on. |

| Special Characters | Function | Example |
| --- | --- | --- |
| x\|y | Matches x or y. | 100\|200 matches "100" or "200".<br>1(2\|3)4 matches "124" or "134", instead of "1234", "14", "1224", and "1334". |
| [xyz] | Matches any single character in the regular expression. | [123] matches the character 2 in "255". |
| [^xyz] | Matches any character that is not in the regular expression. | [^123] matches any character except for "1", "2", and "3". |
| [a-z] | Matches any character within the specified range. | [0-9] matches any character ranging from 0 to 9. |
| [^a-z] | Matches any character beyond the specified range. | [^0-9] matches all non-numeric characters. |
| _ | Matches a comma ",", left brace "{", right brace "}", left parenthesis "(", and right parenthesis ")".<br>Matches the starting position of the input string.<br>Matches the ending position of the input string.<br>Matches a space. | _2008_ matches "2008", "space 2008 space", "space 2008", "2008 space", ",2008,", "{2008}", "(2008)", "{2008)", and "(2008}". |

**NOTE**

Unless otherwise specified, all the characters in the preceding table must be printable characters.

- Degeneration of special characters

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

  - The special characters following "\" match special characters themselves.
  - The special characters "*", "+", and "?" are placed at the starting position of the regular expression. For example, +45 matches "+45" and abc(*def) matches "abc*def".
  - The special character "^" is placed at any position except for the start of the regular expression. For example, abc^ matches "abc^".
  - The special character "$" is placed at any position except for the end of the regular expression. For example, 12$2 matches "12$2".
  - A right parenthesis ")" or right bracket "]" is not paired with a corresponding left parenthesis "(" or bracket "[". For example, abc) matches "abc)" and 0-9] matches "0-9]".

NOTE

Unless otherwise specified, degeneration rules also apply when the preceding regular expressions are subexpressions within parentheses.

- Combination of common and special characters

  In actual usage, regular expressions combine multiple common and special characters to match certain strings.

## Specifying a Filtering Mode in a Command

NOTE

- The device uses a regular expression to implement the pipe character filtering function. A display command supports the pipe character only when there is excessive output information.
- When filtering conditions are set to query output information, the first line of the command output starts with the entire regular expression but not the string to be filtered.

Some commands can carry the keyword **| count** to display the number of matching entries. The keyword **| count** can be used together with other keyword.

Three filtering modes are provided for commands that support regular expressions.

- **| begin** *regular-expression*: displays all the lines beginning with the line that matches the regular expression.

  Filter the character strings to be entered until the specified case-sensitive character string is displayed. All the character strings following this specified character string are displayed on the screen.

- **| exclude** *regular-expression*: displays all the lines that do not match the regular expression.

  If the character strings to be entered do not contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.

- **| include** *regular-expression*: displays all the lines that match the regular expression.

  If the character strings to be entered contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.

NOTE

The value of *regular-expression* is a string of 1 to 255 characters. *regular-expression* cannot contain underlines (_).

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

Example 1: Run the **display interface brief** command to display all the lines that do not match the regular expression GigabitEthernet|NULL|Wlan-Radio. GigabitEthernet|NULL|Wlan-Radio matches GigabitEthernet, NULL or Wlan-Radio.

```
<Huawei> display interface brief | exclude GigabitEthernet|NULL|Wlan-Radio
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(e): ETHOAM down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
Vlanif10                    down  down        --     --          0          0
Vlanif2001                  up    up          --     --          0          0
```

Example 2: Run the **display current-configuration** command to display all the lines that match the regular expression vlan.

```
<Huawei> display current-configuration | include vlan
vlan batch 10 2001
 port trunk allow-pass vlan 2001
```

**NOTE**

The preceding information is used for reference only.

## 8.1.3 Common display Commands

The device provides various **display** commands to display hardware, interface, and software information. The information helps you locate various faults.

The following table lists the commands used to collect fault information.

| Item | Command | Description |
| --- | --- | --- |
| Basic information | **display diagnostic-information** | This command collects basic system information. It displays outputs of multiple **display** commands, including **display device** and **display current-configuration**. This command is necessary for any network problems. Executing this command takes a long time. You can press **Ctrl+C** to pause diagnosis information display on screen. |
| Device information | **display device** | This command displays card status. If the status of a card is displayed as Abnormal, the card is faulty. |
| Interface information | **display interface** | This command displays interface information to help you analyze cause of interface interconnection failures and check statistics on lost packets. |
| Versions | **display version** | Version information is important for device fault location. This command displays versions of the system software, uBoot, MPU, as well as sizes of storage devices. |
| Patch information | **display patch-information** | This command displays current patch information, including the patch package version and patch package name. |
| Electronic label information | **display elabel** | Electronic labels identify information about hardware components of a device. This command displays electronic labels of cards on a device. |

| Item | Command | Description |
| --- | --- | --- |
| Device status | **display health** | This command displays the temperature, power supply information, power, CPU usage, memory usage, and storage medium usage of a device. |
| Current configurations | **display current-configuration** | This command displays all configuration information on a device. You can specify a regular expression to obtain the required configuration information. |
| Saved configurations | **display saved-configuration** | If a device has started but is not working properly, run the **display saved-configuration** command to check the startup files specified by the **startup saved-configuration** command.<br>Run the **display saved-configuration last** command to check the configuration saved last time.<br>Run the **display saved-configuration time** command to check the last time when the configuration is saved. |
| Time | **display clock** | This command displays the current system date and time. |
| User logs | **display logfile buffer** | Executing this command in the diagnostic view can display user logs in the log buffer. |
| Diagnostic log | **display diag-logfile buffer** | Executing this command in the diagnostic view can display user logs in the log buffer. |
| Alarms | **display trapbuffer** | This command displays information recorded in the trap buffer. |
| Memory usage | **display memory-usage** | This command displays memory usage of the device. |
| CPU usage | **display cpu-usage** | This command displays CPU usage of the device. |

# 8.2 reset Commands

**reset** commands are used to clear statistics. These commands help you quickly locate faults.

## 8.2.1 Overview

**reset** commands include:

- Commands used for resetting
- Commands used for clearing statistics

This section involves the **reset** commands clearing statistics.

## 8.2.2 reset Commands Clearing Packet Statistics

**reset counters interface** and **reset ip statistics** are often used to clear packet statistics displayed in the **display interface** and **display ip interface** command output.

- The **display interface** command provides counters to collect statistics on sent and received Layer 2 packets. The **reset counters interface** command resets these counters.
- The **display ip interface** command provides counters to collect statistics on sent and received Layer 3 packets. The **reset ip statistics** command resets these counters.

## 8.2.3 Using reset Commands

### Context

When you use the **ping** command to test link connectivity, you also need to run the **display interface** or **display ip interface** command to check whether packets are correctly sent and received on interfaces and whether a CRC error occurs. Then you can locate the interface where the fault occurs.

The **display interface** or **display ip interface** command output shows packet statistics generated after the device starts or the counter is reset; therefore, the packet statistics may contain unnecessary information that interferes with fault location.

To collect packet statistics accurately, perform the following operations:

### Procedure

**Step 1** Run the **reset counters interface** or **reset ip statistics** command to clear existing packet statistics.

**Step 2** Run the **ping** command to enable router interfaces to send and receive packets.

**Step 3** Run the **display interface** or **display ip interface** command to view the statistics.

**----End**

### Example

For example, after you run the **display interface gigabitEthernet 0/0/0** command, the following statistics are displayed:

```
Input:  736 packets, 344842 bytes
  Unicast:                 0,  Multicast:               714
  Broadcast:              22,  Jumbo:                   0
```

```
  Discard:                  0,  Total Error:                0

  CRC:                      0,  Giants:                     0
  Jabbers:                  0,  Throttles:                  0
  Runts:                    0,  Symbols:                    0
  Ignoreds:                 0,  Frames:                     0

Output:  2911 packets, 514228 bytes
  Unicast:                  0,  Multicast:               2910
  Broadcast:                1,  Jumbo:                      0
  Discard:                  0,  Total Error:                0

  Collisions:               0,  ExcessiveCollisions:        0
  Late Collisions:          0,  Deferreds:                  0
```

If the value of **Total Error** is not 0, there is an error in packet sending and receiving.

To check when the error occurs, run the **reset counters interface gigabitEthernet 0/0/0** command to clear existing statistics, use the **ping** command to send ping packets, and run the **display interface gigabitEthernet 0/0/0** command to view new statistics. If the **Total Error** value is still not 0, the error may need to be rectified.

# 8.3 Ping and Tracert

This section describes how to use **Ping** and **Tracert** commands to check network connectivity and locate network faults. The **Ping** command checks network connectivity and host reachability and the **Tracert** command tracks the gateways that packets pass through from the source host to the destination host.

## Introduction to the Ping Command

Based on the Internet Control Message Protocol (ICMP), the **Ping** command is used to check network connectivity and host reachability. The source sends an ICMP Echo Request message to the destination, and determines reachability. The source determines the quality of the link from which the destination is reachable based on the number of sent ICMP Echo Request messages and received ICMP Echo Response messages, and the round-trip time (RTT) of ping packets.

## Ping Command Format

**NOTE**

*Huawei Wireless Access Points Command Reference* provides detailed description of command parameters and usage. Here lists only some commonly used parameters and their descriptions.

**ping** [ **ip** ] [ **-a** *source-ip-address* | **-c** *count* | **-f** | **-s** *packetsize* | **-t** *timeout* ] * *host*

- -a: specifies the source IP address for sending Echo Request messages. If no source IP address is specified, the IP address of the outbound interface is used as the source IP address.
- -c: specifies the count for sending Echo Request messages. The default value is 5. You can increase the number of outgoing packets to detect the network quality based on the packet loss ratio.
- -f: indicates that packets are not fragmented when they are sent. The device discards the packets if the packet size exceeds the MTU.
- -s: specifies the length of an Echo Request message without the IP header and ICMP header.

- -t: specifies the timeout interval of Echo Response messages. You can set a larger timeout interval if the network is unstable. The default value is 2s. If the device receives no Echo Request message, it determines that the destination is unreachable.
- host: indicates an IP address or a domain name. If it is a domain name, the device performs DNS resolution and displays the resolved IP address.

**NOTE**

You can use the parameters -s and -f simultaneously to test the path MTU (PMTU). For example, if the ping operation succeeds when the parameter -s is set to 1472 but fails when the parameter is set to 1473, the PMTU is 1500, which is the total sum of 1472, 20 (IP header), and 8 (ICMP header).

The ping function varies with the operating system of a PC. The Windows operating system is used as an example.

**ping** [ **-n** *number* ] [ **-t** ] [ **-l** *number* ] [ **-f** ] [ **-a** ] *ip-address*

- -n: specifies the number of ping packets. The default value is 5.
- -t: indicates that the source sends Echo Request messages to the destination continuously until manual operations are involved. You can press **Ctrl**+**Break** to temporarily stop the ping command and view the statistics, and press **Ctrl**+**C** to end the ping operation.
- -l: specifies the number of bytes of data in ping packets. The value ranges from 0 to 65500.
- -f: indicates that packets are not fragmented when they are sent. The device discards the packets if the packet size exceeds the MTU.
- -a: indicates that the device resolves an IP address into a host name.

## Description of the Ping Command Output

```
<Huawei> ping 100.135.18.118
  PING 100.135.18.118: 56  data bytes, press CTRL_C to break
    Reply from 100.135.18.118: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 100.135.18.118: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 100.135.18.118: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 100.135.18.118: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 100.135.18.118: bytes=56 Sequence=5 ttl=255 time=2 ms

  --- 100.135.18.118 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

In this example:

- The device sends five ping packets and receives response for all the five packets.
- The ping packets use the default size, 56 bytes.
- The TTL value is 255, indicating that the source is directly connected to the destination.
- The time is 1 ms, indicating that the device receives an Echo Response message 1 ms after it sends an Echo Request message. This parameter can be used as a reference to determine whether the network is congested.

The device sends five ping packets by default. You can set a larger value of -c to accurately detect the network status. The device determines the network status based on the number of ping packets returned.

| Fault Description | Possible Cause |
| --- | --- |
| All packets can reach the destination but require a long time. | The intermediate network is unstable.<br>QoS is deployed on the gateway, which lowers the forwarding speed. |
| No packet can reach the destination. | Services on the network are interrupted due to device or cable faults.<br>The firewall on the intermediate network discards ICMP packets.<br>A loop occurs on the network and packets are discarded when the TTL value is reduced to 1.<br>Packets are delayed due to network congestion. |
| Some packets cannot reach the destination. | Some ping packets are discarded on the unstable network.<br>Load balancing is configured on the intermediate network and some ping packets are discarded on one path.<br>Packet flooding attacks. |

## Introduction to the Tracert Command

The **Ping** command checks whether the destination host is reachable and the **Tracert** command tracks the gateways that packets pass through from the source host to the destination host. This helps check network connectivity and locate network faults. The tracert process is as follows:

1. The source host sends a UDP packet with TTL 1.
2. The first hop sends back an error ICMP packet, indicating that the packet cannot be sent due to TTL timeout.
3. The source host then sends a packet with TTL 2.
4. The second hop drops the packet and sends an ICMP TTL-expired packet.

This process proceeds until the packet reaches the destination host. The source host obtains the path to the destination host based on the source IP addresses of TTL-expired packets.

## Tracert Command Format

**NOTE**

*Huawei Wireless Access Points Command Reference* provides detailed description of command parameters and usage. Here lists only some commonly used parameters and their descriptions.

**tracert** [ **-a** *source-ip-address* | **-f** *first-ttl* | **-m** *max-ttl* | **-q** *nqueries* | **-w** *timeout* ] * *host*

- -a: specifies the source address. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address of outgoing packets.
- -f: specifies the initial TTL. If the number of hops is smaller than the initial TTL, the source host receives no TTL-expired packet. If a maximum TTL is set, the initial TTL must be smaller than the maximum TTL.
- -m: specifies the maximum TTL. The maximum TTL is usually set to the number of hops through which a Tracert packet passes. If an initial TTL is set, the maximum TTL must be larger than the initial TTL.

- -q: specifies the number of UDP packets sent each time. You can increase this value to ensure that UDP packets can reach the destination host.
- -w: sets the timeout interval of Response messages. If a gateway sends a message indicating TTL timeout, " * " is displayed. You are advised to increase the timeout interval when the network is unstable and the transmission speed is low.
- host: indicates an IP address or a domain name. If it is a domain name, the device performs DNS resolution and displays the resolved IP address.

The tracert function varies with the operating system of a PC. The Windows operating system is used as an example for illustration.

**tracert** [ **-d** ] [ **-h** *maximum_hops* ] [ **-j** *host-list* ] [ **-w** *timeout* ] *ip-address*

- -d: indicates that the host name is not resolved.
- -h: specifies the maximum TTL.
- -j: specifies the loose source address routing list.
- -w: sets the timeout interval of UDP packets, in milliseconds.

## Description of the Tracert Command Output

```
<Huawei> tracert 100.135.18.118
 traceroute to  100.135.18.118(100.135.18.118), max hops: 30 ,packet length:
40,press CTRL_C to break
 1 192.168.200.100 10 ms  2 ms  2 ms
 2  *  *  *
 3 100.135.18.118 10 ms  1 ms  2 ms
```

Information displayed in a line includes the number, IP address where the packet reaches, and three response time. * * * is displayed in the second line, indicating that the ping and tracert operations are not supported on this node.

The **Ping** command can only determine whether the destination is reachable, whereas the **Tracert** command can detect potential loops on a network. If you track an address and the same address is displayed multiple times, a route loop occurs.

# 8.4 Alarms

When a device becomes faulty or works abnormally, the device system generates an alarm according to the types of the fault and faulty module. The system stores the alarm to the alarm buffer and generates logs. If a network management system (NMS) is configured, the device system also sends a trap to the NMS through the Simple Network Management Protocol (SNMP). In addition, the system is capable of detecting changes in operation environment. When a requirement for operation conditions cannot be met, the system generates an alarm.

To view alarm information, enable alarm debugging to display alarm information on the terminal. Alarm information is also stored in the alarm buffer, so you can use commands to view all alarms in the alarm buffer.

Alarms are classified into:

- Fault alarms: generated when hardware faults or exceptions of key functions occur.
- Recovery alarms: generated when faulty devices or abnormal functions recover.
- Event alarms: generated when the user needs to be prompted.

Alarms can be viewed in two ways:

- Display alarms on the graphic user interface (GUI) of the NMS.
- Run the **display trapbuffer** [ **size** *value* ] command to view alarms in the alarm buffer. The displayed alarms vary according to the *value* field. If the actual number of alarms is smaller than the specified number of alarms to be displayed, the actual number of alarms are displayed.

# 8.5 Logs

During device operation, the log module records operations and events on the device. The recorded operations and events are log messages.

The generated logs can be viewed through the Console port or Telnet, or stored to the log server through the syslog protocol.

The syslog protocol is transmitted through UDP port 514. Any UDP datagram on port 514 is recorded in the log.

Logs can be viewed in two ways:

- Display logs on the GUI of the NMS.
- Run the **display logbuffer** [ **size** *value* | **module** *module-name* | **level** *severity* ] command to view logs in the log buffer.

# 8.6 Packet Capturing

Packet capturing is used to obtain packet headers. The device copies packet headers from the mirrored port to an observing port or server. The captured packet headers help you locate faults.

The device cannot analyze packet headers except that a computer with the packet capturing software installed or a tester is connected to the observing port or server. The commonly used packet capturing software is WireShark, and most testers have the packet capturing function.

**NOTE**

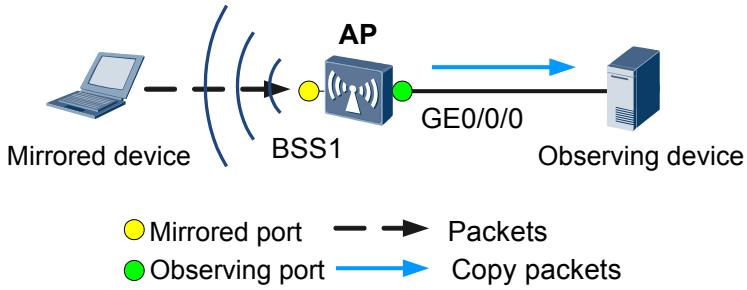
The packets captured for troubleshooting may contain secure communication information. Therefore, Huawei does not capture packets for you. You must capture packets legally and with permission. Ensure that your customers' privacy is protected when collecting communication information.

Two packet capturing methods are available: mirroring packet headers to an observing port and to a remote observing server. The two methods can capture incoming, outgoing, and bidirectional packets.

## Mirroring Packet Headers to an Observing Port

Packet headers are copied from the mirrored port to an observing port. As shown in **Figure 8-1**, the incoming packets on BSS1 are captured to GE0/0/0, and the observing device directly connected to GE0/0/0 analyzes the packet headers.

**Figure 8-1** Mirroring packet headers to an observing port




The procedure is as follows:

1. Set GE0/0/0 on the AP as an observing port.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] observe-port interface gigabitethernet 0/0/0
```

2. Set BSS1 on the AP as a mirrored port and set the mirroring direction to inbound.

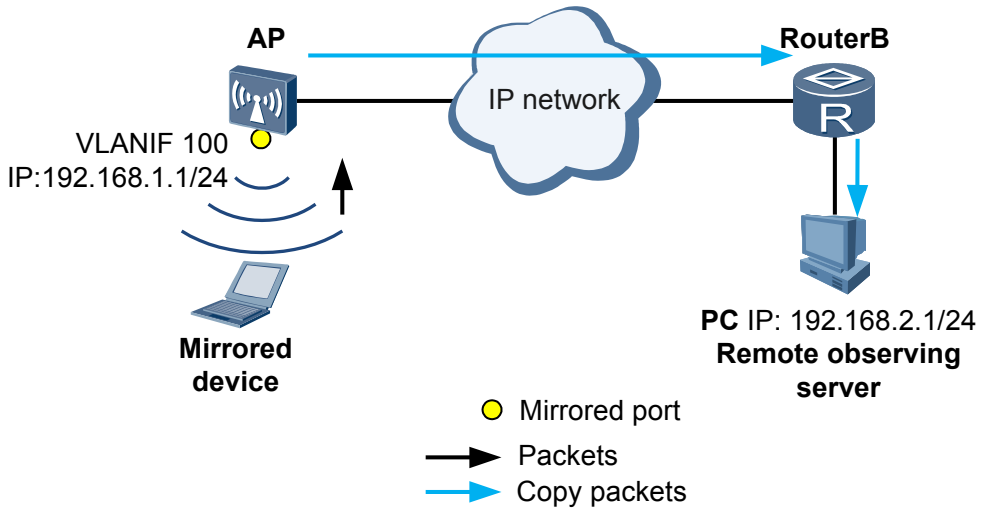
```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] mirror to observe-port inbound
[AP-Wlan-Bss1] quit
[AP] quit
```

## Mirroring Packet Headers to a Remote Observing Server

When using this method, ensure that a reachable route exists between the mirrored device and observing server.

As shown in **Figure 8-2**, BSS1 is added to VLAN 100 and incoming packets on BSS1 are mirrored to a remote observing server, and the observing server analyzes the packet headers. The IP address of VLANIF 100 corresponding to the mirrored port is 192.168.1.1/24. The IP address and mask of the remote observing server is 192.168.2.1 and 24. A reachable route exists between the mirrored port and observing server.

**Figure 8-2** Mirroring packet headers to a remote observing server



The procedure is as follows:

1. Configure the computer as a remote observing server of the AP.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] observe-server destination-ip 192.168.2.1 source-ip 192.168.1.1
```

NOTE

**destination-ip** is the IP address of the remote observing server; **source-ip** is the IP address of the mirrored port. Ensure a reachable route between the observing server and mirrored port. After the mirrored port is specified in the next step, the encapsulated packet headers can be sent to the remote observing server. The **source-ip** parameter can be set to any value; however, the IP address of mirrored port is recommended.

2. Add BSS1 to VLAN 100 and configure an IP address for VLANIF 100.

```
[AP] vlan batch 100
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 100
[AP-Wlan-Bss1] port hybrid untagged vlan 100
[AP-Wlan-Bss1] quit
[AP] interface vlanif 100
[AP-Vlanif100] ip address 192.168.1.1 24
[AP-Vlanif100] quit
```

3. Set BSS1 as a mirrored port and set the mirroring direction to inbound.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] mirror to observe-server inbound
[AP-Wlan-Bss1] quit
[AP] quit
```

# 9 List of Indicators

You can observe indicators on the devices to check device running status, which helps you locate and troubleshoot faults in a timely manner.

For details about indicators on the indoor AP, see Indicator Description. For details about indicators on the outdoor AP, see Indicator Description.