HUAWEI USG6000E

Quick Maintenance Guide

Issue 01

Date 2023-06-30

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: https://e.huawei.com

Contents

1 About This Document

Related Version

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

Product Name	Version
USG6000E	V600R006 V600R007

Intended Audience

This document is intended for installation personnel and administrators who maintain USG. Welcome to provide improvement suggestions or maintenance materials during use.

Symbol Conventions

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

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

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**.
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.

GUI Conventions

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

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

Update History

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

Updates in Issue 01 (2023-06-30)

Initial commercial release.

2 Before You Start

Before taking over the maintenance of devices, you are advised to:

1. Obtain the network topology diagram and data planning tables (including ports, VLANs, and IP addresses), print them, and paste them in your equipment room for quick reference.
2. Prepare the tools and cables that may be used during device maintenance, as listed in **Table 2-1**.

Table 2-1 Common tools and cables for device maintenance

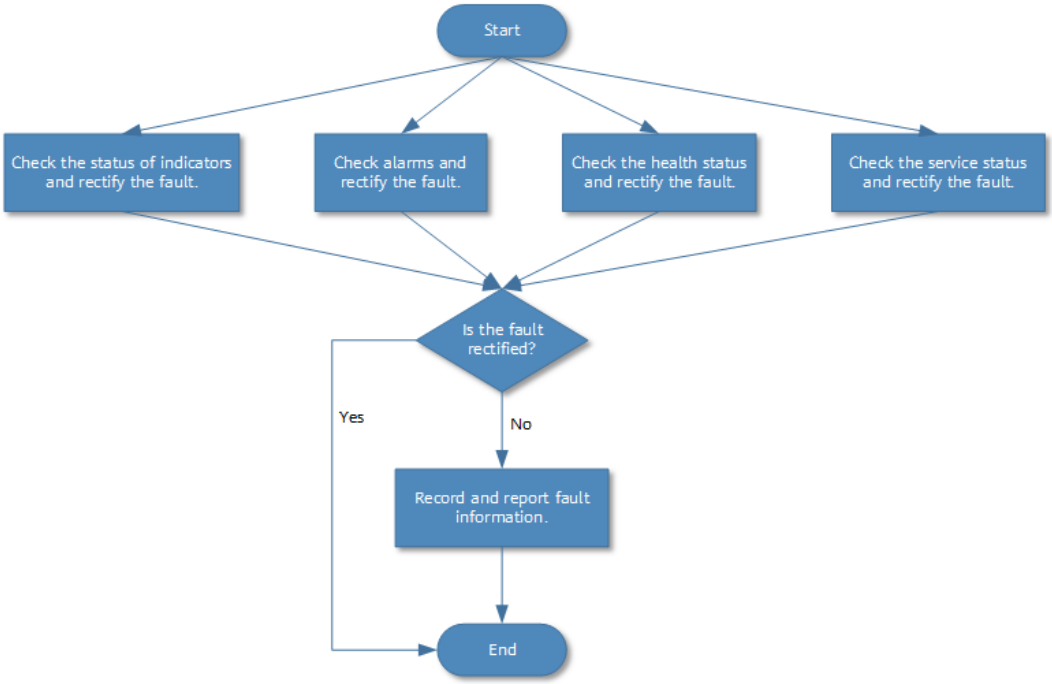
No.	Item	Description
1	Cables	• A console cable: used to log in to the device through the console port. • A console-USB adapter: used to connect the USB port of the maintenance terminal to the console port of the device. • Two straight-through cables: used to commission the management port or other services. • Several extension network cable connectors: used to extend the network cable that is not long enough. • Multiple fibers and SFP/eSFP/SFP+ optical modules: used to connect to other network devices.
2	Maintenance terminal	One maintenance terminal, typically a laptop with serial communication software installed: used to log in to the device.

No.	Item	Description
3	Instruments	• One optical power meter: used to test optical parameters of optical ports (such as optical power and receiver sensitivity). • A hygrothermograph: used to measure the ambient temperature and humidity of the device and the temperature and humidity at the air exhaust vent of the fan. • A network cable tester: used to test the network cable connectivity.
4	Specialized tools	• An SD wrist strap: used to protect the device from electrostatic charges. • A pair of protective gloves: used to protect your hands from sharp objects or knives.

3 How to Quickly Maintain the Device

3.1 Quick Maintenance Process

Through the following flowchart, you can quickly understand and master the key points of device maintenance.



NOTE

To check the alarms, health status, and service status, and record fault information, you must log in to the web system or log in to the device through the console port or using Telnet or STelnet. For details about how to log in to the device, see *Configuration Guide*. If you fail to log in to the device, see **Solution to Device Login Failures**.

3.2 Checking the Indicator Status

The device provides various indicators. By observing these indicators, you can know the operating status of the device and locate and rectify common hardware faults. For the meanings of indicator states, see the *Hardware Guide*. If an indicator is in abnormal state, locate and rectify the fault based on the troubleshooting methods in the **HUAWEI USG6000E, USG6000, USG9500, and NGFW Module Troubleshooting Guide**. If the fault persists, collect and provide feedback on the fault information by referring to **Fault Information Collection and Feedback**.

Table 3-1 lists the normal status of each indicator on the device.

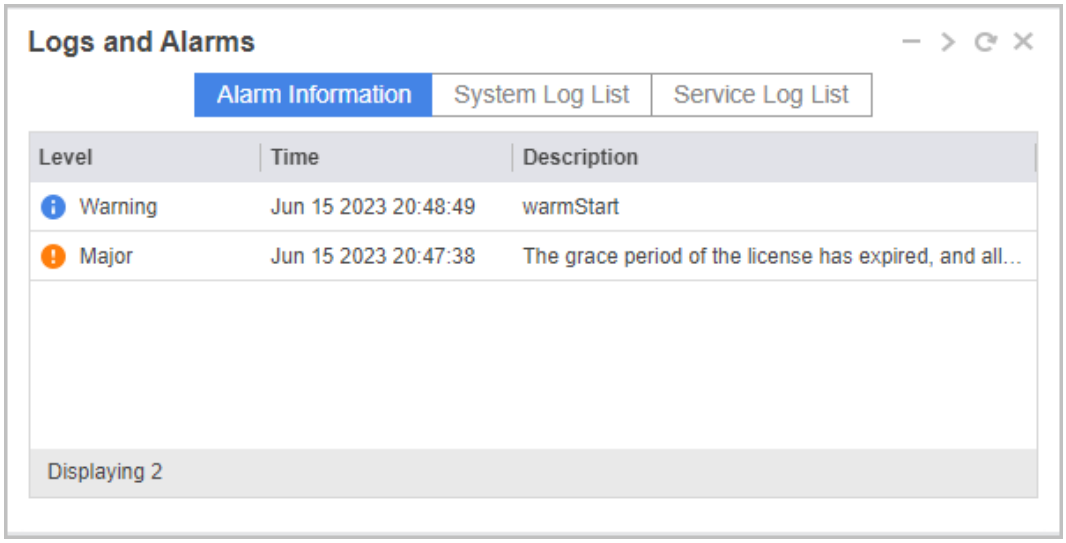
Table 3-1 Quick reference table for normal indicator states

Category	Indicator	Normal State
Device panel	PWR	Steady green
	SYS	Slow blinking green, blinks once every 2 seconds (0.5 Hz)
Power Module	STAT	Steady green
Fan Module	-	Blinking green, blinks once every 2 seconds (0.5 Hz)
Hard Disk	-	• ALM indicator: off • RUN indicator: steady green

3.3 Web: Checking the Device Alarms

Log in to the device through the web UI. Choose **Dashboard** and view the alarm information in the **Logs and Alarms** area, as shown in **Figure 3-1**. For details about the meaning, impact on the system, possible causes, and handling methods of the alarm, see *Alarm Handling*.

Figure 3-1 Logs and alarms



3.4 CLI: Checking the Device Alarms

Run the **display alarm active** command in any view to check all active alarms on the device. For details about the meaning, impact on the system, possible causes, and handling methods of the alarm, see *Alarm Handling*.

Display the contents of all active alarms in the system.

```
<sysname> display alarm active
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  1/Independent/2016-12-28 12:06:38+08:00/-/0xffae201c/hwPowerRemove/Warning/Sta
rt/OID 1.3.6.1.4.1.2011.5.25.219.2.5.1 Power is absent.(Index=68681737, EntityPh
ysicalIndex=68681737, PhysicalName="PWR", EntityTrapFaultID=136448)
```

Table 3-2 Description of the display alarm active command output

Item	Description
Sequence	Sequence number
RootKindFlag	Flag indicating a root-cause alarm or a non-root-cause alarm: • Independent: indicates an alarm for which alarm correlation analysis is not performed. • RootCause: indicates a root-cause alarm. • nonRootCause: indicates a non-root-cause alarm.
Generating time	Time when the alarm is generated
Clearing time	Time when the alarm is cleared

Item	Description
ID	Alarm ID
Name	Alarm name
Level	Alarm severity level
State	Alarm status: • Start • End
Description information for locating	Alarm description
RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm (for non-root-cause alarms only)

3.5 Web: Checking the Health Status

NOTE

Before using this function, check whether the current administrator account has read-write permissions. If not, the permissions shall be added so that the health check can be performed on the device.

Log in to the web UI using the system administrator account and choose **System** > **Administrator** > **Administrator Role**. Under **Administrator List**, click the **Edit** icon. On the **Modify Role** dialog box that is displayed, select **Read/Write** for **Health Check** by clicking the **Monitor** drop-down list box. The system administrator account has read-write permissions by default.

3.5.1 Web: Checking the Device Resource Information

Choose **Dashboard** > **System Resource**, view the CPU usage, memory usage, and CF card usage. If the usage is too high, rectify the fault by referring to "FAQs" in the **Maintenance Guide**.

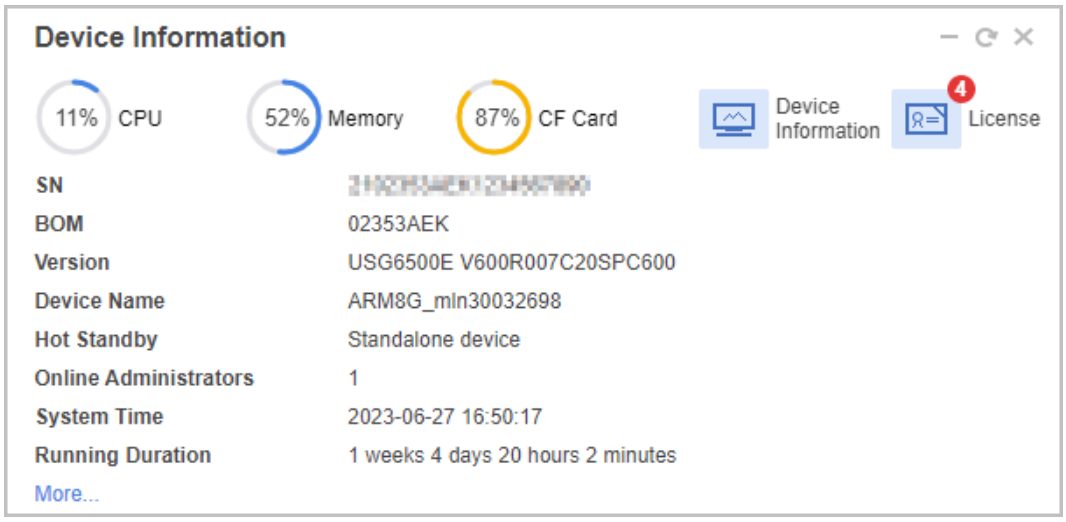


Table 3-3 describes the parameters in the **System Resources** window.

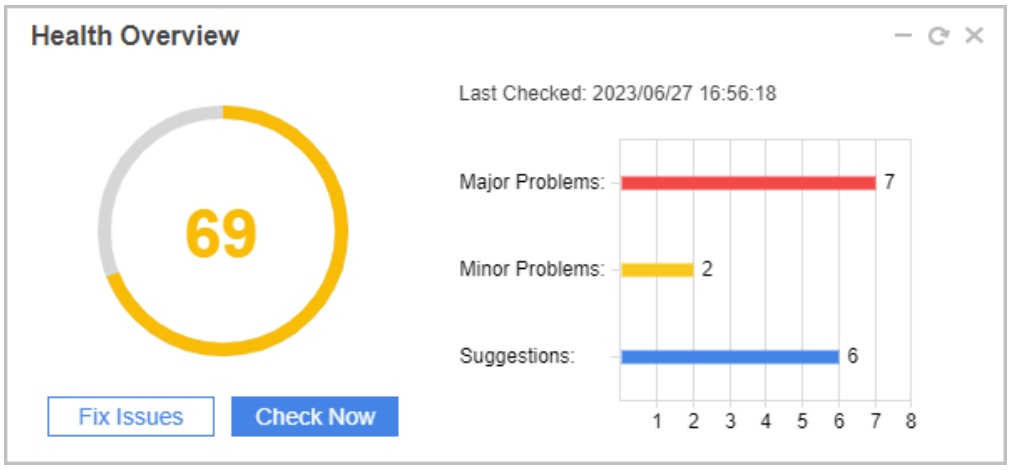
Table 3-3 System resources parameters

Parameter	Description
CPU Usage	As for the CPU usage, the dashboard displays the CPU usage of the integrated device. When you move the cursor over the CPU resource icon, details about the CPU usages of the management plane and service plane are displayed. You can also click the CPU resource icon to view the detailed information.
Memory Usage	Percentage of memory resources used. Move the cursor over the memory meter to view the following information: • Memory Usage: amount of memory resources used, in percentage • Used: indicates the used memory capacity. • Free: indicates the unused memory capacity. • Total: total memory capacity (MB) You can also click the memory resource icon to view the detailed information. **NOTE** The FW whose memory is less than or equal to 4 GB has been preloaded with most services, and the FW has reserved memory resources for these services. Therefore, the memory usage of the entire system is high when the FW has no services configured, but the FW running is not affected. For details about the memory specifications of the FW, see the technical specifications of the corresponding model in the **Hardware Guide > Hardware Introduction > Chassis**.

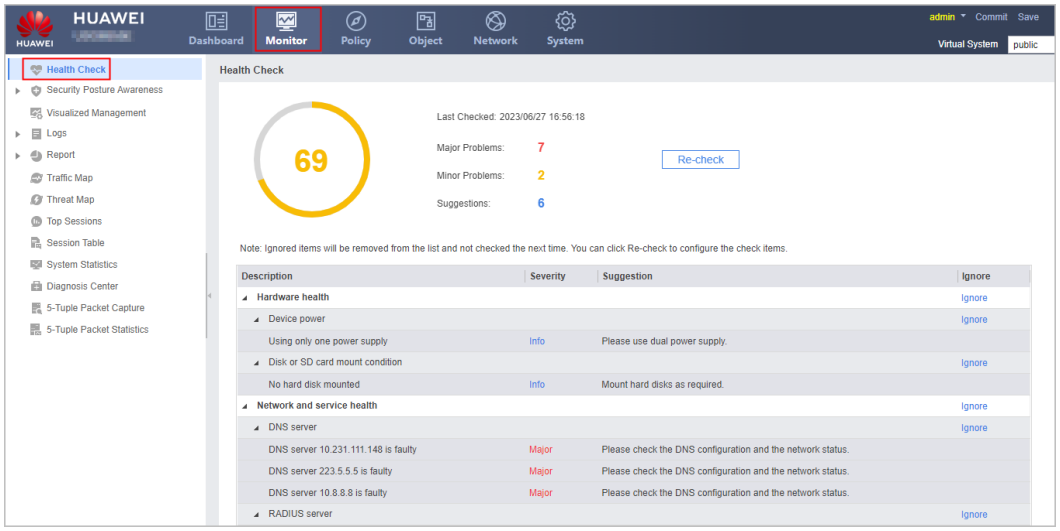
Parameter	Description
CF Card Usage	When you move the pointer to the CF card resource icon, detailed information is displayed, including: ● CF card Usage: amount of CF card resources used, in percentage ● Used: indicates the used CF card capacity. ● Free: indicates the unused CF card capacity. ● Total: total CF card capacity (MB) If the status of the micro SD card is Unmounted, it is possible that the format of the micro SD card does not comply with ext4. In this case, click **Format** to format the SD card. You can also click the CF card resource icon to view the detailed information.
Disk Usage	Percentage of hard disk resources used. Move the cursor over the disk meter to view the following information: ● CF card Usage: amount of CF card resources used, in percentage ● Disk Usage: amount of hard disk resources used, in percentage ● SD card Usage: amount of SD card resources used, in percentage. Only the USG6510E/6510E-POE/6530E support this function. ● Used: used hard disk capacity. ● UnUsed: unused hard disk capacity. ● Size: total hard disk capacity (MB) **NOTE** Only the device with the hard disk, SD Card supports to display the disk usage. You can also click the disk usage resource icon to view the detailed information.

3.5.2 Web: Checking Device Health Information

1. Choose **Dashboard** and click **Check Now** in the **Health Overview** area. After the health check is complete, you can view the device issue statistics.



2. Click **Fix Issues**. On the **Health Check** page, view details about and handling suggestions for the hardware, network, service, resource usage, and signature database update. You can optimize the device based on the handling suggestions.



3.6 CLI: Checking the Health Status

3.6.1 CLI: Checking the Device Resource Information

Run the **display device** command in any view to check the device status. This command displays the status of a component when the component is not running properly. If the usage is too high, rectify the fault by referring to "FAQs" in the **Maintenance Guide**.

Display the status of the USG6655E

```
<sysname> display device
USG6655E's Device status:
Slot  Sub Type       Online    Power     Register      Status     Role
--------------------------------------------------------------------------------
0     -   RPU        Present   PowerOn   Registered    Abnormal   Master
2     -   PWR        Present   PowerOff  Registered    Abnormal   NA
3     -   PWR        Present   PowerOn   Registered    Normal     NA
```



```
4    -  FAN        Present  PowerOn   Registered    Normal    NA
5    -  FAN        Present  PowerOn   Registered    Normal    NA
6    -  FAN        Present  PowerOn   Registered    Normal    NA
7    -  FAN        Present  PowerOn   Registered    Normal    NA
12   -  SPUB       Present  PowerOn   Registered    Normal    NA
13   -  SPUB       Present  PowerOn   Registered    Normal    NA
```

If **Status** is displayed as **Abnormal**, the board runs abnormally. The possible causes are as follows:

1. The corresponding slot does not support the interface card.
2. The interface card is damaged.
3. The pins on the backplane or the MPU are damaged or slanted due to incorrect installation of the board.
4. If the status of a **FAN** is **Abnormal**, the fan is faulty or unavailable.

Run the **display device** *slot-id* command in any view to check detailed information about the board of each slot, including information about the LPU, MPU, SFU, clock board, power module, and fan module. Run the **display devicepic-status** command to view information about cards on all SPUs and LPUs.

3.6.2 CLI: Checking Device Health Information

Run the **display health** command in any view to check the health check information of the FW. The information includes CPU usage and memory usage.

Display information about the health check of the USG6000E

```
<sysname> display health
------------------------------------------------------------------------------
 Slot  Card  Sensor SensorName      Status  Current(V)  Lower(V)    Upper(V)
------------------------------------------------------------------------------
 0     -     0      12V             Normal  0.0000      0.0000      0.0000
------------------------------------------------------------------------------
 Slot  Card  Sensor   Status   Current(C)  Lower(C)    Upper(C)
------------------------------------------------------------------------------
 0     -     0        Normal   48          0           110
       -     1        Normal   49          0           110
------------------------------------------------------------------------------
 PowerID  Online  Mode   State     Current(A)   Voltage(V)   RealPwr(W)
------------------------------------------------------------------------------
 2        Present AC     Supply    5            12           60
 3        Present AC     Supply    5            12           60
------------------------------------------------------------------------------
    FanID   FanNum   Online   Register     Speed      Mode      Airflow
------------------------------------------------------------------------------
    FAN0    [1]      Present  Registered   0  (6840 )  AUTO      Left-to-Right
 System Memory Usage Information:
 System memory usage at 2000-02-08 08:05:21
------------------------------------------------------------------------------
 Slot     Total Memory(MB)   Used Memory(MB)   Used Percentage   Upper Limit
------------------------------------------------------------------------------
  0          3818               1865              48%               90%
------------------------------------------------------------------------------
 System CPU Usage Information:
 System cpu usage at 2000-02-08 08:05:21
------------------------------------------------------------------------------
      Slot             CPU Usage             Upper Limit
------------------------------------------------------------------------------
       0                 71%                   80%
------------------------------------------------------------------------------
 Disk Usage Information:
 System disk usage at 2000-02-08 08:05:21
------------------------------------------------------------------------------
```



```
Slot    Device    Total Memory(MB)    Used Memory(MB)    Used Percentage
--------------------------------------------------------------------------------
 0      hda1:     1561                1008               64%
--------------------------------------------------------------------------------
```

Table 3-4 Description of the **display health** command output

Item	Description
Slot	Slot ID
Card	Slot ID of a subcard
Sensor	Number of a voltage sensor Only the USG6615E/6625E,USG6630E/6650E, USG6635E/6655E, USG6680E, and USG6712E/6716E support this parameter.
SensorName	Name of a voltage sensor Only the USG6615E/6625E,USG6630E/6650E, USG6635E/6655E, USG6680E, and USG6712E/6716E support this parameter.
Status	Voltage alarm severity ● Normal ● Minor ● Major ● Fatal Only the USG6615E/6625E,USG6630E/6650E, USG6635E/6655E, USG6680E, and USG6712E/6716E support this parameter.
Current(V)	Voltage, in V Only the USG6615E/6625E,USG6630E/6650E, USG6635E/6655E, USG6680E, and USG6712E/6716E support this parameter.
Lower(V)	Lowest voltage, in V Only the USG6615E/6625E,USG6630E/6650E, USG6635E/6655E, USG6680E, and USG6712E/6716E support this parameter.
Upper(V)	Highest voltage, in V Only the USG6615E/6625E,USG6630E/6650E, USG6635E/6655E, USG6680E, and USG6712E/6716E support this parameter.
Sensor	Number of a temperature sensor

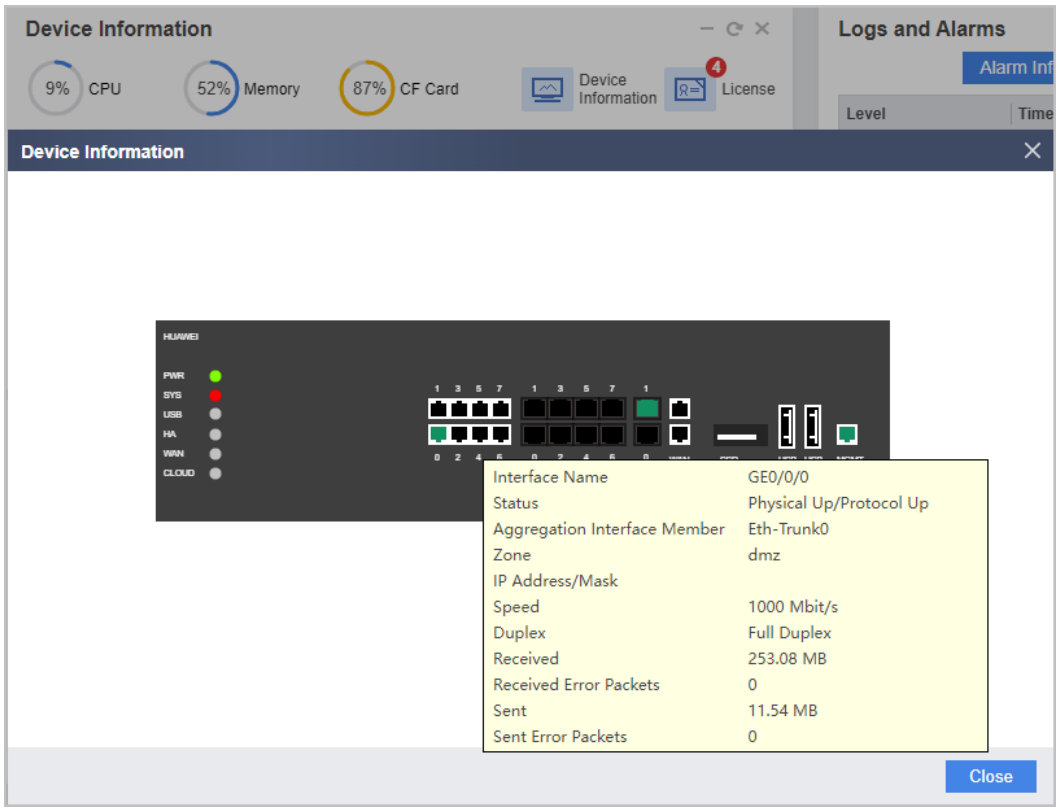
Item	Description
Status	Temperature alarm severity • Normal • Minor • Major • Fatal
Current(C)	Temperature, in C
Lower(C)	Lowest temperature, in C
Upper(C)	Highest temperature, in C
PowerID	Power module ID
Online	Whether a power module is installed • Present • Absent
Mode	Working mode • AC • DC
State	Status of the power module • Supply • NotSupply
Current(A)	Current, in A
Voltage(V)	Voltage, in V
RealPwr(W)	Real power, in W
FanID	ID of a fan module
FanNum	Number of fans
Online	Whether a fan module is installed • Present • Absent
Register	Whether a fan module is registered • Registered • Unregistered
Speed	Fan speed
Mode	Rate adjustment mode of the fan module • AUTO • MANUAL
Airflow	Airflow, such as Left-to-Right

Item	Description
Total Memory(MB)	Total size of the memory, in MB
Used Memory(MB)	Size of used memory, in MB
Used Percentage	Percentage of used memory
Upper Limit	Alarm threshold of memory usage
CPU Usage	CPU usage
Upper Limit	Alarm threshold of the CPU usage
Device	Storage device
Total Memory(MB)	Total size of the memory, in MB
Used Memory(MB)	Size of used memory, in MB
Used Percentage	Percentage of used memory

3.7 Web: Checking the Service Status of the Device

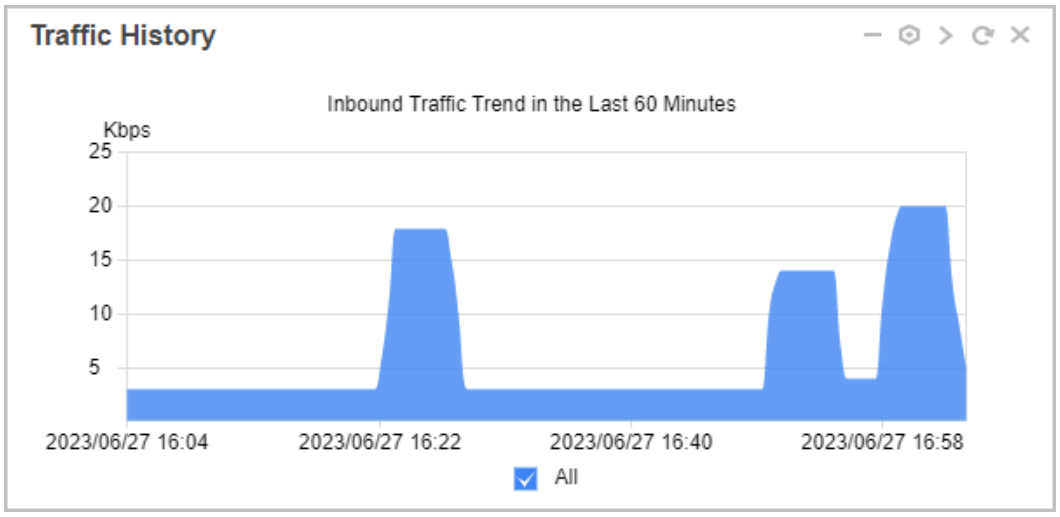
3.7.1 Web: Checking the Interface Traffic

1. Choose **Dashboard** > **Device Information**. Move the pointer to an interface and view information about the interface, as shown in the following figure. Click **Refresh**. Then you can view the latest information about the interface.

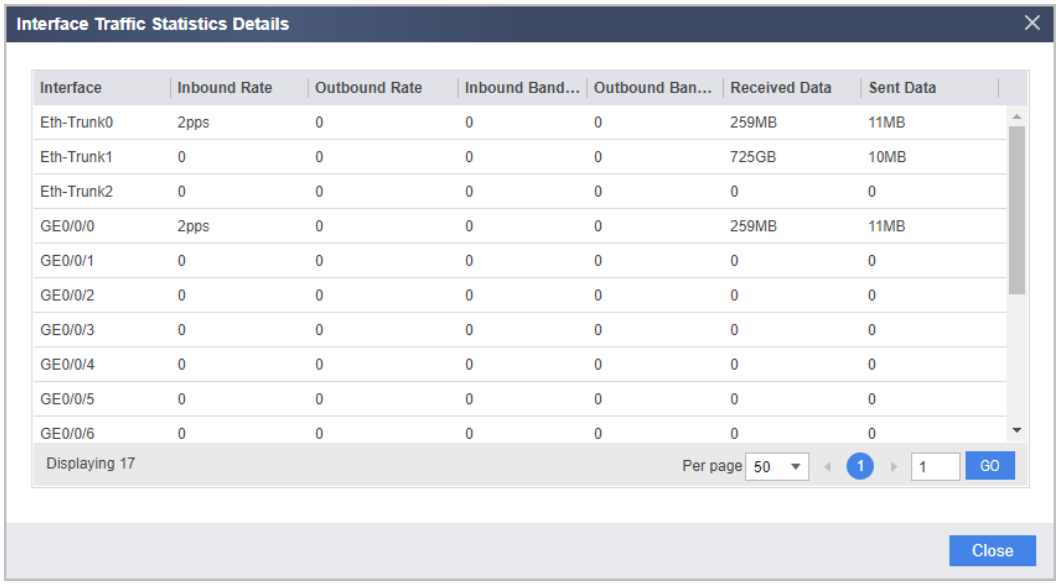


Parameter	Description
Status	X/Y, of which X (Physical UP or Physical DOWN) indicates the physical-layer status of the interface and Y (Protocol UP or Protocol Down) indicates the network-layer status of the interface.
Zone	Indicates the security zone of the interface.
IP/Mask	Indicates the IP address and the subnetwork mask of the interface.
Speed	Indicates the interface rate.
Mode	Indicates the duplex mode of the interface.
Input/Output Traffic	Indicates the incoming/outgoing traffic volume of the interface.
Input/Output Error Packets	Indicates the incoming/outgoing error packet counts of the interface.

2. View interface traffic statistics in the **Traffic History** area.



3. Click > to view details about device interface traffic statistics.



3.7.2 Web: Checking the Session Table

You can check the session table to locate faults.

- If a session entry has been established and traffic is permitted by security policies, the possible causes of service interruptions include but are not limited to:
  - Hardware faults on the outgoing interface (such as physical damage of an interface card or bad cable connections)
  - Packet drop on the downstream device.
  - Incorrect routing configuration.
  - Incorrect packet count on the outgoing interface.
  - Administratively denied packets (packets dropped due to bandwidth management and attack defense policies)
  - Configuration errors.

- If no session entry is established for a service, possible causes include but are not limited to the following:
  - Packets are not forwarded to the FW because of faults on an upstream device or incorrect route configuration.
  - The security policy configured on the FW blocks the packets. For example, the security policy action is configured as **Deny**, or the source IP address is blacklisted.
  - A hardware fault occurs at the incoming interface. For example, an interface card is damaged, or a network cable is not securely connected.
  - Attack defense functions, except blacklist, discard packets.
  - The bandwidth management function restricts the number of sessions. When the number of sessions exceeds the upper threshold, new sessions cannot be established, and packets are therefore discarded.
  - Configuration errors.

To view the session table on the web UI, perform the following steps:

1. Choose **Monitor** > **Session Table**, and view information about session entries on the **Session Table** page.
2. Click **Add Filter** and select query conditions to display session entries that meet the conditions.

   Click ⊕ to add multiple query conditions that are logically ANDed. That is, only sessions satisfying all conditions are displayed.

   You can click ⊖ to delete a query condition.

Condition	Description
Virtual System	Displays session entries of a specified virtual system.
Protocol	Displays session entries of a specified protocol.
Application	Displays session entries of a specified application.
Source Zone/Destination Zone	Displays session entries of a specified source or destination security zone.
Source Address/Destination Address	Displays session entries of a specified source/destination address or address range.
NAT Source Address/NAT Destination Address	Displays session entries of a specified NATed source/destination address or address range.
Source Port/Destination Port	Displays session entries of a specified source/destination port.
NAT Source Port/NAT Destination Port	Displays session entries of a specified NATed source/destination port.
Security Policy	Displays session entries that match a specified security policy.

Condition	Description
User Name	Displays session entries of a specified user.
Time Range	Displays session entries created within a specified time range. For example, if the time range is 5 minutes, session entries created in the last 5 minutes are displayed. **NOTE** Only sessions that are currently alive can be displayed. If a session is soon deleted or aged after being created, information about this session is not displayed.
Outbound Interface	Displays session entries of a specified outbound interface.
Packets	Displays session entries whose number of forward packets, number of reverse packets, or number of two-way packets is no smaller than, smaller than, or equal to a specified value. Forward refers to the direction same as the direction from the source security zone to the destination security zone in the session entry. Reverse refers to the direction opposite to the direction from the source security zone to the destination security zone in the session entry.

NOTE

For NAT64 sessions, if you query a session based on the source/destination address or port, you can use only the address or port before NAT, but not the address or port after NAT.

The session table of a specified time range is displayed as follows:

Figure 3-2 The session table of a specified time range is displayed

Details	Proto...	Source ...	Desti...	Source Address	Destination Addr...	Source P...	Destination ...	Left Time	Outbound In...	Next Hop
	https	trust	local	172.16.10.178	10.18.74.29	62001	8443	00:10:00	InLoopBack0	127.0.0.1
	https	trust	local	172.16.10.133	10.18.74.29	51513	8443	00:10:00	InLoopBack0	127.0.0.1
	https	trust	local	172.16.10.134	10.18.74.29	59740	8443	00:09:56	InLoopBack0	127.0.0.1
	https	trust	local	172.16.10.134	10.18.74.29	59723	8443	00:08:24	InLoopBack0	127.0.0.1

Click in the Details column to view details on the session table. The following table lists the meaning of each field.

Field	Description
Creation Time	Time for creating the session.
Protocol	Protocol type of the session.
Source Virtual System/Destination Virtual System	Source and destination virtual system of the session.
Source Zone/ Destination Zone	Source and destination security zones of the session.
Source Address/ Destination Address	Source and destination IP addresses of the session.
NAT Source Address/NAT Destination Address	Source and destination NAT addresses of the session.
Source Port/ Destination Port	Source and destination port of the session.
NAT Source Port/NAT Destination Port	Source and destination NAT port of the session.
Forward Packets/ Forward Bytes	Number of packets and bytes in the forward direction of the session
Reverse Packets/ Reverse Bytes	Number of packets and bytes in the reverse direction of the session
Outbound Interface/MAC Address	Outbound interface of a session or MAC address of the outbound interface
Next Hop	Next-hop IP address of the session.
Security Policy	Security policy that session matches.
Application	Type of application of the session.
User name	User name of the session.
Session Timeout	Aging time of the session.
Time Left	Remaining lifetime of the session.

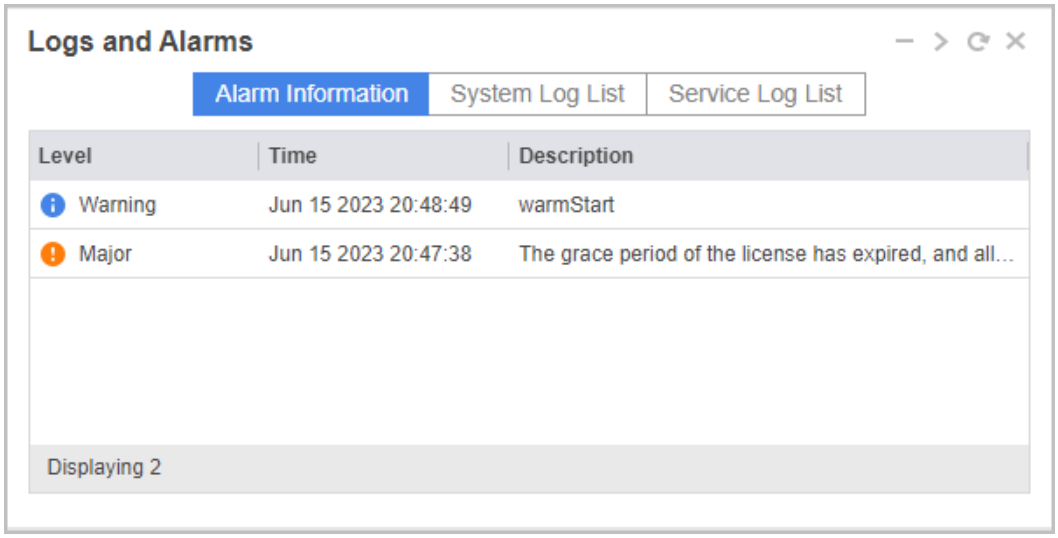
3.7.3 Web: Checking Logs

Checking Logs

Log in to the device through the web UI. Choose **Dashboard** and view the current log information in the **Logs and Alarms** area, as shown in **Figure 3-3**. For details

about the meaning, parameter description, causes, and handling methods of the log, see *Log Reference*.

Figure 3-3 Logs and alarms



Support for web-based log querying and exporting when a hard disk/SD card is in or not in position (USG6000E)

Function	Hard Disk/SD Card in Position	Hard Disk/SD Card Not in Position
Querying and exporting traffic logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting threat logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting URL logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting content logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.

Function	Hard Disk/SD Card in Position	Hard Disk/SD Card Not in Position
Querying and exporting bandwidth ip connections logs	Supported by all models except USG6510E/6510E-POE/6530E, USG6635E/6655E and USG6680E and USG6712E/6716E.	Supported by all models except USG6510E/6510E-POE/6530E, USG6635E/6655E and USG6680E and USG6712E/6716E.
Querying and exporting operation logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting system logs	Supported by all models.	Supported by all models.
Querying and exporting user activity logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting policy matching logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting sandbox detection logs	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting mail filtering logs	Supported by all models.	Supported by all models except USG6110E/6307E/6311E/6311E-POE/6331E/6510E/6510E-POE/6510E-DK/6530E.
Querying and exporting audit logs	Supported by all models.	Supported by all models.

3.7.4 Web: Check the Report

This section describes the report-related operations.

Context

When you view the reports of the certain category on the FW, the log system analyzes and summarizes the corresponding log data stored in the local hard disks or memory to form the reports.

NOTE

If a lot of logs are generated, you are advised to configure a hard disk for the device to prevent log information loss caused by log overwriting.

The FW supports the following categories of reports:

- Traffic reports
- Threat reports
- Bandwidth ip connections dimension reports
- Bandwidth policy reports
- URL reports
- Policy matching reports
- File blocking reports
- Data filtering reports
- Intelligent report retrieval
- Customizing reports
- Customizing and subscribing to reports

Procedure

1. Choose **Monitor** > **Report** > **Traffic Report**.
2. Select the category of reports. Take **Traffic Report** as an example.
3. Select the type of reports.

   For USG6000E, choose **Source Address**, **Destination Address**, **Interface, User**, **Application**, **Application Category**, **Application Subcategory**, **Virtual System, Address Type** or **Security Policy** to view the traffic trend and top flows.
4. Select a time range in the **Time Range** check box or **User-Defined** time area.
5. Click **Search** to display traffic trend and traffic ranking in different dimensions.

   NOTE

   Traffic information about unidentified users and applications is not counted in the traffic statistics.

   Move the pointer to the point at which the fold angle changes. The traffic values are displayed.
6. **Optional:** Click **Export** to export operation logs in CSV format to the management PC.

3.7.5 Web: Checking VPN Status

Viewing IPSec Status

View IPSec status using the web UI:

1. Choose **Network** > **IPSec** > **Monitor**.
2. The IPSec tunnels being negotiated and already negotiated are displayed in the **IPSec monitoring List**. For each IPSec tunnel, the tunnel name, status, local address, peer address, algorithm, negotiated data flow, duration, and sending and receiving rates are displayed.

Viewing L2TP Status

View L2TP status using the web UI:

1. Choose **Network** > **L2TP** > **Monitor**.
2. Click **Refresh**. You can view the following information about established L2TP tunnels.

Parameter	Description
Local Tunnel ID	Tunnel ID of the local device. The value must be the same as the **Tunnel ID on Peer** value of the peer device.
Peer Tunnel ID	Tunnel ID of the peer device. The value must be the same as the **Tunnel ID on Local** value of the peer device.
Local Address	Local IP address of the L2TP tunnel of the local device.
Peer Address	Peer IP address of the tunnel of the peer end.
Port	UDP port of the peer end of a tunnel. If the local end is a LAC, the UDP port of the peer end is 1701.
Number of Sessions	Number of sessions within the tunnel.
Peer Tunnel Name	Peer tunnel name.
Disconnect	Disconnects the tunnel manually. • Click of the L2TP tunnel to disconnect the tunnel and clear all control connections and session connections from the tunnel. • Clicking tears down all tunnels and clears all control and session connections on the tunnels.

Viewing GRE Status

View GRE status using the web UI:

1. Choose **Network** > **GRE** > **Monitor**.
2. Click **Refresh** to view GRE tunnel information.

Table 3-5 Parameters of GRE tunnel information

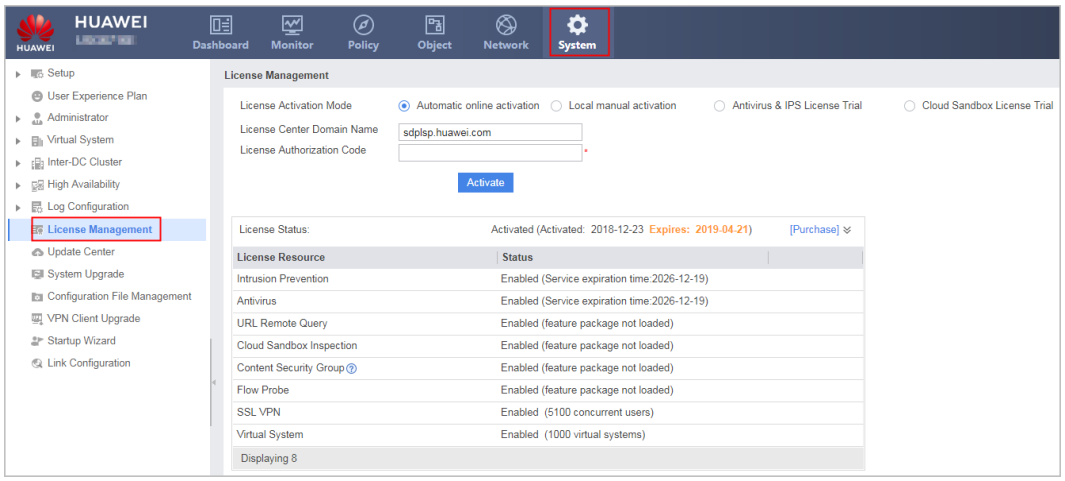
Parameter	Description
Received GRE Packets	Indicates that the following information is the statistics of received GRE packets.
Number of Received Packets	Number of the packets received over the GRE tunnel (Fragments of a packet are regarded as packets.)
Number of Received Bytes	Number of the bytes received over the GRE tunnel
Sum of Packets and Fragments	Total number of the packets received over the GRE tunnel (Fragments of a packet are regarded as packets.)
GRE Version Errors	Number of errors caused by incorrect version information
GRE Checksum Errors	Number of errors caused by incorrect GRE checksum and calculation
GRE Key Errors	Number of key inconsistency errors
Transmitted GRE Packets	Indicates that the following information is the statistics of transmitted GRE packets.
Number of Packets to Be Transmitted	Number of the packets to be transmitted over the GRE tunnel
Number of Bytes to Be Transmitted	Number of the bytes to be transmitted over the GRE tunnel
Number of Transmitted Error Packets	Number of the packets that fail to be sent
Packets Exceeded Recursion Limit	Number of errors caused by tunnel nesting
Number of Transmitted Packets	Number of the GRE packets that are properly transmitted

3.7.6 Web: Check the License Usage

After the license is installed, you can log in to the web interface and choose **System** > **License Management** to view the activation status and entitlement information of the license.

NOTE

The supported license resources vary with models. The screenshot in this section is for reference only. License control items support details, please refer to the *License Usage Guide-License Control Items*.



3.8 CLI: Checking the Service Status of the Device

3.8.1 CLI: Checking the Interface Traffic

Run the **display interface** command in any view to query the IP addresses of the interfaces, the status of the physical layer and link layer, and the descriptions of interfaces.

Display the current operating status of and statistics about GigabitEthernet 0/0/1

```
<sysname> display interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
Description :  Interface Route Port
The Maximum Transmit Unit is 1500 bytes, Hold timer is 10(sec)
Internet Address is 10.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0022-a106-0e5b
Media type is twisted pair, loopback not set, promiscuous mode not set
1000Mb/s-speed mode, full-duplex mode, link type is auto negotiation
Max-bandwidth : 1000000 kbps
Last physical up time   : -
Last physical down time : 2018-01-16 20:33:13
Current system time: 2018-01-17 10:08:18
Top 3 input bit rate: 672688 bits/sec at 2018-01-15
11:11:41                                                    20872 bits/sec at 2018-01-15
11:11:40                                                    17456 bits/sec at 2018-01-14
19:23:00                                          Top 3 output bit rate: 672000 bits/sec at
2018-01-15 11:11:41                                                    19568 bits/sec at
2018-01-15 11:11:40                                                    9064 bits/sec at
2018-01-14 11:11:53                                       Top 3 input packet rate: 8008
packets/sec at 2018-01-15 11:11:41                                                  248
packets/sec at 2018-01-15 11:11:40                                                  216
packets/sec at 2018-01-14 11:11:56                                  Top 3 output packet rate:
8000 packets/sec at 2018-01-15 11:11:41
232 packets/sec at 2018-01-15 11:11:40                                              80
packets/sec at 2018-01-14 11:11:53
Last 300 seconds input rate 2619  bytes/sec, 16  packets/sec
Last 300 seconds output rate 28627  bytes/sec, 26  packets/sec
   Input: 277618 packets, 46890659 bytes
        275866 unicasts, 1740 broadcasts, 12 multicasts, 0 pauses
        0 overruns, 0 runts, 0 jumbos, 0 FCS errors
        0 length errors,  0 code errors, 0 align errors
```



```
    0 fragment errors,  0 giants, 0 jabber errors
    0 dribble condition detected,  0 other errors
Output: 303774 packets, 157242945 bytes
    285539 unicasts, 6 broadcasts, 18229 multicasts, 0 pauses
    0 underruns, 0 runts, 0 jumbos, 0 FCS errors
    0 fragment errors, 0 giants, 0 jabber errors
    0 collisions, 0 late collisions
    0 ex. collisions, 0 deferred, * other errors
```

Table 3-6 Description of the **display interface** command output

Item	Description
current state	Physical status of the interface: ● UP: The physical layer status of the interface is normal. ● DOWN: The physical layer of the interface fails. ● Administratively down: The **shutdown** command is run on the interface by the administrator. ● Flow Down: The status of the data flow on the interface is Down. This status is consistent with the status of the bound mVRRP virtual router. If the status of the bound mVRRP virtual router is Backup or Initialize, the status of the data flow on the service interface is Down.
Line protocol current state	Status of the link protocol of the interface: ● UP: The link protocol status of the interface is normal. ● DOWN: The link protocol status of the interface fails or the interface is not configured with an IP address. ● UP (spoofing): The link protocol status of the interface has the spoofing feature. That is, the link protocol status of the interface keeps Up.
Description	Description about the interface. Up to 80 characters can be entered. The description can help the user to get familiar with the interface function.
The Maximum Transmit Unit	The packet larger than the MTU is fragmented before being sent. If the non-fragmentation is configured, the packet is discarded.
Hold timer	Life cycle of the packet. If the packet is not sent out during the life cycle, it is discarded.
Internet Address	IP address and the subnet mask of the interface.

Item	Description
IP Sending Frames' Format	Format of Ethernet frames sent by the interface: ● Ethernet_2 ● Ethernet_SNAP ● 802.2 ● 802.3 The default value is Ethernet_2.
Hardware address	MAC address of the interface.
Max-bandwidth	Maximum bandwidth of the interface.
Last physical up time	The last time when the interface is up.
Last physical down time	The last time when the interface is down.
Current system time	The time of the current system.
Top 3 input bit rate	Top 3 bits inputted per second on the interface.
Top 3 output bit rate	Top 3 bits outputted per second on the interface.
Top 3 input packet rate	Top 3 packets inputted per second on the interface.
Top 3 output packet rate	Top 3 packets outputted per second on the interface.
Last 300 seconds input/output rate	Average rate of packets received/sent within the last 300s. The time range can be set through **set flow-stat interval**.

Item	Description
Input	Total number of packets and bytes received by the interface: **NOTE** On the USG6510E/6510E-POE, USG6530E, USG6515E/6550E/6560E/6580E, and USG6525E/6555E/6565E/6585E, unicast, broadcast, and multicast statistics packets contain Grant packets. ● unicasts: number of unicast packets. ● broadcasts: number of broadcast packets. ● multicasts: number of multicast packets. ● pauses: number of received pause frames. ● overruns: number of packets discarded because of overflow errors. ● runts: number of frames less than 64 bytes, in the correct format, and containing valid CRC fields ● jumbos: number of frames greater than 1518 bytes (greater than 1522 bytes if VLAN is involved) and less than the maximum jumbo length in a scenario where jumbo is enabled ● FCS errors: number of received packets with CRC errors and normal length ● length errors: number of packets with incorrect packet length when the value in the length field of a standard Ethernet frame is inconsistent with the actual packet length (46 to 1500) bytes ● code errors: number of packets with invalid data after the valid carrier ● align errors: number of packets with align errors, that is, the transmitted packets have incomplete bytes, including preambles and interframe gaps ● fragment errors: number of received packets less than 64 bytes and with incorrect CRCs ● giants: number of oversized packets of 1519 to 16383 bytes ● jabber errors: number of jabber errors, in which only frames (for CRC error packets) greater than the maximum length of the jumbo can be counted into the jabber when jumbo is enabled ● dribble condition detected: number of incorrect packets with 4bit data after CRC checks ● other errors: number of other error packets

Item	Description
output	Total number of packets and bytes sent by the interface: **NOTE** On the USG6510E/6510E-POE, USG6530E, USG6515E/6550E/6560E/6580E, and USG6525E/6555E/6565E/6585E, unicast, broadcast, and multicast statistics packets contain Grant packets. ● unicasts: number of unicast packets. ● broadcasts: number of broadcast packets. ● multicasts: number of multicast packets. ● pauses: number of sent pause frames. ● underruns: number of packets discarded when the sending rate of the port exceeds the processing capability of the sending queue ● runts: number of frames less than 64 bytes, in the correct format, and containing valid CRC fields ● jumbos: number of frames greater than 1518 bytes (greater than 1522 bytes if VLAN is involved) and less than the maximum jumbo length in a scenario where jumbo is enabled ● FCS errors: number of sent frames with CRC errors and normal length ● fragment errors: number of sent packets less than 64 bytes and with incorrect CRCs ● giants: number of oversized packets of 1519 to 16383 bytes ● jabber errors: number of jabber errors, in which only frames (for CRC error packets) greater than the maximum length of the jumbo can be counted into the jabber when jumbo is enabled ● collisions: number of packets that are not sent when a collision is detected ● late collisions: number of delayed collision frames because a collision is detected when the first 512 bits of a frame are sent ● ex. collisions: number of times that a collision occurs after 16 consecutive frame collisions (For example, if one collision occurs again, the count is 1; if two consecutive collisions occur, the count is 2.) ● deferred: number of packets delayed from transmitting due to collisions detected before the transmission ● other errors: number of other error packets

3.8.2 CLI: Checking the Session Table

You can check the session table to locate faults.

- If a session entry has been established and traffic is permitted by security policies, the possible causes of service interruptions include but are not limited to:
  - Hardware faults on the outgoing interface (such as physical damage of an interface card or bad cable connections)
  - Packet drop on the downstream device.
  - Incorrect routing configuration.
  - Incorrect packet count on the outgoing interface.
  - Administratively denied packets (packets dropped due to bandwidth management and attack defense policies)
  - Configuration errors.
- If no session entry is established for a service, possible causes include but are not limited to the following:
  - Packets are not forwarded to the FW because of faults on an upstream device or incorrect route configuration.
  - The security policy configured on the FW blocks the packets. For example, the security policy action is configured as **Deny**, or the source IP address is blacklisted.
  - A hardware fault occurs at the incoming interface. For example, an interface card is damaged, or a network cable is not securely connected.
  - Attack defense functions, except blacklist, discard packets.
  - The bandwidth management function restricts the number of sessions. When the number of sessions exceeds the upper threshold, new sessions cannot be established, and packets are therefore discarded.
  - Configuration errors.

To view the session table using the CLI, perform the following steps:

1. Access the system view.

   system-view
2. Check IPv4 session table information.
   - **display firewall session table** [**verbose**] [**vsys** *vsys-name*] [**source-zone** *source-zone* | **destination-zone** *destination-zone* | { **default-policy** | **policy** *policy-name* } | **source-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **source** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **destination-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **destination** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **slot** *slot-id* **cpu** *cpu-id* | **protocol** { *id* | **tcp** | **udp** | **sctp** | **icmp** | **ah** | **esp** | **gre** } | **application** *application-name* | **source-port** { **inside** *port-number* | **global** *port-number* } | **destination-port** { **inside** *port-number* | **global** *port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **service** *service-type* | **vlan** *vlan-id* | **created-in** *time* | **long-link** | **user** *user-name* | { **local** | **remote** } | **uniderection**] *

- **display firewall session table verbose** [**vsys** *vsys-name*] [**source-zone** *source-zone* | **destination-zone** *destination-zone* | { **default-policy** | **policy** *policy-name* } | **source-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **source** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **destination-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **destination** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **slot** *slot-id* **cpu** *cpu-id* | **protocol** { *id* | **tcp** | **udp** | **sctp** | **icmp** | **ah** | **esp** | **gre** } | **application** *application-name* | **source-port** { **inside** *port-number* | **global** *port-number* } | **destination-port** { **inside** *port-number* | **global** *port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **service** *service-type* | **vlan** *vlan-id* | **created-in** *time* | **long-link** | **user** *user-name* | { **local** | **remote** } | **uniderection** | { **reverse-packet** | **forward-packet** | **total-packet** } { **over** | **below** | **equal** } *packet-value*] *
- **display firewall session table** [**verbose**] **all-systems** [**source-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **source** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **destination-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **destination** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **slot** *slot-id* **cpu** *cpu-id* | **protocol** { *id* | **tcp** | **udp** | **sctp** | **icmp** | **ah** | **esp** | **gre** } | **source-port** { **inside** *port-number* | **global** *port-number* } | **destination-port** { **inside** *port-number* | **global** *port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **service** *service-type* | **vlan** *vlan-id* | **created-in** *time* | **long-link** | { **local** | **remote** }] *
- **display firewall session table verbose all-systems** [**source-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **source** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **destination-cpe** *start-ipv6-address* [**to** *end-ipv6-address*] | **destination** { **inside** *start-ip-address* [**to** *end-ip-address*] | **global** *start-ip-address* [**to** *end-ip-address*] } | **slot** *slot-id* **cpu** *cpu-id* | **protocol** { *id* | **tcp** | **udp** | **sctp** | **icmp** | **ah** | **esp** | **gre** } | **source-port** { **inside** *port-number* | **global** *port-number* } | **destination-port** { **inside** *port-number* | **global** *port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **service** *service-type* | **vlan** *vlan-id* | **created-in** *time* | **long-link** | { **local** | **remote** } | { **reverse-packet** | **forward-packet** | **total-packet** } { **over** | **below** | **equal** } *packet-value*] *
- **display firewall session table** [**verbose**] **slb** [**destination** { **vip** *start-vip-address* [**to** *end-vip-address*] | **rip** *start-rip-address* [**to** *end-rip-address*] } | **source** *start-source-address* [**to** *end-source-address*] | **destination-port** { **vport** *vport-number* | **rport** *rport-number* } | **source-port** *source-port-number* | **slot** *slot-id* **cpu** *cpu-id*] *
- **display firewall session table** [**verbose**] **session-id** *session-id*

In the dual system hot backup environment, you can run the **display firewall session table** command with **local** or **remote** to display the session table on the local or remote device.

A session table typically contains a large number of entries. Therefore, to narrow down the displayed entries and increase fault locating efficiency, the following command provides multiple parameters for you to select the type of entries to be displayed.

NOTE

For NAT64 sessions, if you query a session based on the source/destination address or port, you can use only the address or port before NAT, but not the address or port after NAT.

If the IP address is an IPv4 address before NAT, use the **display firewall session table** [**verbose**] command and one or more of the following parameters for a query: **source inside** *start-ip-address* [**to** *end-ip-address*], **destination global** *start-ip-address* [**to** *end-ip-address*], **source-port inside** *port-number*, and **destination-port global** *port-number*

If you do not use parameter **verbose**, only the abbreviated session information is displayed, as shown in the following screenshot:

```
Current Total Sessions : NUM
 TYPE VPN:SRCVPN --> DSTVPN SRCIP --> DSTIP
```

If you use parameter **verbose**, as shown in the following screenshot:

```
Current Total Sessions : NUM
 TYPE VPN:SRCVPN --> DSTVPN ID: ID-NUMBER
Zone: SRCZONE--> DSTZONE Remote TTL: TOTALTIME Left: LEFTTIME
Interface: OUTINTERFACE Nexthop: IP-ADDRESS MAC: MACADDRESS
<-- packets:NUMBER bytes:BYTES --> packets:NUMBER bytes:BYTES
SRCIP --> DSTIP PolicyName: POLICYNAME
TCP State: TCP State
```

Table 3-7 shows the meaning of each parameter. Parameters in *italics* can very under actual situations.

Table 3-7 Parameters of a session entry

Parameter	Description
TYPE	Protocol type of the session. The value range of the parameter is the same as that of the *protocol* parameter in the **display firewall session table** command.
VPN:*SRCVPN --> DSTVPN*	Source and destination VPN instances of the session
ID: *ID-NUMBER*	ID number of the session.
Zone: *SRCZONE--> DSTZONE*	Source and destination security zones of the session
Remote	In a hot standby scenario, **Remote** indicates that the current session is a backup session, which is backed up from the peer device.
TTL: *TOTALTIME*	Lifetime of the session entry
Left: *LEFTTIME*	Remaining lifetime of the session entry
Interface: *OUTINTERFACE*	Outgoing interface
Nexthop: *IP-ADDRESS*	Next-hop IP address
MAC: *MACADDRESS*	Next-hop MAC address

Parameter	Description
<-- **packets**:*NUMBER* **bytes**:*BYTES*	Reverse packets and bytes of the session <== indicates that hardware-based fast forwarding is implemented for the reverse packets of the session, and <-- indicates that hardware-based fast forwarding is not implemented for the reverse packets of the session.
--> **packets**:*NUMBER* bytes:*BYTES*	Forward packets and bytes of the session. In normal cases, the numbers of forward packets and bytes would be the same as those of the reverse packets and bytes. If the numbers of forward packets and bytes are smaller than those of the reverse packets and bytes, some packets are discarded. ==> indicates that hardware-based fast forwarding is implemented for the forward packets of the session, and --> indicates that hardware-based fast forwarding is not implemented for the forward packets of the session.
SRCIP --> *DSTIP*	Source IP address, source port, destination IP address, and destination port of the session The address format is x.x.x.x:portx[y.y.y.y:porty], where **portx** is the source port and **porty** the destination port. The address in the square brackets is the post-NAT IP address. If NAT is not implemented, no content is displayed in the square brackets.
PolicyName: *POLICYNAME*	Packet matching policy name.
TCP State	TCP connection status. This field is displayed only for TCP sessions. ● connecting: The device receives the first SYN packet, indicating that the TCP connection is being established. ● Established: The device receives an ACK packet, indicating that the TCP connection has been established. ● fin-1: The device receives the first FIN packet, indicating that the TCP connection is being torn down. ● close: The device receives the second FIN packet, indicating that the TCP connection has been torn down.

3. Display the IPv6 session table.
   – **display firewall ipv6 session table** [**vsys** *vsys*] [**source-zone** *source-zone* | **destination-zone** *destination-zone*| { **default-policy** | **policy** *policy-name* } | **source** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*]

| **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **destination** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*] | **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **application** *application-type* | **protocol** { *id* | **tcp** | **udp** | **icmp** | **ah** | **esp** | **gre** } | **service** *service-type* | **source-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **destination-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **vlan** *vlan-id* | **created-in** *time* | **long-link** | **user** *user-name* | { **local** | **remote** } | **slot** *slot-id* **cpu** *cpu-id*] *

- **display firewall ipv6 session table verbose** [**vsys** *vsys*] [**source-zone** *source-zone* | **destination-zone** *destination-zone*| { **default-policy** | **policy** *policy-name* } | **source** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*] | **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **destination** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*] | **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **application** *application-type* | **protocol** { *id* | **tcp** | **udp** | **icmp** | **ah** | **esp** | **gre** } | **service** *service-type* | **source-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **destination-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **vlan** *vlan-id* | **created-in** *time* | **long-link** | **user** *user-name* | { **local** | **remote** } | **slot** *slot-id* **cpu** *cpu-id* | { **reverse-packet** | **forward-packet** | **total-packet** } { **over** | **below** | **equal** } *packet-value*] *
- **display firewall ipv6 session table all-systems** [**source** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*] | **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **destination** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*] | **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **protocol** { *id* | **tcp** | **udp** | **icmp** | **ah** | **esp** | **gre** } | **service** *service-type* | **source-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **destination-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **vlan** *vlan-id* | **created-in** *time* | **long-link** | { **local** | **remote** } | **slot** *slot-id* **cpu** *cpu-id*] *
- **display firewall ipv6 session table verbose all-systems** [**source** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*] | **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **destination** { **inside** *start-ipv6-address* [**to** *end-ipv6-address*] | **global** *start-ipv6-address* [**to** *end-ipv6-address*] } | **protocol** { *id* | **tcp** | **udp** | **icmp** | **ah** | **esp** | **gre** } | **service** *service-type* | **source-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **destination-port** { **inside** *inside-port-number* | **global** *global-port-number* } | **interface** { *interface-name* | *interface-type interface-number* } | **vlan** *vlan-id* | **created-in** *time* | **long-link** | { **local** | **remote** } | **slot** *slot-id* **cpu** *cpu-id* | { **reverse-packet** | **forward-packet** | **total-packet** } { **over** | **below** | **equal** } *packet-value*] *
- **display firewall ipv6 session table** [**verbose**] **session-id** *session-id*

NOTE

For NAT64 sessions, if you query a session based on the source/destination address or port, you can use only the address or port before NAT, but not the address or port after NAT.

If the IP address is an IPv6 address before NAT, use the **display firewall ipv6 session table** [**verbose**] command and one or more of the following parameters for a query: **source inside** *start-ipv6-address* [**to** *end-ipv6-address*], **destination global** *start-ipv6-address* [**to** *end-ipv6-address*], **source-port inside** *port-number*, and **destination-port global** *port-number*

4. Configure the device to send session details to the specified FTP server (such as a PC).

   export firewall session table ftp-server *server-address username password file-name*

   NOTE

   All models except USG6635E/6655E, USG6680E and USG6712E/6716E support this command.

   The FTP server must use the default port number 21. Otherwise, session messages fail to be sent.

3.8.3 CLI: Checking Logs

Run the commands listed in **Table 3-8** in any view to check the log configuration result.

Table 3-8 Checking log configuration results

Operation	Command
Check log configuration and statistics.	**display firewall log** { **configuration** [**vsys** *vsys-name*] | **statistic** [**vsys** *vsys-name*] [**host** *host-id* [**secondary**]] }
Check statistics in the information buffer.	**display buffer** [*feature-name* [*buffer-name*]]
Check the channel configuration.	**display channel** [*channel-number* | *channel-name*]
Check information recorded by the information center.	**display info-center** [**statistics** [**module-id** *id* | **module-name** *name*]]

Operation	Command
Check information in the log buffer.	**display logbuffer** [**common-log** | **sec-log**] [**size** *size-value* | **module** *module-name* | **security** | **level** { *severity* | **emergencies** | **alert** | **critical** | **error** | **warning** | **notification** | **informational** | **debugging** } | **slot** *slot-number* | **vsys** *vsys-name*] * **display logbuffer summary** [**level** *severity* | **slot** *slot-number*] *
Check log file information.	**display logfile** *driver path file-name* [*offset* | **hex**] *
Check information about a specified log ID in the filtering table.	**display info-center filter-id** [**bymodule-alias** *modname alias*]
Check rate limit records in the information center.	**display info-center rate-limit record**
Check rate limit records in the information center.	**display info-center rate-limit threshold**
Check the template of session log .	**display session-log template**

3.8.4 CLI: Checking VPN Status

Viewing IPSec Status

View IPSec status using the CLI:

- Run the **display ike sa** command, view IPSec tunnel status.
- Run the **display ipsec sa** command, view IPSec tunnel details.
- Run the **display ipsec statistics** command, view IPSec packet statistics.

Viewing L2TP Status

View L2TP status using the CLI, In any view:

- Run the **display l2tp tunnel** command, view L2TP tunnel information.
- Run the **display l2tp session** command, view L2TP session information.
- Run the **display l2tp statistics** command, view L2TP packet statistics.

Viewing GRE Status

View GRE status using the CLI, run the **display gre statistic** command in any view to check GRE statistics.

3.8.5 CLI: Check the License Usage

Run the **display license** command in any view to check detailed information about activated license files.

Table 3-9 Description of the **display license** command output

Item	Description
Device ESN is	Equipment Serial Number (ESN) of the device. Each device has a unique serial number.
License file ESN is	ESN used to apply for the license file.
The file activated is	License file that is activated currently.
The time when activated is	Activation time.
The time when expired is	Time when the license file is expired.
Virtual System	Number of virtual systems.
SSL VPN Concurrent User	Maximum number of concurrent SSL VPN users supported by the license file.
Content Security Group	Content security group.
IPS Update	Whether IPS is supported.
Anti Virus Update	Whether antivirus is supported.
URL Remote Query	Whether URL remote query is supported.
Cloud Sandbox Inspection	Whether the cloud sandbox inspection service is supported.

3.9 Web: Backing Up a Configuration File

You need to back up the running configuration file on a scheduled basis to the administrator PC for security concerns.

Background

Modified configurations take effect immediately but are not automatically saved to the configuration file. The modification will be lost after the device is powered off. Therefore, after all modifications are complete, choose **System** > **Configuration File Management** or run the **save** command to save the configurations. This section describes only how to back up the configuration file.

Prerequisites

The running configuration is correct and has been saved.

Maintenance Interval

Every week

Operation

1. Choose **System** > **Configuration File Management**.
2. Click **Export** in **Current Configuration**.
3. Click **Save** and select a path on the terminal to save the configuration file.

Follow-up Operation

After you back up the configuration file to the PC, check whether the size of the backup configuration file on the PC is the same as the size of the configuration file on the device. If the sizes are different, an anomaly may have occurred during file backup. You need to back up the configuration file again.

3.10 CLI: Backing Up a Configuration File

You need to back up the running configuration file on a scheduled basis to the administrator PC for security concerns.

Background

Modified configurations take effect immediately but are not automatically saved to the configuration file. The modification will be lost after the device is powered off. Therefore, after all modifications are complete, choose **System** > **Configuration File Management** or run the **save** command to save the configurations. This section describes only how to back up the configuration file.

Prerequisites

The running configuration is correct and has been saved.

Maintenance Interval

Every week

Operation

This section describes how to back up the configuration file on the CLI when the device functions as an FTP client.

NOTE

SFTP is more secure than FTP and TFTP. Therefore, SFTP is recommended for file transmission.

1. Start the FTP server application program on the PC and set the configuration file path, FTP server IP address and port as well as FTP user name and password.

2. Set interface IP addresses, assign the interfaces to security zones, and configure security policies. Ensure that the device is reachable to the PC and can use FTP.
3. Log in to the FTP server.

```
<sysname> ftp 10.110.24.254
Trying 10.110.24.254 ...
Press CTRL+K to abort
Connected to 10.110.24.254.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user   //WFTPD is the local FTP server program.
User(10.135.86.164:(none)):admin123   //Enter the user name.
331 Give me your password, please
Enter password:   //Enter the password.
230 Logged in successfully

[ftp]
```

4. Back up the configuration file.

```
[ftp] put config.cfg
200 Port command successful.
150 Opening data connection for config.cfg.
226 File received ok
FTP: 1257 byte(s) sent in 0.03 second(s) 40.55Kbyte(s)/sec.
```

Follow-up Operation

After you back up the configuration file to the PC, check whether the size of the backup configuration file on the PC is the same as the size of the configuration file on the device. If the sizes are different, an anomaly may have occurred during file backup. You need to back up the configuration file again.

3.11 Fault Information Collection and Feedback

3.11.1 Collecting Basic Fault Information

Collect the information listed in **Table 3-10** before contacting Huawei technical support.

Table 3-10 Basic fault information

No.	Item	Description
1	Fault occurrence time	Record the time when the fault occurs and last time when the fault occurred, accurate to minutes.
2	Fault symptom	Record fault symptoms in detail. If multiple faults occur simultaneously, describe their symptoms one by one. If the environment is changed before the fault occurs, record the changes in detail.
3	Fault impact	Record the fault severity and impacted services, such as the number of affected devices.

No.	Item	Description
4	Software version	Collect information about the software version on the Console through the **display version** command when you can log in to the device through Telnet or the Console interface.
5	Networking information	Provide a networking diagram showing upstream and downstream devices and connected ports, especially the device or port where the fault occurs.
6	Measures that have been taken	Record the measures that have been taken and effect of these measures (including command execution procedure and output).

3.11.2 Collecting Running Information

To collect device fault information, run the commands listed in **Table 3-11** in any view.

Table 3-11 Collection of device fault information

No.	Collecting Item	Collection Method
1	Device information	Run the **display device** command.
2	Temperature	Run the **display temperature slot** *slot-id* command.
3	CPU usage	Run the **display cpu-usage** command.
4	Routing table information	Run the **display ip routing-table** command.
5	Logs	Run the **display logbuffer** command.
6	Traps	Run the **display trapbuffer** command.
7	Configuration	Run the **display current-configuration** command.
8	Diagnostic information about the device	Run the **display diagnostic-information** command.
9	Interface information	Run the **display interface** command.
10	Network connectivity information	Run the **ping** command to collect information about the network connectivity and record the results.

NOTE

- When you collect fault information through command lines, you can copy the information displayed on the console, including the Console interface or the Telnet terminal, and then attach it to a **.txt** file for a record.
- When a device runs normally, you are advised to back up the historical traps and logs in the CF card through the Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP).
- Collecting diagnostic information may affect system performance. For example, the CPU usage increases. If the CPU or memory usage is high, wait until them fall below the corresponding thresholds before running the **display diagnostic-information** command.

4 Solution to Device Login Failures

If you fail to log in to the web system of the device or remotely log in to the device using Telnet/STelnet, log in to the device through the console port and check the web system or Telnet/STelnet configuration. If you fail to log in to the device through the console port, you cannot perform any operations related to the CLI. In this case, perform the following steps:

WARNING

Before performing the following operations, ensure that the user service is interrupted. If the user service is not interrupted, do not perform these operations. Instead, collect the fault information and then contact your agent or Huawei after-sales service hotline.

1. Check and recover the power supply system.

   If all indicators are off and the fans do not work, the power supply system may be faulty.

   a. Check whether the Input or STATUS indicator of the power module is on. If the indicator is off, the power module input is abnormal. Request the electrician to recover the power lines in the equipment room, rack, or cabinet.

   b. Perform a cross-check to check whether the power module is faulty. Replace the power module with a new one and test whether the new power module works properly. If so, the original power module is faulty. If not, check whether the software or hardware is faulty.

   c. If the fault is rectified, the fault is caused by a known software issue. If the fault persists after the device restarts, the power slot of the device is faulty. In this case, replace the device.

2. Check and modify the communication parameters of the COM port on your computer.

   Check whether the communication parameters of the serial port are the same as those of the device's console port. If not, modify the communication parameters.

   The default settings of the device's console port are as follows: 9600 bit/s, 8 data bits, 1 stop bit, no parity check, and no flow control.

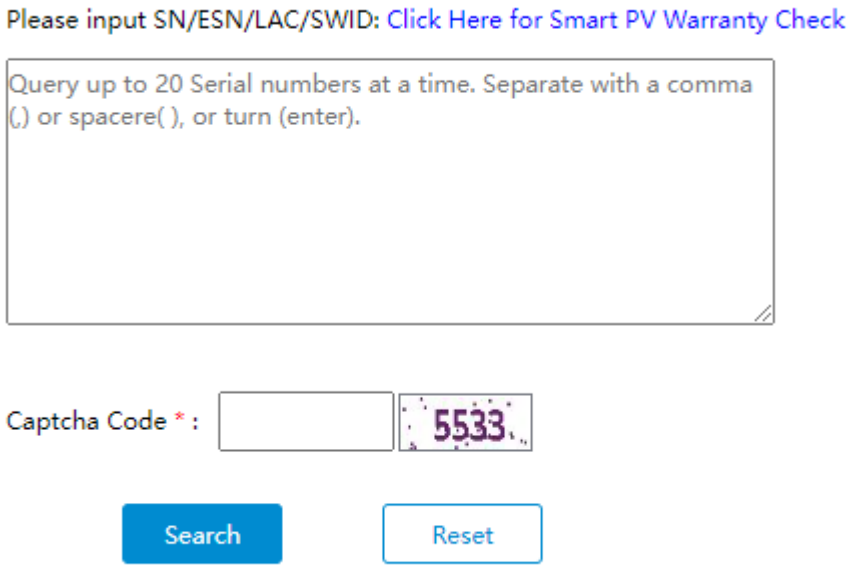
3. Restart the device.

   If the fault persists, restart the device by powering off and then on the device to solve the problem.

5 Measures for Returning Faulty Hardware for Repair

If a hardware fault is detected, perform the following steps:

1. Check whether the device is within the warranty period. If so, Huawei will provide in-warranty repair.
   a. Log in to the **Huawei enterprise technical support website** and click **Maintenance Status**. The **maintenance information query** page is displayed.



   b. Enter the device serial number and verification code to view the hardware service start time and end time.
2. Check whether the spare parts service is included and use the **RMA Delivery Status Inquiry** tool to query the spare parts delivery status.
   – If the spare parts service is included, the customer service personnel of the service hotline will submit a spare parts service application for you. After the application is approved, Huawei will deliver the functional parts

to you within seven days. Send the faulty parts back to Huawei Maintenance Service Center within 30 days after receiving the functional parts.

- If the spare parts service is not included, send the faulty parts to Huawei Maintenance Service Center. Huawei will repair and send them back to you within 30 days after receiving the faulty parts.

3. Fill in the **Fault Tag** and send it together with the faulty parts to Huawei Maintenance Service Center.

Fault Tag

*Customer name:										
Address:										
Contact person:										
Tel.:				Fax:						
Category*: □ Replacement □ Repair □ Analysis										
RMA code/SR*	Bom Code*	SN	Goods Description	Whether the Data in the Parts Removed	Fault Occurring Date*	Description of the Fault Phenomena*	Category No.*	Software Version	Customer Name	Property Owner*
				□ Yes □ No						
				□ Yes □ No						
				□ Yes □ No						
				□ Yes □ No						
Please help confirm the information below: 1. If the above returned BOM Code has the function of saving data, please delete the data saved in this BOM Code before returning to Huawei or removing the storage medium, like HD or CF Card. □ Yes □ No 2. Record any data that should be remained as follows:										
Definition of Huawei Category No.: F001–Wear out Damaged, F003–Dead on arrival of spare parts, F005–Active Batch replacement by R&D request, F006–Faulty parts from Customer's R&R request, F009–Damaged by irresistible natural force (such as Earthquake, Lightning strike, Ground sea, Rainstorm, Flood), F056–Internal Return, F060–Good parts Return for testing										

Note:

1. **Items marked with asterisks (*) are mandatory.**
2. **Data Removal Notice:** Removal/Deletion of Data prior to handing over products to Huawei for repair, replacement or other purposes is at customer's sole discretion. Huawei usually sends products to local, Hungary or China service centers and for data removal (hereafter "Send-Delete Operations"). **It is considered that customer authorizes Huawei to take the Send-Delete Operations for products in case there is any data on the products received from customers.**
   "Data" as used in this Notice means any data, fact or other information, including but not limited to information that could be used to identify an individual, e.g. name, email address, title, occupation, industry, telephone number, employer, family address, postal or other address, other contact information, and financial information.

   Customers should refer to Product Manuals for methods of deletion of data on the products. If there is no methods of deletion of data described in the Product Manuals or the methods described cannot be used, customer may adopt alternative means to delete data, such as degaussing or removing storage media from products.

   Huawei usually erases all the Data contained in the products received from customers. For product that is unrepairable or unreusable, Huawei implements irreversible means to destroy it, or follow customer's requirements.

   The information set forth in this Notice is only provided "as is" and is not considered any representation, warranty or guarantee from Huawei.

6 Risky Operations

Risky Hardware Operations

Table 6-1 describes the risky hardware maintenance operations.

Table 6-1 Risky hardware maintenance operations

Category	Caution	Risk
Button operation	Press the **RST** button on the front panel.	If you press the **RST** button on the front panel, the running device will be restarted. This operation must be performed by qualified maintenance personnel during severe system faults. If the **RST** button is pressed the device will be restarted.
Cable operation	Insert or remove the network cables inside the cabinet only when necessary.	The network cables inside the cabinet are used for communication between the device and the maintenance terminal or between upstream and downstream devices. If the network cables are removed and inserted randomly, the maintenance terminal may fail to log in to the FW and the FW services may be interrupted.
Power supply operation	Operate the power supply switch of the power distribution frame in the cabinet only when necessary.	Power supply operations can only be performed upon upgrades, capacity expansion, parts replacement, or fatal faults. While performing power supply operations, maintenance personnel must follow related operation guidelines. Care should also be taken in operating power supply switches since improper operating on the switches may hinder device running or cause service interruption.

Risky Command Executions

CAUTION

The following commands can only be executed by qualified and trained maintenance personnel.

Table 6-2 describes the risky maintenance commands

Table 6-2 Risky maintenance commands

Category	Command	Function	View	Risk
Restart operation	**reboot**	Restart the system	User view	This command is used only in product deployment or upgrades and only by qualified personnel; otherwise, services may be interrupted completely.
Format operation	**format** *device-name*	Format a storage device	User view	The use of this command results in an irrecoverable loss of all the files on the specified storage device.
Deleting operation	**delete** [**/unreserved**] [**/quiet**] { *filename* | *device-name* }	Delete the specified files on the FW storage device	User view	This command is used to delete specified files on the storage device of the FW. The use of the parameter **unreserved** results in an irrecoverable loss of the specified files.
User interface	**authentication-mode**	Authenticate users	User-interface view	The authentication mode for users such as Console or VTY is password authentication or AAA authentication. The username and password must be configured before such a user logs in to the system; otherwise, the login fails.

Category	Command	Function	View	Risk
System maintenance	**startup system-software**	Configure the system file to be used on the next startup of the FW.	User view	The system file used for the next startup must be correct; otherwise, the system version or configuration may go wrong.

Risky Web Operations

CAUTION

Risky web operations must be run by well-trained and qualified maintenance personnel.

Table 6-3 describes the risky web operations.

Table 6-3 Risky web operations

Category	Web UI Path	Function	Risk
Restart operation	**System** > **Setup** > **Restart**	Restarting the System	This operation is used only in product deployment or upgrades and only by qualified personnel; otherwise, services may be interrupted completely.
Restoring factory settings	**System** > **Configuration file Management**, Click **Restore Factory Settings**.	Restoring factory settings	This operation must be performed by qualified maintenance personnel during severe system faults. Otherwise, services will be interrupted.
System maintenance	**System** > **Configuration file**	Set the system file for the next startup.	The system file used for the next startup must be correct; otherwise, the system version or configuration may go wrong.

7 Technical Support

You can seek technical support for maintenance using the following methods:

- Access **Huawei's intelligent Q&A customer service system for enterprise business**.
- Visit **Huawei technical support website for enterprise business** and search for **Knowledge Base** or post your questions on **Support Community**.
- Visit **Huawei technical support website for enterprise business** and search for *Hardware Description* and *Troubleshooting Guide* in **Documentation**.
- Contact Huawei customer service center: **Enterprise user global service hotline and email address**.

