Network O&M

Foreword

- Routine maintenance and troubleshooting are required to ensure the proper running of network functions. Routine maintenance is preventive and planned maintenance, and troubleshooting is event-triggered maintenance.
- Good routine maintenance habits help network engineers detect risks in advance. Once an exception or fault occurs on a device, network engineers have to accurately collect events that occur during device running. Routine maintenance and troubleshooting depend on network information collection.
- This course describes the precautions for routine maintenance and common tools for information collection.

Objectives

- Upon completion of this course, you will be able to:
  - Understand check items in routine maintenance.
  - Understand the functions and features of Huawei datacom product information center.
  - Use common maintenance tools.

Contents

Overview of Network Maintenance

- The lifecycle of a network involves network planning and design, network implementation, and network maintenance and optimization. Network maintenance involves routine maintenance and troubleshooting.
- Routine maintenance is performed to prevent problems and minimize the possibility of unexpected faults. Fault causes found during the troubleshooting can be used as a reference for routine maintenance.
- Network maintenance is related to not only technology but also management. Routine maintenance does not pose high technical requirements for operators, but poses high requirements on operation standardization. Through routine maintenance, you can obtain various parameters of the network that is working properly, such as network device version, network bandwidth, and network security parameters, which helps you rectify faults.

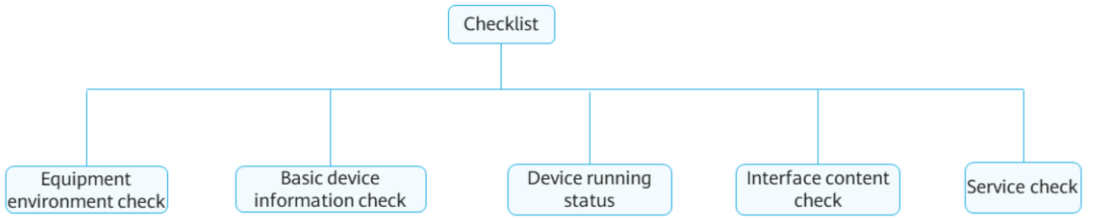
- Maintenance is also called "O&M", "operation", or "operation and maintenance."
- Network planning is the starting point of a project. Complete and detailed planning will lay a solid foundation for subsequent project implementation. Specific tasks in network planning are as follows:
  - In the project planning phase, investigate and understand the project background. Properly prepare for project implementation, which ensures the smooth progress of the project.
  - In the project planning phase, the implementation scope of the network project must be specified.
  - Draw up the project budget based on the project objective, project scope, and work content.
  - In the project planning phase, the network design guidelines must be specified to provide guidance and basis for subsequent network design.

Routine Maintenance — Content and Methods

- Routine maintenance involves the following:
  - Device running environment:
    - The hardware running environment refers to the peripheral environment that covers equipment rooms, power supply system, and heat dissipation system. The hardware running environment is the basis for the proper running of devices.
    - To maintain the device running environment, an engineer has to visit a site in person or uses some professional tools to observe and assess the environment.
  - Device software and hardware running status:
    - The running status of software and hardware is closely related to specific services running on a device. Network engineers must be familiar with common maintenance commands provided by the Versatile Routing Platform (VRP) that Huawei datacom devices.
    - Maintenance personnel can maintain the software and hardware of a device onsite or remotely mainly by running display commands.
- Either of the following methods can be used to perform routine maintenance:
  - Onsite observation: Observe the hardware running environment of devices.
  - Remote operation: Check the running status of the software and hardware of devices.

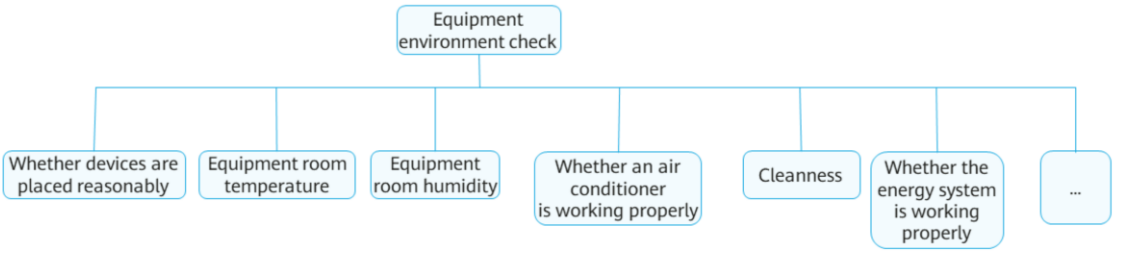
Routine Maintenance — Checklist

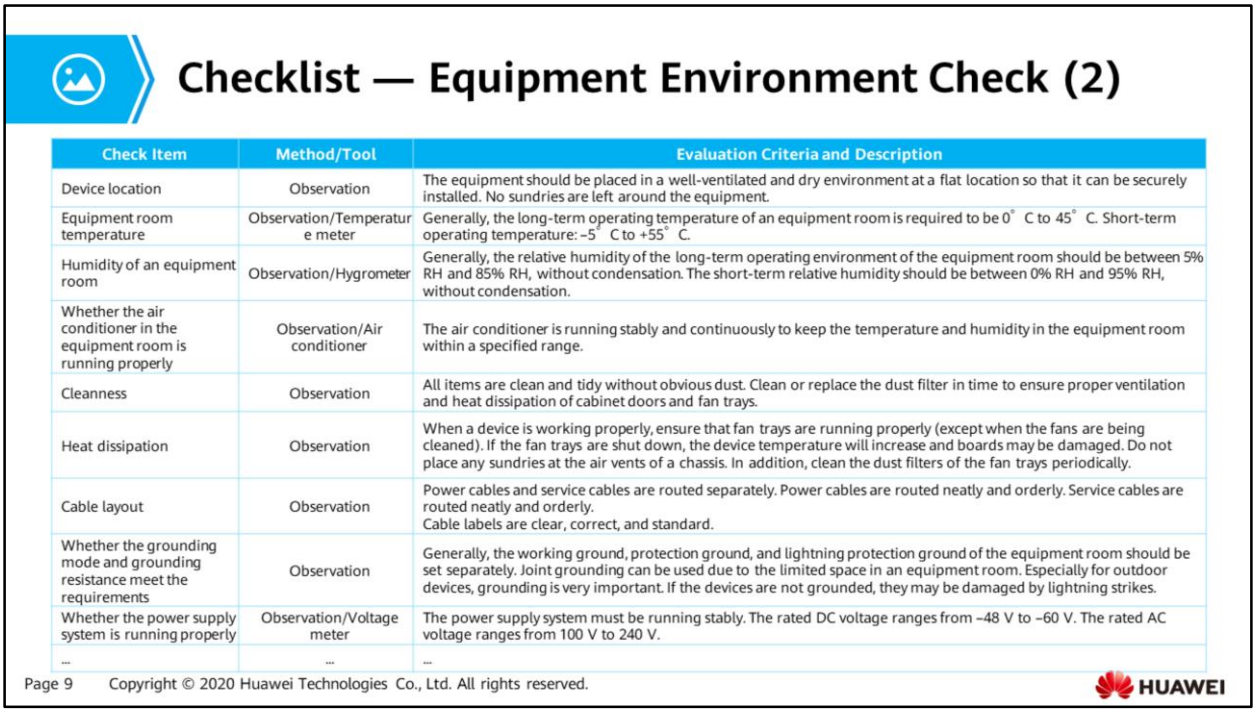
Routine maintenance is a planned routine task. It is necessary to prepare a checklist for operations. For details about the checklists for different network devices, see related product documentation. Items to be checked during routine maintenance can also be defined by customers.



Checklist — Equipment Environment Check (1)

- A proper running environment is the prerequisite for the proper running of a device.
- In practice, however, the device environment is not checked immediately once a fault occurs. Compared with other factors, the device environment is more stable and is less prone to faults.





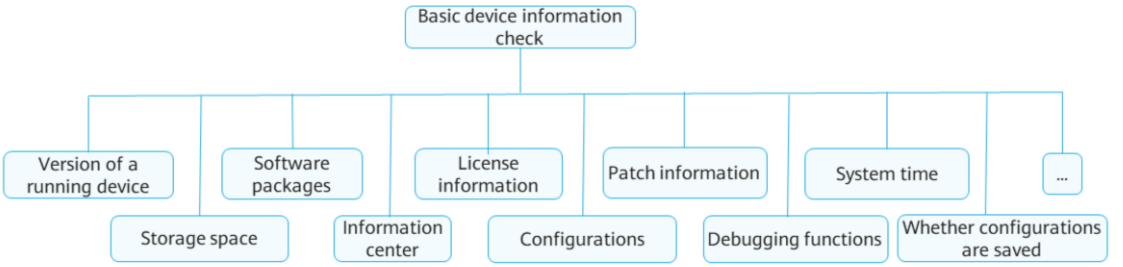
Checklist — Equipment Environment Check (2)

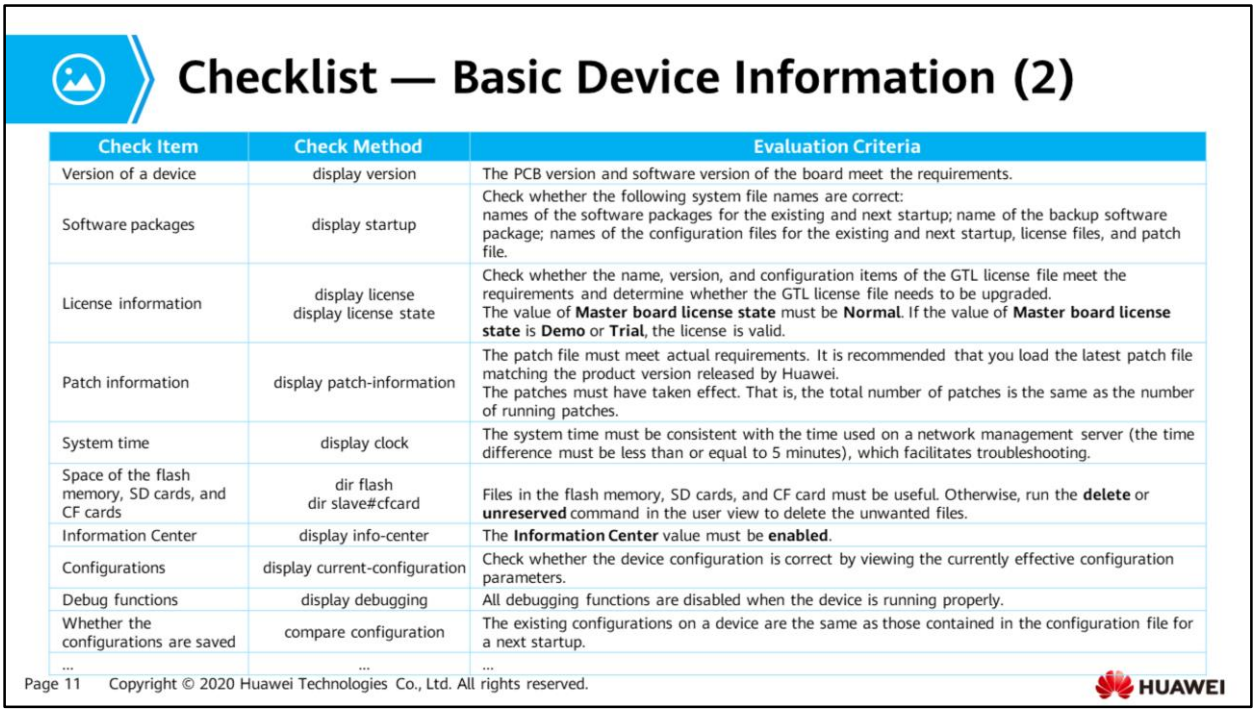
Check Item	Method/Tool	Evaluation Criteria and Description
Device location	Observation	The equipment should be placed in a well-ventilated and dry environment at a flat location so that it can be securely installed. No sundries are left around the equipment.
Equipment room temperature	Observation/Temperature meter	Generally, the long-term operating temperature of an equipment room is required to be 0° C to 45° C. Short-term operating temperature: –5° C to +55° C.
Humidity of an equipment room	Observation/Hygrometer	Generally, the relative humidity of the long-term operating environment of the equipment room should be between 5% RH and 85% RH, without condensation. The short-term relative humidity should be between 0% RH and 95% RH, without condensation.
Whether the air conditioner in the equipment room is running properly	Observation/Air conditioner	The air conditioner is running stably and continuously to keep the temperature and humidity in the equipment room within a specified range.
Cleanness	Observation	All items are clean and tidy without obvious dust. Clean or replace the dust filter in time to ensure proper ventilation and heat dissipation of cabinet doors and fan trays.
Heat dissipation	Observation	When a device is working properly, ensure that fan trays are running properly (except when the fans are being cleaned). If the fan trays are shut down, the device temperature will increase and boards may be damaged. Do not place any sundries at the air vents of a chassis. In addition, clean the dust filters of the fan trays periodically.
Cable layout	Observation	Power cables and service cables are routed separately. Power cables are routed neatly and orderly. Service cables are routed neatly and orderly. Cable labels are clear, correct, and standard.
Whether the grounding mode and grounding resistance meet the requirements	Observation	Generally, the working ground, protection ground, and lightning protection ground of the equipment room should be set separately. Joint grounding can be used due to the limited space in an equipment room. Especially for outdoor devices, grounding is very important. If the devices are not grounded, they may be damaged by lightning strikes.
Whether the power supply system is running properly	Observation/Voltage meter	The power supply system must be running stably. The rated DC voltage ranges from –48 V to –60 V. The rated AC voltage ranges from 100 V to 240 V.
...	...	...

- A proper running environment is the prerequisite for the proper running of a device.
- Temperature and humidity easily affect the proper running of devices. Standard equipment rooms should be equipped with thermometers and hygrometers, and check and record of the temperature and humidity should be performed on a daily basis.
- The cleanness and neatness of the equipment room also affect the proper running of the equipment.
    - Cleanness affects heat dissipation.
    - Tidiness refers to the proper layout of devices and cables. Devices must be installed and cables must be routed according to installation and deployment requirements. However, during network operation, temporary adjustments, such as temporary jumper tests, are often made. After such activities are taken for a period of time, the equipment room becomes disordered. The purpose of checking the equipment environment is to find out and rectify these problems in time.
- For nonstandard equipment rooms, checking the equipment environment more carefully. For example, check the cleanness and heat dissipation of equipment rooms on floors.
- The preceding check items may vary according to devices. For details, see the product documentation of each type of device.

Checklist — Basic Device Information (1)

Basic device information check involves checking the software version, license, and storage space.





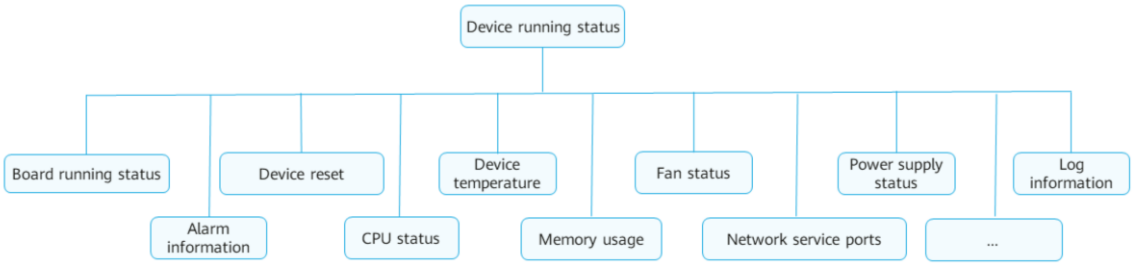
Checklist — Basic Device Information (2)

Check Item	Check Method	Evaluation Criteria
Version of a device	display version	The PCB version and software version of the board meet the requirements.
Software packages	display startup	Check whether the following system file names are correct: names of the software packages for the existing and next startup; name of the backup software package; names of the configuration files for the existing and next startup, license files, and patch file.
License information	display license display license state	Check whether the name, version, and configuration items of the GTL license file meet the requirements and determine whether the GTL license file needs to be upgraded. The value of **Master board license state** must be **Normal**. If the value of **Master board license state** is **Demo** or **Trial**, the license is valid.
Patch information	display patch-information	The patch file must meet actual requirements. It is recommended that you load the latest patch file matching the product version released by Huawei. The patches must have taken effect. That is, the total number of patches is the same as the number of running patches.
System time	display clock	The system time must be consistent with the time used on a network management server (the time difference must be less than or equal to 5 minutes), which facilitates troubleshooting.
Space of the flash memory, SD cards, and CF cards	dir flash dir slave#cfcard	Files in the flash memory, SD cards, and CF card must be useful. Otherwise, run the **delete** or **unreserved** command in the user view to delete the unwanted files.
Information Center	display info-center	The **Information Center** value must be **enabled**.
Configurations	display current-configuration	Check whether the device configuration is correct by viewing the currently effective configuration parameters.
Debug functions	display debugging	All debugging functions are disabled when the device is running properly.
Whether the configurations are saved	compare configuration	The existing configurations on a device are the same as those contained in the configuration file for a next startup.
...	...	...

- Software version running on a device:
  - The running software version of a device should be confirmed in project implementation. In normal cases, the version information does not change. Pay attention to any change in version information. This situation is usually caused by nonstandard management.
  - If a device is newly added, the software version may be different from the existing software version. Some devices may be upgraded or downgraded due to other reasons. Especially on a large-scale network, the same type of device may run different versions. In this case, verify that different versions can meet the same network function requirements.
- Startup information:
  - Multiple software packages of different versions or configuration files may be stored on a device. In this case, changing startup information may cause great risks to the proper running of the network. Once the device is restarted (for example, if power supply is faulty), the running of the entire network may be adversely affected.
- License information:
  - License rules vary according to devices. The licenses of some devices have validity periods.
- Storage space:
  - Although most devices provide storage space of dozens of GBs or even hundreds of GBs, storage resources are consumed when some files, such as log files, are continuously generated during device running. In some abnormal situations, for example, when a device is attacked or device information changes frequently, the number of log files increases sharply. If this phenomenon persists, the storage space of the device may be exhausted, and as a result, key information may be lost.

Checklist — Device Running Status (1)

- When checking the running status of a device, pay attention to the hardware running status, such as board status, power supply status, fan status, temperature, CPU usage, and memory usage. Alarm indicators on devices can help you find the abnormal status onsite.
- Check the running status of components such as cards, power modules, and fan trays according to instructions provided by manufacturers. If necessary, contact the manufacturers for instructions. If hardware is faulty, contact vendors who may replace hardware or provide support for troubleshooting.



Checklist — Device Running Status Check (2)

Check Item	Check Method	Evaluation Criteria
Board running status	display device	Check whether the in-position status and working status of a board are normal. The **Online** value is **Present**. The **Power** value is **PowerOn**. The **Register** value is **Registered**. The value of **Alarm** is **Normal**.
Device reset	display reset-reason display reboot-info	Check the reset information (including the reset time and cause) to ensure that no abnormal reset occurs.
Device temperature	display temperature display environment	The current temperature of each module must be between the upper and lower thresholds.
Fan status	display fan	If the **Present** value is **YES**, the status is normal.
Power supply status	display power	If the **State** value is **Supply**, the power supply is normal.
FTP network service port	display ftp-server	The FTP network service ports that are not used must be disabled.
Alarm information	display alarm all	No alarm is generated. If an alarm is generated, record the alarm. If a major or critical alarm is generated, analyze and handle the alarm immediately.
CPU status	display cpu-usage	The CPU usage of each module is normal. Pay special attention to CPU usage that exceeds 80%.
Memory usage	display memory-usage	Memory usage must be normal. Pay special attention to the **Memory Using Percentage** value that exceeds 60%.
Log information	display logbuffer display trapbuffer	No exception information exists.
Master/Slave status of main control boards	display switchover state	If both the master and slave main control boards are equipped, the status information about both the boards must be correct. After a master/slave main control board switchover is complete and the device is working properly, this command is expected to display **realtime or routine backup** for the master main control board.
...	...	...

Checklist — Device Interface Check

- Network devices exchange data packets through interfaces. Interface information is very important. Abnormal interface status adversely affects network functions.
- If a large number of error packets are generated on an interface and the number of error packets increases continuously within a short period of time, a link (as well as physical interfaces) may be faulty.

Check Item	Check Method	Evaluation Criteria
Error packets on an interface	display interface	When services are running, check whether there are error packets on the interface, including CRC error packets.
Interface negotiation mode	display interface	The negotiation mode of the interface must be correct. The negotiation modes of the two interfaces on both ends must be the same. The half-duplex mode is not allowed.
Interface configuration	display current-configuration interface	Interface configuration items, such as the duplex mode, negotiation mode, rate, and loopback configuration, must be correct.
Interface status	display interface brief	The up/down status of an interface meets planning requirements. Check whether the traffic sent or received by the interface is too heavy. (The long-term traffic volume is greater than 70% of the interface capacity.)
PoE power supply	display port power-state interface *interface-type interface-number*	The PoE power supply status of an interface must be normal. The **Delivering-power** value must be **Delivering-power** for an interface whose **Port power ON/OFF** value is **ON**.
...	...	...

Checklist — Service Running Status Check

Service running status refers to the running status of network protocols.

Check Item	Check Method	Evaluation Criteria
MAC address table information	display mac-address	The MAC address table information must be correct.
VLAN information	display vlan	Basic information about all VLANs must be correct.
Routing table information	display ip routing-table	Check the default routes or others specific routes, information of which is used for remote fault locating. If the devices at the same layer of a network run the same routing protocol, the number of routes on each device should be close. (The number of routes may vary according to the number of static routes.)
OSPF neighbor status IS-IS neighbor status BGP peer status	display ospf peer display isis peer display bgp peer	OSPF neighbor status: The **State** value is **Full** or **2-Way**. IS-IS neighbor status: The **State** value is **Up**. BGP peer status: The **State** value is **Established**.
VRRP status	display vrrp display vrrp statistics	The VRRP status of devices in a VRRP group cannot be **Master** at the same time.
MSTP status	display stp brief	The **STP Status** values of the designated port and root port are **FORWARDING**.
...	...	...

Routine Maintenance — Software and Configuration Backup

- The purpose of backup is to restore network functions in extreme cases. Backup is to transfer files to a backup server. There are many backup methods. Generally, a device functions as an FTP or TFTP client and transfers files to a server through the CLI.
- You are advised to back up configuration files every week. In addition, back up the configuration file before the configuration on a device is changed.
- Both software and configuration (including license files) need to be backed up. The purpose of backup is to restore network functions in extreme cases.
  - Service restoration will be delayed without a backup configuration file in case of a hardware fault-induced restart failure or replacement by a device of the same model.
  - The software package also needs to be backed up. The software package of a specific product and a specific version is backed up only once. You can also obtain the corresponding software package from the vendor's official website and store it on a local computer.
  - A license file is a special file that is configured for a specific product. If the license file is missing due to an incident (for example, by mistake), a new license file must be applied for through the vendor's process. In this process, some proof materials (such as the contract number and device SN) must be provided. Consequently, the application period is long. If a backup license file is available, the license file can be quickly restored on the device.

Contents

HUAWEI

Information Center Overview

- The information center is an information hub on a device. Log, trap, and debugging information generated by the device are sent to the information center. The information center manages and controls all information and flexibly outputs the information.
- The information center can be configured to classify or filter the information by type and severity and to output the information in different directions (such as the console, user terminal, and log host). In this way, users or network administrators can collect device information, which is used to monitor the device running status and locate faults.

Information Type	Description
Log information	Logs record information about user operations, system faults, and system security. • User logs: record user operations and system running information. • Security logs: record information about account management, protocols, attack defense, and attack defense status. • Diagnostic logs: record information that helps locate faults.
Trap information	Traps are notifications generated once a system detects faults. Traps record system status information, for example, faults. This type of information is different from log information. The major characteristic of trap information is that administrators must be notified and alerted immediately, and trap information is sensitive to time.
Debugging information	Debugging information is output by a device and used to monitor the internal running of the device. The device can generate debugging information only after the debugging of a specific module is enabled.

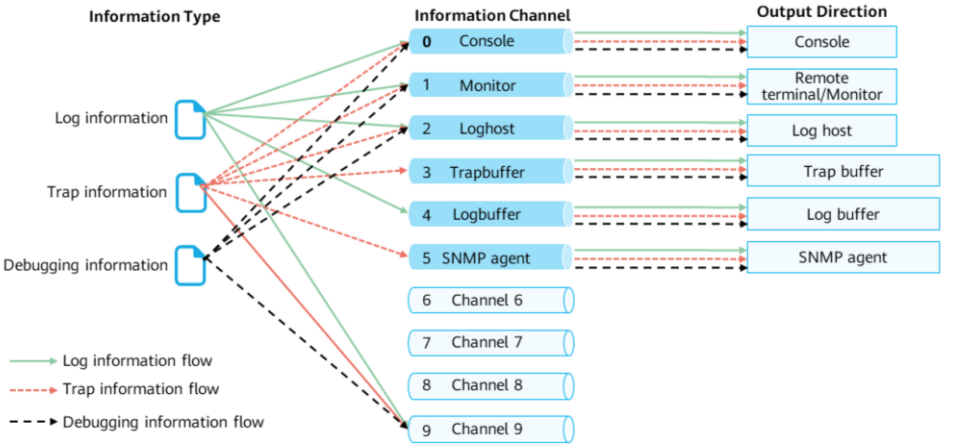
Information Severity

- When a large amount of information is generated on a device, it is difficult to tell which information can be ignored and which information indicates a fault to be dealt with. Information is classified into different levels, which helps users efficiently take measures or shield unnecessary information.
- Information is classified into eight levels based on its severity and urgency. A lower value indicates a higher severity level.

Value	Severity	Description
0	Emergency	A fatal exception occurs on a device, and the device cannot recover. You must restart the device. For example, a program exception causes the device to restart and memory usage is incorrect.
1	Alert	A major exception occurs on a device and measures must be taken immediately. For example, the memory usage of a device reaches a specified upper limit.
2	Critical	The device is abnormal. You need to take measures to handle a fault or analyze causes. For example, the memory usage of a device is lower than a specified lower threshold or the device is unreachable after BFD detection is performed.
3	Error	Incorrect operations or abnormal device processes occur, which do not affect subsequent services. However, you need to pay attention to and analyze causes. For example, incorrect commands, incorrect passwords, or incorrect protocol packets are detected.
4	Warning	A device running exception may cause a service fault. For example, a routing process is disabled, a packet loss event is detected by BFD or incorrect protocol packets are detected.
5	Notification	Key operation information about the proper running of the device. For example, the interface is shut down, neighbor discovery is performed, and the protocol state machine changes normally.
6	Informational	General operation information about the proper running of the device. For example, a user runs a display command.
7	Debugging	Informational only, and no action is required.

Information Output

The information generated by a device can be output to a remote terminal, console, log buffer, log file, or SNMP agent. To facilitate the output control of information in different directions, the information center defines 10 information channels. The information is output separately in each direction.



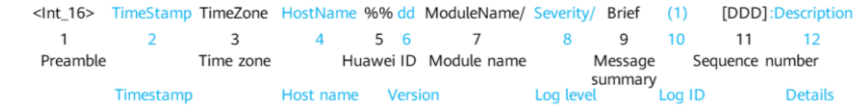
- You can configure information output rules as needed to control the output of various types and levels of information along information channels in different output directions.
- A remote terminal is used to log in to a device through a VTY interface to receive logs, traps, and debugging information, facilitating remote maintenance.

Information Filtering

- The information center can filter information to flexibly control the output of information. When a device is running properly, each module reports information during service processing. To filter out unnecessary information about service modules or information of specified levels, you can configure the information filtering function.
- The information center uses the information filtering table to filter information along the channels. The information filtering table is used to filter the information output in each direction based on the Information Severity, level, and source.
- The information filtering table provides the following information:
  - Sequence number of an information module
  - Status of the log output function
  - Level of log information to be output
  - Trap output status
  - Level of trap information to be output
  - Debugging information output status
  - Level of debugging information to be output

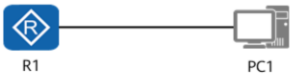
Information Output Format

- Log output format



- Trap output format

Application Scenarios of the Information Center

Outputting logs to a log host	Outputting traps to an NMS	Outputting debugging information to the console
		
The information center outputs logs of a specified level to a log host. Maintenance personnel can obtain the running status of the device by querying logs.	The information center outputs traps to an NMS. The NMS monitors the running status of a device based on the received traps.	The information center sends debugging information to the console. Maintenance personnel can obtain the running status of a device by checking the debugging information.

Information Center Commands (1)

1. Enable the information center function.

   [HUAWEI] **info-center enable**

   By default, the information center is enabled.

2. Specify the name of an information channel with a specified ID.

   [HUAWEI] **info-center channel** *channel-number* **name** *channel-name*

3. Enable a device to filter logs or traps.

   [HUAWEI] **info-center filter-id** { *id* | **bymodule-alias** *modname alias* } [**bytime** *interval* | **bynumber** *number*]

   bymodule-alias: outputs log or trap information of a module with a specified name.

4. Enable the device to send log information to the log buffer.

   [HUAWEI] **info-center logbuffer**

   By default, a device is enabled to send logs to the log buffer.

- Enable a device to send information to a log host.
  - [HUAWEI] **info-center loghost ip-address** { **source-ip** *source-ip-address* } | **transport { udp | tcp ssl-policy** *policy-name* }]

Information Center Commands (2)

1. Configure an information channel used to output information.

   [HUAWEI] **info-center** { **console** | **logbuffer** | **logfile** | **monitor** | **snmp** | **trapbuffer** } **channel** { *channel-number* | *channel-name* }

2. Enable the terminal to display information sent by the information center.

   [HUAWEI] **terminal monitor**

   By default, the console is enabled to display information, and a user terminal is disabled from displaying information.

3. Enable the terminal to display debugging information.

   [HUAWEI] **terminal debugging**

   By default, a terminal is disabled from displaying debugging information.

4. Enable the terminal to display log information.

   [HUAWEI] **terminal logging**

   By default, a terminal is enabled to display log information.

Information Center Commands (3)

1. Query information recorded in the log buffer.

   [HUAWEI] **display logbuffer** [**size** *size* | **slot** *slot-id* | **module** *module-name* | **security** | **level** { *severity* | *level* }]

2. Query information in a log file.

   [HUAWEI] **display logfile** *file-name* [*offset* | **hex**]

3. Query information recorded in the trap buffer of the information center.

   [HUAWEI] **terminal debugging**

4. Query debugging information that can be sent by a device.

   [HUAWEI] **display debugging**

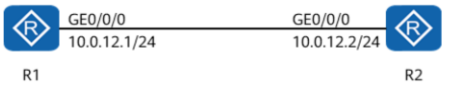
5. Query the output direction configuration of the information center.

   [HUAWEI] **display info-center**

Example for Configuring the Information Center

Enable OSPF on GE 0/0/0 of R1 and R2. Log in to R1 through the console and check the following information on R1:

- Trap information
- Log information
- Debugging information




```
<R1> terminal monitor //By default, the console is enabled to display information.
<R1> terminal logging //By default, a terminal is enabled to display log information.
<R1> terminal debugging //By default, the terminal is disabled from displaying debugging information.
<R1> terminal trapping //By default, the terminal is enabled to display trap information.
<R1> system-view
[R1] info-center enable //By default, the information center function is enabled.
```

Information Channel

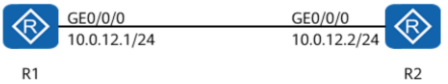
```
<R1> display channel
 channel number: 0,  channel name: console
MODU_ID  NAME     ENABLE  LOG_LEVEL      ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
 ffff0000 default  Y       warning        Y       debugging   Y       debugging
 channel number: 2,  channel name: loghost
MODU_ID  NAME     ENABLE  LOG_LEVEL      ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
 ffff0000 default  Y       informational  Y       debugging   N       debugging
 channel number: 3,  channel name: trapbuffer
MODU_ID  NAME     ENABLE  LOG_LEVEL      ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
 ffff0000 default  N       informational  Y       debugging   N       debugging
 channel number: 4,  channel name: logbuffer
MODU_ID  NAME     ENABLE  LOG_LEVEL      ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
 ffff0000 default  Y       warning        N       debugging   N       debugging
  ...      ...      ...     ...
```

Information is classified into eight levels based on its severity and urgency. The more serious the information is, the lower the severity level is.
By default:

- Warning is level 4, which indicates an abnormal point in device running, which may cause service faults and requires attention. For example, a routing process is disabled, a packet loss event is detected by BFD or incorrect protocol packets are detected.
- Debugging is level 7, which indicates general information about the proper running of a device. No action is required for such information.

R1 provides four channels: console, log host, trap buffer, and log buffer.

Traps



Query information recorded in the trap buffer of the information center.

```
<R1> display trapbuffer
Trapping buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 256
Channel number: 3, Channel name: trapbuffer
Dropped messages: 0
Overwritten messages: 0
Current messages: 1
#Jun 23 2020 08:38:51-08:00 R1 LLDP/4/ADDCHGTRAP:OID: [OID] Local management add
ress is changed. (LocManIPAddr=[IPADDR])
```

By default, traps are output through information channel 3.

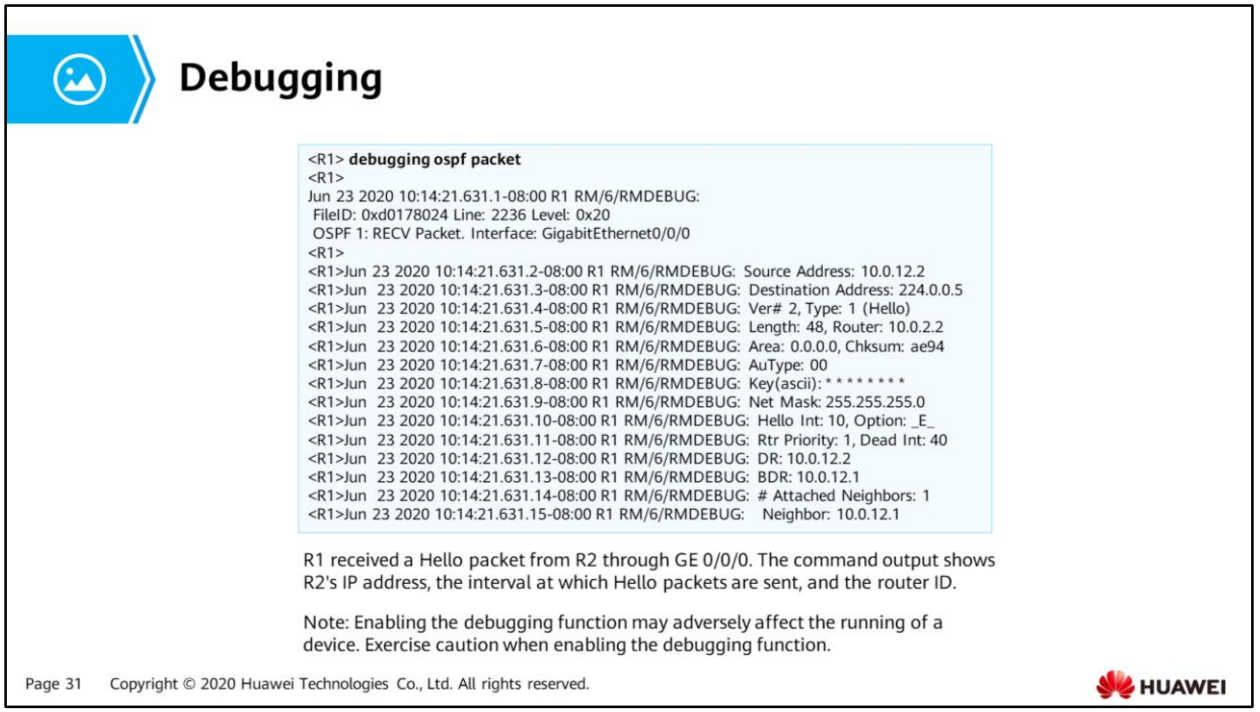
Logs

```
<R1> display log cli all
------------------------------------------------------------------------------
No.   UserName                  Domain          IP-Address
  35                            --              Serial
Time: 2020-06-23 09:34:35-08:00
Cmd:  quit
------------------------------------------------------------------------------
No.   UserName                  Domain          IP-Address
  34                            --              Serial
Time: 2020-06-23 09:34:33-08:00
Cmd:  ip address 10.0.12.1 24
------------------------------------------------------------------------------
No.   UserName                  Domain          IP-Address
  33                            --              Serial
Time: 2020-06-23 09:34:29-08:00
Cmd:  interface gi 0/0/0
------------------------------------------------------------------------------
No.   UserName                  Domain          IP-Address
  32                            --              Serial
Time: 2020-06-23 09:34:26-08:00
Cmd:  system-view
```

Query all commands entered by users. As shown in the figure, the IP address of GE 0/0/0 on R1 has been configured.

```
<R1>
Jun 23 2020 10:09:57-08:00 R1 %%01OSPF/4/NBR_CHANGE_E(l)[0]:Neighbor
changes event: neighbor status changed.
(ProcessId=256,NeighborAddress=10.0.12.2, NeighborEvent=HelloReceived,
NeighborPreviousState=Down, NeighborCurrentState=Init)
<R1>
Jun 23 2020 10:09:57-08:00 R1 %%01OSPF/4/NBR_CHANGE_E(l)[1]:Neighbor
changes event: neighbor status changed.
(ProcessId=256,NeighborAddress=10.0.12.2, NeighborEvent=2WayReceived,
NeighborPreviousState=Init, NeighborCurrentState=2Way)
...
<R1>
Jun 23 2020 10:09:57-08:00 R1 %%01OSPF/4/NBR_CHANGE_E(l)[5]:Neighbor
changes event: neighbor status changed.
(ProcessId=256,NeighborAddress=10.0.12.2, NeighborEvent=LoadingDone,
NeighborPreviousState=Loading, NeighborCurrentState=Full)
```

The OSPF neighbor status change of R1 is automatically displayed in the log format on the console port.



- To facilitate display, the debugging information displayed on this page is adjusted.
- The content of the Hello packet sent by R1 through GE 0/0/0 is as follows:

  <R1>

  Jun 23 2020 10:14:21.751.1-08:00 R1 RM/6/RMDEBUG:

  FileID: 0xd0178025 Line: 559 Level: 0x20

  OSPF 1: SEND Packet. Interface: GigabitEthernet0/0/0

  <R1>Jun 23 2020 10:14:21.751.2-08:00 R1 RM/6/RMDEBUG: Source Address: 10.0.12.1

  <R1>Jun 23 2020 10:14:21.751.3-08:00 R1 RM/6/RMDEBUG: Destination Address: 224.0.0.5

  <R1>Jun 23 2020 10:14:21.751.4-08:00 R1 RM/6/RMDEBUG: Ver# 2, Type: 1 (Hello)

  <R1>Jun 23 2020 10:14:21.751.5-08:00 R1 RM/6/RMDEBUG: Length: 48, Router: 10.0.12.1

  <R1>Jun 23 2020 10:14:21.751.6-08:00 R1 RM/6/RMDEBUG: Area: 0.0.0.0, Chksum: ae94

  <R1>Jun 23 2020 10:14:21.751.7-08:00 R1 RM/6/RMDEBUG: AuType: 00

  <R1>Jun 23 2020 10:14:21.751.8-08:00 R1 RM/6/RMDEBUG: Key(ascii): * * * * * * * *

  <R1>Jun 23 2020 10:14:21.751.9-08:00 R1 RM/6/RMDEBUG: Net Mask: 255.255.255.0

Contents

Packet Information Obtaining

When the service traffic of a device becomes abnormal, for example, the traffic status is inconsistent with the traffic model, you can use the packet information obtaining function for analysis. In this way, invalid packets can be processed in time to ensure proper transmission of network data.


```
<R1> system-view
[R1] capture-packet interface gigabitethernet 0/0/0 destination terminal
Info: Captured packets will be shown on terminal.
[R1]ping 10.0.12.2
[R1]
  Packet: 1
---------------------------------------------------------------
ff ff ff ff ff ff 00 e0 fc 9f 4b 1d 08 06 00 01
08 00 06 04 00 01 00 e0 fc 9f 4b 1d 0a 00 0c 02
00 00 00 00 00 00 0a 00 0c 02 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
---------------------------------------------------------------

  Packet: 2
---------------------------------------------------------------
ff ff ff ff ff ff 00 e0 fc 9f 4b 1d 08 06 00 01
08 00 06 04 00 01 00 e0 fc 9f 4b 1d 0a 00 0c 02
00 00 00 00 00 00 0a 00 0c 02 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
---------------------------------------------------------------
```

ARP request packets sent by R2
Destination MAC address: ffff-ffff-ffff
Source MAC address: 00e0-fc9f-4b1d
Type: 0806, indicating ARP

HUAWEI

- Only one packet information obtaining instance can run at a time. That is, if a previous process is not complete, a next process cannot be started.
- The rate of packets whose information is to be obtained is limited. If burst traffic exceeds the rate limit configured for obtained packet information, packet loss may occur.
- The **capture-packet** command obtains header information in the service packets that match the configured rules and sends the obtained information to the terminal for display or saves the obtained information on a local device.
  - **capture-packet interface** *interface-type interface-number* [**acl** *acl-number*] **destination** { **terminal** | **file** *file-name* } * [**car cir** *car-value* | **time-out** *time* | **packet-num** *number* | **packet-len** { *length* | **total-packet** }] *
    - **terminal**: sends the obtained information to the terminal for display.
    - **file** *file-name*: saves the obtained information in a specified file.

Contents

LLDP Application Example

- Link Layer Discovery Protocol (LLDP) is a link layer topology discovery protocol defined in IEEE 802.1ab. It can accurately locate the interfaces on devices and the interfaces connected to other devices, and display information about paths between clients, switches, routers, application servers, and network servers.
- In actual networking, you can use LLDP to obtain physical connection information of devices.

Enable LLDP on R1 and R2.

```
<R1> system-view
[R1] lldp enable
```

```
<R2> system-view
[R2] lldp enable
```

```
<R1> display lldp neighbor
GigabitEthernet0/0/0 has 1 neighbors:

Neighbor index               : 1
Chassis type                 : macAddress
Chassis ID                   : 00e0-fc9f-4b1d
Port ID type                 : interfaceName
Port ID                      : GigabitEthernet0/0/0
Port description             : HUAWEI, AR Series, GigabitEthernet0/0/0 Interface
System name                  : R2
System description           : Huawei AR2220 Huawei Versatile Routing Platform
                               Software VRP (R) software,Version 5.130 (AR2220
                               V200R003C00) Copyright (C) 2011-2012 Huawei
                               Technologies Co., Ltd

Management address type      : ipV4
Management address           : 10.0.12.2
Expired time                 : 109s
```

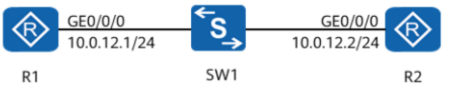
The preceding command output shows that GE 0/0/0 on R1 is connected to GE 0/0/0 on R2. R2 is an AR2220, and GE 0/0/0's IP address is 10.0.12.2.

Contents

HUAWEI

Traffic Statistics Collection

Traffic statistics collection helps you learn about traffic passing and discarding after a traffic policy is applied. You can analyze and determine whether a traffic policy is properly applied, and locate faults.



1. Configure an ACL rule.
[R2] **acl 2000**
[R2-acl-basic-2000] **rule permit source 10.0.12.1 0**
[R2-acl-basic-2000] **quit**
2. Configure a traffic classifier.
[R2] **traffic classifier c1**
[R2-classifier-c1] **if-match acl 2000**
[R2-classifier-c1] **quit**
3. Configure a traffic behavior.
[R2] **traffic behavior b1**
[R2-behavior-b1] **statistic enable**
[R2-behavior-b1] **quit**

4. Create a traffic policy.
[R2] **traffic policy p1**
[R2-trafficpolicy-p1] **classifier c1 behavior b1**
[R2-trafficpolicy-p1] **quit**
5. Apply the traffic policy to an interface.
[R2] **interface GigabitEthernet 0/0/0**
[R2-GigabitEthernet0/0/0] **traffic-policy p1 inbound**
[R2-GigabitEthernet0/0/0] **quit**

```
R2]display traffic policy statistics interface GigabitEthernet 0/0/0 inbound
 Interface: GigabitEthernet0/0/0
 Traffic policy inbound: test
 Rule number: 1
 Current status: OK!
Item                Sum(Packets/Bytes)        Rate(pps/bps)
-------------------------------------------------------------
Matched             0/0                       0/0
Passed              0/0                       0/0
Dropped             0/0                       0/0
Filter              0/0                       0/0
CAR                 0/0                       0/0
Queue Matched       0/0                       0/0
```

The preceding command output shows that R2 does not receive ICMP messages. Based on the preceding information, you can check whether a physical link is faulty or whether the VLAN configuration of SW1 is incorrect.

Quiz

1. (Multiple) Which of the following statements about network maintenance functions are correct?
   A. Routine maintenance is a type of preventive work.
   B. Routine maintenance helps you obtain the network baseline, which lays a solid foundation for troubleshooting.
   C. Routine maintenance poses high technical requirements for operators, but does not pose high requirements for operation standardization.
   D. Network maintenance is not only a technical issue, but also a management issue.
2. (TorF) packet information obtained by a tool can be displayed only on the CLI of a device and cannot be saved in a file.
3. (TorF) R1 and R2 are directly connected. If the interface IP addresses of R1 and R2 are on different network segments, the host names of the two devices cannot be obtained using LLDP.

1. ABD
2. F
3. F

Summary

- Network maintenance includes routine maintenance and troubleshooting. This course describes the routine maintenance and its check items, such as equipment environment check, basic equipment information check, and equipment running status check. During routine maintenance, you must periodically back up device configurations and software packages. By doing so, you can use the backup data to restore network functions in extreme situations.
- Troubleshooting is network maintenance driven by fault events. A large amount of information needs to be collected during troubleshooting. A device provides the information center function. The information center provides log, trap, and debugging information and 10 information channels. You can configure rules for outputting information to control the output of various types and levels of information through different information channels.
- This course also introduces tools for obtaining information, such as Packet Information Obtaining, traffic statistics collection, and LLDP. The use of these tools helps you efficiently rectify faults.


Thank You
www.huawei.com