Network Fault Troubleshooting

Foreword

- Digital transformation of medium- and large-sized enterprises is implemented using multiple technologies, such as cloud computing, big data, artificial intelligence (AI), and Internet of Things (IoT). These technologies are all supported by data communications networks. A stable data communications network requires fully prepared network design, construction, and maintenance.
- An enterprise data communications network accommodates various types of devices that are connected by multiple types of physical links. In addition, to accurately forward data packets, the devices run multiple protocols. Network devices, cables, and protocols may encounter faults. How to quickly rectify faults is a basic skill of senior network engineers.
- This course describes common network faults, how to troubleshoot them in an effort to help network engineers build capabilities of troubleshooting faults in various scenarios.

Objectives

- Upon completion of this course, you will be able to:
  - Understand the troubleshooting methods.
  - Analyze loop faults.
  - Analyze failures to establish neighbor relationships of routing protocols.
  - Write a troubleshooting guide.

Contents

What Is a Network Fault?

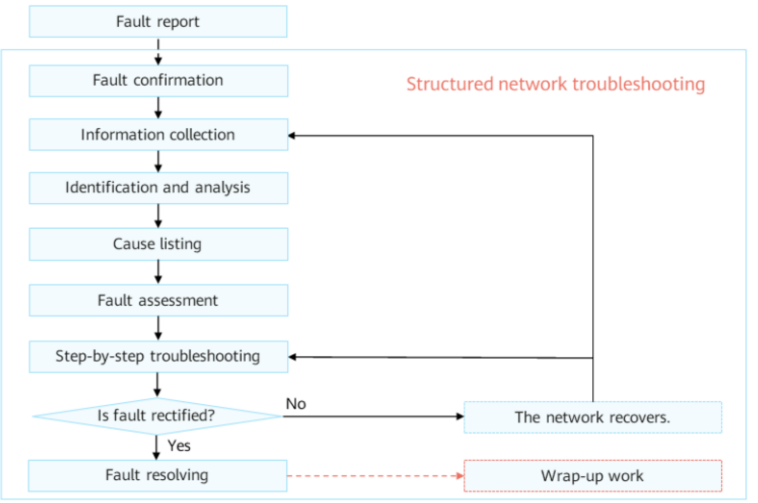
- A network fault refers to the phenomenon that a network loses a specific function and adversely affects services due to some reasons.
- From the perspective of users, any phenomenon that adversely affects services can be defined as a fault.
- The common fault symptoms and categories are as follows:

Symptom / Category	Alarm	Loop	Service Forwarding Failure	Service Interruption	Transient Service Interruption	Packet Loss	Protocol Anomaly	Protocol Flapping	Route Anomaly
Hardware	√			√		√			
Configuration		√	√				√		√
Network		√	√	√	√	√	√	√	√
Performance	√				√	√		√	√
Software							√		√
Interconnection		√	√				√		
Others	√		√	√	√	√			

- Mapping between the preceding fault symptoms and categories varies according to scenarios.

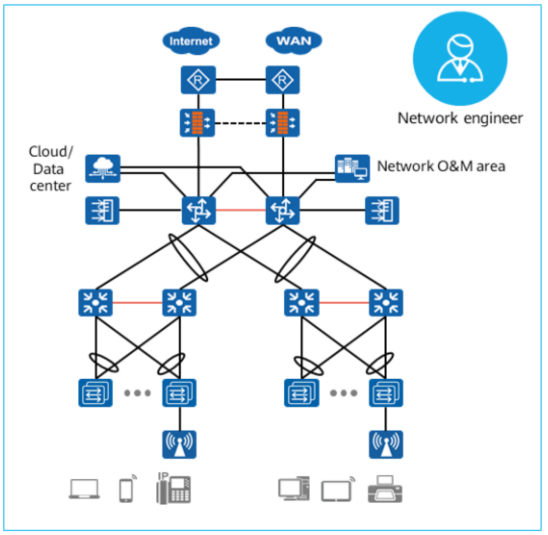
Contents

Structured Network Troubleshooting Process



- If an unstructured network troubleshooting is carried out, steps are performed repeatedly, leading to low efficiency even though a solution to the fault is found.
- In a complex network environment, a new fault may be caused due to an unstructured network fault rectification process, making network fault rectification more difficult.

Fault Report



- An enterprise has multiple departments, such as finance, human resource, logistics, marketing, and R&D departments. These departments need to communicate. To properly guarantee network operations, enterprises may take the following measures:
  - Large- and medium-sized enterprises set up network maintenance departments to build professional network teams.
  - To reduce expenses, small-sized enterprises do not set up an independent network maintenance department. Instead, they entrust their networks to professional network maintenance companies.
  - Contact device manufacturers for after-sales service.
- Generally, the person who first percepts network faults is from a department related to services, rather than a network maintenance engineer. Network engineers often receive calls for help, such as "the computer suddenly cannot access the Internet", "the web page cannot be displayed normally", and "the game is stuck".

What should network engineers do when they receive a call?

Fault Report — Proactive Communication and Confirmation

Fault reporter	Name, department, position, work content, computer location (floor, room, wireless or wired access), and website that the computer attempts to access.
Fault frequency	Check whether the fault occurs suddenly, occasionally, or frequently.
User operation	Operations performed by a user on a terminal before and after a fault occurs. For example, the IP address and DNS parameters are changed, desktop firewall software is installed, and security control software is installed.

Ask a user for the preceding information through a phone and record the information in a troubleshooting report.

- Why do we need to know the positions and work content of users?
  - In an enterprise environment, network access permissions to be granted vary according to positions. Even users of the same position may have only the permission to use network services related to their work content.

Fault Confirmation

- Four factors for determining a fault:
  - Subject: network service that becomes faulty
  - Symptom: symptom of the fault
  - Time: the time when a fault was found and the fault occurrence time estimated by professional personnel
  - Location: network component that becomes faulty
- Describe the fault symptom accurately.
- Ultimately, check whether the fault is within the responsibility scope, that is, whether related permissions have been granted to rectify the fault.

- Why do we need to confirm a fault?
  - The user description may be ambiguous, and the reported fault may not be the actual faulty point. In this situation, experienced engineers have to confirm the fault.

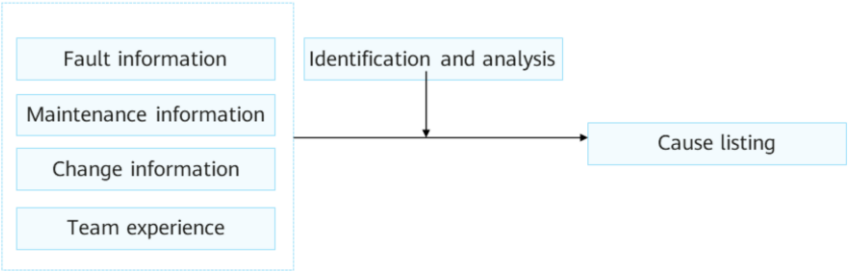
Information Collection

- Which information needs to be collected?
  - In the information collection phase, fault-related information, such as documents and network changes, is collected.
- How to collect the information:
  - Run commands on an involved device. Use information collection tools, such as the packet information obtaining tool and network management software.
- Obtaining permissions:
  - In a network environment that poses high requirements on information security, information collection must be authorized. Sometimes, a written authorization file must be signed.
- Risk assessment in the information collection phase:
  - Some information collection operations, such as running a debug command on a router or switch, may cause high CPU usage. In worse cases, a device may even stop responding to instructions, causing more faults. When collecting information, you must evaluate risks, balance the risks of introducing new faults and the urgency of rectifying existing faults, and notify users of the risks. Then, users determine whether to collect information in case of high risks.

Identification and Analysis

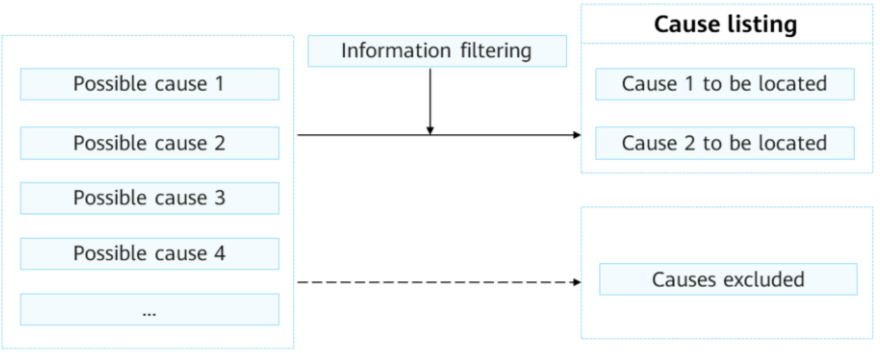
In the identification and analysis phase, the collected information is analyzed and sorted.

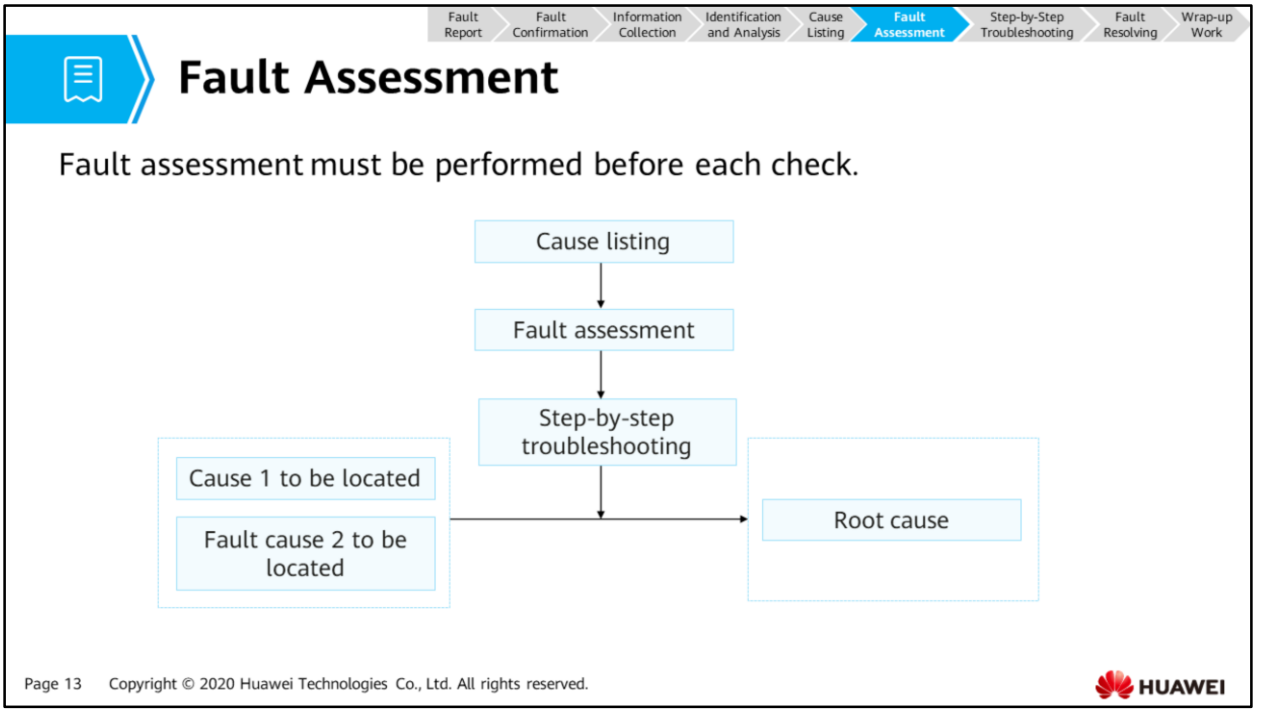
- By summarizing the fault, maintenance, and version-specific change information and using team (or personal) experience, you can obtain the list of possible causes for network faults.



Cause Listing

In the cause listing phase, you must list all possible fault causes, sort out the most likely causes, and exclude the least possible causes to narrow down the troubleshooting scope.

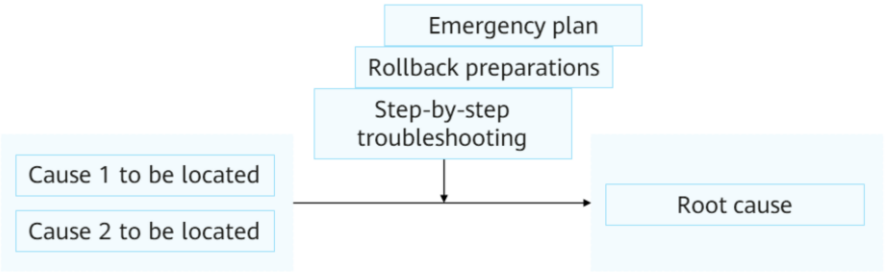




- A temporary network environment may need to be built for fault evaluation.
  - If a complex network fault cannot be rectified within a short period of time after being evaluated and a user wants to immediately restore network availability, you advise the user to temporarily skip the faulty node and build an alternative network environment.
  - When building a temporary network environment, fully consider the urgency of solving problems and the risk of bypassing certain security restrictions. Fully communicate with users and implement the environment only after obtaining permissions.

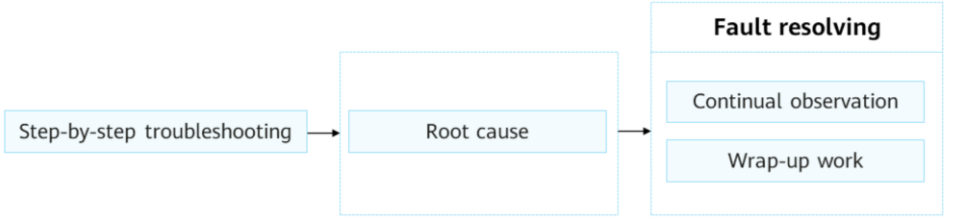
Step-by-Step Troubleshooting

- In the phase of step-by-step troubleshooting, the conflict between the urgency of solving problems and the risk of introducing new faults must be balanced. Therefore, users must be clearly informed of the risks that may be induced the process. Perform the check only after being authorized.
- In some cases, network changes may be involved in the verification process. In this case, a complete emergency plan and rollback preparations must be made.



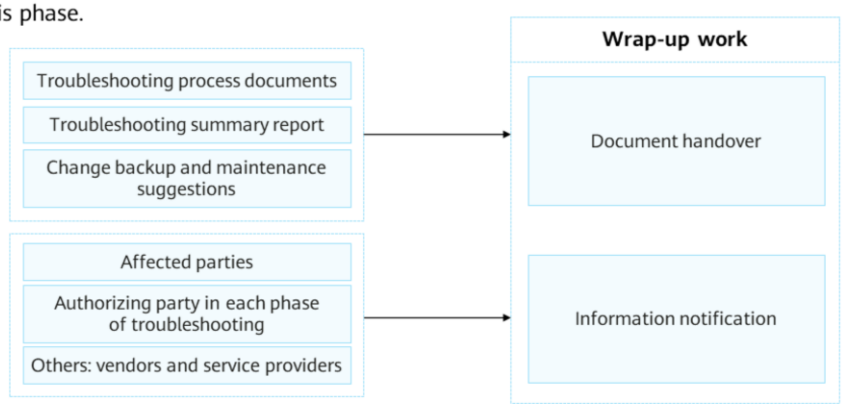
Fault Resolving

- After the root cause is found and the fault is rectified, the troubleshooting is complete.
- In a complex network environment, you have to observe the network for a period of time after the fault symptom disappears. On the one hand, you can confirm that the fault reported by the user has been rectified. On the other hand, you can confirm that no new fault is introduced during the troubleshooting process.



Wrap-up Work

Wrap-up work involves arranging related documents and sending notifications. Back up all changed configurations or software in the previous network troubleshooting process, and sort out and hand over troubleshooting documents. To prevent the same fault from occurring again, provide improvement suggestions for users in this phase.

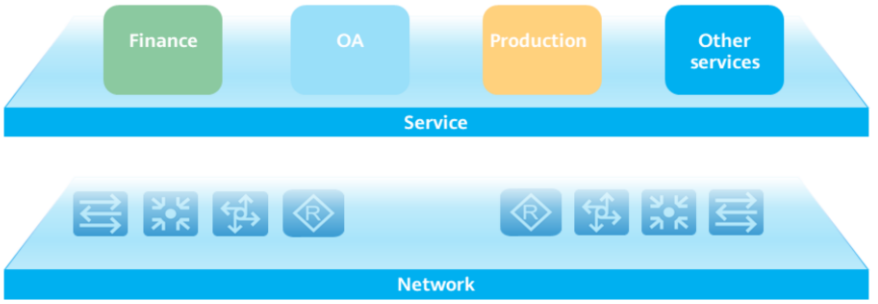


Contents

HUAWEI

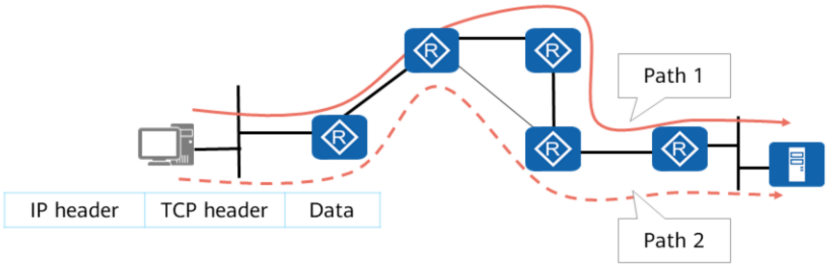
Service Traffic Path-Centric Troubleshooting Ideals

The path along which service traffic passes is usually designed in the network planning phase. You merely need to know the round-trip path of service traffic adversely affected by a network fault, trace the path, and rectify the fault step by step.



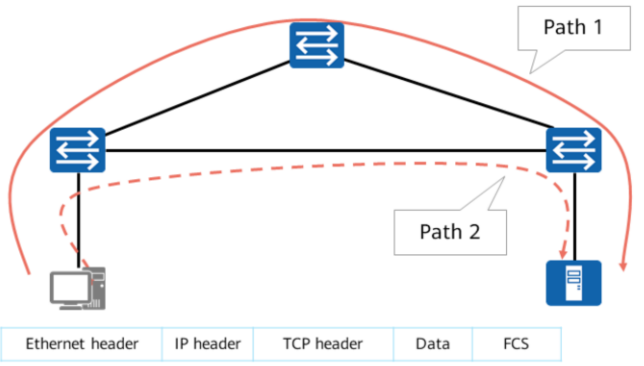
Determining a Service Traffic Path — Network Layer

Multiple paths may exist during packet forwarding. Therefore, you need to determine the path over which service traffic is transmitted based on the packet forwarding process.



Determining a Service Traffic Path — Data Link Layer

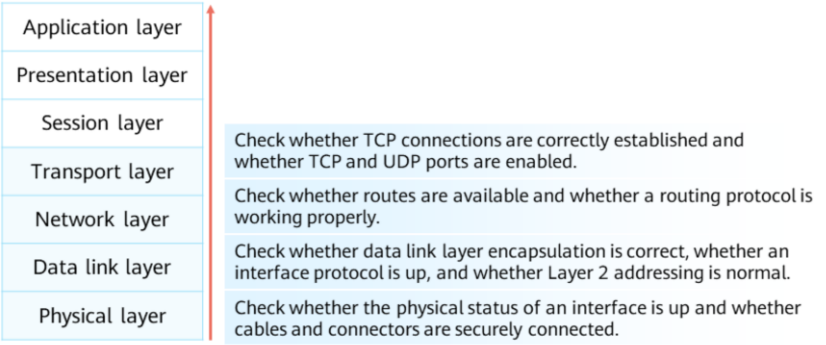
Check how data frames of service traffic are forwarded by switches on a Layer 2 network.



Ethernet header	IP header	TCP header	Data	FCS

Layered Troubleshooting Approach

The layered troubleshooting approach is simple, because all working models follow a simple rule: the upper-layer structure of any model can work properly as long as the lower-layer structure is working properly.



Configuration Comparison Approach

- Compare configurations, software versions, and hardware models in normal and faulty states to find differences.
- Network troubleshooting personnel with less experience will use this method more frequently in practice.

```
#
 sysname r1
#
isis 1
 network-entity 49.0001.1000.0000.0001.00
#
interface Serial4/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 isis enable 1
 isis timer hello 30
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
 isis enable 1
#
```

Compare them

```
#
 sysname r1
#
isis 1
 network-entity 49.0001.1000.0000.0001.00
#
interface Serial4/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 isis enable 1
 isis timer hello 120
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
 isis enable 1
#
```

Block-based Troubleshooting Approach

- The configuration files of Huawei network devices, such as switches and routers, are edited in a clear structure.
- If a fault occurs, you can narrow down the fault locating scope by classifying the fault into one or several categories:
  - Management (router name, password, service, and log)
  - Ports (address, encapsulation, cost, and authentication)
  - Routing protocols (static route, RIP, OSPF, BGP, and route import)
  - Policies (routing policy, policy-based routing, and security configuration)
  - Access (console port login, Telnet login, dial-up)
  - Applications (DNS, DHCP, and VPN configuration)

Block-based Troubleshooting Approach — Example

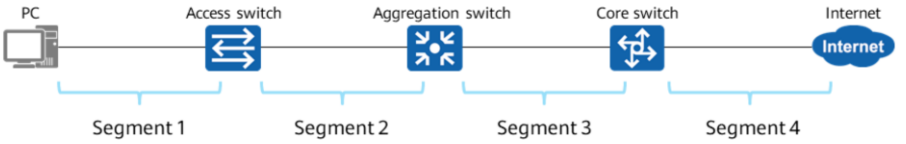
After the **display ip routing-table** command is run, only direct routes are displayed. What are possible causes?

```
<R2>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.12.1/32  Direct  0    0           D   10.0.12.1       Serial4/0/0
        10.0.12.2/32  Direct  0    0           D   127.0.0.1       Serial4/0/0
      10.0.12.255/32  Direct  0    0           D   127.0.0.1       Serial4/0/0
        10.0.23.0/24  Direct  0    0           D   10.0.23.2       GigabitEthernet0/0/0
        10.0.23.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
      10.0.23.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
```

The fault is related to the following blocks: routing protocols, policies, and ports. If no routing protocol is configured or a routing protocol is incorrectly configured, the routing table may be empty. If an ACL is incorrectly configured, route update may be adversely affected. If the IP address, mask, or authentication configuration of an interface is incorrect, the routing table may be incorrect.

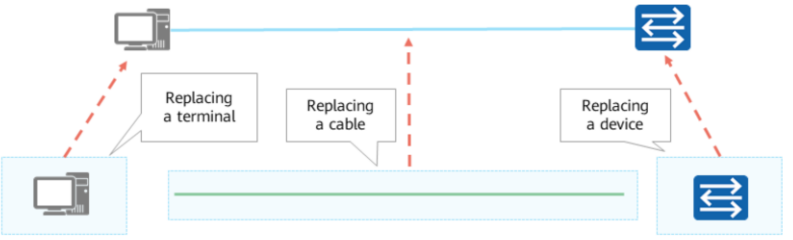
Segment-based Troubleshooting Approach

Since data packets may pass through multiple routers and physical links, each segment may encounter a fault. In this situation, the segment-based approach applies.



Replacement Approach

- The replacement approach is one of the most common methods for checking hardware problems.
- If a network cable may be faulty, replace it with another one in good condition. If an interface module may fail, replace it with another interface module that is working properly.



Requirements for Network Maintenance and Management Personnel

- Have an in-depth understanding of protocol requirements.
- Be able to guide a customer to describe the fault symptom and related information in detail.
- Fully understand the networks managed and maintained.
- Record troubleshooting documents and summarize troubleshooting experience.
- Be familiar with network troubleshooting approaches and combine them flexibly.

Quiz

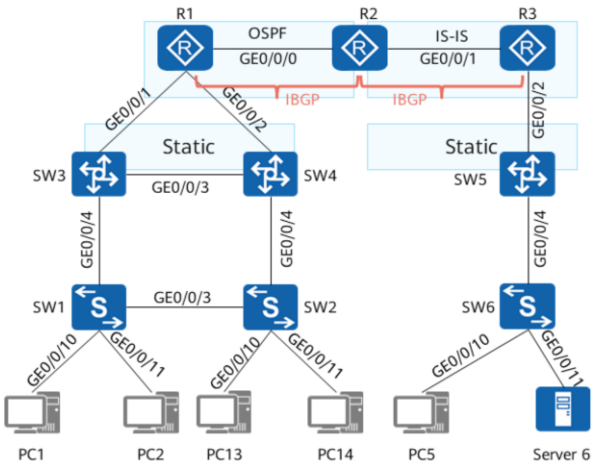
1. (Multiple) In the wrap-up work of a structured network troubleshooting process, which of the following parties should be notified of information?
   A. Related parties affected by the fault
   B. Authorizing parties in each phase of troubleshooting
   C. Manufacturer and service providers
   D. Other irrelevant personnel who are interested in the root cause
2. (TorF) On a large-scale network, the comparison approach is the most effective method for troubleshooting faults.

1. ABC
2. False

Contents

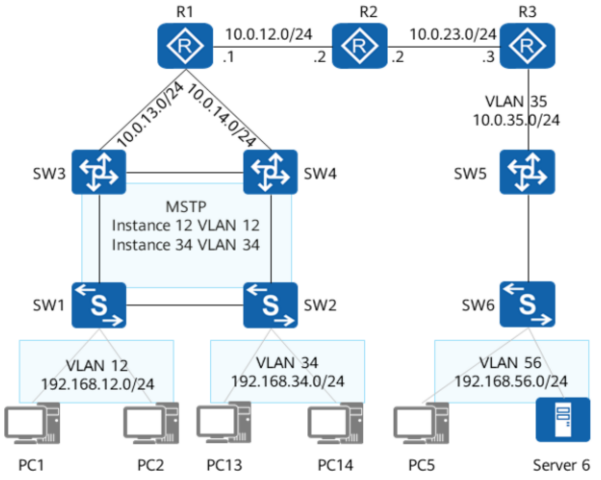
HUAWEI

Troubleshooting Common Network Faults – Topology (1)



- During network maintenance, network engineers may encounter various network faults, such as login, route, and IP service faults. The left figure shows a part of the network architecture, which is used as an example to describe how to troubleshoot common network faults.
- Routing protocol overview:
  - OSPF: runs between R1 and R2. OSPF is enabled on all interfaces of R1, and GE 0/0/0 belongs to area 0.
  - IS-IS: runs between R2 and R3.
  - BGP: R1 and R3 establish IBGP peer relationships with R2 and function as clients of R2, namely, the RR.
  - Static route: SW3, SW4, and SW5 use static routes to connect to routers.

Troubleshooting Common Network Faults – Topology (2)

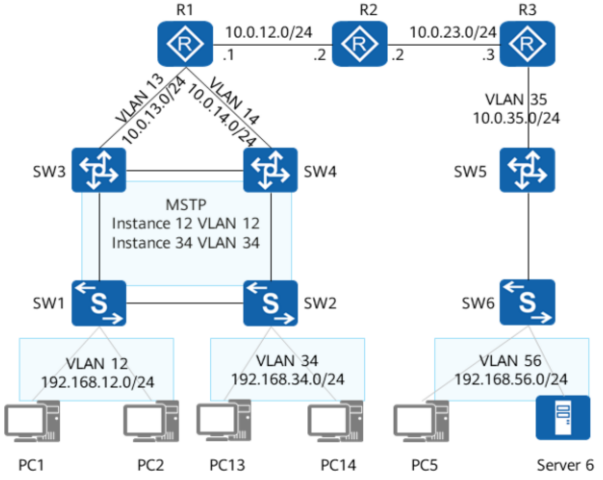


- IP address planning:
  - Loopback0: are 10.0.1.1/32, 10.0.2.2/32, and 10.0.3.3/32 on R1, R2, and R3, respectively.
  - Interconnection interfaces: The network segment is shown in the preceding figure, and the decimal number of the right-most octet in an IP address is a device ID.
  - Terminals: The network segment is shown in the figure. A gateway has the largest IP address on a network segment. PC5 obtains an IP address using DHCP, and R3 functions as a DHCP server. Other terminals use static IP addresses, with the decimal number of the right-most octet in an IP address indicating a device ID.
- Route advertisement planning:
  - On R2, configure OSPF and IS-IS to import routes from each other, so that Loopback0 addresses on R1, R2, and R3 are reachable.
  - R1 imports static routes destined for 192.168.12.0/24 and 192.168.34.0/24 into the BGP routing table.
  - R3 imports the static route destined for 192.168.56.0/24 into the BGP routing table.

HUAWEI

- R3 and SW5 are connected through Layer 3 sub-interfaces.

Troubleshooting Common Network Faults – Topology (3)



- MSTP planning:

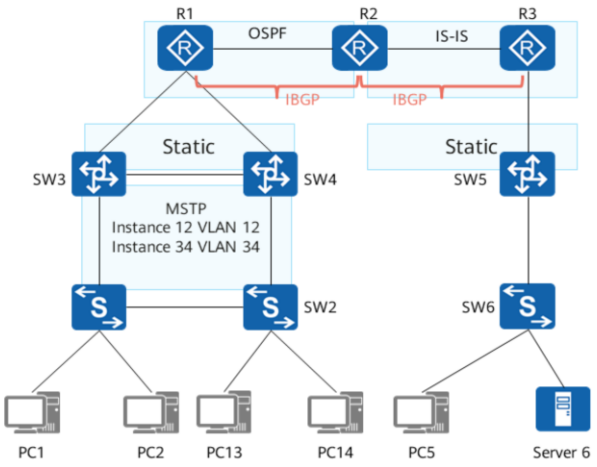
Instance ID	VLAN ID	Root Bridge	Backup Bridge
Instance 12	VLAN 12	SW3	SW4
Instance 34	VLAN 34	SW4	SW3

- VRRP planning:

Network Segment	Master Gateway	Backup Gateway	VRID	Virtual IP
192.168.12.0/24	SW3	SW4	1	192.168.12.254
192.168.34.0/24	SW4	SW3	2	192.168.34.254

- The Telnet username and password for login are Huawei and Huawei@123, respectively.

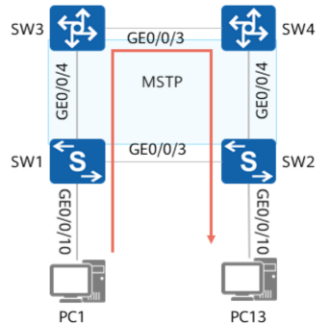
Common Network Troubleshooting – Symptom



- The following symptoms are found:
  - PC1 and PC13 cannot communicate.
  - Server 6 provides the FTP service, but PC1 cannot use this service.
  - PC5 cannot communicate with any host.
- There are multiple possible causes. The preceding approaches are used to demonstrate how to troubleshoot the three faults.
- Assume that the symptoms have been confirmed. Skip the following steps in the subsequent troubleshooting: fault report, fault confirmation, information collection, and wrap-up work.

Symptom – PC1 and PC13 Cannot Communicate (1)

Simplified topology:



The figure on the left shows the planned path for PC1-to-PC13 traffic. Use the layered, segment-based, and forwarding path-centric approaches to analyze the faults. PC1 and PC13 fail to communicate due to the following causes:

- Physical link fault
- Incorrectly configured IP address
- VLAN configuration error
- Loop
- VRRP fault

HUAWEI

- This section describes common troubleshooting methods and tools, providing guidance for network maintenance personnel. The processing sequence in actual scenarios can be different from that in the example.

Symptom – PC1 and PC13 Cannot Communicate (2)

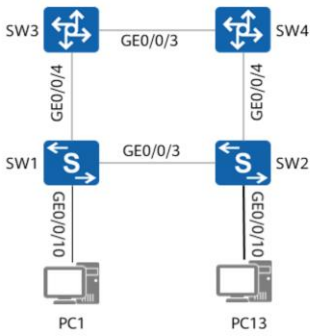
Physical link fault

Incorrectly configured IP address

VLAN configuration error

Loop

VRRP fault



- On PC1 and PC13, choose **Control Panel** > **Network and Internet** > **Network Connection** > **Ethernet Cable** to check Ethernet cables and ensure that the physical cable connections to the PCs are correct. (The preceding path varies according to an operating system and version.)
- Check the physical interface status on each involved switch (SW1, for example). If the physical status of an interface is not up, use another interface to connect the switch to a PC.

```
<SW1>display interface brief | include up
```

Interface	PHY	Protocol	InUti	OutUti	inErrors	outErrors
GigabitEthernet0/0/3	up	up	0%	0%	0	0
GigabitEthernet0/0/4	up	up	0%	0%	0	0
GigabitEthernet0/0/10	up	up	0%	0%	0	0
GigabitEthernet0/0/11	up	up	0%	0%	0	0

- Ping 192.168.34.13 from PC1 and check whether the number of packets sent and received by the interface increases. If so, the physical link is working properly. If not, use another interface or replace the network cable.

```
<SW1>display interface GigabitEthernet 0/0/10
Description:
Switch Port, PVID :  12, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-cc69-6d7b
Hardware address is 4c1f-cc69-6d7b
  Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
  Last 300 seconds output rate 0 bytes/sec, 0 packets/sec
  Input: 430 bytes, 6 packets
  Output: 197137 bytes, 1659 packets
```


HUAWEI

- This section uses the Windows 10 OS as an example to describe how to check the physical connection status of a PC.
- InUti: input bandwidth utilization
- OutUti: output bandwidth utilization

Symptom – PC1 and PC13 Cannot Communicate (3)

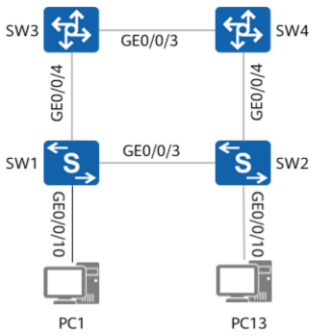
Physical link fault

Incorrectly configured IP address

VLAN configuration error

Loop

VRRP fault



- Check that PC1's physical IP address is set to 192.168.12.1 and the gateway address is set to 192.168.12.254.
- Check the IP addresses on SW3 and SW4 and ensure that the IP addresses are correctly configured. (A VLANIF interface without an IP address assigned will not go up and cannot implement Layer 3 forwarding.)

<SW3>display ip interface brief

Interface	IP Address/Mask	Physical	Protocol
MEth0/0/1	unassigned	down	down
NULL0	unassigned	up	up(s)
Vlanif1	unassigned	up	down
Vlanif12	192.168.12.3/24	up	up
Vlanif34	192.168.34.3/24	up	up

<SW4>display ip interface brief

Interface	IP Address/Mask	Physical	Protocol
MEth0/0/1	unassigned	down	down
NULL0	unassigned	up	up(s)
Vlanif1	unassigned	up	down
Vlanif12	192.168.12.4/24	up	up
Vlanif34	192.168.34.4/24	up	up

- The preceding information indicates that the IP addresses of the interfaces on SW3 and SW4 have been correctly configured.

Symptom – PC1 and PC13 Cannot Communicate (4)

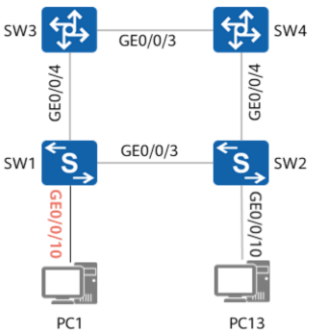
Physical link fault

Incorrectly configured IP address

VLAN configuration error

Loop

VRRP fault



- Query the switch port and VLAN configuration.

```
[SW1]display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------------------------
12   common  TG:GE0/0/11(U)      TG:GE0/0/10(U)
34   common  TG:GE0/0/11(U)      TG:GE0/0/10(U)
VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
12   enable  default       enable  disable    VLAN 0012
34   enable  default       enable  disable    VLAN 0034
```

- According to the preceding information, VLAN configurations of GE 0/0/10 and GE 0/0/11 on SW1 are incorrect. Correct VLAN configuration errors. Repeat the preceding step to verify the configurations on the other three switches.
- After the VLAN is correctly configured on the switches, check whether PC1 can communicate with other IP addresses on the same network segment. For example, run the **ping 192.168.12.13** command on PC1. The command output shows that packet loss occurs and the delay is long.

HUAWEI

- GE 0/0/10 belongs to VLAN 12 and VLAN 34 and works in tagged mode, indicating that the interface is configured as a trunk interface and the PVID is not 12.

Symptom – PC1 and PC13 Cannot Communicate (5)

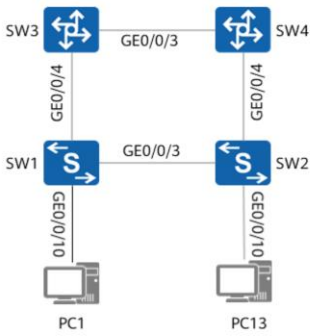
Physical link fault

Incorrectly configured IP address

VLAN configuration error

Loop

VRRP fault



- Check the MSTP status on each switch. All ports on SW4 are in the Forwarding state.

```
<SW4>display stp brief
 MSTID     Port                        Role  STP         State
   0       GigabitEthernet0/0/2        DESI  FORWARDING  NONE
   0       GigabitEthernet0/0/3        DESI  FORWARDING  NONE
   0       GigabitEthernet0/0/4        DESI  FORWARDING  NONE
  12       GigabitEthernet0/0/2        DESI  FORWARDING  NONE
  12       GigabitEthernet0/0/3        DESI  FORWARDING  NONE
  12       GigabitEthernet0/0/4        DESI  FORWARDING  NONE
  34       GigabitEthernet0/0/2        DESI  FORWARDING  NONE
  34       GigabitEthernet0/0/3        DESI  FORWARDING  NONE
  34       GigabitEthernet0/0/4        DESI  FORWARDING  NONE
```

- MSTP faults may be caused by an incorrect domain name setting, incorrect binding between instances and VLANs, or incorrect binding between ports and VLANs. Check the MSTP configuration on SW4.

```
<SW4>display current-configuration | begin region-configuration
stp region-configuration
 region-name TEST //The correct domain name is test, not TEST.
 instance 12 vlan 12
 instance 34 vlan 34
 active region-configuration
#
```

- Correct the domain name on SW4. Ping 192.168.12.13 from PC1. As a result, packet loss occurs now and then.

HUAWEI

- A Layer 2 loop causes the following failures:
  - An attempt to remotely log in to a device fails.
  - An interface receives a large number of broadcast packets, which can be viewed in the **display interface** command output.
  - An attempt to log in to a device through the serial port is time consuming.
  - CPU usage exceeds 70%.
  - High packet loss occurs when a ping command is used.
  - The indicator of the VLAN interface with the loop occurring frequently blinks.
  - A PC receives a large number of broadcast packets.
  - A loop alarm is generated if loop detection is configured on a switch.

Symptom – PC1 and PC13 Cannot Communicate (6)

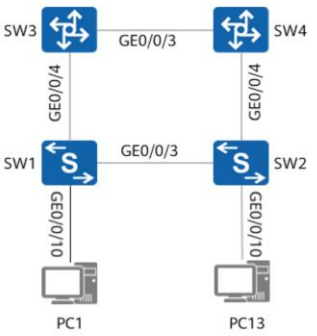
Physical link fault

Incorrectly configured IP address

VLAN configuration error

Loop

VRRP fault



- Check whether packet loss is caused by the loop. Check whether MAC address flapping detection is enabled on each involved switch and whether MAC address flapping is detected.

```
[SW3]display mac-address flapping
Mac-address Flapping Configurations :
------------------------------------------------------------
 Flapping detection          : Enable
 Aging  time(sec)            : 300
 Quit-vlan Recover time(min) : 10
 Exclude vlan-list  : -
------------------------------------------------------------
<SW3>display mac-address flapping record
Info: The mac-address flapping record does not exist.
```

- After observing for a while, find that the fault occurs during working hours. When the fault occurs, check the MAC address table, and find that the MAC address table is unstable. Then check STP statistics.

```
<SW3>display stp tc-bpdu statistics
------------------------- STP TC/TCN information ---------------
MSTID          Port                TC(Send/Receive)    TCN(Send/Receive)
   12          GigabitEthernet0/0/1      13/56               -/-
   12          GigabitEthernet0/0/3      22/18               -/-
   12          GigabitEthernet0/0/4      29/66               -/-
```

- During working hours, a switch port frequently alternates between up and down, and sends a large number of TC BPDUs. In this case, configure the switch port connected to the PC as an edge port.

HUAWEI

- After receiving STP TC BPDUs, the STP-enabled switch clears the MAC address table and re-learns MAC addresses. During this period, data forwarding is interrupted for a short period, causing packet loss.

Symptom – PC1 and PC13 Cannot Communicate (7)

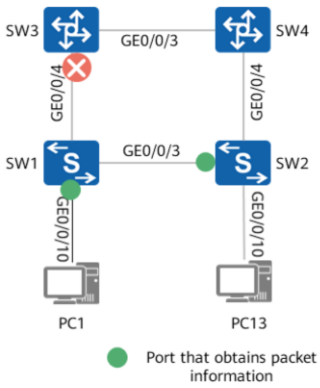
Physical link fault

Incorrectly configured IP address

VLAN configuration error

Loop

VRRP fault



- Shut down SW3's GE 0/0/4. PC1 cannot ping PC13, causing a large number of packets to be discarded in a short period. After SW3 is restarted, the following alarm is generated on SW3:

```
<SW3>
ARP/4/ARP_DUPLICATE_IPADDR(l)[0]:Received an
ARP packet with a duplicate IP address from the interface.
(IpAddress=192.168.12.254, InterfaceName=Vlanif12, MacAddress=0000-5e00-
0101)
```

- The IP address is a virtual IP address. VRRP may be defective. Obtain packet information on SW1's GE 0/0/10 and SW2's GE 0/0/3. The addresses marked red are source MAC and IP addresses. SW2 fails to obtain data packet information.

```
[SW1]capture-packet interface GigabitEthernet 0/0/10 destination terminal
Packet: 6
-----------------------------------------------------------------
00 00 5e 00 01 03 54 89 98 1f 5a 8d 81 00 00 0c
08 00 45 00 00 3c 39 aa 40 00 80 01 11 b8 c0 a8
0c 01 c0 a8 22 0d 08 00 f9 d1 82 3b 0a 71 08 09
0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19
1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27
-----------------------------------------------------------------
```


HUAWEI

- The **capture-packet** command obtains information in service packets that match a configured rule. The obtained information is saved in a local file.
  - **capture-packet** { **interface** *interface-type interface-number* | **acl** *acl-number* } * [**vlan** *vlan-id* | **cvlan** *cvlan-id*] * **destination terminal** [**car cir** *car-value* | **time-out** *time-out-value* | **packet-num** *number* | **packet-len** *length*] *
  - Information in packets on the management interface cannot be obtained.
  - This command can only obtain information received by an interface, not information sent by an interface.

Symptom – PC1 and PC13 Cannot Communicate (8)

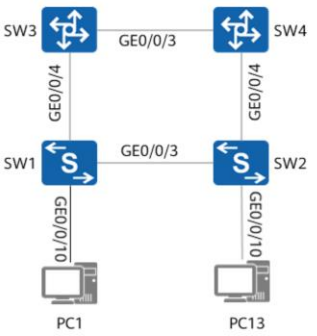
Physical link fault

Incorrectly configured IP address

VLAN configuration error

Loop

VRRP fault



- As shown in the preceding slide, packets are dropped between SW1 and SW2, and the destination MAC address is 00 00 5e 00 01 03. The VRRP ID is 3, which should have been 2 as planned. Check the VRRP status and configuration of SW3.

```
<SW3>display vrrp
  Vlanif12 | Virtual Router 3
    State : Master
    Virtual IP : 192.168.12.254
    Master IP : 192.168.12.3
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Virtual MAC : 0000-5e00-0103
<SW3>display current-configuration interface Vlanif 12
#
interface Vlanif12
 ip address 192.168.12.3  255.255.255.0
 vrrp vrid 3 virtual-ip 192.168.12.254
#
```

- According to the preceding analysis, a VRRP dual-master fault occurs because the VRID is incorrectly set. As a result, packet loss occurs during a VRRP switchover. Correct the configuration of SW3.
- Carry out a reliability test again. Find that no packet loss occurs during the switchover. Then, the fault is rectified.

HUAWEI

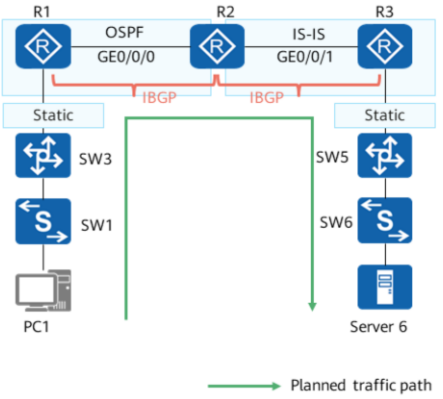
- The VRRP group numbers on SW3 and SW4 are different. After the VRRP group on SW3 detects a downlink fault, the VRRP status on SW4 does not change. The VRRP status on SW4 remains in the Master state. In this situation, sending gratuitous ARP messages is not triggered for an ARP entry update on the terminal.
- The destination MAC address of data frames sent from PC1 to a gateway is still 00 00 5e 00 01 03.
- After the link between SW1 and SW3 is disconnected, SW1 cannot forward packets to SW2, because SW1 does not have the MAC address entry of 00 00 5e 00 01 03.

Contents

HUAWEI

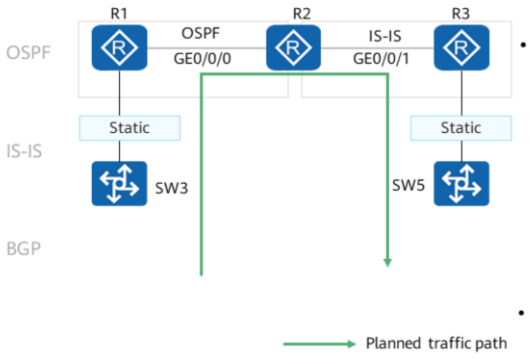
Fault Symptom – PC1 Cannot Use the FTP Service (1)

Simplified topology:



- In the preceding example, measures are taken to ensure no fault occurs between PC1 and SW3 and between server 6 and SW5.
- As shown in the figure on the left, possible causes for an FTP failure on PC1 are as follows:
  - Physical link fault (done)
  - Route faults
    - Static route
    - OSPF
    - BGP
    - IS-IS
  - Traffic control fault
  - Server fault (done)
- This section describes how to troubleshoot route faults and traffic control faults.

Fault Symptom – PC1 Cannot Use the FTP Service (2)

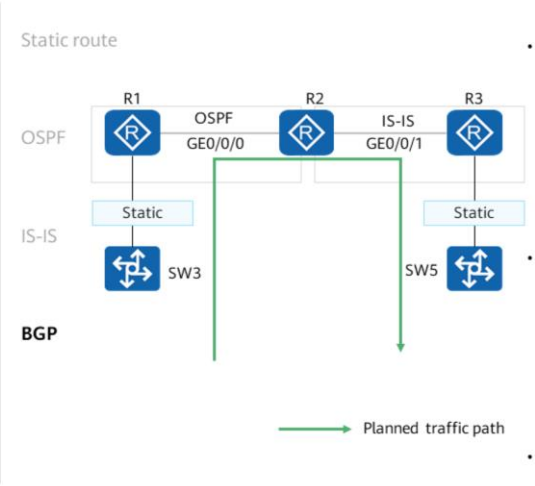


- Data packets are forwarded hop by hop. All routing devices along a path must have routes to the destination. First, check whether routes destined for server 6 exist on all devices through which data packets sent from PC1 to server 6 pass.
- Check the static route configuration on SW3.
  - When configuring a static route, specify only the outbound interface name for a P2P interface. For a broadcast interface, also specify a next-hop IP address.

```
<SW3>display ip routing-table protocol static
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      0.0.0.0/0     Static  60   0           RD  10.0.13.1       Vlanif13
```

- The command output indicates that the static route has been correctly configured on SW3.

Fault Symptom – PC1 Cannot Use the FTP Service (3)



- Check the routing table on R1.

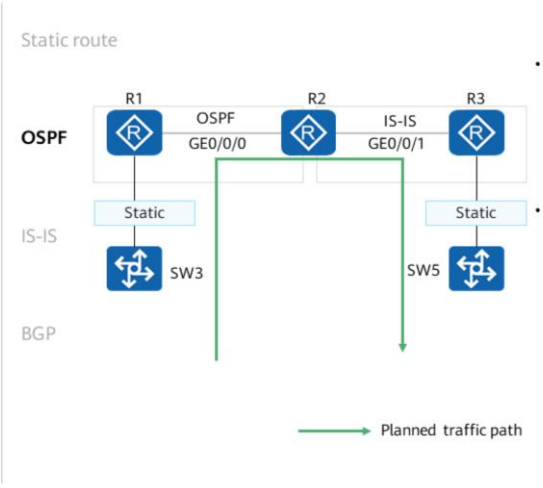
```
<R1>display ip routing-table 192.168.56.0
```

- The command output shows that R1 does not have a route to 192.168.56.0. Check whether a BGP peer relationship is properly established between R1 and R2.

```
<R1>display bgp peer
BGP local router ID : 10.0.1.1
Local AS number : 100
Total number of peers : 1    Peers in established state : 0
  Peer        AS    MsgRcvd  MsgSent  OutQ  Up/Down     State  PrefRcv
  10.0.2.2    100   0        0        0     0:00:05     Idle   0
```

- The preceding command output shows that the BGP peer relationship fails to be established. Possible causes are as follows:
  - The loopback0 interface of the remote device is unreachable.
  - The AS number of the local or remote device is incorrect.
  - The **peer ebgp-max-hop** command used to allow the establishment of an indirect EBGP peer relationship is not run.
  - Router IDs on both ends are the same.
- According to the command output, the numbers of sent and received BGP packets are 0, indicating that the loopback0 interface on the remote device may be unreachable.

Fault Symptom – PC1 Cannot Use the FTP Service (4)



- On R1, check the route destined for the BGP peer.

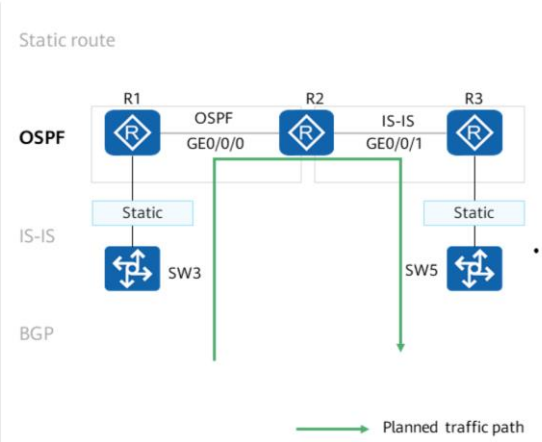
```
<R1>display ip routing-table 10.0.2.2
```

- The command output shows that R1 does not have a route to 10.0.2.2. Check whether an OSPF neighbor relationship is properly established between R1 and R2.

```
<R1>display ospf peer
                OSPF Process 1 with Router ID 10.0.1.1
```

- The preceding command output shows that the OSPF neighbor relationship fails to be established. Possible causes are as follows:
  - Router IDs on both ends are the same.
  - Area IDs do not match on both ends.
  - Network masks do not match on both ends.
  - MTUs do not match on both ends.
  - On an MA network, DR priorities of all devices are set to 0.
  - Authentication passwords do not match on both ends.
  - An interface is configured as a silent interface.
  - Time parameters do not match on both ends.

Fault Symptom – PC1 Cannot Use the FTP Service (5)



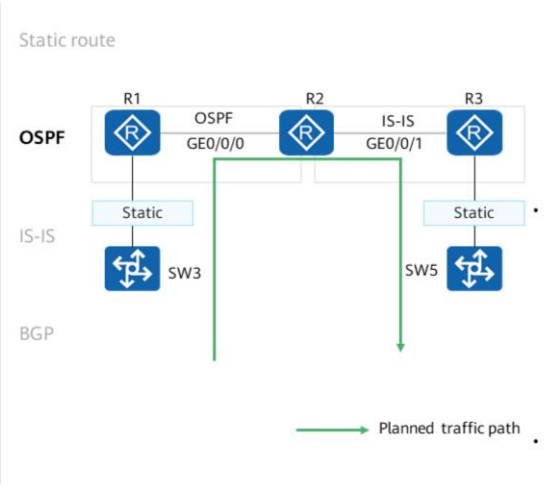
- Check OSPF error information on R1.

```
[R1]display ospf error
General packet errors:
 0    : IP: received my own packet      0    : Bad packet
 0    : Bad version                     0    : Bad checksum
 0    : Bad area id                     0    : Drop on unnumbered interface
 0    : Bad virtual link                0    : Bad authentication type
 0    : Bad authentication key          0    : Packet too small
 0    : Packet size > ip length         0    : Transmit error
 0    : Interface down                  0    : Unknown neighbor
 0    : Bad net segment                 0    : Extern option mismatch
 133  : Router id confusion
```

- The preceding command output shows that a router ID conflict may cause a failure to establish an OSPF neighbor relationship. To accurately locate the fault, enable OSPF debugging on R1.

```
<R1>terminal debugging
Info: Current terminal debugging is on.
<R1>debugging ospf packet interface GigabitEthernet 0/0/0
```

Fault Symptom – PC1 Cannot Use the FTP Service (6)



- Check the configuration of the local OSPF protocol.

```
<R1>display ospf interface GigabitEthernet 0/0/0 verbose
                OSPF Process 1 with Router ID 10.0.1.1
 Interface: 10.0.12.1 (GigabitEthernet0/0/0)
 Cost: 1        State: DR       Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 10.0.12.1
 Backup Designated Router: 0.0.0.0
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
  IO Statistics
        Type       Input     Output
        Hello         36         36
```

- Check OSPF error information in the debugging information on R1. Some information is as follows:

```
: Source Address: 10.0.12.2
: Destination Address: 224.0.0.5
: Ver# 2, Type: 1 (Hello)
: Length:  44, Router: 10.0.1.1
: Area: 0.0.0.0, Chksum: db9c
: AuType: 00
: Key(ascii):********
: Net Mask: 255.255.255.0
: Hello Int: 10, Option: _E_
: Rtr Priority: 1, Dead Int: 40
```

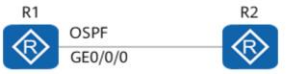
- After comparison, it is found that the interval at which Hello packets are sent, mask, and authentication information on one end matches those on the other end, and only the router ID conflict occurs.

HUAWEI

- The debugging information on R1 shows that the OSPF router ID carried in the Hello packets sent from 10.0.12.2 is the same as the OSPF router ID on R1.

Fault Symptom – PC1 Cannot Use the FTP Service (7)

Static route



OSPF → **Telnet**

IS-IS

BGP

- Log in to R2 and change the OSPF router ID. However, the attempt to use Telnet to log in to R2 fails.
- Common causes of Telnet login failures are as follows:
  - A route is unavailable, and a TCP connection cannot be established between the client and server.
  - Telnet is disabled on the server.
  - The number of users logging in to a device reaches a specified upper limit.
  - An ACL is bound to a VTY user interface.
  - An access protocol configured in the VTY user interface view is incorrect. If the **protocol inbound ssh** command is used, the attempt to use Telnet for login fails.
- Log in to R1 through the console port and check whether Telnet is enabled.

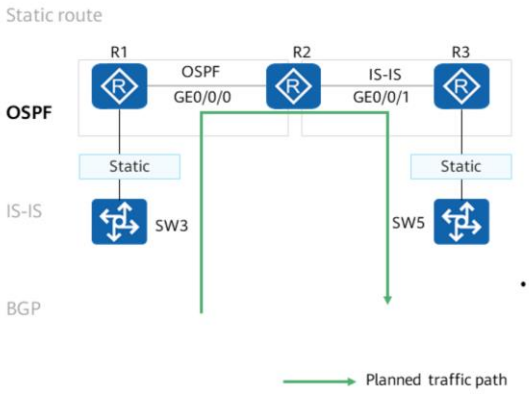
```
[R2]display telnet server status
TELNET IPV4 server                :Enable
TELNET IPV6 server                :Enable
TELNET server port                :23
```

- Check whether Telnet is allowed in the VTY view.

```
[R2-ui-vty0-4]display this
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
```

- Modify the configuration of R2 to support Telnet in the VTY user interface view. The test result shows that the attempt to log in to R2 is successful.

Fault Symptom – PC1 Cannot Use the FTP Service (8)



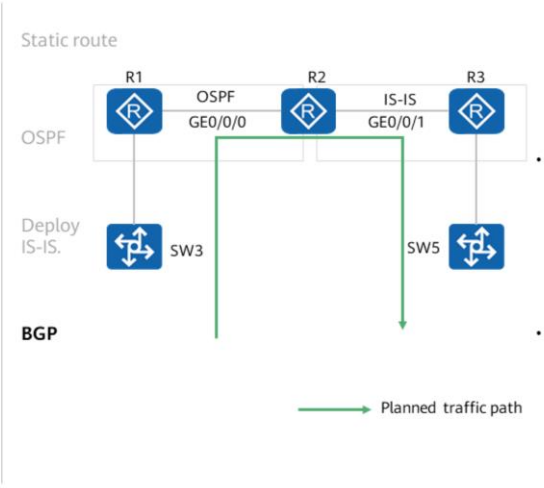
- Change the OSPF router ID on R2, restart the OSPF process to make the router ID take effect, and check the OSPF neighbor relationship status.

```
<R2>display ospf peer
                OSPF Process 1 with Router ID 10.0.12.2
                        Neighbors
Area 0.0.0.0 interface 10.0.12.2(GigabitEthernet0/0/0)'s neighbors
Router ID: 10.0.1.1          Address: 10.0.12.1
  State: Full  Mode:Nbr is  Slave  Priority: 1
  DR: 10.0.12.2  BDR: 10.0.12.1  MTU: 0
  Dead timer due in 35  sec
  Retrans timer interval: 5
  Neighbor is up for 00:09:17
  Authentication Sequence: [ 0 ]
```

- Check whether the route to 10.0.2.2 exists on R1.

```
<R1>display ip routing-table 10.0.2.2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      10.0.2.2/32   OSPF    10   1           D   10.0.12.2       GE0/0/0
```

Fault Symptom – PC1 Cannot Use the FTP Service (9)



- Check the BGP peer relationship status on R1.

```
<R1>display bgp peer
BGP local router ID : 10.0.1.1
Local AS number : 100
Total number of peers : 1    Peers in established state : 1

  Peer        AS  MsgRcvd  MsgSent  Up/Down     State
  10.0.2.2    100     25       26    0:19:22   Established
```

- Check whether the BGP routing table of R1 contains a route destined for 192.168.56.0/24.

```
<R1>display bgp routing-table
BGP Local router ID is 10.0.1.1
Total Number of Routes: 2
      Network          NextHop  MED  LocPrf  Path/Ogn
 *>192.168.12.0/24     0.0.0.0    0       0         ?
```

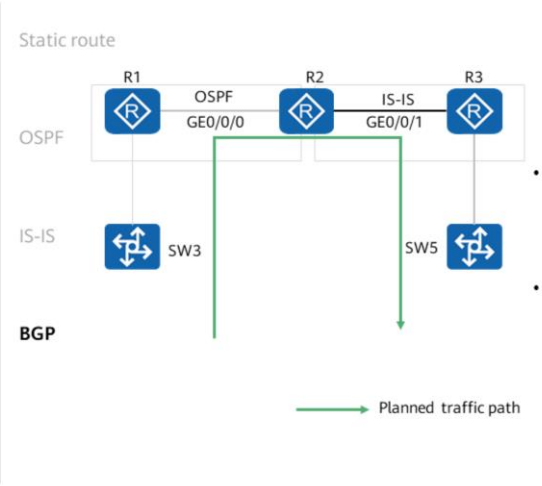
- R1 still does not have an available route. As R1 should have imported the route from R3, check whether the route is imported into the BGP routing table on R3.

```
<R3>display bgp routing-table
BGP Local router ID is 10.0.3.3
Total Number of Routes: 1
      Network          NextHop  MED  LocPrf  Path/Ogn
 *> 192.168.56.0       0.0.0.0    0       0         ?
```


HUAWEI

- On R3, the command output shows that the route to 192.168.56.0/24 has been imported into the BGP routing table.

Fault Symptom – PC1 Cannot Use the FTP Service (10)



- Check the BGP peer status on R3.

```
<R3>display bgp peer
BGP local router ID : 10.0.3.3
Local AS number : 100
Total number of peers : 1    Peers in established state : 0
  Peer        AS  MsgRcvd  MsgSent  OutQ  Up/Down   State  PrefRcv
  10.0.2.2   100        0        0     0  0:00:05    Idle        0
```

- The BGP peer relationship is not established between R3 and R2. Check whether a route destined for 10.0.2.2/32 exists on R3.

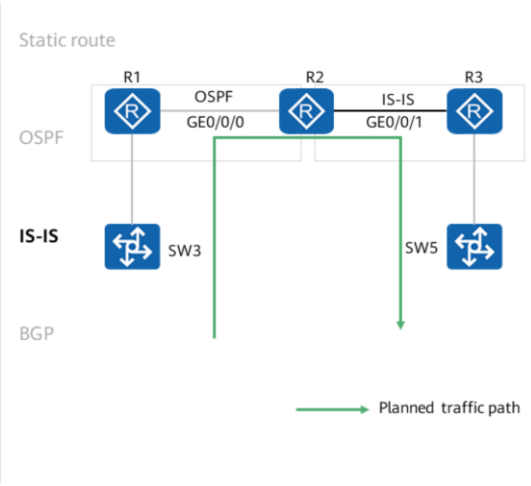
```
<R3>display ip routing-table 10.0.2.2
```

- R3 does not have the route to 10.0.2.2/32. As IS-IS runs between R2 and R3, check whether an IS-IS neighbor relationship is properly established between R3 and R2.

```
<R3>display isis peer
                Peer information for ISIS(1)
  SystemId      Interface     CircuitId         State Type PRI
0100.0000.2002  GE0/0/1       0100.0000.2002.01 Up    L2   64
```


- Possible causes for the failure to establish an IS-IS neighbor relationship are as follows:
  - Area IDs do not match on both ends. (The inconsistency adversely affects only level-1 neighbor relationships.)
  - IS-IS levels do not match on both ends. (Note that on Huawei devices if the system level differs from the interface circuit level, the system level takes effect.)
  - Interface authentication settings do not match on both ends.
  - System ID lengths do not match or system ID conflict occurs.
  - The IP addresses are on different network segments. (Source check is enabled for IS-IS on a broadcast network, and can be disabled.)

Fault Symptom – PC1 Cannot Use the FTP Service (11)



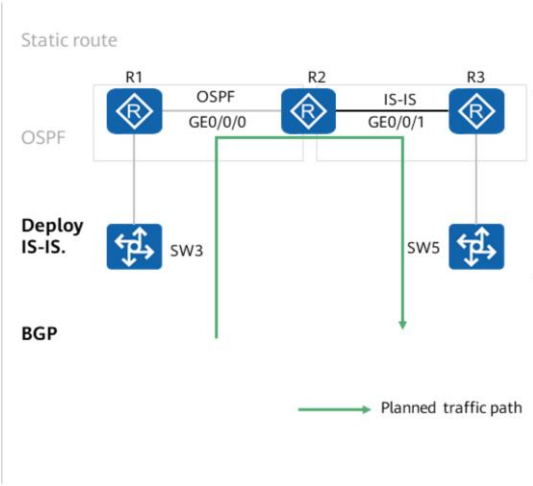
- The IS-IS neighbor relationship is properly established, but R3 cannot obtain the route to 10.0.2.2/32. Possible causes are as follows:
  - IS-IS is not enabled on an interface.
  - Cost styles do not match on both ends.
  - A routing policy is configured on the device.
  - Network types do not match on both ends.
- Check information about an IS-IS interface on R1.

```
<R2>display isis interface
                Interface information for ISIS(1)

 Interface   Id   IPV4.State   MTU   Type    DIS
 GE0/0/1     1        Up      1497  L1/L2   No/Yes
  Loop0      1        Up      1500  L1/L2    --
```

- Check the IS-IS configuration on R1.

```
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0001.0100.0000.2002.00
 import-route ospf 1
 #
```

Fault Symptom – PC1 Cannot Use the FTP Service (12)



- Check the IS-IS configuration on R3.

```
isis 1
 is-level level-2
 network-entity 49.0001.0100.0000.3003.00
 #
```

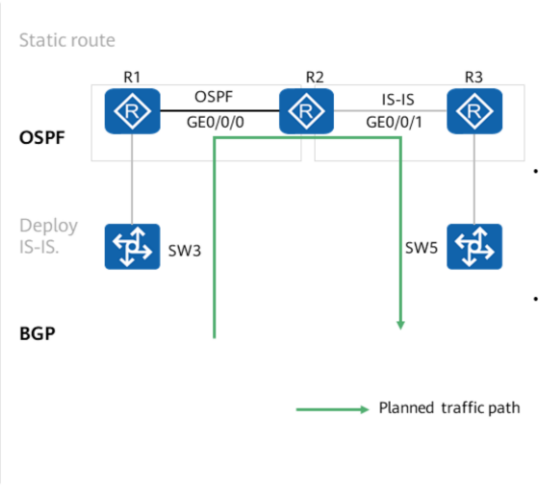
- The following information shows that the cost style of R2 does not match that of R3. Change the cost style of R3 to wide. Then, check whether R3 has a route to 10.0.2.2/32.

```
<R3>display ip routing-table 10.0.2.2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
10.0.2.2/32         ISIS-L2 15   10D       10.0.23.2       GE0/0/1
```

- Check whether the BGP peer relationship on R3 is restored and check the BGP routing table of R3.

```
<R3>display bgp peer
 BGP local router ID : 10.0.23.3
  Peer        AS  MsgRcvd  MsgSent  Up/Down      State
 10.0.2.2    100       8        7   0:04:42 Established
<R3>display bgp routing-table
Total Number of Routes: 2
     Network            NextHop        MED        LocPrf    Path/Ogn
*>I 192.168.12.0       10.0.1.1         0          100          ?
*>  192.168.56.0       0.0.0.0          0            0          ?
```

Fault Symptom – PC1 Cannot Use the FTP Service (13)



- R3 has correctly advertised routes and learned the route to 192.168.12.0/24. Check whether R1 has a route to 192.168.56.0/24.

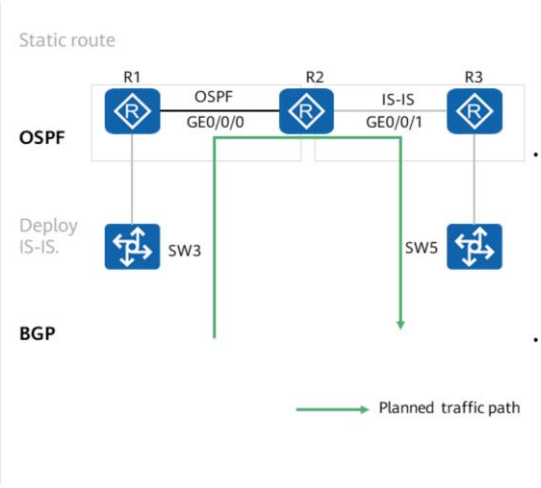
```
<R1>display bgp routing-table
BGP Local router ID is 10.0.1.1
     Network         NextHop  MED  LocPrf  Path/Ogn
*>   192.168.12.0    0.0.0.0  0    0       ?
I    192.168.56.0    10.0.3.3 0    100     ?
```

- R1 has received the BGP route from R3, but the route is unavailable. The possible cause is that the next hop is unreachable. On R1, check whether there is a route to 10.0.3.3/32.

```
<R1>display ip routing-table 10.0.3.3
```

- The command output shows that the routing table of R1 does not contain the route to 10.0.3.3/32. This route should have been imported by R1 from IS-IS into the OSPF routing table. Possible causes are as follows:
  - A routing policy is configured on R1.
  - R2 does not import IS-IS routes into the OSPF routing table.
  - Type 5 LSAs are filtered out in the outbound direction of R2's interface.

Fault Symptom – PC1 Cannot Use the FTP Service (14)



- Check the LSDB of R1.

```
<R1>display ospf lsdb
  OSPF Process 1 with Router ID 10.0.1.1
        Area: 0.0.0.0
  Type      LinkStateID     AdvRouter     Age  Len  Sequence   Metric
  Router    10.0.2.2        10.0.2.2      5    48   80000003   1
  Router    10.0.1.1        10.0.1.1      3    48   8000000D   1
  Network   10.0.12.1       10.0.1.1      3    32   80000002   0
```

- R1 does not have Type 5 LSAs. Check whether R1 imports IS-IS routes into the OSPF routing table.

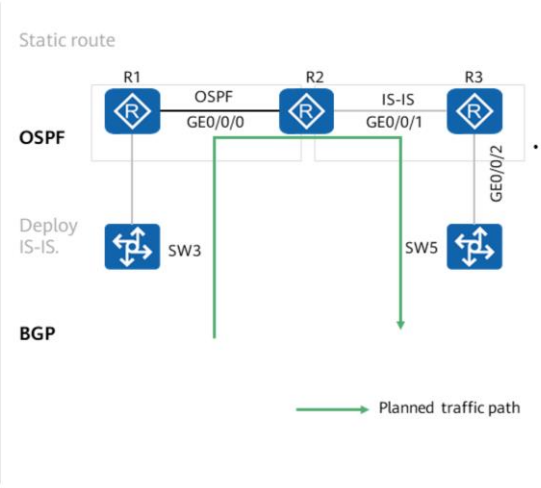
```
<R2>display current-configuration configuration ospf
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.2.2 0.0.0.0
  network 10.0.12.2 0.0.0.0
#
```

- Modify the configuration of R2, import IS-IS routes into the OSPF routing table, and then check the routing table of R1.

```
<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      10.0.3.3/32   O_ASE   150  1           D   10.0.12.2       GE0/0/0
  192.168.56.0/24   IBGP    255  0           RD  10.0.3.3        GE0/0/0
```


- After the configuration of R2 is modified, the route to 10.0.3.3/32 is displayed on R1.

Fault Symptom – PC1 Cannot Use the FTP Service (15)



- Run the **traceroute 192.168.56.6** command on PC1.

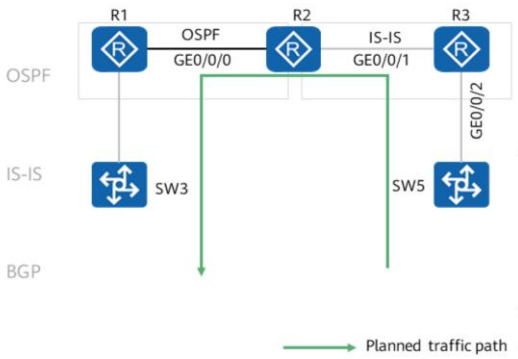
```
traceroute to 192.168.56.6, 8
 1  192.168.12.3   63 ms   46 ms   47 ms
 2  10.0.13.1      78 ms   63 ms   62 ms
 3  10.0.12.2      94 ms   63 ms   78 ms
 4  10.0.23.3      94 ms   62 ms   63 ms
 5  * * *
```

- R3 does not respond to the received data packets. Enable traffic statistics collection on R3's GE 0/0/2 and check whether R3 sends the data packets through GE0/0/2.

```
[R3] acl 3000
[R3-acl-adv-3000]rule 5 permit ip source 192.168.12.1 0 destination
192.168.56.6 0
[R3-acl-adv-3000]quit
[R3]traffic classifier trafficSta
[R3-classifier-trafficSta]if-match acl 3000
[R3-classifier-trafficSta]quit
[R3]traffic behavior trafficSta
[R3-behavior-trafficSta]statistic enable
[R3-behavior-trafficSta]quit
[R3]traffic policy trafficSta
[R3-trafficpolicy-trafficSta]classifier trafficSta behavior trafficSta
[R3-trafficpolicy-trafficSta]quit
[R3]interface GigabitEthernet0/0/2.35
[R3-GigabitEthernet0/0/2.35]traffic-policy trafficSta outbound
```


- After R1 learns the route, PC1 still cannot access the FTP service provided by server 6. In this case, run the **traceroute** command to check connectivity between R1 and server 6.
- Based on traffic statistics, the analysis is as follows:
  - Check whether the traffic reaches the inbound interface of the device and determine whether packet loss occurs on the upstream device.
  - Check whether the traffic is forwarded to the outbound of the device and determine whether packet loss occurs on the device.
  - Check whether Layer 2 and Layer 3 information about traffic on the inbound interface of the device is correct and determine whether the upstream device forwards and encapsulates packets properly.
  - Check whether the Layer 2 and Layer 3 information about the outbound interface is correct and determine whether the device forwards and encapsulates packets properly.
  - Check whether transient traffic flapping occurs due to MAC address flapping, route changes, or IP address conflicts.
- Procedure for configuring traffic statistics collection:
  - Configure an ACL rule to match traffic to be collected.
  - Configure a traffic classifier.
  - Configure a traffic behavior and configure traffic statistics collection in the traffic behavior.
  - Configure a traffic policy; bind the traffic classifier and behavior to the traffic policy; apply the traffic policy to the inbound direction of the switch to collect statistics on packets of different users.

Fault Symptom – PC1 Cannot Use the FTP Service (16)



- Check traffic statistics on R3. No packet loss occurs on R3.

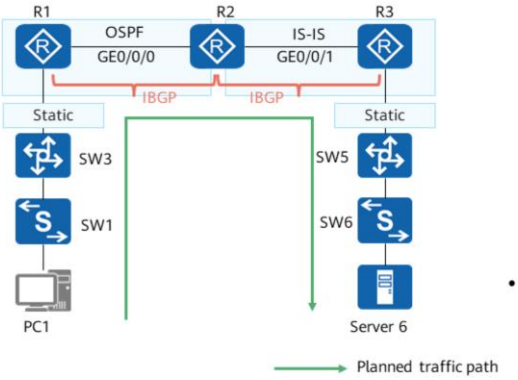
```
<R3> display traffic policy statistics interface GigabitEthernet0/0/2.35 outbound
Interface:GigabitEthernet0/0/2.35
 Traffic policy inbound: trafficSta
 Rule number: 1
 Current status: OK!
Item                Sum(Packets/Bytes)
-----------------------------------------
Matched             50/400
  Passed            50/400
  Dropped           0/0
```

- Check the routing table of SW5 in the direction where server 6 sends data packets.

```
[SW5]display ip routing-table
  Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        10.0.35.0/24  Direct  0    0           D   10.0.35.5       Vlanif35
      192.168.56.0/24 Direct  0    0           D   192.168.56.5    Vlanif56
```

- SW5 does not have a static route to PC1. Configure a static route on SW5.
- Check whether PC1 and server 6 can communicate and use the FTP service properly.
- After the preceding operations are complete, the troubleshooting is complete.

Fault Symptom – PC1 Cannot Use the FTP Service

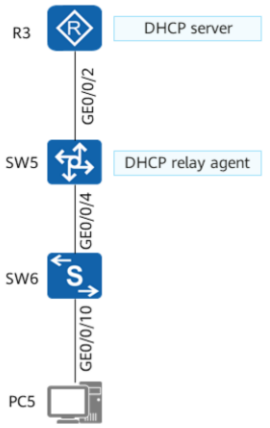


- The following faulty points are involved in the troubleshooting:
  - Incorrect static route configuration
  - Failure to establish an OSPF neighbor relationship
  - Incorrect IS-IS route calculation
  - Failure to establish a BGP peer relationship
  - Incorrect BGP route selection
  - Telnet login failure
- The following tools are used:
  - packet information obtaining tool
  - Traffic statistics collection tool
  - Tracert

Contents

Fault Symptom – PC5 Cannot Communicate with Any Host (1)

Simplified topology:

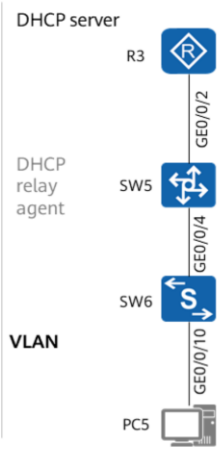


- PC5 cannot communicate with any host. The possible cause is that the physical link to PC5 is abnormal, or PC5's IP address is incorrect.
- Check the IP address of PC5. PC5 fails to obtain an IP address.

```
PC>ipconfig
IPv4 address          0.0.0.0
Subnet mask           0.0.0.0
Gateway               0.0.0.0
Physical address      54-89-98-39-22-B7
DNS server            0.0.0.0
```

- PC5 obtains an IP address using DHCP. The common causes of DHCP faults are as follows:
  - The link between the client and server becomes faulty.
  - The DHCP function is disabled on a device.
  - The DHCP address allocation mode is not selected on a VLANIF interface.
  - No IP address is available in an address pool.
  - If the client and server are on different network segments and a relay agent is deployed between them:
    - The link between the DHCP relay agent and server becomes faulty.
    - The DHCP function is not enabled globally on a device. As a result, the DHCP function does not take effect.
    - No DHCP server is specified on the DHCP relay agent.
    - The DHCP relay agent and server are unreachable.

Fault Symptom – PC5 Cannot Communicate with Any Host (2)



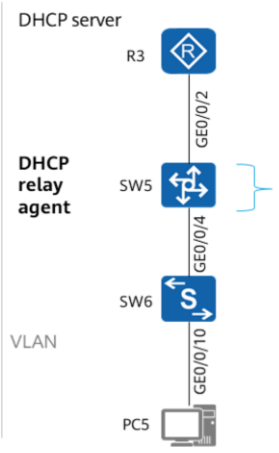
- Check whether the physical link to PC5 is normal.
- Check whether a Layer 2 loop occurs on SW6 and check the VLAN configuration.

```
<SW6>display stp brief
 MSTID        Port                      Role  STPState
    0         GigabitEthernet0/0/4      ROOT  FORWARDING
    0         GigabitEthernet0/0/10     DESI  FORWARDING
    0         GigabitEthernet0/0/11     DESI  FORWARDING

<SW6>display vlan
The total number of vlans is : 2
--------------------------------------------------------------------------------
56   common  TG:GE0/0/4(U) GE0/0/10(U) UT: GE0/0/11(U)
```

- The preceding information shows that the physical status of GE 0/0/10 is normal, but GE 0/0/10 is configured as a trunk interface. Modify the configuration on SW6 to configure GE 0/0/10 as an access interface and set the VLAN ID to 56.
- After the modification, check whether PC5 can properly obtain an IP address.

```
PC>ipconfig
IPv4 address          0.0.0.0
Subnet mask           0.0.0.0
Gateway               0.0.0.0
Physical address      54-89-98-39-22-B7
DNS server            0.0.0.0
```

Fault Symptom – PC5 Cannot Communicate with Any Host (3)



- SW5 is a DHCP relay agent. Query the global configuration of SW5.

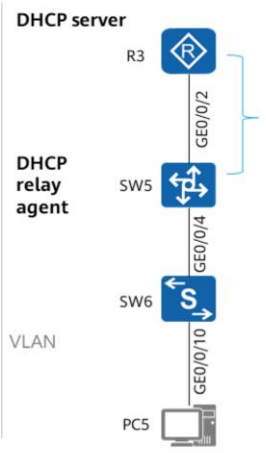
```
<SW5>display current-configuration
dhcp enable
#
interface Vlanif35
 ip address 10.0.35.5 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 10.0.35.3
#
```

- The DHCP service has been enabled on SW5 and the DHCP relay agent has been configured. However, after the data packets sent by PC5 pass through SW6, SW6 adds the tag with VLAN ID 56 to the packets before forwarding them. As a result, the DHCP relay interface configured on SW5 is incorrect.
- Modify the configuration of SW5:

```
[SW5]interface Vlanif 56
[SW5-Vlanif56]dhcp select relay
[SW5-Vlanif56]dhcp relay server-ip 10.0.35.3
```

- After the modification, PC5 still cannot obtain an IP address.

Fault Symptom – PC5 Cannot Communicate with Any Host (4)



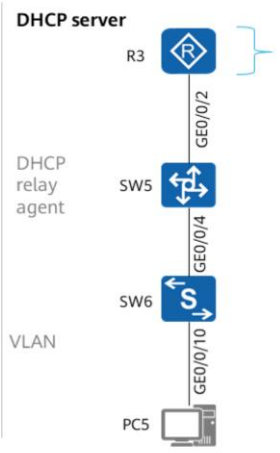
- Query the DHCP relay status of SW5.

```
[SW5]display dhcp relay statistics
The statistics of DHCP RELAY:
  DHCP packets received from clients    : 11
    DHCP DISCOVER packets received      : 11
    DHCP REQUEST packets received       : 0
    DHCP RELEASE packets received       : 0
    DHCP INFORM packets received        : 0
    DHCP DECLINE packets received       : 0
  DHCP packets sent to clients          : 0
  DHCP packets received from servers    : 0
  DHCP packets sent to servers          : 11
```

- SW5 has sent packets to the DHCP server, but does not receive any responses.
- Check the DHCP server configuration on R3.

```
<R3>display  current-configuration
dhcp enable
#
ip pool test
 gateway-list 192.168.56.254
 network 192.168.56.0  mask 255.255.255.0
 excluded-ip-address 192.168.56.6
 dns-list 192.168.1.1
#
interface GigabitEthernet0/0/2
dhcp select global
```

Fault Symptom – PC5 Cannot Communicate with Any Host (5)



- R3 and SW5 are connected through sub-interfaces. Therefore, enable the DHCP server service on a sub-interface, instead of the physical interface GE0/0/2.

```
[R3]interface GigabitEthernet 0/0/2.35
[R3-GigabitEthernet0/0/2.35]dhcp select global
```

- After the preceding configurations are complete on R3, check the status of the DHCP server on R3.

```
<R3>display dhcp server statistics
DHCP Server Statistics:
Client Request                  2
  Dhcp Discover                 1
  Dhcp Request                  1
Server Reply                    2
  Dhcp Offer                    1
  Dhcp Ack                      1
Bad Messages                    0
```

- Check the IP address on PC5.

```
PC>ipconfig
IPv4 address          192.168.56.253
Subnet mask           255.255.255.0
Gateway               192.168.56.254
Physical address      54-89-98-39-22-B7
DNS server            192.168.1.1
```

- PC5 has obtained an IP address and can use it to communicate with all hosts. The troubleshooting is complete.

Quiz

1. (Multiple) Which of the following causes are possible for a failure to establish an OSPF neighbor relationship?
   A. Router ID conflict
   B. Area ID inconsistency
   C. Interface mask inconsistency
   D. Process ID inconsistency
2. (TorF) If the level of an interface on an IS-IS router is different from the global router level, the level of the interface takes effect.
3. (Multiple) Which of the following faults may occur in case of a Layer 2 loop?
   A. An attempt to remotely log in to a device fails.
   B. An interface receives a large number of broadcast packets, which can be viewed in the **display interface** command output.
   C. An attempt to log in to a device through the serial port is time consuming.
   D. CPU usage exceeds 70%.

1. ABC
2. False
3. ABCD

Summary

- The structured troubleshooting process involves fault report, fault confirmation, information collection, identification and analysis, cause listing, assessment, step-by-step troubleshooting, fault resolving, and wrap-up work.
- The purpose of troubleshooting is to restore the proper service running status. First, determine a service traffic path before troubleshooting. The layered, comparison, block-based, segment-based, and replacement approaches are used.
- On a LAN, the commonly used methods are to replace hardware to rectify link or device faults and to use STP to rectify LAN loops.
- Network-layer faults are mainly caused by unavailable routes. This course describes the causes and troubleshooting procedures for the failures to establish OSPF and IS-IS neighbor relationships and BGP peer relationships.
- Troubleshooting personnel must have abundant knowledge and be skilled in using multiple troubleshooting approaches. Troubleshooting experience summary also matters.


Thank You
www.huawei.com