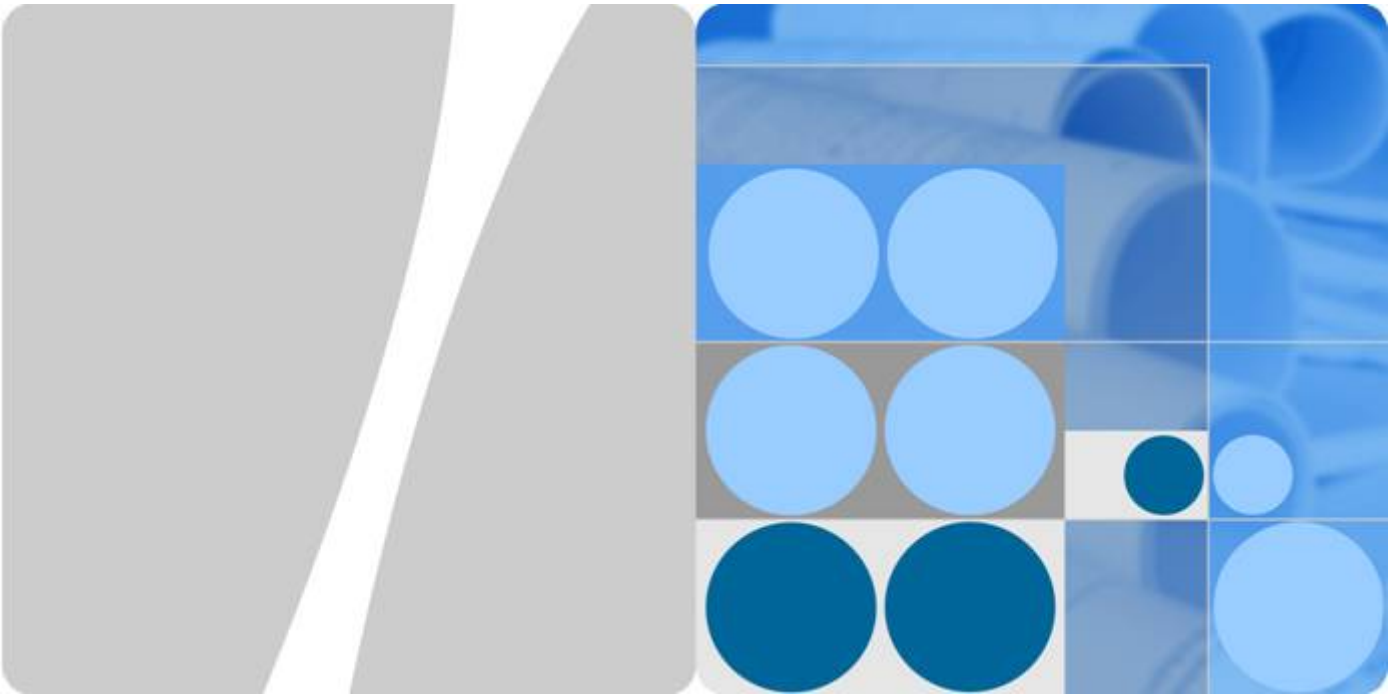


Quidway S3700 Series Ethernet Switches

V100R006C01

Troubleshooting

Issue 01

Date 2011-10-26

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2011. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes the procedure for troubleshooting various services supported by the S3700 in terms of common causes, flowchart, troubleshooting procedure, alarms and logs, and case studies.

This document is intended for:

- System maintenance engineers
- Commissioning engineers
- Network monitoring engineers

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Copyright © Huawei Technologies Co., Ltd.

Command Conventions

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

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

Change History

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

Changes in Issue 01 (2011-10-26)

Initial commercial release.

Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document.....ii

1 Collecting Fault Information.....1

2 Hardware.....3

2.1 PoE Troubleshooting.....4

2.1.1 PoE Function Does Not Take Effect.....4

2.1.2 PSE Cannot Detect a PD.....5

2.1.3 PSE Cannot Provide Power for a PD.....7

3 System.....12

3.1 CPU Troubleshooting.....13

3.1.1 CPU Usage Is High.....13

3.2 Stack Troubleshooting.....18

3.2.1 Stacking Failures Occur.....18

3.3 AutoConfig Troubleshooting.....25

3.3.1 Unconfigured Switch Fails to Obtain an IP Address After Startup.....25

3.3.2 Unconfigured Switch Fails to Obtain Files.....30

3.4 ALS Troubleshooting.....35

3.4.1 Laser Status Does Not Change at ALS Pulse Intervals When a Fiber Link Fails.....35

3.4.2 Interface Cannot Become Up After the Fiber Link Recovers.....37

3.5 Telnet Troubleshooting.....40

3.5.1 The User Fails to Log in to the Server Through Telnet.....40

3.6 FTP Troubleshooting.....43

3.6.1 The User Fails to Log in to the Server Through FTP.....43

3.6.2 The FTP Transmission Fails.....47

3.6.3 The FTP Transmission Rate Is Low.....49

3.7 SNMP Troubleshooting.....50

3.7.1 An SNMP Connection Cannot Be Established.....50

3.7.2 The NMS Fails to Receive Trap Messages from the Host.....54

3.8 RMON Troubleshooting.....57

3.8.1 NM Station Cannot Receive RMON Alarms.....57

3.9 NQA Troubleshooting.....61

3.9.1 A UDP Jitter Test Instance Fails to Be Started.....61

3.9.2 A Drop Record Exists in the UDP Jitter Test Result.....63

Copyright © Huawei Technologies Co., Ltd.

3.9.3 A Busy Record Exists in the UDP Jitter Test Result....64
3.9.4 A Timeout Record Exists in the UDP Jitter Test Result....66
3.9.5 The UDP Jitter Test Result Is "Failed", "No Result" or "Packet Loss"....67
3.10 NTP Troubleshooting....70
3.10.1 The Clock Is Not Synchronized....70
3.11 HGMP Troubleshooting....71
3.11.1 A Candidate Switch Directly Connected to the Administrator Switch Cannot Be Added to the Cluster....71
3.12 LLDP Troubleshooting....78
3.12.1 An Interface Cannot Discover Neighbors....78
3.13 NAP-based Remote Deployment Troubleshooting....81
3.13.1 Fail to Log In to the Newly Deployed Device Through NAP....81
4 Physical Connection and Interfaces....85
4.1 Ethernet Interface Troubleshooting....86
4.1.1 Connected Ethernet Interfaces Down....86
4.1.2 An Ethernet Interface Frequently Alternates Between Up and Down....91
4.2 Eth-Trunk Interface Troubleshooting....95
4.2.1 Eth-Trunk Interface Cannot Forward Traffic....95
4.2.2 Troubleshooting Cases....100
5 LAN....105
5.1 VLAN Troubleshooting....106
5.1.1 Users in a VLAN Cannot Communicate with Each Other....106
5.2 MAC Address Table Troubleshooting....110
5.2.1 Correct MAC Address Entries Cannot Be Generated....110
5.3 QinQ Troubleshooting....115
5.3.1 Traffic Forwarding Fails on a QinQ Interface....115
5.4 MSTP Troubleshooting....119
5.4.1 MSTP Topology Change Leads to Service Interruption....119
5.5 GVRP Troubleshooting....125
5.5.1 No Dynamic VLAN Can Be Created on an Interface....125
5.5.2 Dynamic VLAN Flapping Occurs....129
5.6 MAC Swap Loopback Troubleshooting....131
5.6.1 No Remote Loopback Traffic Is Received by the Tester....132
5.6.2 No Local Loopback Traffic Is Received by the Tester....136
5.7 VLAN Mapping Troubleshooting....140
5.7.1 Users Cannot Communicate After VLAN Mapping Is Configured....140
5.8 Loop Troubleshooting....143
5.8.1 Loops Cause Broadcast Storms....143
5.9 Loopback Detection Troubleshooting....148
5.9.1 Broadcast Storms Still Exist After Loopback Detection Is Configured....148
6 Multicast....151
6.1 Layer 2 Multicast Troubleshooting....152

Copyright © Huawei Technologies Co., Ltd.

6.1.1 Users in User VLANs Fail to Receive Multicast Packets (IGMP snooping)....152
6.1.2 Troubleshooting Cases....155
6.2 Layer 3 Multicast Troubleshooting....157
6.2.1 Multicast Traffic Is Interrupted....157
6.2.2 The PIM Neighbor Relationship Remains Down....160
6.2.3 The RPT on a PIM-SM Network Fails to Forward Data....163
6.2.4 The SPT on a PIM-SM Network Fails to Forward Data....167
6.2.5 MSDP Peers Cannot Generate Correct (S, G) Entries....173
6.2.6 Troubleshooting Cases....177
7 Security....183
7.1 AAA Troubleshooting....185
7.1.1 A User Fails in the RADIUS Authentication....185
7.1.2 A User Fails in the HWTACACS Authentication....190
7.1.3 Troubleshooting Cases....195
7.2 ARP Security Troubleshooting....201
7.2.1 The ARP Entry of an Authorized User Is Modified Maliciously....201
7.2.2 The Gateway Address Is Changed Maliciously....204
7.2.3 User Traffic Is Interrupted by a Large Number of Bogus ARP Packets....206
7.2.4 IP Address Scanning Occurs....209
7.2.5 ARP Learning Fails....211
7.3 NAC Troubleshooting....214
7.3.1 802.1x Authentication of a User Fails....214
7.3.2 MAC Address Authentication of a User Fails....218
7.3.3 MAC Address Bypass Authentication of a User Fails....222
7.3.4 Web Authentication of a User Fails....222
7.4 DHCP Snooping Troubleshooting....225
7.4.1 Users Fail to Go Online After DHCP Snooping Is Configured....225
7.4.2 Troubleshooting Cases....228
7.5 Traffic Suppression Troubleshooting....229
7.5.1 Broadcast Suppression Fails to Take Effect on an Interface....229
7.6 CPU Defense Troubleshooting....231
7.6.1 Protocol Packets Fail to Be Sent to the CPU....231
7.6.2 Blacklist Function Fails to Take Effect....234
7.6.3 Attack Source Tracing Fails to Take Effect....235
7.7 MFF Troubleshooting....237
7.7.1 Users Fail to Access the Internet After MFF Is Configured....237
7.8 ACL Troubleshooting....241
7.8.1 A User-Defined ACL Fails to Take Effect....241
7.8.2 Troubleshooting Cases....243
7.9 PPPoE+ Troubleshooting....245
7.9.1 PPPoE Users Fail to Access the Internet....246
8 QoS....250

Copyright © Huawei Technologies Co., Ltd.

8.1 Traffic Policy Troubleshooting....251
8.1.1 Traffic Policy Fails to Take Effect....251
8.1.2 Troubleshooting Cases....256
8.2 Priority Mapping Troubleshooting (S3700SI or S3700EI)....263
8.2.1 Packets Enter Incorrect Queues....263
8.2.2 Priority Mapping Results Are Incorrect....266
8.2.3 Troubleshooting Cases....268
8.3 Priority Mapping Troubleshooting (S3700HI)....272
8.3.1 Packets Enter Incorrect Queues....272
8.3.2 Priority Mapping Results Are Incorrect....276
8.3.3 Troubleshooting Cases....279
8.4 Traffic Policing Troubleshooting....284
8.4.1 Traffic Policing Based on Traffic Classifiers Fails to Take Effect....284
8.4.2 Interface-based Traffic Policing Results Are Incorrect....284
8.4.3 Troubleshooting Cases....286
8.5 Traffic Shaping Troubleshooting....289
8.5.1 Traffic Shaping Results of Queues Are Incorrect....289
8.5.2 Troubleshooting Cases....293
8.6 Congestion Avoidance Troubleshooting....295
8.6.1 Congestion Avoidance Fails to Take Effect (S3700SI or S3700EI)....295
8.6.2 Congestion Avoidance Fails to Take Effect (S3700HI)....301
8.7 Congestion Management Troubleshooting....304
8.7.1 Congestion Management Fails to Take Effect....304
8.7.2 Troubleshooting Cases....307
9 Reliability....313
9.1 Smart Link Troubleshooting....314
9.1.1 Active/Standby Switchover Failure in a Smart Link Group....314
9.1.2 Monitor Link Group Status Is Down....317
9.2 VRRP Troubleshooting....319
9.2.1 VRRP Group Flaps....319
9.2.2 Two Master Devices Exist in a VRRP Group....323
9.2.3 Trouble Cases....326
9.3 Ethernet OAM Troubleshooting....330
9.3.1 MAC Trace Based on Ethernet OAM 802.1ag Fails....330
9.4 Y.1731 Troubleshooting....333
9.4.1 Troubleshooting of the Fault that One-way Delay Is Not Collected Though One-way Frame Delay Measurement Is Configured for a VLAN....333
9.4.2 Troubleshooting of the Fault that Two-way Delay Is Not Collected Though Two-way Frame Delay Measurement Is Configured for a VLAN....336
9.5 BFD Troubleshooting....339
9.5.1 BFD Session Cannot Go Up....339
9.5.2 Interface Forwarding Is Interrupted After a BFD Session Detects a Fault and Goes Down....343
9.5.3 Changed BFD Session Parameters Do Not Take Effect....344

Copyright © Huawei Technologies Co., Ltd.

9.5.4 Dynamic BFD Session Fails to Be Created....346
9.5.5 Trouble Cases....349
9.6 DLDP Troubleshooting....350
9.6.1 DLDP Fails to Detect a Directly Connected Neighbor....350
9.7 RRPP Troubleshooting....352
9.7.1 RRPP Loop Occurs Temporarily....352
9.8 SEP Troubleshooting....355
9.8.1 Traffic Forwarding Fails on a SEP Link....356

Copyright © Huawei Technologies Co., Ltd.

1 Collecting Fault Information

Collecting Fault Information

After a device fault occurs, collect fault information first. This helps you locate the fault accurately. The following table lists the commands used to collect fault information.

Item	Command	Description
General information	**display diagnostic-information**	This command collects general information about the system. The command output includes the output of the **display current-configuration** and **display device** commands. The general information must be provided when any fault occurs on a network device. Using this command in the Telnet window is recommended. If you run the command on the console port, the command execution lasts a long time and cannot be stopped.
Version information	**display version**	-
Hot patch information	**display patch-information**	-
Device status	**display device**	-
System temperature	**display environment**	-
Current configuration	**display current-configuration**	This command displays all configuration information on a device. You can specify a regular expression to obtain the required configuration information.
System time	**display clock**	-

Copyright © Huawei Technologies Co., Ltd.

Item	Command	Description
Logs	**display logbuffer**	-
Alarms	**display trapbuffer**	-
Interface information	**display interface**	This command displays the status information about all interfaces, whereas the **display current-configuration** command displays the configurations of all interfaces. You can also use the **display current-configuration interface** *interface-type* [*interface-number*] command to check the configuration of a specified interface.
Memory usage	**display memory-usage**	-
CPU usage	**display cpu-usage**	-

Rectifying the Fault

The common troubleshooting methods are:

- Fix or replace the faulty lines.
- Modify the configuration data.
- Restart the system.

After rectifying the fault, you need to run the **save** command in the user view to save current configurations. Otherwise, the configurations you made will be lost if the device restarts.

Copyright © Huawei Technologies Co., Ltd.

2 Hardware

About This Chapter

2.1 PoE Troubleshooting
This chapter describes common causes of power over Ethernet (PoE) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

2.1 PoE Troubleshooting

This chapter describes common causes of power over Ethernet (PoE) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

2.1.1 PoE Function Does Not Take Effect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when the PoE function does not take effect.

Common Causes

This fault is commonly caused by one of the following:

- No PoE power supply is installed.
- The PoE power supply is not functioning properly.

Troubleshooting Flowchart

None.

Troubleshooting Procedure

The following information is displayed when you run **display poe device** command:

```
Error: No current active POE board.
```

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the PoE power supply is installed.

The S3700 PWR model can provide the PoE function only after a PoE power supply is installed. The S3700 uses AC power supplies to provide the PoE function. Each PoE power supply has a fan. Before using the PoE function, ensure that a PoE power supply is installed.

- If the PoE power supply is not installed, install it.
- If the PoE power supply is installed, go to step 2.

Step 2 Check that the PoE power supply is functioning properly.

Run the **display power** command to check the status of the PoE power supply.

- If the PoE power supply is in Abnormal state, replace the PoE power supply.
- If the PoE power supply is in Normal state, the PoE power supply is functioning properly. Go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

2.1.2 PSE Cannot Detect a PD

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the failure to detect a powered device (PD).

Common Causes

This fault is commonly caused by one of the following:

- The PSE is not grounded.
- The network cable between the power source equipment (PSE) and the powered device (PD) is damaged.
- The PD fails.
- The PSE does not support the PD.

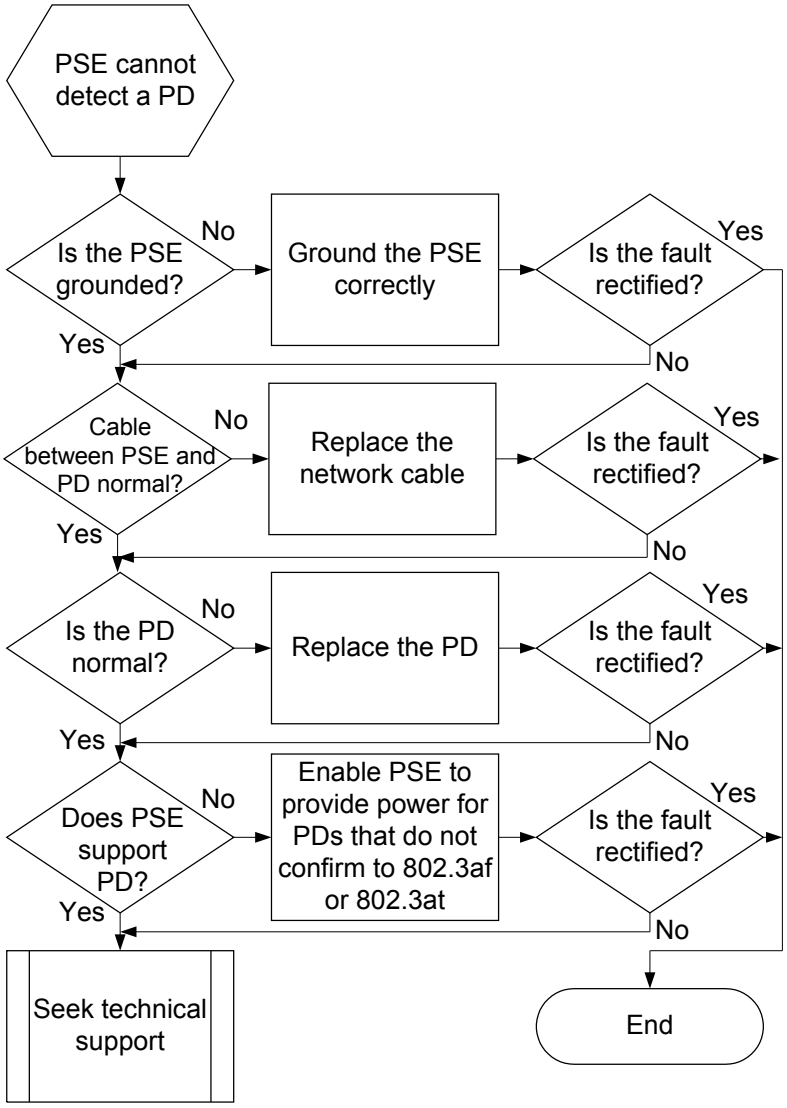
Troubleshooting Flowchart

A PD is connected to a port of the S3700. After the **display poe power-state slot** *slot-id* command is run on the port, the command output shows that the port is in detecting state.

Figure 2-1 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Troubleshooting flowchart for the failure to detect a PD



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the S3700 is grounded.

- If the S3700 is not grounded, ground the S3700 properly.
- If the S3700 is grounded, go to step 2.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The network cable may undergo interference signals, for example, from a high-power base station. If the S3700 is not grounded, the interference signals may affect the detection signals in the network cable. In this case, the S3700 cannot detect the PD, and hence cannot provide power for the PD.

Step 2 Check whether the network cable between the PD and the S3700 functions properly.

- If the network cable is damaged, replace the network cable.
- If the network cable functions properly, go to step 3.

Step 3 Check whether the PD functions properly.

Connect the PD to another working port, and then run the **display poe power-state slot** *slot-id* command to check the port status. If the port is in **Powered** state, the previous port is faulty. If this port is still in Detecting state, the PD is faulty.

- If the PD is faulty, replace the PD.
- If the PD functions properly, go to step 4.

Step 4 Check that the compatibility test function is enabled on the PSE.

Run the **display this** command on the interface connected to the PD to check whether the compatibility test function is enabled.

- If the compatibility test function is not enabled, run the **poe legacy enable** command to enable this function.
- If the compatibility test function is enabled, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

2.1.3 PSE Cannot Provide Power for a PD

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the failure to provide power for a powered device (PD).

Common Causes

This fault is commonly caused by one of the following:

Copyright © Huawei Technologies Co., Ltd.

- The power management mode of the device is manual, but the port is not enabled to provide power for the PD.
- PoE function is not enabled on the port.
- The available power of the device is smaller than the reference power of the PD.
- High PoE power is reserved, so the PoE power supply cannot provide power for PDs.
- The total power consumption of all the PDs on the device reaches the maximum power configured for PDs.

Troubleshooting Flowchart

After a PD is connected to a port of the S3700 (PSE), the S3700 detects the PD but cannot provide power for the PD.

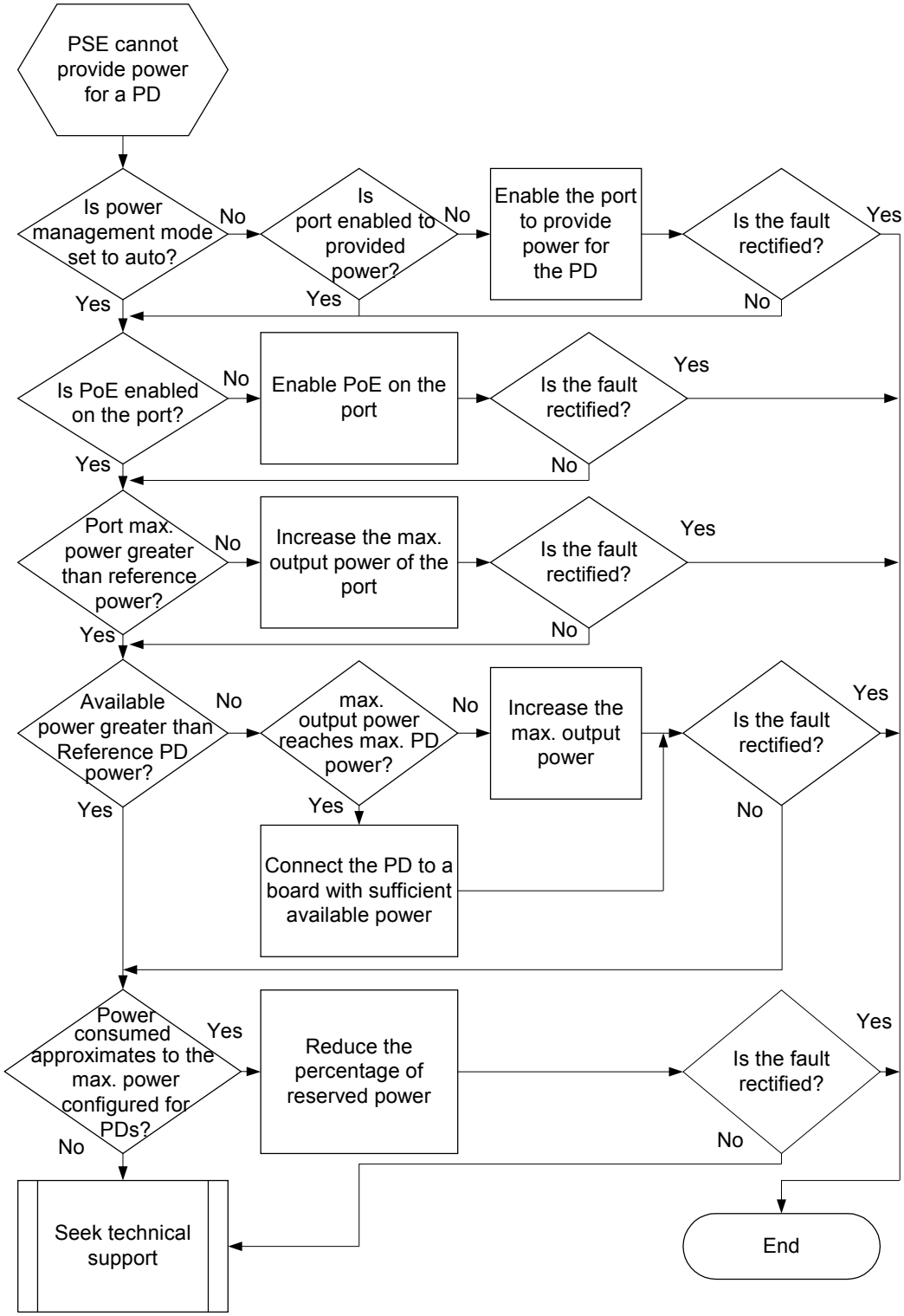
The troubleshooting roadmap is as follows:

- Check whether the PoE power management mode is set to auto or manual.
- Check whether the PoE function is enabled on the port.
- Check whether the maximum power of the port is smaller than the reference power of the port.
- Check whether the available power of the device is smaller than the reference power of the port.
- Check whether the power consumption of all PDs on the S3700 reaches the maximum power configured for PDs.

Figure 2-2 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Troubleshooting flowchart for the failure to provide power for a PD



Troubleshooting Procedure

Copyright © Huawei Technologies Co., Ltd.

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check the power management mode of the device.

NOTE

The power management mode can be auto or manual. The default power management mode is auto. In this mode, the PSE automatically provides power for a PD after detecting and classifying the PD. Run the **display poe information** command to check the power management mode.

- If the power management mode of the device is manual, check whether the port is enabled to provide power for the PD.

  Run the **display poe power-state slot** *slot-id* command. The **PowerOn/Off** field in the command output indicates whether the port is enabled to provide power for the PD.

  - If the port is not enabled to provide power for the PD, run the **poe power-on interface** *interface-type interface-number* command in the system view to enable this function.
  - If the port is enabled to provide power for the PD, go to step 2.
- If the power management mode of the device is auto, go to step 2.

Step 2 Check that the PoE function is enabled on the port.

Run the **display poe power-state slot** *slot-id* command to check whether the PoE function is enabled on the port. If the **Enabled** field is displayed as **enable**, the PoE function is enabled.

- If the PoE function is not enabled, run the **poe enable** command in the interface view to enable it.
- If the PoE function is enabled, go to step 3.

Step 3 Check that the maximum power of the port is greater than the reference power of the PD.

The system identifies the maximum power of a PD, classifies the PD into a certain level, and defines the reference power of each level. Run the **display poe power-state interface** *interface-type interface-number* command to check the maximum power and reference power of the PD connected to the port.

- If the maximum power of the port is smaller than the reference power of the PD, run the **undo poe power** command in the interface view to restore the default maximum power of the port. Alternatively, run the **poe power** command to set a value larger than the reference power after restoring the default maximum power.
- If the maximum power of the port is greater than the reference power of the PD, go to step 4.

Step 4 Check that the available power of the device is greater than the reference power of the PD.

Run the **display poe information** command to check the PoE information of the device, The available power of the device is **Available Total Power**.

- If the available power of the device is smaller than the reference power of the PD, follow these instructions:
  - If the maximum output power configured for the device is smaller than the real maximum power that the device can provide (obtained by the system), run the **poe max-**

Copyright © Huawei Technologies Co., Ltd.

power *slot_max_power* **slot** *slot-id* command to increase the maximum output power of the device. Ensure that available power of the device is then greater than the reference power of the PD.

- If the maximum output power configured for the device has reached the maximum power that the device can provide, the device cannot provide power for any PD.

- If the available power of the PoE is greater than the reference power of the PD, go to step 5.

Step 5 Check that the available power of the power supply is greater than the reference power of the PD.

Certain PoE power may be reserved on the device to meet emergency requirements. By default, 20% PoE Power is reserved. The maximum power for PDs is the total PoE power minus the reserved power.

Run the **display poe-power** command to check the PoE information. In the command output, **Available power value(mW)** indicates the total PoE power in the system, and **Reserved power percent** indicates the percentage of the reserved power. If 100% of the PoE power is reserved, no power can be provided for PDs.

Run the **display poe information** command. In the command output, **Total Power Consumption(mW)** indicates the total PoE power consumption in the system.

- If the total power consumption of all PDs approximates to the maximum power configured for PDs, the device cannot provide power for new PDs. To increase the maximum power for PDs, run the **poe power-reserved** *power-reserved* command to reduce the reserved power.
- If the total power consumption of all PDs on the device is smaller than the maximum power configured for PDs, go to step 6.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

3 System

About This Chapter

3.1 CPU Troubleshooting

3.2 Stack Troubleshooting

3.3 AutoConfig Troubleshooting

3.4 ALS Troubleshooting

3.5 Telnet Troubleshooting

3.6 FTP Troubleshooting

3.7 SNMP Troubleshooting

3.8 RMON Troubleshooting

3.9 NQA Troubleshooting

3.10 NTP Troubleshooting

3.11 HGMP Troubleshooting

3.12 LLDP Troubleshooting
This chapter describes common causes of the LLDP fault, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

3.13 NAP-based Remote Deployment Troubleshooting

Copyright © Huawei Technologies Co., Ltd.

3.1 CPU Troubleshooting

3.1.1 CPU Usage Is High

Common Causes

CPU usage is the percentage of the time during which the CPU executes codes to the total time period. CPU usage is an important index to evaluate device performance.

To view CPU usage, run the **display cpu-usage** command. If you see that CPU usage exceeds 70%, CPU usage is high. A high CPU usage will cause service faults, for example, failed device login. To rectify service faults, see the related troubleshooting.

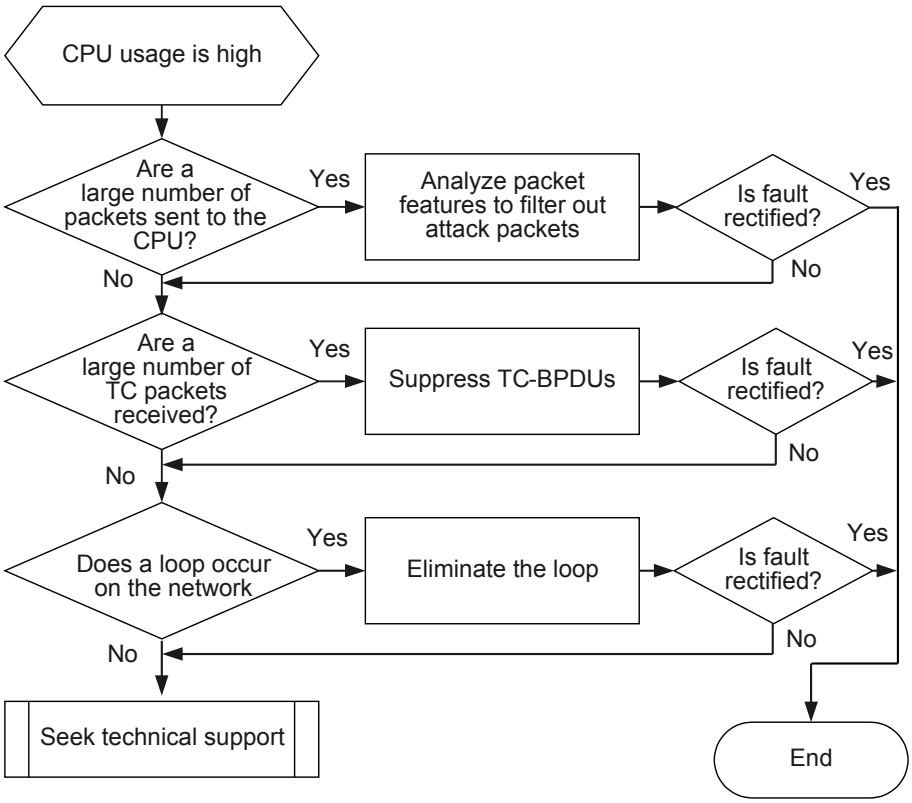
High system CPU usage occurs when CPU usage of some tasks remains high. This fault is commonly caused by one of the following:

- A large number of packets are sent to the CPU when loops or DoS packet attacks occur.
- STP flapping frequently occurs and a large number of TC packets are received, causing the device to frequently delete MAC address entries and ARP entries.

Troubleshooting Flowchart

Figure 3-1 shows the troubleshooting flowchart.

Figure 3-1 CPU usage is high



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

The following procedures can be performed in any sequence.

The command output in the following procedures varies according to the device model. The following procedures describe how to view related information.

Procedure

Step 1 Check the names of tasks with a high CPU usage.

Run the **display cpu-usage** command to check the CPU usage of each task .

Record the names of tasks with CPU usage exceeding 70%.

NOTE

CPU usage of 70% does not necessarily affect services. Services may not be affected when some tasks consume 70% CPU resources but may be affected when some tasks consume 30% CPU resources. This depends on the actual situation.

```
<Quidway> display cpu-usage
CPU Usage Stat. Cycle: 10 (Second)
CPU Usage            : 3% Max: 100%
CPU Usage Stat. Time : 2008-01-04  23:06:09
CPU utilization for five seconds: 3%: one minute: 3%: five minutes: 3%.

TaskName        CPU  Runtime(CPU Tick High/Tick Low)  Task Explanation
BOX              0%         0/   564bd       BOX Output
_TIL             0%         0/       0       Infinite loop event task
_EXC             0%         0/       0       Exception Agent Task
VIDL            97%         0/4ce55d20       DOPRA IDLE
TICK             0%         0/  26a398
bcmRX            0%         0/   97b1a       bcmRX
STND             0%         0/   15efb       STNDStandby task
DEV              0%         0/       0       DEV  Device
FCAT             0%         0/    202a       FCAT FECD task for catch packet
FTS              0%         0/   5b2c0       FTS
RTMR             0%         0/   73ccf       RTMR
IPCQ             0%         0/   2b636       IPCQIPC task for single queue
IPCR             0%         0/       0       IPCR
VP               0%         0/       0       VP  Virtual path task
VPRE             0%         0/       0       VPRE
RPCQ             0%         0/    88d8       RPCQRemote procedure call
XMON             0%         0/       0       XMONVxworks system monitor
VFS              0%         0/       0       VFS Virtual file system
VMON             0%         0/       0       VMONSystem monitor
PNGI             0%         0/       0       PNGI
co0              0%         0/    f4f4       co0 Line user's task
BFDS             0%         0/       0       BFDS
1AGAGT           0%         0/       0       1AGAGT
tExcTask         0%         0/     bbd       tS00
tLogTask         0%         0/       0       tS01
tShell           0%         0/       0       tS02
root             0%         0/       0       tS03
bcmDPC           0%         0/    2c43       tS09
bcmCNTR.0        0%         0/  208b59       tS0a
bcmTX            0%         0/    3ea1       tS0b
bcmL2X.0         0%         0/  46ba9d       tS0c
frag_add         0%         0/       0       tS0d
```


Copyright © Huawei Technologies Co., Ltd.

```
frag_del          0%          0/       0       tS0e
linkscan          0%          0/  1a70d8       tS0f
INFO              0%          0/    d6db       INFOInformation center
SAPP              0%          0/    2d67       SAPP
NQAC              0%          0/       0       NQAC
NQAS              0%          0/       0       NQAS
ALM               0%          0/       0       ALM  Alarm
SRM               0%          0/    9493       SRM  System Resource Manage
U  0              0%          0/       0       U  0 user command process task
FIB6              0%          0/       0       FIB6IPv6 FIB
BFD               0%          0/   3199f       BFD Bidirection Forwarding Detect
SNPG              0%          0/   4a29a       SNPG Multicast Snooping
OAM1              0%          0/       0       OAM1 EOAM Adapter
NAP               0%          0/       0       NAP
EOAM              0%          0/    2b41       EOAMEthernet OAM 802.1ag
1731              0%          0/    49ee       1731Ethernet OAM Y1731
MCSW              0%          0/       0       MCSW Mulitcast Switch
L3M4              0%          0/       0       L3M4
L3I4              0%          0/       0       L3I4
NDMB              0%          0/       0       NDMB
NDIO              0%          0/       0       NDIO
L3MB              0%          0/       0       L3MB
L3IO              0%          0/       0       L3IO
PNGM              0%          0/       0       PNGM
FECD              0%          0/    2aa4       FECD Forward Equal Class Develope
PPI               0%          0/    5cf7       PPI Product Process Interface
IFPD              0%          0/  825989       IFPD Ifnet Product Adapt
STFW              0%          0/       0       STFW Super task forward
XQOS              0%          0/   62a2a       XQOS Quality of service
SMLK              0%          0/   204a4       SMLK Smart Link Protocol
CDM               0%          0/    22d9       CDM
SOCK              0%          0/   4bdc1       SOCKPacket schedule and process
FIB               0%          0/       0       FIB Forward Information Base
MFIB              0%          0/       0       MFIBMulticast forward info
IFNT              0%          0/       0       IFNTIfnet task
VT0               0%          0/  1ea87f       VT0 Line user's task
VTYD              0%          0/   3641d       VTYDVirtual terminal
RSA               0%          0/       0       RSA RSA public-key algorithms
AGNT              0%          0/       0       AGNTSNMP agent task
TRAP              0%          0/   8b66f       TRAPSNMP trap task
NTPT              0%          0/  5128c0       NTPTNetwork time protocol task
CFM               0%          0/       0       CFM Configuration file management
HS2M              0%          0/       0       HS2MHigh available task
WEBS              0%          0/   88878       WEBSERVER
ACL               0%          0/    1f19       ACL
SECE              0%          0/   55eea       SECE Security
DEFD              0%          0/     589       DEFD CPU Defend
STRA              0%          0/     502       STRA Source Track
MFF               0%          0/    3665       MFF MAC Forced Forwarding
LDT               0%          0/    1eac       LDT  Loopback Detect
BFDA              0%          0/       0       BFDA BFD Adapter
MSYN              0%          0/   1ed40       MSYN Mac Synchronization
UCM               0%          0/     95a       UCM  User Control Management
AM                0%          0/    4c35       AM   Address Management
DHCP              0%          0/    4c49       DHCP Dynamic Host Config Protocol
AAA               0%          0/       0       AAA  Authen Account Authorize
TM                0%          0/       0       TM   Transmission Management
RDS               0%          0/       0       RDS  Radius
TACH              0%          0/   256ae       TACHWTACACS
WEB               0%          0/       0       WEB  Web
PTAL              0%          0/       0       PTAL Portal
EAP               0%          0/    1327       EAP  Extensible Authen protocol
SAM               0%          0/       0       SAM  Service Agent Module
POE+              0%          0/       0       POE+ PPP Over Ethernet Plus
U 34              0%          0/     d94       U 34 user command process task
SMAG              0%          0/       0       SMAG Smart Link Agent
GVRP              0%          0/       0       GVRP Protocol
DLDP              0%          0/    2eaa       DLDP Protocol
LLDP              0%          0/    280c       LLDP Protocol
```


Copyright © Huawei Technologies Co., Ltd.

```
BPDU              0%          0/     8dc       BPDU Adapter
EFMT              0%          0/       0       EFMTEST 802.3AH Test
ADPT              0%          0/       0       ADPT Adapter
VT1               0%          0/    a4e7       VT1 Line user's task
MSTP              0%          0/    369e       MSTP_ADP MSTP Adapter
ALS               0%          0/   27b9f       ALS  Loss of Signal
U 35              0%          0/       0       U 35 user command process task
ROUT              0%          0/  2178e6       ROUTRoute task
UTSK              0%          0/       0       UTSK
APP               0%          0/       0       APP
IP                0%          0/   59b3c       IP
LINK              0%          0/   5501c       LINK
VRPT              0%          0/    4bb5       VRPT
HOTT              0%          0/       0       HOTT
TNQA              0%          0/    491d       TNQAC
TTNQ              0%          0/       0       TTNQAS
TARP              0%          0/       0       TARPING
L2                0%          0/   26b69       L2
VRRP              0%          0/  182af6       VRRP
L2_P              0%          0/   5e1e7       L2_PR
ARP               0%          0/       0       ARP
SRMT              0%          0/  1e2d41       SRMT System Resource Manage Timer
INTR              0%          0/       0       INTR External Interrupt
RMON              0%          0/    3ee5       RMONRemote monitoring
VT                0%          0/       0       VT   Virtual Transfer
OS                3%          0/ 260d360       Operation System
```

The following table lists common tasks.

Task	Description
VIDL	Idle task. A higher CPU usage of the VIDL task indicates that the CPU is more idle.
SOCK	Packet receiving and processing task. If this task has a high CPU usage, the CPU receives and processes a large number of protocol packets, which may be caused by IP packet attacks.
RPCQ	Inter-board communication task. The RPCQ task and SOCK task need to be analyzed together. If the device receives a large number of packets and needs to respond to these packets, the RPCQ task has a high CPU usage. This may be caused by packet attacks.
ROUT	Route processing task. When a large number of routes need to be learned or many of them flap, the ROUT task has a high CPU usage. Check whether the routing module is faulty according to the related routing information.
bcmRX	Bottom-layer packet receiving task. A higher CPU usage of the bcmRX task indicates that the CPU receives a larger number of packets.

Step 2 Check whether a large number of packets are sent to the CPU.

Run the **display cpu-defend statistics** command to check statistics about the packets sent to the CPU and focus on the **Drop** field.

Copyright © Huawei Technologies Co., Ltd.

```
<Quidway> display cpu-defend statistics
Statistics on slot 0:
------------------------------------------------------------------------------
Packet Type         Pass(Bytes)  Drop(Bytes)   Pass(Packets)   Drop(Packets)
------------------------------------------------------------------------------
arp-miss                   N/A          N/A               0               0
arp-request                N/A          N/A            5608               0
bgp                        N/A          N/A               0               0
dns                        N/A          N/A               0               0
fib-hit                    N/A          N/A               0               0
ftp                        N/A          N/A               0               0
hotlimit                   N/A          N/A               0               0
http                       N/A          N/A               0               0
hw-tacacs                  N/A          N/A               0               0
icmp                       N/A          N/A               5               0
icmpv6                     N/A          N/A               0               0
isis                       N/A          N/A               0               0
nd                         N/A          N/A               0               0
ntp                        N/A          N/A               0               0
ospf                       N/A          N/A               0               0
ospfv3                     N/A          N/A               0               0
radius                     N/A          N/A               0               0
reserved-multicast         N/A          N/A               0               0
rip                        N/A          N/A               0               0
ripng                      N/A          N/A               0               0
snmp                       N/A          N/A               0               0
ssh                        N/A          N/A               0               0
tcp                        N/A          N/A               0               0
telnet                     N/A          N/A            2046               0
ttl-expired                N/A          N/A               0               0
------------------------------------------------------------------------------
```

- If the value of the **Drop** field of a certain type of packets is great and CPU usage is high, packet attacks occur. Go to step 5.
- If the value of the **Drop** field is within the specified range, go to step 3.

Step 3 Check whether a large number of TC packets are received.

If STP is enabled on a device, the device deletes MAC address entries and ARP entries when receiving TC-BPDUs. If an attacker sends pseudo TC-BPDUs to attack the device, the device will receive a large number of TC-BPDUs within a short period of time and frequently delete MAC address entries and ARP entries. As a result, CPU usage of the device becomes high.

Run the **display stp tc-bpdu statistics** command to check statistics about the received TC packets and TCN packets.

```
<Quidway> display stp tc-bpdu statistics
 -------------------------- STP TC/TCN information --------------------------
 MSTID Port                      TC(Send/Receive)      TCN(Send/Receive)
 0     Ethernet0/0/1             1/0                   0/0
 0     Ethernet0/0/2             1/0                   0/0
 0     Ethernet0/0/3             1/0                   0/0
 0     Ethernet0/0/4             1/0                   0/0
 0     Ethernet0/0/24            1/0                   0/0
```

- If a large number of TC packets and TCN packets are received, run the **stp tc-protection** command in the system view to suppress TC-BPDUs. After this command is used, only three TC packets are processed within a Hello interval by default. Run the **stp tc-protection threshold** command to set the maximum number of TC packets that can be processed. To change the hello interval, run the **stp timer hello** command.

  ```
  [Quidway] stp tc-protection
  [Quidway] stp tc-protection threshold 5
  [Quidway] stp timer hello 120
  ```

- If a small number of TC packets are received, go to step 4.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Check whether loops occur on the network.

When multiple interfaces of a device belong to the same VLAN, if a loop occurs between two interfaces, packets are forwarded only between these interfaces in the VLAN. Consequently, CPU usage of the device becomes high.

Run the **display this** command in the VLAN view to check whether the device is enabled to generate an alarm when MAC address flapping is detected.

```
[Quidway-vlan7] display this
#
vlan 7
 loop-detect eth-loop alarm-only
#
```

- If this function is not configured, run the **loop-detect eth-loop alarm-only** command to configure this function. If a loop occurs on the network, an alarm is generated when two interfaces of the device learn the same MAC address entry. For example:

  ```
  Jan 17 2011 19:40:16 L2_SRV_78 L2IFPPI/4/MFLPVLANALARM:OID
  1.3.6.1.4.1.2011.5.25.160.3.7 Loop exists in vlan 7, for flapping mac-address
  0000-0000-0004 between port Eth0/0/2 and port Eth0/0/3
  ```

  Check the interface connection and networking information according to the alarm:

  - If no ring network is required, shut down one of the two interfaces according to the networking diagram.
  - If the ring network is required, disable the MAC flapping alarm function and enable loop prevention protocols such as STP.
- If the **loop-detect eth-loop alarm-only** command is used on the device but no alarm is generated, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the device

----End

Relevant Alarms and Logs

Relevant Alarms

None

Relevant Logs

- VOSCPU/4/CPU_USAGE_HIGH

3.2 Stack Troubleshooting

NOTE

The S3700HI does not support stack.

3.2.1 Stacking Failures Occur

Copyright © Huawei Technologies Co., Ltd.

Common Causes

Switches in a stack can form a ring or chain topology, as shown in **Figure 3-2** and **Figure 3-3**. Stack cables are connected to stack ports on the switches.

Figure 3-2 Ring topology

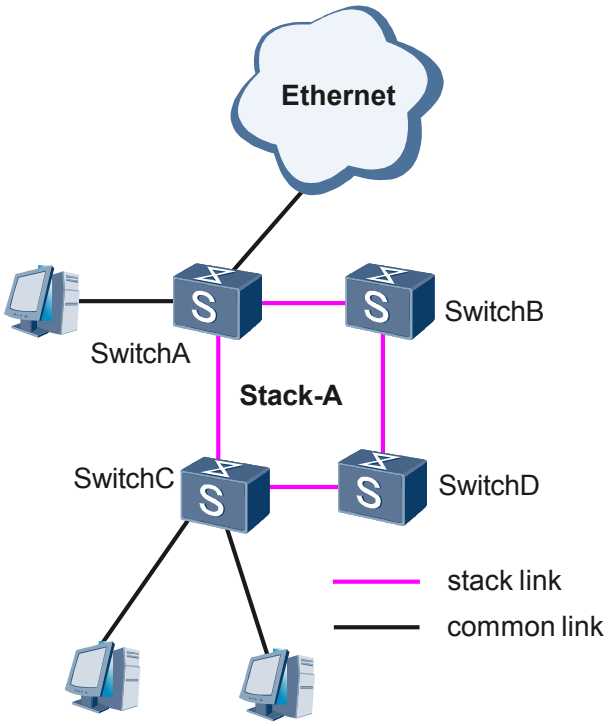
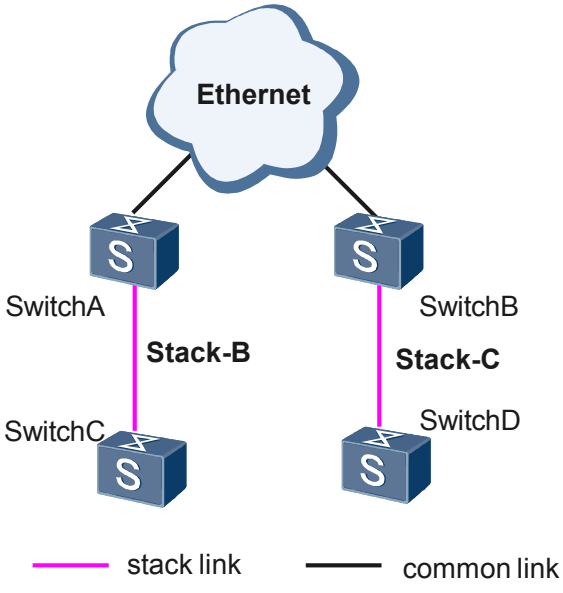


Figure 3-3 Chain topology



Copyright © Huawei Technologies Co., Ltd.

A stacking failure refers to one of the following situations:

- Switches cannot set up a stack.
- A switch fails to join a stack.
- A stack cannot be set up again after it splits.

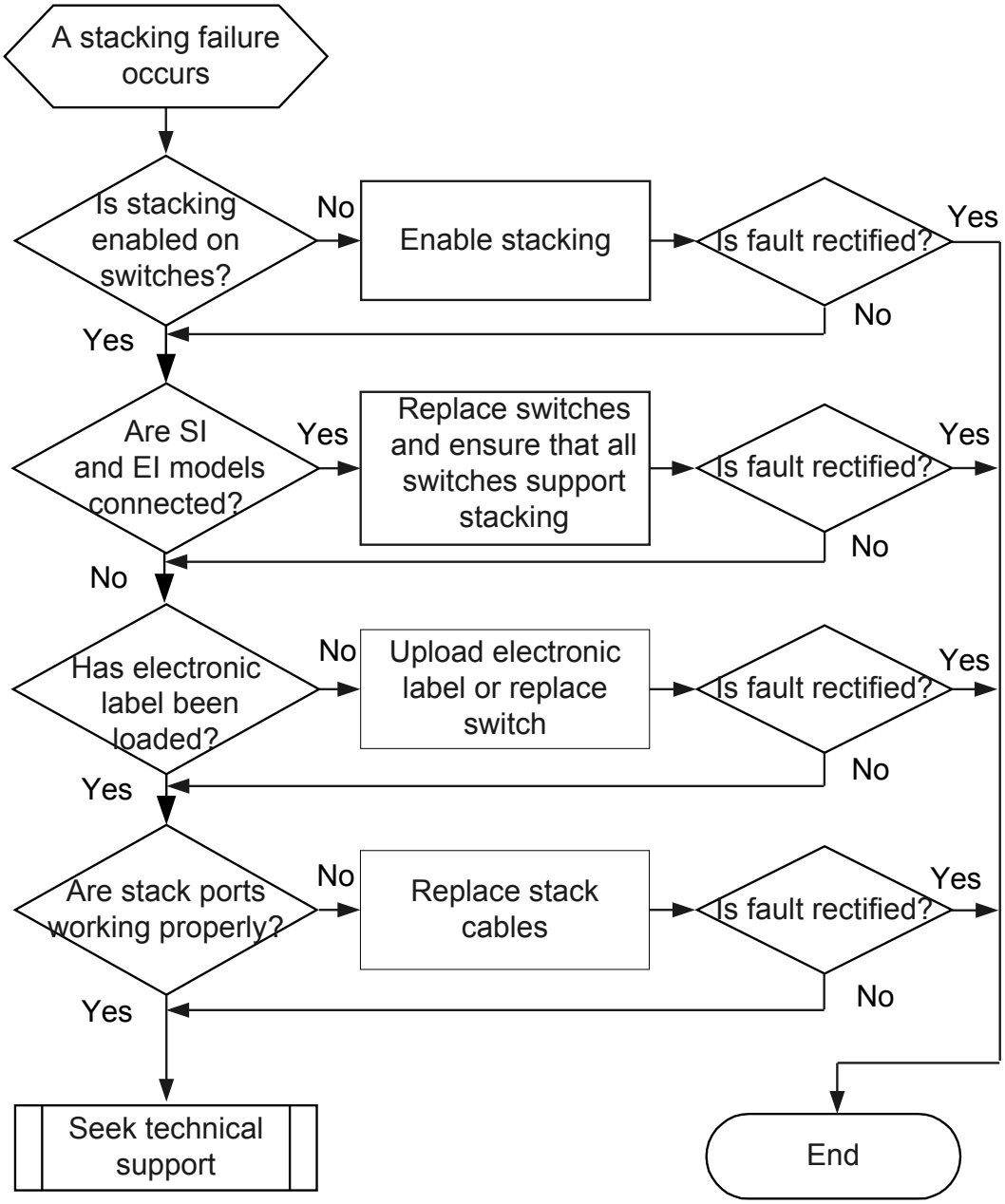
This fault is commonly caused by one of the following:

- The stacking function is disabled on the switches.
- The switch models are different. For example, an EI model is connected to an SI model.
- Some switches, for example, S3700-52P-EI version A, do not support the stacking function.
- A switch does not have any electronic label or has an incorrect electronic label.
- Some stack cables are faulty.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Stack troubleshooting flowchart



Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

CAUTION

Before replacing a switch, power off the switch.

Perform the following steps on each switch where a stacking failure occurs.

Procedure

Step 1 Check that the stacking function is enabled on the switch.

Run the **display stack** command to check the stack status.

- If the following information is displayed, the stacking function is disabled.

```
<Quidway> display stack
Error: The stack function is not enabled.
```

  1. Run the **stack enable** command in the system view to enable the stacking function, and then restart the switch.
  2. Check whether the stack cables are installed properly. If a stack cable is loose, reconnect it. S3700s can form a ring stack or chain stack. The ring stack is recommended because it is more stable and reliable.

- If the following information is displayed, the stacking function is enabled. Go to step 2.

```
<Quidway> display stack
Stack topology type:
Link
Stack system MAC:
0200-0001-0000
MAC switch delay time:
never
Stack reserved vlanid :
4093
Slot#     role        Mac address      Priority   Device
type
------    ----        --------------   ------
-------
    1     Master      0200-0001-0000   100        S3700-28TP-PWR-
EI
```

Step 2 Check the device model.

Run the **display elabel** command to view the electronic label. The **Description** field in the command output indicates the device model.

```
<Quidway> display elabel
/$[System Integration Version]
/$SystemIntegrationVersion=3.0


[Slot_0]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0


[Main_Board]


/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0
```


Copyright © Huawei Technologies Co., Ltd.

```
[Board Properties]
BoardType=CX22EMGEB
BarCode=21023518320123456789
Item=02351832
Description=Quidway S3700-28TP-PWR-EI,LS3Z728CM,S3700-28TP-PWR-EI
Mainframe
Manufactured=2009-02-05
VendorName=Huawei
IssueNumber=
CLEICode=
BOM=
```

- If the switch is not of a different model from other switches, replace the switch.

  NOTE

  Switches of EI and SI models cannot form a stack.

- If all the switches are of the same model, go to step 3.
- If the device model is **S3700-52P-EI**, run the **display version** command to check the version of the print circuit board (PCB). If the PCB version is **VER A**, the switch does not support stacking. Remove the switch from the stack or replace it with a switch that supports stacking.

```
<Quidway> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.70 (S3700-52 V100R006C00)
Copyright (C) 2003-2010 HUAWEI TECH CO., LTD
Quidway S3700-52P-EI Routing Switch uptime is 0 week, 3 days, 18 hours, 28 min
utes

EFFEC 0(Master) : uptime is 0 week, 3 days, 18 hours, 27 minutes
128M bytes DDR Memory
16M bytes FLASH
Pcb      Version :  VER A
Basic  BOOTROM  Version :  330 Compiled at Nov 24 2010, 21:55:11
CPLD   Version : 9
Software Version : VRP (R) Software, Version 5.70 (S3700-52 V100R006C00)
FANCARD information
Pcb      Version : FAN VER B
PWRCARD I information
Pcb      Version : PWR VER A
```

Step 3 Check that the correct electronic label has been loaded to the switch.

Run the **display elabel** command to view the electronic label.

- If all fields under **[Board Properties]** are empty, no electronic label is loaded to the switch. Replace the switch.

```
<Quidway> display
elabel
/$[System Integration
Version]
/
$SystemIntegrationVersion=3.0


[
Slot_0]
/$[Board Integration
Version]
/
$BoardIntegrationVersion=3.0


[
Main_Board]


/$[ArchivesInfo
```


Copyright © Huawei Technologies Co., Ltd.

```
Version]
/
$ArchivesInfoVersion=3.0


[Board
Properties]
BoardType=
BarCode=
Item=
Description=
Manufactured=
VendorName=
IssueNumber=
CLEICode=
BOM=
```

- If fields under **[Board Properties]** are not empty, the electronic label has been loaded to the switch. Go to step 4.

```
<Quidway> display
elabel
/$[System Integration
Version]
/
$SystemIntegrationVersion=3.0


[
Slot_0]
/$[Board Integration
Version]
/
$BoardIntegrationVersion=3.0


[
Main_Board]


/$[ArchivesInfo
Version]
/
$ArchivesInfoVersion=3.0


[Board
Properties]
BoardType=CX22EFFEC

BarCode=21023518320123456789
Item=02351832
Description=Quidway S3700-28TP-PWR-EI,LS3Z728CM,S3700-28TP-PWR-EI
Mainframe
Manufactured=2009-02-05
VendorName=Huawei
IssueNumber=
CLEICode=
BOM=
```

Step 4 Check that the stack cables are functioning properly.

Stack ports on an S3700 are 100/1000BASE-X Ethernet ports but not combo ports. Ensure that stack cables are connected to correct ports. For the positions of the stack cables, see the hardware description.

Run the **display stack port all** command to check the status of all stack ports.

- If all stack ports are Up, go to step 5.

Copyright © Huawei Technologies Co., Ltd.

```
<Quidway> display stack port all
Show stack port info:
Slot 0:
STACK 1,     status: UP,      peer: 1
STACK 2,     status: UP,      peer: 1
Slot 1:
STACK 1,     status: UP,      peer: 0
STACK 2,     status: UP,      peer: 0
```

- If a stack port is Down, check whether the device connected to the port has been powered off or is restarting. If so, check the port status after the remote device restarts. If not, replace the stack cable on this port.

```
<Quidway> display stack port all
Show stack port info:
Slot 0:
STACK 1,     status: DOWN,      peer:
NONE
STACK 2,     status: DOWN,      peer:
NONE
```

If the fault persists, go to 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the S3700s

----End

Relevant Alarms and Logs

Relevant Alarms

- A stack port goes Up: FSP_1.3.6.1.4.1.2011.5.25.183.1.22.1 hwStackLinkUp
- A stack port goes Down: FSP_1.3.6.1.4.1.2011.5.25.183.1.22.2 hwStackLinkDown
- A switch has joined a stack: FSP_1.3.6.1.4.1.2011.5.25.183.1.22.6 hwStackStackMemberAdd
- A switch has left a stack: FSP_1.3.6.1.4.1.2011.5.25.183.1.22.7 hwStackStackMemberLeave

Relevant Logs

None.

3.3 AutoConfig Troubleshooting

3.3.1 Unconfigured Switch Fails to Obtain an IP Address After Startup

Common Causes

Copyright © Huawei Technologies Co., Ltd.

In AutoConfig implementation, the DHCP server and switches can be deployed in the same network segment or different network segments, as shown in **Figure 3-5** and **Figure 3-6**. No configuration has been performed on SwitchA, SwitchB, and SwitchC.

Figure 3-5 AutoConfig network diagram (in the same network segment)

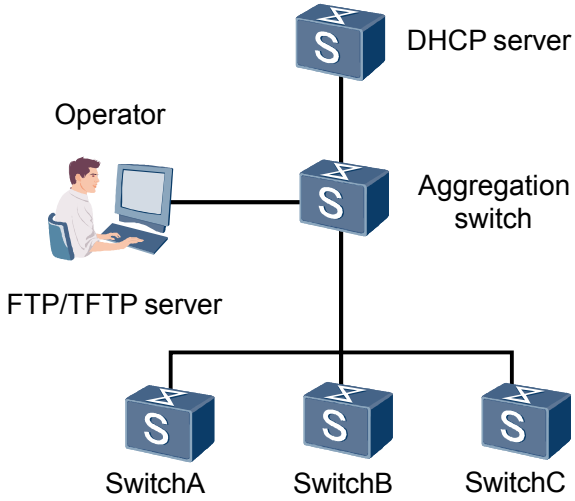
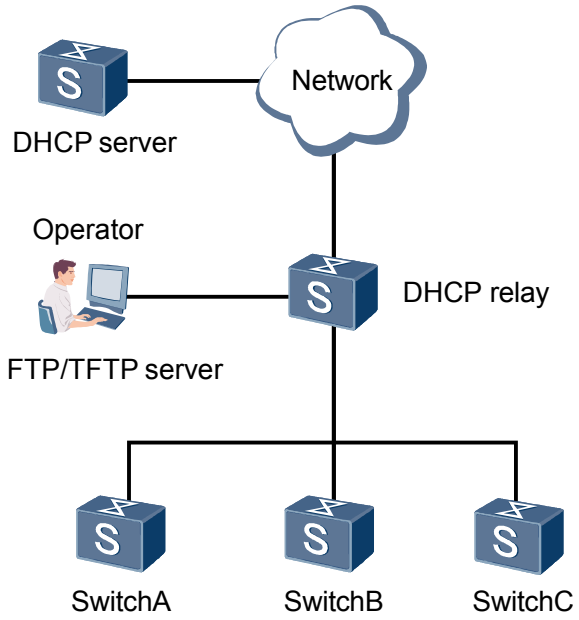


Figure 3-6 AutoConfig network diagram (in different network segments)



An unconfigured switch has started and been running for 5 minutes, but no IP address is allocated to it from the DHCP server.

This fault is commonly caused by one of the following:

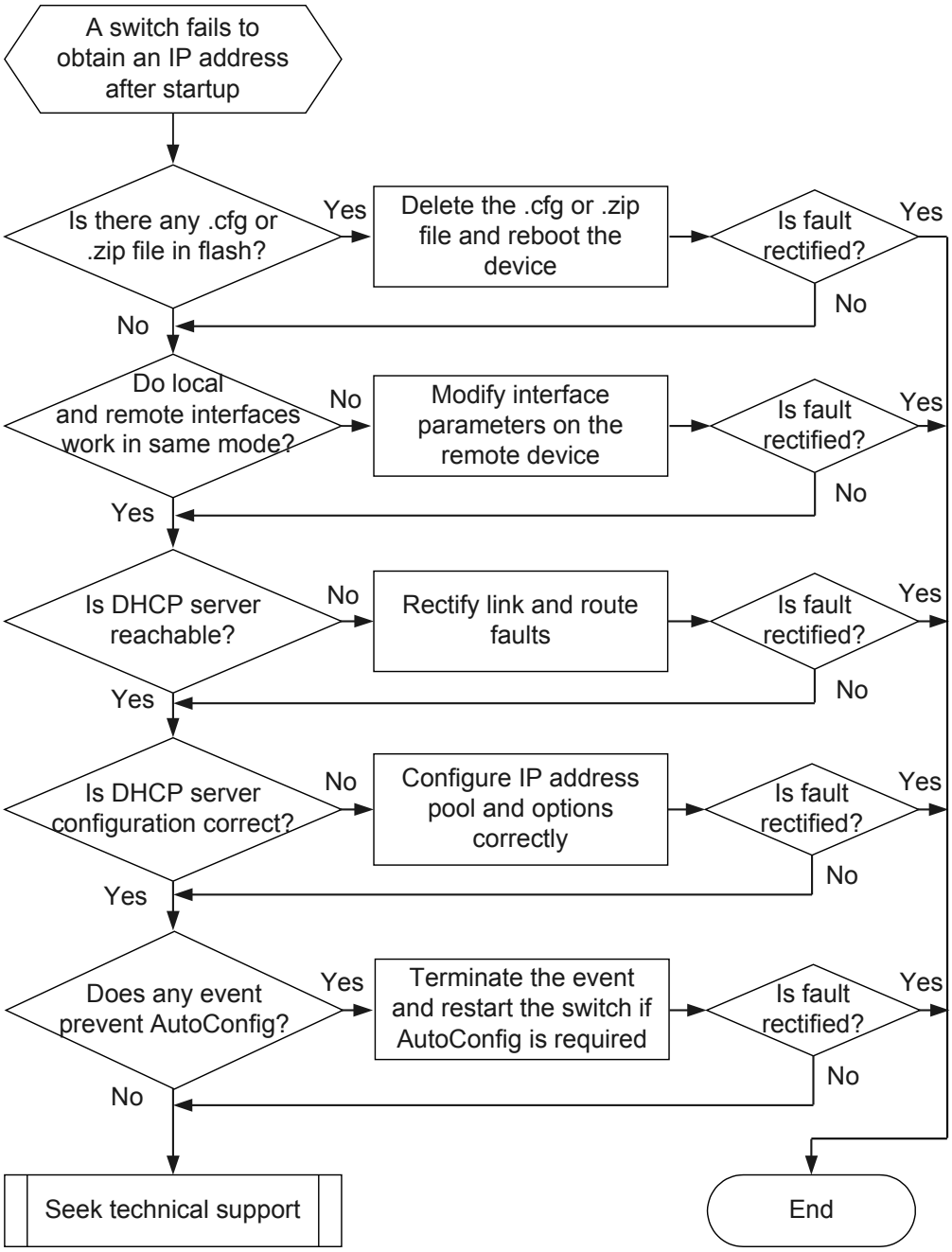
- There is a .cfg or .zip file in the flash memory.

Copyright © Huawei Technologies Co., Ltd.

- The local interface parameters such as the rate and duplex mode are different from those of the remote interface.
- There is no reachable route between the DHCP server and the switch.
- The DHCP server configuration (IP address pool and option configuration) is incorrect.
- An event prevents the AutoConfig process. For example, the switch joins a Huawei Group Management Protocol (HGMP) cluster, or the switch obtains a file from the USB port.

Troubleshooting Flowchart

Figure 3-7 Troubleshooting flowchart for an IP address allocation failure in the AutoConfig process



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the switch has a configuration file.

Check whether there is any .cfg or .zip file (other than *web.zip or web.zip) in the flash memory. Log in to the switch from the console port and run the **dir** command.

- If a .cfg or .zip file is displayed, run the **delete** command to delete the file, and then reboot the switch.
- If no .cfg or .zip file is displayed, go to step 2.

Step 2 Check the physical connection between the local and remote devices.

The connected interfaces must work in the same mode. By default, 10M electrical ports, 100M electrical ports, GE electrical ports, and GE optical ports on Huawei switches work in auto-negotiation mode; 100M optical ports work in non-auto negotiation mode. If the interfaces work in different modes, modify interface parameters on the remote device, that is, the DHCP relay agent or DHCP server.

If the interfaces work in the same mode, go to step 3.

Step 3 Ensure that there is a reachable route between the DHCP server and the switch.

Packets sent from an unconfigured switch are untagged. The DHCP server can allocate an IP address to the switch only if it can receive the untagged packets.

Check whether any DHCP relay agent is deployed between the DHCP server and the switch to determine whether they are in the same network segment.

- If they are in the same network segment, ensure that the untagged packets sent from the switch can reach the DHCP server, and that the IP address of the DHCP server interface connected to the switch is in the same network segment as the address pool on the DHCP server.
- If they are in different network segments, ensure that:
  - On the DHCP relay agent closest to the switch, the interface connected to the switch can process untagged packets.
  - The interface IP address is within the range specified in the IP address pool on the DHCP server and is the gateway address of the DHCP server.
  - There is a reachable route between the interface and the DHCP server.

If there is a reachable route between the DHCP server and the switch, go to step 4.

Step 4 Check the DHCP server configuration required for AutoConfig.

Copyright © Huawei Technologies Co., Ltd.

Item	Solution
IP address pool	If the DHCP server has no IP address pool, configure one according to the IP address plan.
Option 147, Option 143, Option 150, and Option 66	1. Check whether Option 147 is configured. If Option 147 is not configured or is set to AutoConfig (case-sensitive), go to step b. If it is set to a value other than AutoConfig, change it to AutoConfig. 2. Check whether Option143 (FTP server IP address), Option 150 (TFTP server IP address), or Option 66 (TFTP server name) is configured. If none of them is configured, configure one of them. If Option 143 is configured, you must also configure Option 141 (FTP user name) and Option 142 (FTP password). If Option 66 is configured, you must also configure Option 6 (DNS server name).

If the DHCP server configuration is correct, go to step 5.

Step 5 Check whether any event conflicting with the AutoConfig process has occurred.

The AutoConfig process stops when any of the following events occur:

- The switch has joined a Huawei Group Management Protocol (HGMP) cluster.

  You can log in to the switch and run the **display cluster** command to check the role of the switch in the cluster.
- The USB port of the switch is connected to a storage device and the switch has obtained a version file or configuration file from the storage device.

When any of the events occurs, determine whether the AutoConfig process is required. If yes, terminate the event and restart the switch. If the fault persists, go to step 6.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

3.3.2 Unconfigured Switch Fails to Obtain Files

Common Causes

In the AutoConfig process, after an unconfigured switch is assigned an IP address and obtains the file server IP address, it starts to obtain required files, including the version file, patch file, configuration file, and Web system file. You can view logs on the file server to check whether the switch has successfully obtained the files. Alternatively, run the **display autoconfig-status** command on the switch. If the AutoConfig status is suspend, the switch fails to obtain the files.

NOTE

Among the preceding files, the configuration file is mandatory for a switch, and the other files are optional.

If the switch fails to obtain the files, it starts the retry timer and restarts the AutoConfig process when the retry timer expires. The retry timer length is 30 minutes within 3 days after the first failure to obtain the files, and is 2 hours 3 days later. If the switch fails to obtain the files within 30 days, the AutoConfig process stops.

You can also run the **autoconfig getting-file restart** command in the system view to start the AutoConfig process immediately. If the switch fails to obtain the files after the command is executed, the system attempts to obtain the files at intervals.

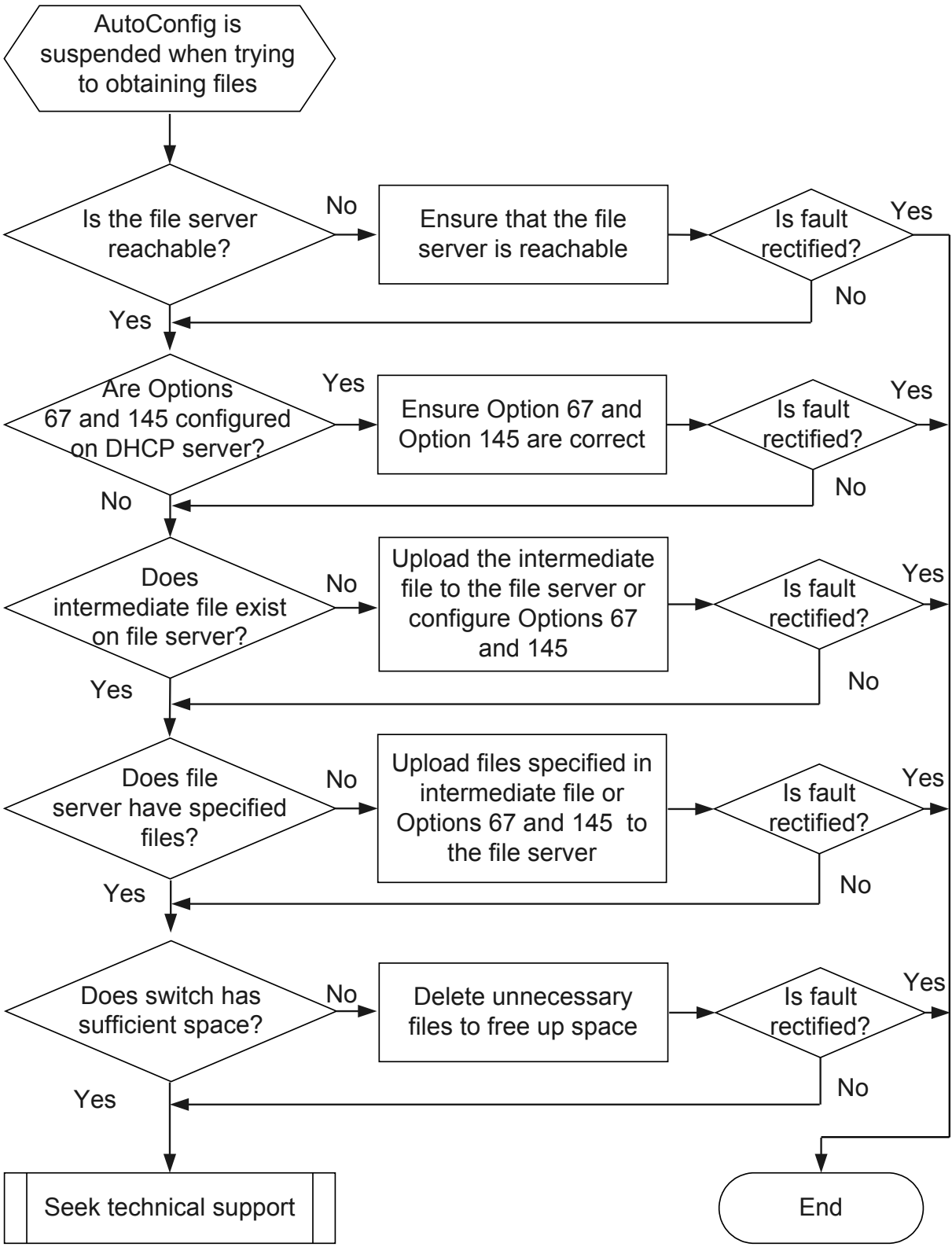
This fault is commonly caused by one of the following:

- The file server, a TFTP server or an FTP server, is unreachable. For example, there is no reachable route to the file server or the FTP user name and password are incorrect.
- Option 67 is not configured on the DHCP server and no intermediate file is available on the file server.
- Option 67 is not configured and the intermediate file does not contain the configuration file name, that is, cfgfile.
- The vrpVer field indicating the version name in Option 145 or the intermediate file does not contain the version number.
- The current system software version name is the same as that defined in Option 145 or the intermediate file, but the version numbers are different.
- The flash memory does not have sufficient space for the files.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 3-8 Troubleshooting flowchart for a failure to obtain the files



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

- The following is the general troubleshooting procedure. You can also log in to the unconfigured switch, run the **display autoconfig-status** command to check the causes of the failure, and rectify the fault accordingly. After the fault is rectified, run the **autoconfig getting-file restart** command to restart the AutoConfig process.
- Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the TFTP server or FTP server is reachable.

1. Check the route between the switch and the server.

   Use the **ping** command to check whether the switch can ping the server.

   - If the ping operation fails, rectify the link fault according to A Ping Operation Fails.
   - If the ping operation succeeds, go to step b.

2. Check the options configured on the DHCP server.

   The switch checks for the following options in a DHCP reply packet in sequence. If any of the options is found in the reply packet, the switch processes the packet.

Option	Description
Option 150	TFTP server IP address.
Option 143	FTP server IP address. Option 143 is used with Option 141 (FTP user name) and Option 142 (FTP user password).
Option 66	TFTP server name. Option 66 is used with Option 6 (DNS server IP address).

If the file server is reachable, go to step 2.

Step 2 Check whether Option 67 and Option 145 are configured on the DHCP server.

- Option 67 specifies the configuration file name; Option 145 specifies the version file name, version number, patch file name, and Web system file name and is optional. If the two options are configured, the switch obtains the files specified by the options. Check whether the file names in the options are the same as those on the file server. Check the contents of the intermediate file and go to step 4.

  NOTE

  The following is an example of Option 145:

  vrpfile=S3700V100R006C00.cc;vrpver=V100R006C00;patchfile=S3700-pat.pat;webfile=V100R006C00web.zip

  In Option 145, the vrpfile field must contain the version number. The file name is in the SxxxxVxxxRxxxCxxSPCxxx.cc format. SPCxxx is optional.

Copyright © Huawei Technologies Co., Ltd.

- If neither Option 67 nor Option 145 is configured, the AutoConfig process searches for the configuration file name in the intermediate file. Go to step 3.

Step 3 Check whether an intermediate file exists on the file server.

Searches for the file named **lswnet.cfg**.

- If the file does not exist on the file server, upload the file to the file server or configure Option 67 and Option 145 on the DHCP server.
- If the intermediate file exists on the file server, the AutoConfig process searches for the configuration file and other required files in the intermediate file. Check the contents of the intermediate file and go to step 4.

  NOTE

  The intermediate file contains information about a maximum of 2000 devices. Each device is identified by its MAC address or equipment serial number (ESN). If more than 2000 devices are configured in the intermediate file, the AutoConfig process will be suspended.

  The following is an intermediate file sample:

  MAC=0001-0203-0405;vrpfile=S3700 V100R006C00.cc;vrpVer=V100R006C00;cfgfile=vrpcfg01.cfg;patchfile=S3700-pat.pat;webfile=V100R006C00web.zip;

  The list contains no space and must end with a semicolon (;). The MAC/ESN field and the cfgfile field are mandatory and the other fields are optional. **Table 3-1** describes the fields in the intermediate file.

Table 3-1 Fields in the intermediate file

Field	Description
MAC/ESN	MAC address or ESN of a device. The AutoConfig process finds each device to configure according to this field.
vrpfile	Version file name. The value of this field must contain the version number. The file name is in the SxxxxVxxxRxxxCxxSPCxxx.cc format. SPCxxx is optional.
vrpVer	Version number.
cfgfile	Configuration file name. The configuration file cannot be a compressed file.
patchfile	Patch file name.
webfile	Web system file name. The Web system file name must end with web.zip, for example, S3700V100R006C00web.zip.

Step 4 Check whether the configuration file, version file, patch file, and Web system file exist on the file server.

Copyright © Huawei Technologies Co., Ltd.

Search for the configuration file, version file, patch file, and Web system file specified in Option 67 and Option 145 or in the intermediate file.

- If the specified files do not exist on the file server, upload them to the server.
- If the specified files exist, check whether the vrpVer value in Option 145 or the intermediate file is the same as the current system software version. If they are different, change the vrpVer value to the actual system software version number.

If the specified files exist and the version number is correct, go to step 5.

Step 5 Check whether the switch has sufficient space for the files.

Run the **dir** command in the user view to check the available space in the storage device. If the space is not enough for the files, run the **delete** command to delete unneeded files.

NOTE

Alternatively, set opervalue to 1 in Option 146 on the DHCP server so that the switch will delete the previous system files when there is no space for the new files. Exercise caution when setting opervalue to 1. This configuration takes effect after the AutoConfig restarts.

Step 6 After all the files are uploaded to the file server, restart the AutoConfig process.

Use either of the following methods to restart the AutoConfig process:

- Run the **autoconfig getting-file restart** command in the system view to restart the AutoConfig process immediately.
- Wait the AutoConfig process to restart automatically after the retry timer expires. The retry timer length is 30 minutes within 3 days after the first failure to obtain the files, and is 2 hours 3 days later. If the switch fails to obtain the files within 30 days, it stops the AutoConfig process and does not reset the retry timer. Run the **autoconfig getting-file restart** command in the system view to restart the AutoConfig process.

Step 7 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

3.4 ALS Troubleshooting

3.4.1 Laser Status Does Not Change at ALS Pulse Intervals When a Fiber Link Fails

Common Causes

This fault is commonly caused by one of the following:

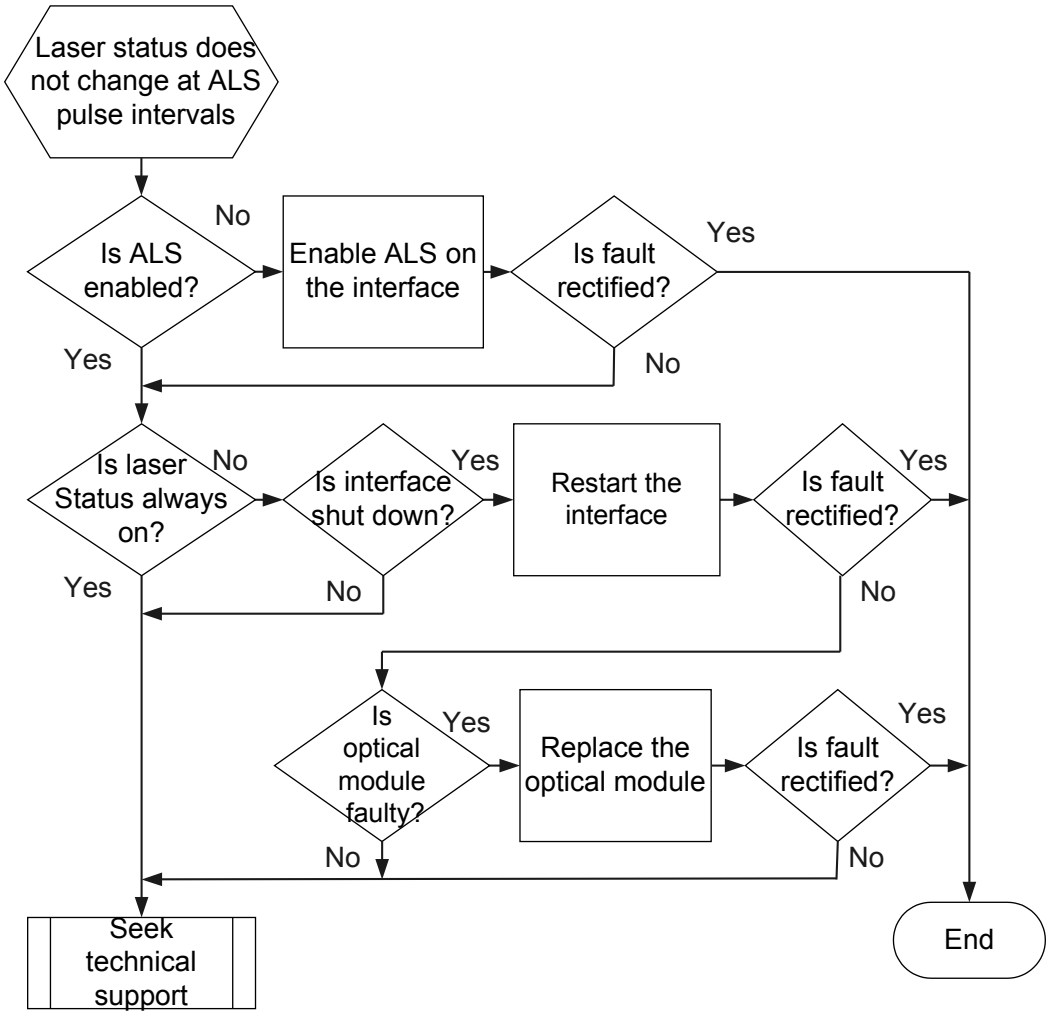
- Automatic laser shutdown (ALS) is disabled on an interface.
- The interface has been shut down.
- The optical module fails.

Troubleshooting Flowchart

The laser of an S3700 interface works in automatic restart mode, the laser status does not change at ALS pulse intervals when a fiber link fails. When this fault occurs, rectify the fault according to **Figure 3-9**.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-9 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether ALS is enabled.

Run the **display als configuration** command to check the **ALS Status** field. If the value of the **ALS Status** field is **Enable**, ALS is enabled. If the value of the **ALS Status** field is **Disable**, ALS is disabled.

- If ALS is disabled, run the **als enable** command on the interface to enable ALS.
- If ALS is enabled, go to step 2.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Check whether the laser status is always on or off.

By default, after ALS is enabled, If there is a fault on the link, a laser automatically turns on and off according to the default pulse interval and width. Run the **display als configuration** command to check the **Laser Status** field repeatedly. The value of the **Laser Status** field is changed between "on" and "off".

NOTE

By default, a laser works in automatic restart mode, and the ALS pulse interval and width are 100s and 2s. That is, a laser automatically turns on for 2s every 100s. The laser works for a short period of time; therefore, the laser status may be always displayed as off when you run the **display als configuration** command. Increase the ALS pulse width to check whether the laser status changes.

- If the value of **Laser status** is always **Off**, go to step 3.
- If the value of **Laser status** is always **On**, go to step 5.

Step 3 Check whether the interface has been shut down.

- If the interface has been shut down, run the **undo shutdown** command to restart the interface.
- If the interface has not been shut down, go to step 4.

Step 4 Check whether the optical module fails.

- If the optical module fails, replace the optical module.
- If the optical module is running properly, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

3.4.2 Interface Cannot Become Up After the Fiber Link Recovers

Common Causes

This fault is commonly caused by one of the following:

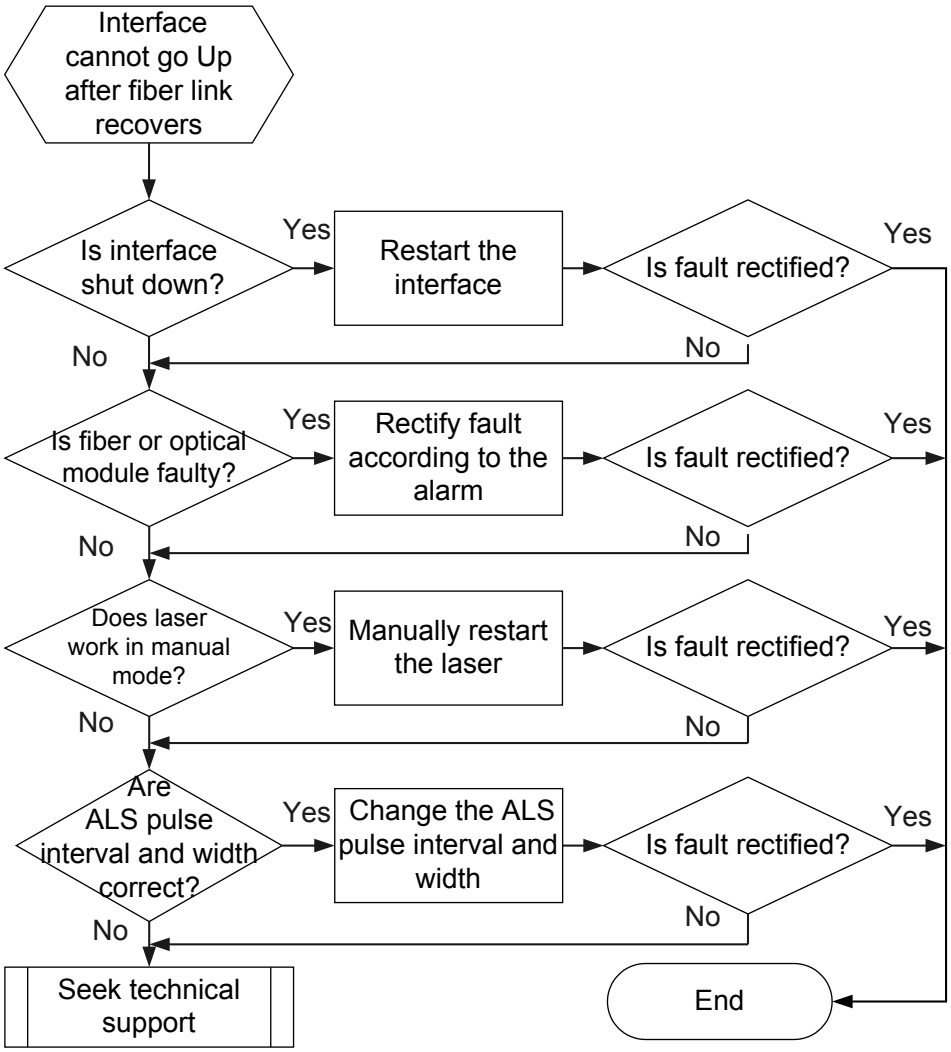
- The interface has been shut down or the optical module is damaged.
- The laser works in manual restart mode but has not been started manually.

Copyright © Huawei Technologies Co., Ltd.

- The laser works in auto restart mode but the ALS pulse interval is too long or the pulse width is too short.

Troubleshooting Flowchart

Figure 3-10 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the interface has been shut down.

Copyright © Huawei Technologies Co., Ltd.

- If the interface has been shut down, run the **undo shutdown** or **restart** command to restart the interface.
- If the interface has not been shut down, go to step 2.

Step 2 Check whether the optical module or fiber fails.

- If the optical module or fiber fails, replace the optical module.
- If the fiber fails, replace the fiber.
- If the optical module and fiber are running properly, go to step 3.

Step 3 Check whether the laser works in manual restart mode.

Run the **display als configuration** command to check the **Restart Mode** field. If the value of the **Restart Mode** field is **Manual**, the laser works in manual restart mode. If the value of the **Restart Mode** field is **Auto**, the laser works in automatic mode.

- If the lasers at the two ends of the link work in manual restart mode, run the **als restart** command at one end to manually start the lasers. If the link is still Down, go to step 5.
- If either of the two lasers works in automatic mode, go to step 4.

Step 4 Check whether the ALS pulse interval and width are correct.

Run the **display als configuration** command on the end where the laser works in automatic mode to check the ALS pulse interval and width.

In the command output, the **Interval(s)** field indicates the ALS pulse interval and the **Width (s)** field indicates the ALS pulse width. By default, the ALS pulse interval is 100s and the ALS pulse width is 2s. That is, the laser works for 2 seconds every 100 seconds. If the ALS pulse interval is long, the peer device waits for a long time to receive pulses. During this period, an LoS persists on the interface and the interface cannot go Up.

To change the ALS pulse interval, run the **als restart pulse-interval** command on the interface.

To change the ALS pulse width, run the **als restart pulse-width** command on the interface.

If the fault persists, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

3.5 Telnet Troubleshooting

3.5.1 The User Fails to Log in to the Server Through Telnet

Common Causes

This fault is commonly caused by one of the following:

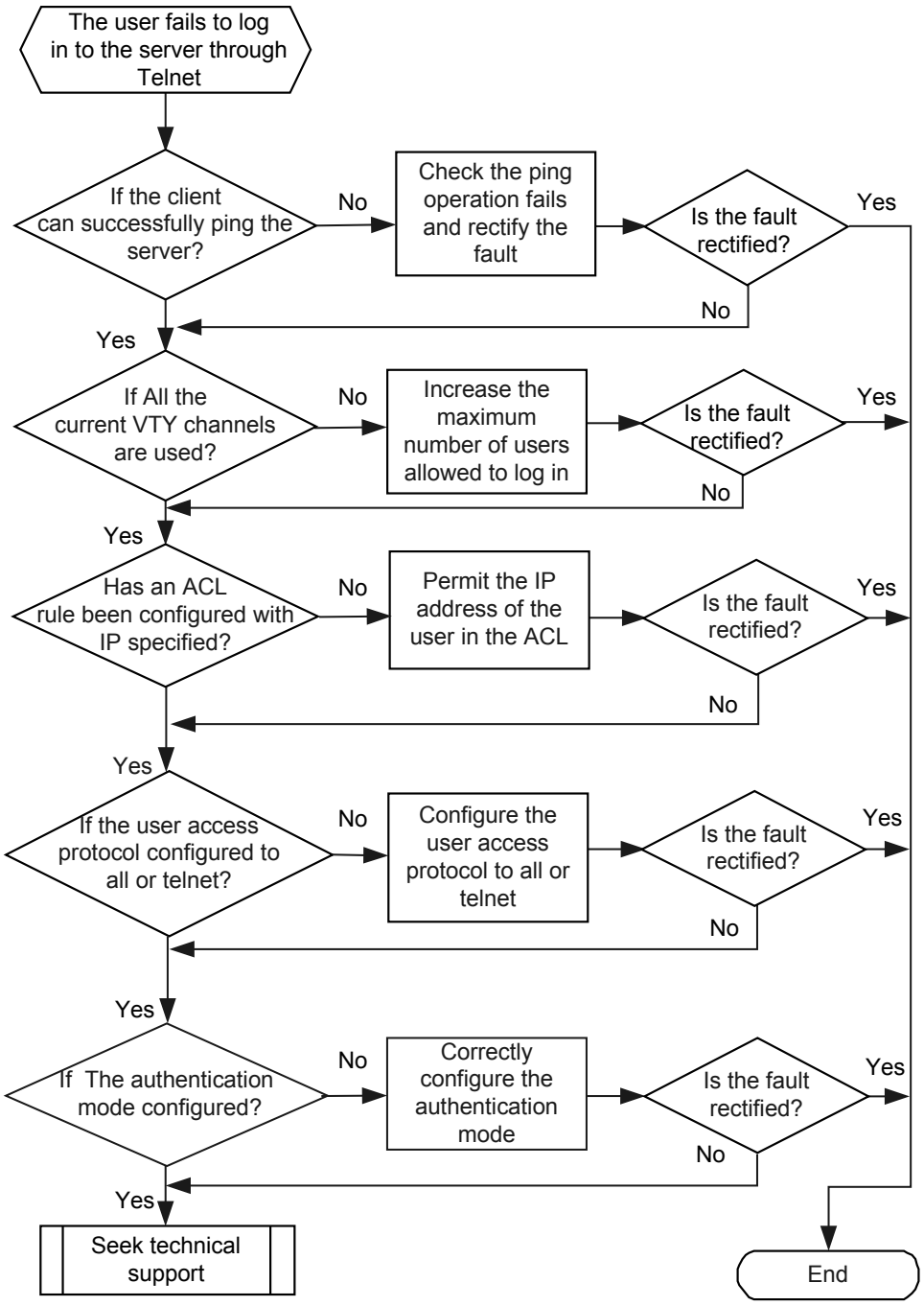
- The route is unreachable and the user cannot set up a TCP connection with the server.
- The number of users logging in to the server reaches the upper threshold.
- An ACL is configured in the VTY user interface view.
- The access protocol specified in the VTY user interface view is incorrect. For example, when the the access protocol is configured to SSH through the **protocol inbound ssh** command, the user cannot log in to the server through Telnet.

Troubleshooting Flowchart

Figure 3-11 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-11 Troubleshooting flowchart for the fault that the client fails to log in to the server through Telnet



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check whether the Telnet client can ping through the server.

Run the **ping** command to check the network connectivity. If the ping fails, the Telnet connection cannot be established between the user and server.

If the ping fails, see A Ping Operation Fails to locate the problem so that the Telnet client can ping through the server.

Step 2 Check whether the number of users logging in to the server reaches the upper threshold.

Log in to the server through a console interface and then run the **display users** command to check whether all the current VTY channels have been used. By default, a maximum of 5 users can log in to the server through VTY channels. Run the **display user-interface maximum-vty** command to view the allowed maximum number of login users.

```
<Quidway> display user-interface maximum-vty
 Maximum of VTY user:5
<Quidway> display users
  User-Intf    Delay    Type   Network Address     AuthenStatus    AuthorcmdFlag
+ 0   CON 0   00:00:00                                              no
  Username : Unspecified

  34  VTY 0   00:13:39  TEL    10.138.78.107                         no
  Username : Unspecified
```

If the number of users logging in to the server reaches the upper threshold, you can run the **user-interface maximum-vty** *vty-number* command to increase the maximum number of users allowed to log in to the server through VTY channels to 15.

```
<Quidway> system-view
[Quidway] user-interface maximum-vty 15
```

Step 3 Check that an ACL is configured in the VTY user interface view.

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] display this
user-interface vty 0 4
 acl 2000 inbound
 authentication-mode aaa
 user privilege level 3
 idle-timeout 0 0
```

If an ACL is configured but the IP address of the client to be permitted is not specified in the ACL, the user cannot log in to the server through Telnet. To enable a user with a specific IP address to log in to the server through Telnet, you need to permit the IP address of the user in the ACL.

Step 4 Check that the access protocol configured in the VTY user interface view is correct.

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] display this
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 idle-timeout 0 0
 protocol inbound ssh
```

Run the **protocol inbound** { **all** | **ssh** | **telnet** } command to configure the user access protocol. By default, the user access protocol is Telnet.

- If the user access protocol is SSH, the user cannot log in to the server through Telnet.
- If the user access protocol is "all", the user can log in to the server through Telnet or SSH.

Copyright © Huawei Technologies Co., Ltd.

Step 5 Check that the authentication mode is configured in the user interface view.

- If you run the **authentication-mode password** command to configure the authentication mode for the user logging in to the server through the VTY channel to **password**, you should run the **set authentication password** command to set the authentication password.
- If you run the **authentication-mode aaa** command to configure the authentication mode to **aaa**, you should run the **local-user** command to add a local user.
- If you run the **authentication-mode none** command to configure the authentication mode to **none**, the authentication mode does not affect your login.

Step 6 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

SHELL/4/TELNETFAILED:Failed to login through telnet. (Ip=[STRING], UserName=[STRING], Times=[ULONG])

3.6 FTP Troubleshooting

3.6.1 The User Fails to Log in to the Server Through FTP

Common Causes

This fault is commonly caused by one of the following:

- The route between the client and the server is unreachable.
- The FTP server is disabled.
- The port to be monitored by the FTP is not the default port and the port is not specified through with the client logs in to the server through FTP.
- The authentication information and working directory of the FTP user are not configured.
- The number of users logging in to the server through FTP reaches the upper threshold.
- An ACL rule is configured on the FTP server to limit client's access.

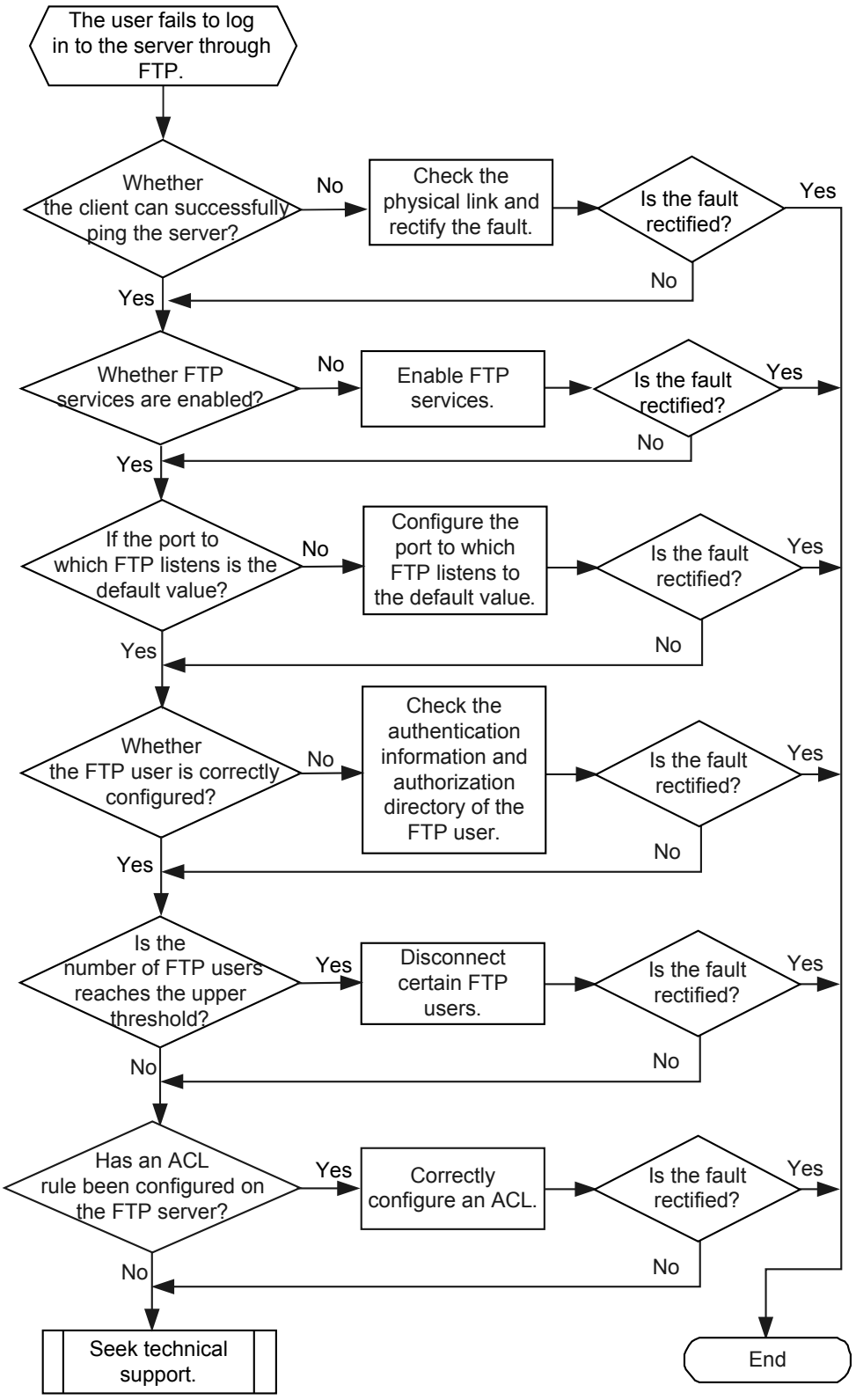
Troubleshooting Flowchart

The client fails to log in to the FTP server.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-12 shows the troubleshooting flowchart.

Figure 3-12 Troubleshooting flowchart for the fault that the client fails to log in to the FTP server



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the client and the server can successfully ping each other.

Run the **ping** command to check whether the client can successfully ping the FTP server.

```
<Quidway> ping 10.164.39.218
  PING 10.164.39.218: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.164.39.218 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

- If the ping fails, the FTP connection cannot be established between the client and the server. To locate this problem, see A Ping Operation Fails so that the FTP client can ping through the FTP server.
- If the ping succeeds, go to **Step 2**.

Step 2 Check that the FTP server is enabled.

Run the **display ftp-server** command in any view to check the status of the FTP server.

- If the FTP server is disabled, the command output is as follows:
  ```
  <Quidway> display ftp-server
  Info: The FTP server is already disabled.
  ```
  Run the **ftp server enable** command in the system view to enabled the FTP server.
  ```
  <Quidway> system-view
  [Quidway] ftp server enable
  Info: Succeeded in starting the FTP server.
  ```
- If the FTP server is enabled, the command output is as follows.
  ```
  <Quidway> display ftp-server
     FTP server is running
     Max user number                 5
     User count                      0
     Timeout value(in minute)        30
     Listening port                  21
     Acl number                      0
     FTP server's source address     0.0.0.0
  ```
  Go to **Step 3**.

Step 3 Check that the port listened by the FTP server is the default port.

1. Run the **display tcp status** command in any view to check the listening status of the current TCP port and the default port 21.
   ```
   <Quidway> display tcp status
   TCPCB    Tid/Soid Local Add:port        Foreign Add:port      VPNID  State
   2a67f47c  6  /1    0.0.0.0:21            0.0.0.0:0             23553
   ```


Copyright © Huawei Technologies Co., Ltd.

```
Listening
2b72e6b8  115/4    0.0.0.0:22            0.0.0.0:0             23553
Listening
3265e270  115/1    0.0.0.0:23            0.0.0.0:0             23553
Listening
2a6886ec  115/23   10.137.129.27:23      10.138.77.43:4053     0
Establish
ed
2a680aac  115/14   10.137.129.27:23      10.138.80.193:1525    0
Establish
ed
2a68799c  115/20   10.137.129.27:23      10.138.80.202:3589    0
Establish
ed
```

2. Run the **display ftp-server** command in any view to check the port listened by the FTP server.

```
<Quidway> display ftp-server
   FTP server is running
   Max user number                 5
   User count                      0
   Timeout value(in minute)        30
   Listening port                  21
   Acl number                      0
   FTP server's source address     0.0.0.0
```

- If the port listened by the FTP server is not port 21, run the **ftp server port** command to set the port to be listened by the FTP server to port 21.

```
<Quidway> system-view
[Quidway] undo ftp server
[Quidway] ftp server port 21
```

- If the port listened by the FTP server is port 21, go to **Step 4**.

Step 4 Check that the authentication information and the authorization directory for the FTP user are configured.

- The name, password, and working directory are mandatory configuration items for an FTP user. A common cause of the fault that the user fails to log in to the server through FTP is because the working directory is not specified.

  1. Run the **aaa** command to enter the AAA view.
  2. Run the **local-user** *user-name* **password** { **simple** | **cipher** } *password* command to configure the name and password for a local user.
  3. Run the **local-user** *user-name* **ftp-directory** *directory* command to configure the authorization directory for the FTP user.

- The access type is an optional item. By default, the system supports all access types. If one access type or several access types are configured, the user can log in to the server only through the configured access types.

  Run the **local-user** *user-name* **service-type ftp** command to configure the access type to FTP.

- If the authentication information and authorization directory are configured for the FTP user, go to **Step 5**.

Step 5 Check that the number of users logging in to the FTP server reaches the upper threshold.

Run the **display ftp-users** command to check whether the number of users logging in to the FTP server reaches 5.

- If the number of users logging in to the FTP server is greater than or equal to 5, run the **quit** command in the FTP client view to tear down the connection between a user and the FTP server.

Copyright © Huawei Technologies Co., Ltd.

- If the number of users logging in to the FTP server is smaller than 5, go to **step 6**.

Step 6 Check that no ACL rule is configured on the FTP server.

Run the **display** [**ipv6**] **ftp-server** command to check whether no ACL rule is configured on the FTP server.

- If an ACL rule is configured, the system allows only the client with the IP address permitted by the ACL rule to log in to the FTP server.
- If no ACL rule is configured, go to **step 7**.

Step 7 Contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

FTPS/3/LOGIN_FAIL:The user failed to log in. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]")

FTPS/5/LOGIN_OK:The user succeeded in login. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]")

FTPS/5/REQUEST:The user had a request. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]", Request=[string])

3.6.2 The FTP Transmission Fails

Common Causes

This fault is commonly caused by one of the following:

- The source path or the destination path of a FTP connection contains characters that the device does not support,such as the character of blank space.
- The number of files in the root directory of the FTP server reaches the upper threshold.
- The available space of the root directory of the FTP server is insufficient.

Troubleshooting Flowchart

None.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the source path or the destination path of a FTP connection contains characters that the device does not support,such as the character of blank space..

- If contains, change the path.
- If does not contains, go to **Step 2**.

Step 2 Check that the number of files in the root directory of the FTP server reaches the upper threshold.

At present, a maximum of 40 files can be saved in the root directory of the FTP server. When the number of files in the root directory of the FTP server is greater than 40 and unnecessary files are not cleared in time, new files cannot be saved.

Run the **dir** command on the FTP server to view the number of files in the root directory of the FTP server.

- If the number of files in the root directory of the FTP server is greater than or equal to 40, run the **delete** command in the user view to delete unnecessary files to release the storage space.
- If the number of files in the root directory of the FTP server is smaller than 40, go to **Step 3**.

Step 3 Check that the available space of the root directory of the FTP server is sufficient.

Run the **dir** command on the FTP server to view the available space of the root directory on the FTP server.

- If there is no sufficient space, run the **delete /unreserved** command in the user view to delete unnecessary files.
- If there is sufficient space, go to **Step 4**.

Step 4 Contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

FTPS/3/TRS_FAIL:The user failed to transfer data. (UserName="[string]", IpAddress=[string], VpnInstanceName="[string]")

Copyright © Huawei Technologies Co., Ltd.

FTPS/5/SENDDATA:The FTP server sent [ULONG] bytes to the client [STRING]. (IpAddress=[STRING], VpnInstanceName="[string]")

FTPS/5/RECVDATA:The FTP server received [ULONG] bytes from the client [STRING]. (IpAddress=[STRING], VpnInstanceName="[string]")

3.6.3 The FTP Transmission Rate Is Low

Common Causes

This fault is commonly caused by one of the following:

- The storage media is the Flash memory.
- Packets are retransmitted because the network is unstable.

Troubleshooting Flowchart

None.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 The S3700 uses the flash memory as the storage medium.

The reading rate of the Flash memory is fast but the writing rate of the Flash memory is slow. Table 3-2 shows the FTP transmission data obtained in the laboratory. The data show that compared with other storage media, the writing rate of the Flash memory is the lowest.

Table 3-2 List of the FTP transmission rate

Item	get	put
Flash - Flash	**0.55 kbit/s**	**0.51 kbit/s**
Flash - hda	**0.51 kbit/s**	16.05 kbit/s
Flash - CFcard	**1.63 kbit/s**	58.66 kbit/s
hda - Flash	32.19 kbit/s	**1.51 kbit/s**
hda - hda	32.91 kbit/s	25.70 kbit/s
hda - CFcard	21.33 kbit/s	54.69 kbit/s
CFcard - Flash	51.23 kbit/s	**0.55 kbit/s**
CFcard - hda	40.19 kbit/s	14.23 kbit/s
CFcard - CFcard	33.21 kbit/s	59.14 kbit/s

Copyright © Huawei Technologies Co., Ltd.

Step 2 Check that packets are retransmitted.

Capture packets and analyze the packet contents through tools to check whether TCP packets are retransmitted on client PC. Packet retransmission is usually cause by the network instability.

Figure 3-13 shows packets captured through Ethereal. As shown in the diagram, a log of TCP retransmission are received.

Figure 3-13 Diagram of packets captured through Ethereal

	Time	Source	Destination	Protocol	Info
21	0.076377	192.168.2.1	192.168.2.5	TCP	[TCP Dup ACK 14#4] 4
22	0.509676	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
23	0.516849	192.168.2.1	192.168.2.5	TCP	49772 > 2712 [ACK] S
24	0.516886	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
25	0.516899	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
26	0.516910	192.168.2.5	192.168.2.1	TCP	[TCP Retransmission]
27	0.516952	192.168.2.5	192.168.2.1	TCP	2712 > 49772 [ACK] S

Step 3 Contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

3.7 SNMP Troubleshooting

3.7.1 An SNMP Connection Cannot Be Established

Common Causes

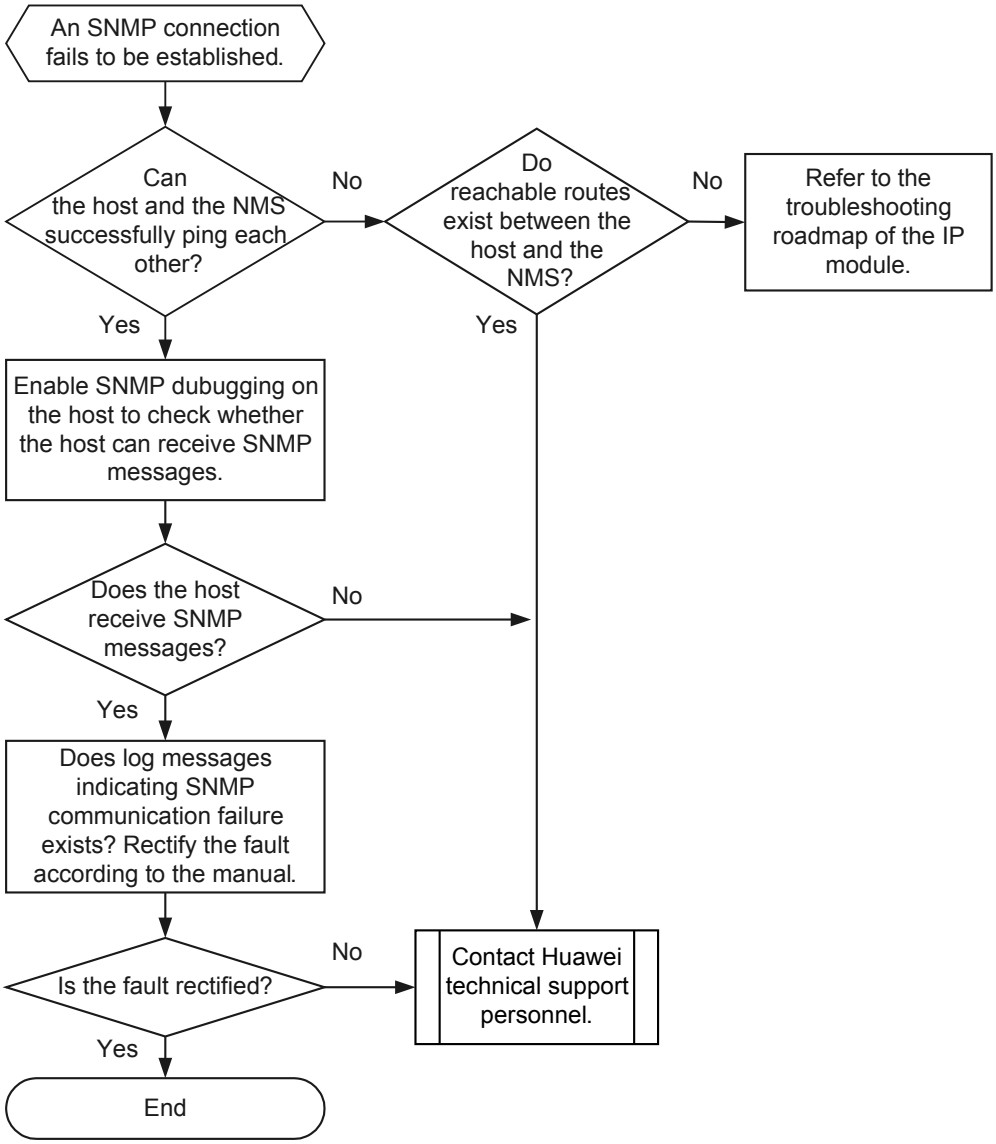
This fault is commonly caused by one of the following:

- Packets cannot be exchanged between the host and the NMS.
- Configurations are incorrect.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 3-14 Troubleshooting flowchart for the fault that an SNMP connection cannot be established



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **ping** command to check whether the host and the NMS can successfully ping each other.

- If the ping succeeds, it indicates that the host and the NMS are reachable. Go to Step 2.

Copyright © Huawei Technologies Co., Ltd.

- If the ping fails, see A Ping Operation Fails to locate the problem so that the host and the NMS can ping through each other.

Step 2 Run the **display logbuffer** command to check whether login failure logs exist on the host.

- If no login failure log exists on the host, go to Step 3.
- If login failure logs exist on the host, analyze the logs.

Table 3-3 Log description and solution

Logs	Description	Solution
Failed to login through SNMP, because the version was incorrect. (Ip=[STRING], Times=[ULONG])	The SNMP version used by the NMS to send login requests is not supported on the host.	1. Run the **display snmp-agent sys-info version** command to check whether the host supports the SNMP version used by the NMS to send login requests. ● If the host supports the SNMP version, go to Step c. ● If the host does not support the SNMP version, go to Step b. 2. Run the **snmp-agent sys-info version** command to configure the SNMP version supported by the host. ● If the fault is rectified, go to Step d. ● If the fault persists, go to Step c. 3. Contact Huawei technical support personnel. 4. End.
Failed to login through SNMP, because the packet was too large. (Ip=[STRING], Times=[ULONG])	Packet bytes received by the host exceeds the threshold.	1. Run the **snmp-agent packet max-size** command to increase the maximum packet bytes of the host. ● If the fault persists, go to Step b. ● If the fault is rectified, go to Step c. 2. Contact Huawei technical support personnel. 3. End.
Failed to login through SNMP,because messages was failed to be added to the message list. (Ip=[STRING], Times=[ULONG])	The message list is filled up.	Contact Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Logs	Description	Solution
Failed to login through SNMP, because of the decoded PDU error. (Ip=[STRING], Times=[ULONG])	An unknown error occurs during packet decoding.	Contact Huawei technical support personnel.
Failed to login through SNMP, because the community was incorrect. (Ip=[STRING], Times=[ULONG])	The community string is incorrect.	1. Run the **display snmp-agent community** command to can view the community string configured on the host. ● If the community string used by the NMS to send a login request is the same as that configured on the host, go to Step c. ● If the community string used by the NMS to send a login request is different from that configured on the host, go to Step b. 2. Run the **snmp-agent community** command to configure a read-write community string, which must be identical with that configured on the host. ● If the fault is rectified, go to Step d. ● If the fault persists, go to Step c. 3. Contact Huawei technical support personnel. 4. End.
Failed to login through SNMP, because of the ACL filter function. (Ip=[STRING], Times=[ULONG])	The IP address from which the NMS sends a login request is denied by the ACL.	1. Run the **display acl** command to view the ACL configuration on the host. ● If the IP address from which the NMS sends login requests is denied by the ACL, go to Step b. ● If the IP address from which the NMS sends login requests is permitted by the ACL, go to Step c. 2. Run the **rule** command to enable the ACL to permit the IP address from which the NMS sends login requests. ● If the fault is rectified, go to Step d. ● If the fault persists, go to Step c. 3. Contact Huawei technical support personnel. 4. End.

Copyright © Huawei Technologies Co., Ltd.

Logs	Description	Solution
Failed to login through SNMP, because of the contextname was incorrect. (Ip= [STRING], Times= [ULONG])	The "contextname " in the login request is incorrect.	Contact Huawei technical support personnel.

Step 3 Contact Huawei technical support personnel.

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

```
SNMP/4/ACL_FAILED
SNMP/4/AR_PAF_FAILED
SNMP/6/CNFM_VERSION_DISABLE
SNMP/4/COMMUNITY_ERR
SNMP/4/CONTEXTNAME_ERR
SNMP/4/DECODE_ERR
SNMP/4/INVAILDVERSION
SNMP/4/MSGTBL_ERR
SNMP/4/PACKET_TOOBIG
SNMP/4/PARSE_ERR
SNMP/4/SNMP_SET
SNMP/4/TRAP_SEND_ERR
SNMP/4/SHORT_VB
```

3.7.2 The NMS Fails to Receive Trap Messages from the Host

Common Causes

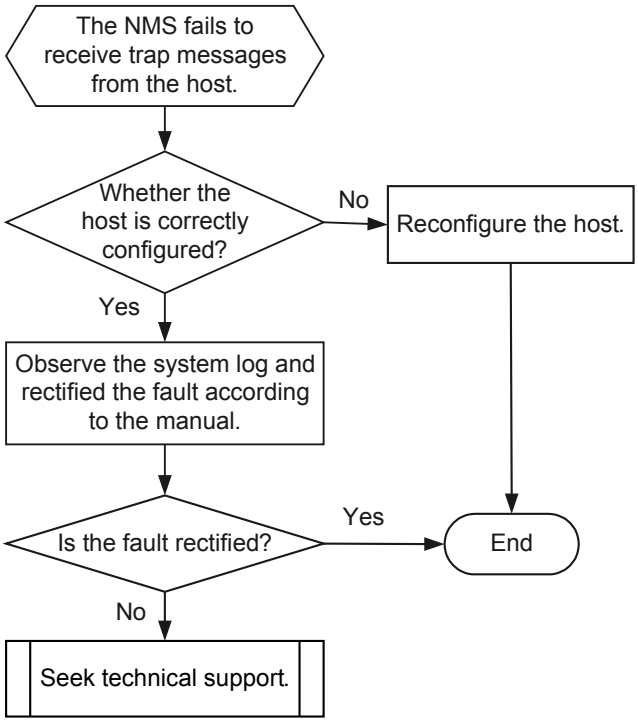
This fault is commonly caused by one of the following:

- The trap message is lost.
- The SNMP configuration on the host is incorrect. As a result, the host is unable to send trap messages.
- No trap message is generated on the host-side service module, or the trap message is generated on the host-side service module, but the format of the trap messages is incorrect. As a result, the trap message cannot be sent.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 3-15 Troubleshooting flowchart for the fault that the NMS fails to receive trap messages from the host



Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the SNMP configurations on the host are correct.

- If the SNMP configurations are correct, go to Step 2.
- If the SNMP configurations are incorrect, change the configuration according to the following configuration cases.

Copyright © Huawei Technologies Co., Ltd.

Table 3-4 Typical SNMP configurations

Configuration Case	Command
Configure a destination host running SNMPv2c, with the destination port being the default 162, the username being huawei, and the IP address being 192.168.1.1. **NOTE** **huawei** must be an existing username.	<Quidway> **system-view** [Quidway] **snmp-agent target-host trap address udp-domain 192.168.1.1 params securityname huawei v2c**
Configure a destination host running SNMPv2c, with the destination port being the default 162, the username being huawei, and the IP address being 192.168.1.1. Trap messages are sent through a VPN network named VPN-Test. **NOTE** **huawei** must be an existing username.	<Quidway> **system-view** [Quidway] **snmp-agent target-host trap address udp-domain 192.168.1.1 udp-port 162 vpn-instance VPN-TEST params securityname huawei v2c**
Configure a destination host running SNMPv3, with the username being huawei. The user belongs to the user group named huawei_group and has Huawei_view as the notify rights (notify-view). **NOTE** With Huawei_view, the user can access all nodes from the iso subtree. **huawei** must be an existing username.	# Configure a MIB view. <Quidway> **system-view** [Quidway] **snmp-agent mib-view included Huawei_view iso** # Configure a user group. [Quidway] **snmp-agent group v3 huawei_group read-view Huawei_view write-view Huawei_view notify-view Huawei_view** # Configure a user. [Quidway] **snmp-agent usm-user v3 huawei huawei_group**
Configure a destination host running SNMPv3, with the username being huawei and the IP address being 192.168.1.1. **NOTE** **huawei** must be an existing username.	<Quidway> **system-view** [Quidway] **snmp-agent target-host trap address udp-domain 192.168.1.1 params securityname huawei v3**
Configure a destination host running SNMPv3, with the destination port being 163, the username being huawei, and the IP address being 192.168.1.1. Trap messages are sent through a VPN network named VPN-Test. **NOTE** **huawei** must be an existing username.	<Quidway> **system-view** [Quidway] **snmp-agent target-host trap address udp-domain 192.168.1.1 udp-port 163 vpn-instance VPN-TEST params securityname huawei v3**

Step 2 Run the **display snmp-agent trap all** command to check whether the trap function is enabled on all feature modules.

- If the trap function is not enabled on all feature modules, go to Step 3.

Copyright © Huawei Technologies Co., Ltd.

- If the trap function is enabled on all feature modules, go to Step 4.

Step 3 Run the **snmp-agent trap enable feature-name trap-name** command to enable the host to send trap messages and configure parameters for trap messages.

- If the NMS can receive trap messages sent from the host, go to Step 7.
- If the NMS fails to receive trap messages sent from the host, go to Step 4.

Step 4 Check whether the log message indicating that a specific trap is generated exists on the host.

- If the log message indicating that a specific trap is generated does not exist on the host, it indicates that the trap is not generated. In this case, go to Step 6.
- If the log message indicating that a specific trap is generated exists on the host, it indicates that the trap has been generated but the NMS fails to receive the trap message. In this case, go to Step 5.

  NOTE

  The log message indicating that a specific trap is generated is as follows: #Jun 10 2010 09:55:03 Quideway IFNET/2/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Int erface 109 turned into DOWN state.

Step 5 Configure trap messages to be sent in Inform mode.

NOTE

Trap messages are transmitted through UDP. UDP transmission is unreliable, which may cause trap messages to be lost on the link.Inform mechanism ensures that trap messages are sent in a reliable manner. For configuration details, refer to the chapter "SNMP Configuration" in the *Quidway S3700 Series Configuration Guide - Network Management*.

- If the NMS can receive trap messages sent from the host, go to Step 7.
- If the NMS fails to receive trap messages sent from the host, go to Step 6.

Step 6 Contact Huawei technical support personnel.

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

3.8 RMON Troubleshooting

3.8.1 NM Station Cannot Receive RMON Alarms

Common Causes

This fault is commonly caused by one of the following:

- There is no reachable route between the router and the NM station.

Copyright © Huawei Technologies Co., Ltd.

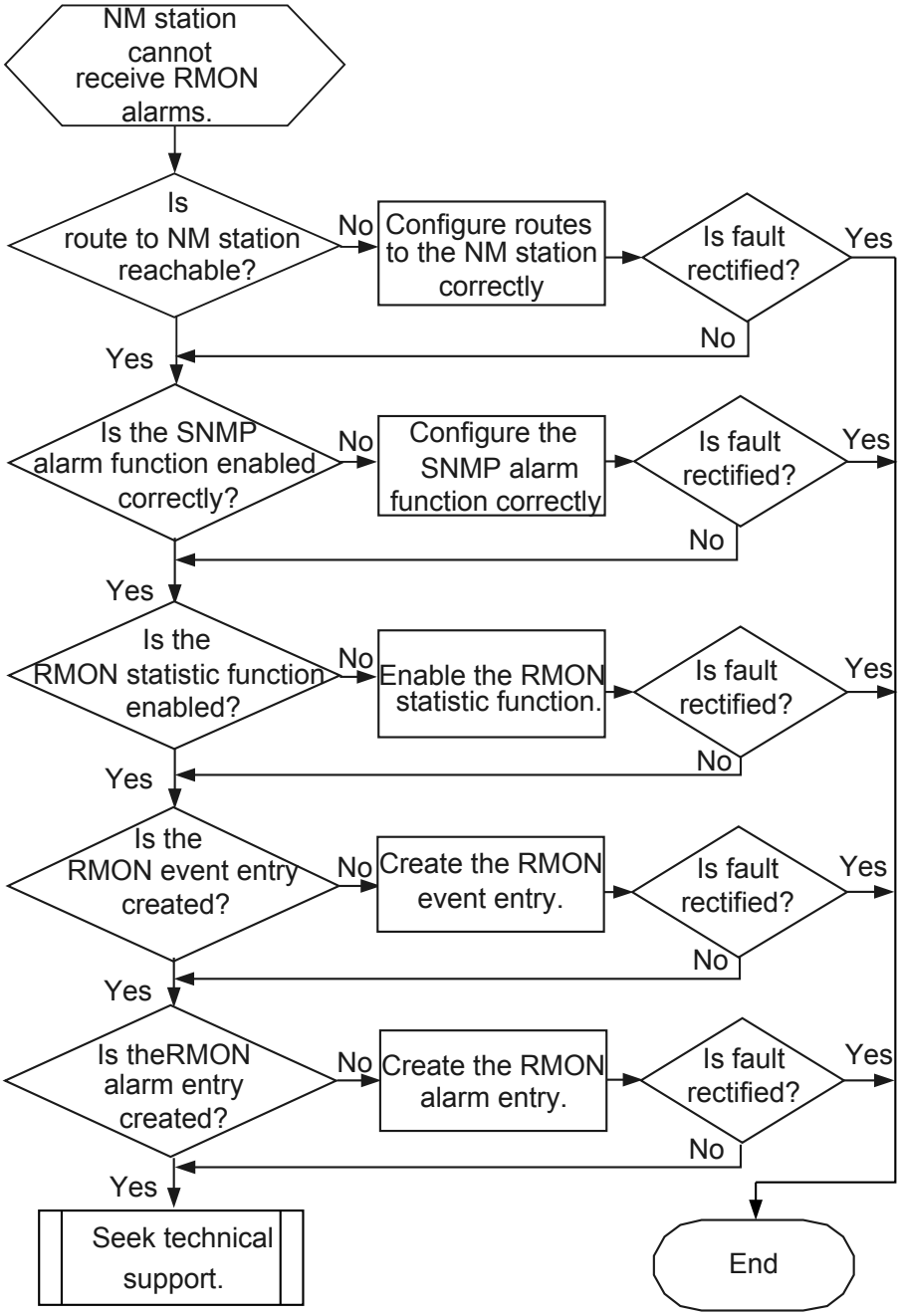
- The SNMP alarm function is not configured correctly.
- RmonStatsTable is not configured.
- The statistics of RMON is not enabled.
- The RMON eventTable is not enabled.
- The RMON alarmTable is not enabled.
- The alarm variables are not configured correctly.

Troubleshooting Flowchart

When the traffic that flows in and out of the LAN exceeds the configured threshold, the NM station fails to receive alarms. **Figure 3-16** shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-16 Troubleshooting flowchart for the failure of the NMS to receive RMON alarms



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check whether there are reachable routes between the switch and the NM station.

Ping the NM station interface from the switch.

- If the ping succeeds, it indicates that the routes between the switch and the NM station are reachable,go to Step 2.
- If the ping fails, check the routes between the switch and the NM station. For details of routing troubleshooting, see the section A Ping Operation Fails.

Step 2 Check that the SNMP alarm function is configured correctly.

Check whether the NM station can receive other alarms. If not, do as follows:

- Run the **display snmp-agent trap feature-name rmon all** command to check whether the alarm function of the switch is enabled
- Run the **display snmp-agent target-host** command to check whether the NM address through which the switch sends alarms is correct

Step 3 Check that rmonStatsTable is configured.

Run the **display rmon statistics** [**ethernet** *interface-number* | **gigabitethernet** *interface-number*] command on the switch to check whether rmonStatsTable is configured. If rmonStatsTable is null, run the **rmon statistics** *entry-number* [**owner** *owner-name*] command to create entries of the table.

Step 4 Check that the statistics of RMON is enabled.

Run the **display rmon statistics** [**ethernet** *interface-number* | **gigabitethernet** *interface-number*] command on the switch to check whether the statistics of RMON is enabled on the interface. If no statistics is recorded in the table, run the **rmon-statistics enable** command to enable the statistics of RMON on the interface.

Step 5 Check that the RMON eventTable is enabled.

Run the **display rmon event** [*entry-number*] command on the switch interface to check whether the RMON eventTable is enabled. If the eventTable is null, run the **rmon event** command to create entries of the table.

Step 6 Check that the RMON alarmTable is enabled.

Run the **display rmon alarm** [*entry-number*] command on the switch interface to check whether the RMON alarmTable is enabled. If the alarmTable is null, run the **rmon alarm** command to create entries of the table.

Step 7 Check that the alarm variables are configured correctly.

Run the **display rmon alarm** [*entry-number*] command on the switch interface to view the value of the configured alarm variables. On the NM station, check that the values of alarm variables of the interface are consistent with those values configured on the switch interface. If the values are inconsistent, modify the values of the alarm variables to be consistent.

After the preceding operations are complete, if the NM station cannot receive the alarm values of the RMON module on the switch, contact the Huawei technical personnel.

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

3.9 NQA Troubleshooting

3.9.1 A UDP Jitter Test Instance Fails to Be Started

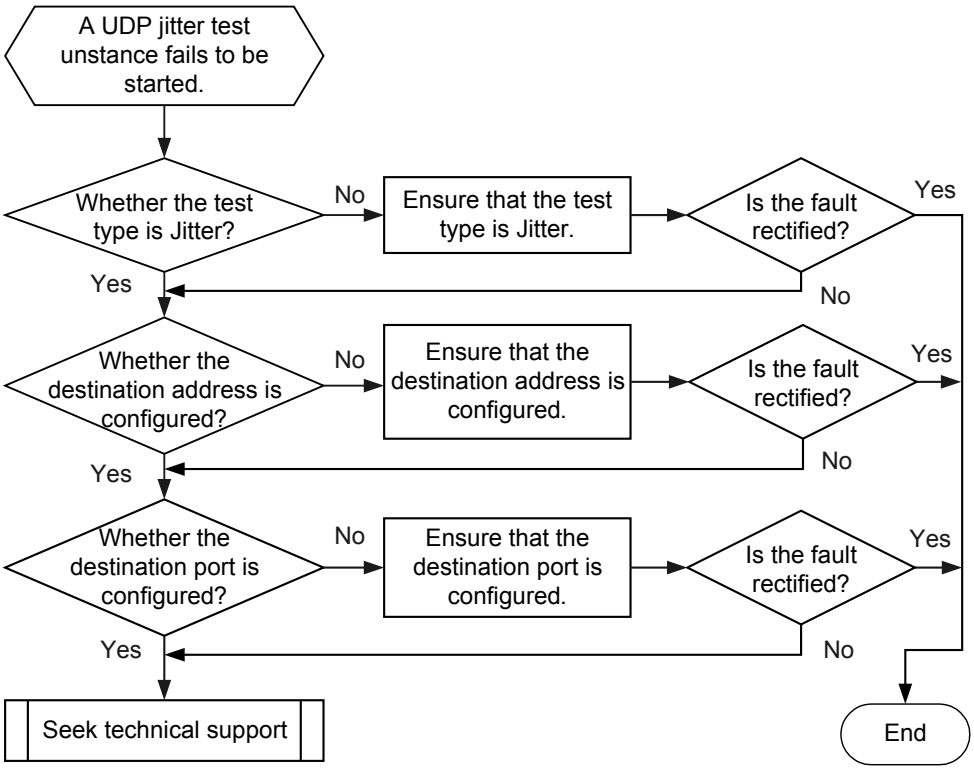
Common Causes

This fault is commonly caused by one of the following:

- The mandatory parameter of the test instance is incorrect.

Troubleshooting Flowchart

Figure 3-17 Troubleshooting flowchart for the fault that a UDP Jitter test instance fails to be started



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Unless otherwise stated, all the following commands, except display commands that can be run in all views, need to be run in the NQA test instance view.

Procedure

Step 1 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA client or the **display this** command in the NQA test instance view to check whether the test type is Jitter.

- If the test type is Jitter, go to Step 2.
- If the test type is not Jitter, run the **test-type jitter** command to configure the test type to UDP Jitter.
  - If the fault is rectified, go to Step 5.
  - If the fault persists, go to Step 2.

Step 2 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA client or the **display this** command in the NQA test instance view to check whether the destination IP address is configured.

- If the destination IP address is configured, go to Step 3.
- If the destination IP address is not configured, run the **destination-address ipv4** *ip-address* command in the NQA test instance view to configure the destination IP address.
  - If the fault is rectified, go to Step 5.
  - If the fault persists, go to Step 3.

Step 3 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA client or the **display this** command in the NQA test instance view to check whether the destination port is configured.

- If the destination port is configured, go to Step 4.
- If the destination port is configured, run the **destination-port** *port-number* command in the NQA test instance view to configure the destination port.
  - If the fault is rectified, go to Step 5.
  - If the fault persists, go to Step 4.

Step 4 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Copyright © Huawei Technologies Co., Ltd.

Relevant Logs

None.

3.9.2 A Drop Record Exists in the UDP Jitter Test Result

Common Causes

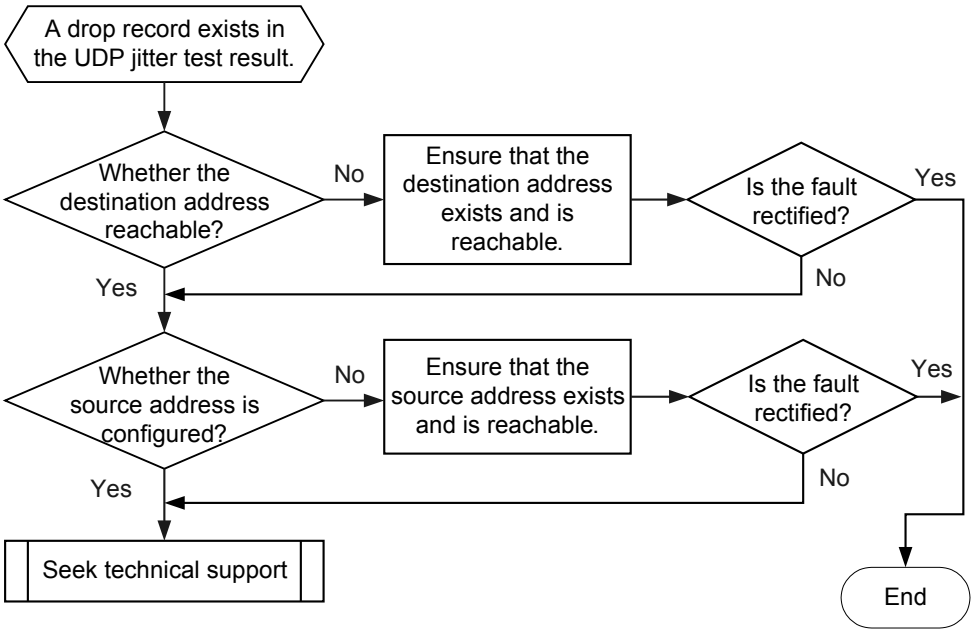
If the UDP jitter test result has drop records. It means that the value of the "Drop operation number" field in the **display nqa results** command output is not 0.

This fault is commonly caused by one of the following:

- The destination IP address does not exist or the route to the network segment to which the destination IP address belongs does not exist in the routing table.
- The source IP address is incorrect.

Troubleshooting Flowchart

Figure 3-18 Troubleshooting flowchart for the fault that a drop record exists in the UDP jitter test



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display ip routing-table** command on the NQA client to check whether route along the test path exists.

Copyright © Huawei Technologies Co., Ltd.

- If the route exists, run the **ping** command to check whether devices can successfully ping each other.
  - If devices can successfully ping each other, go to Step 2.
  - If devices cannot successfully ping each other, see A Ping Operation Fails.
- If the route does not exist, run the corresponding command to reconfigure the route.

Step 2 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA client or the **display this** command in the NQA test instance view to check whether the source IP address is configured.

- If the source IP address is configured, run the **display ip interface brief** on the NQA client to check whether the interface configured with the source IP address exists.
  - If the interface exists, run the **display ip routing-table** command on the NQA server to check whether the route to the source IP address exists.
    - If the route exists, run the **ping** command to check whether the source IP address is reachable.
      - If the source IP address is reachable, go to Step 3.
      - If the source IP address is unreachable, see A Ping Operation Fails.
    - If the route does not exist, run the corresponding command to reconfigure the route.
  - If the interface configured with the source IP address does not exist, run the corresponding command to reconfigure IP addresses and recheck the configuration about NQA.
- If the source IP address is not configured, go to Step 3.

Step 3 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

3.9.3 A Busy Record Exists in the UDP Jitter Test Result

Common Causes

If the UDP jitter test result has busy records. It means that the value of the "System busy operation number" field in the **display nqa results** command output is not 0.

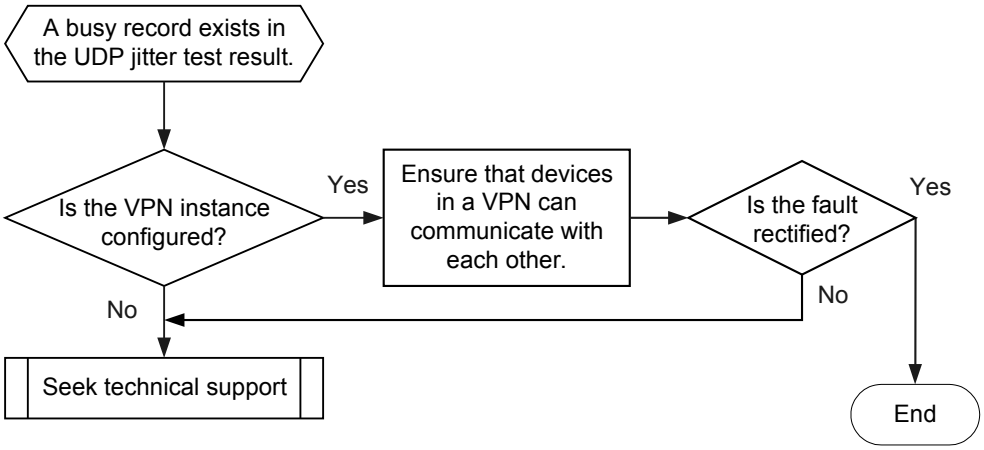
This fault is commonly caused by one of the following:

- The VPN route instance that is configured in the UDP Jitter test instance is unreachable.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 3-19 Troubleshooting flowchart for the fault that a busy record exists in the UDP jitter test



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA client or the **display this** command in the NQA test instance view to check whether the VPN instance is configured.

- If the VPN instance is configured, go to Step 2.
- If the VPN instance is not configured, go to Step 3.

Step 2 Run the **ping -vpn-instance** *vpn-instance-name* command on the NQA client to check whether the destination address is reachable.

- If the destination address is reachable, go to Step 3.
- If the destination address is unreachable, see the section A Ping Operation Fails.

Step 3 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Copyright © Huawei Technologies Co., Ltd.

Relevant Logs

None.

3.9.4 A Timeout Record Exists in the UDP Jitter Test Result

Common Causes

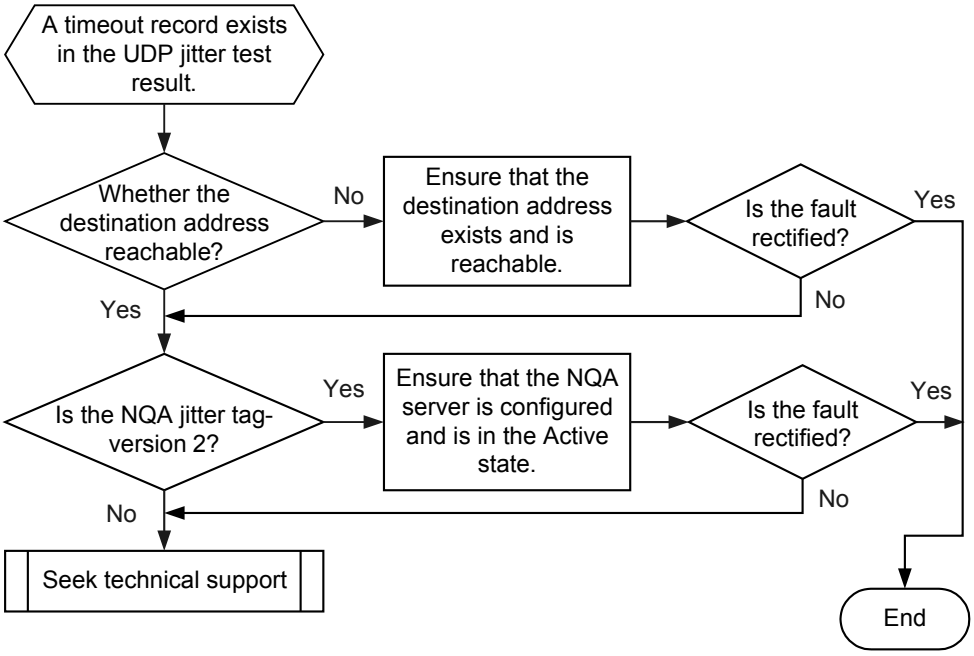
If the UDP jitter test result has timeout records. It means that the value of the "operation timeout number" field in the **display nqa results** command output is not 0.

This fault is commonly caused by one of the following:

- The destination address does not exist, but the route to the network segment of the destination address exists in the routing table.
- The value of the parameter "nqa-jitter tag-version" is 2, and the receiver is not configured with a UDP server.

Troubleshooting Flowchart

Figure 3-20 Troubleshooting flowchart for the fault that a timeout record exists in the UDP jitter test



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Unless otherwise stated, all the following commands, except display commands that can be run in all views, need to be run in the NQA test instance view.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **ping** command on the NQA client to check whether the route to the destination address is reachable.

- If the route to the destination address is reachable, go to Step 2.
- If the route to the destination address is unreachable, see the section A Ping Operation Fails.

Step 2 Run the **display this** command in the system view on the NQA client to check whether the value of the parameter "nqa-jitter tag-version" is 2. When the value of this parameter is set to 1 (the default value), this parameter is not displayed in the configuration file. This parameter is displayed in the configuration file when its value is set to 2.

- If the value of the parameter "nqa-jitter tag-version" is 2, go to Step 3.
- If the value of the parameter "nqa-jitter tag-version" is not 2, go to Step 4.

Step 3 Run the **display nqa-server** command on the NQA server to check whether the **nqa-server udpecho** *ip-address port-number* command has been configured on the NQA server.

- If the **nqa-server udpecho** *ip-address port-number* command has been configured on the NQA server and is in the Active state, go to Step 4.
- If the **nqa-server udpecho** *ip-address port-number* command is not configured on the NQA server, run the command to configure the NQA server. Note that the IP address of the NQA server must be identical with the destination IP address configured through the **destination-address ipv4** *ip-address* command on the NQA client; the port number configured on the NQA server must be identical with that configured through the **destination-port** *port-number* command on the NQA client.
  - If the fault is rectified, go to Step 5.
  - If the fault persists, go to Step 4.

Step 4 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

3.9.5 The UDP Jitter Test Result Is "Failed", "No Result" or "Packet Loss"

Common Causes

The UDP jitter test result displayed in the **display nqa results** command output can be "failed", "no result", or "packet loss". In the command output,

Copyright © Huawei Technologies Co., Ltd.

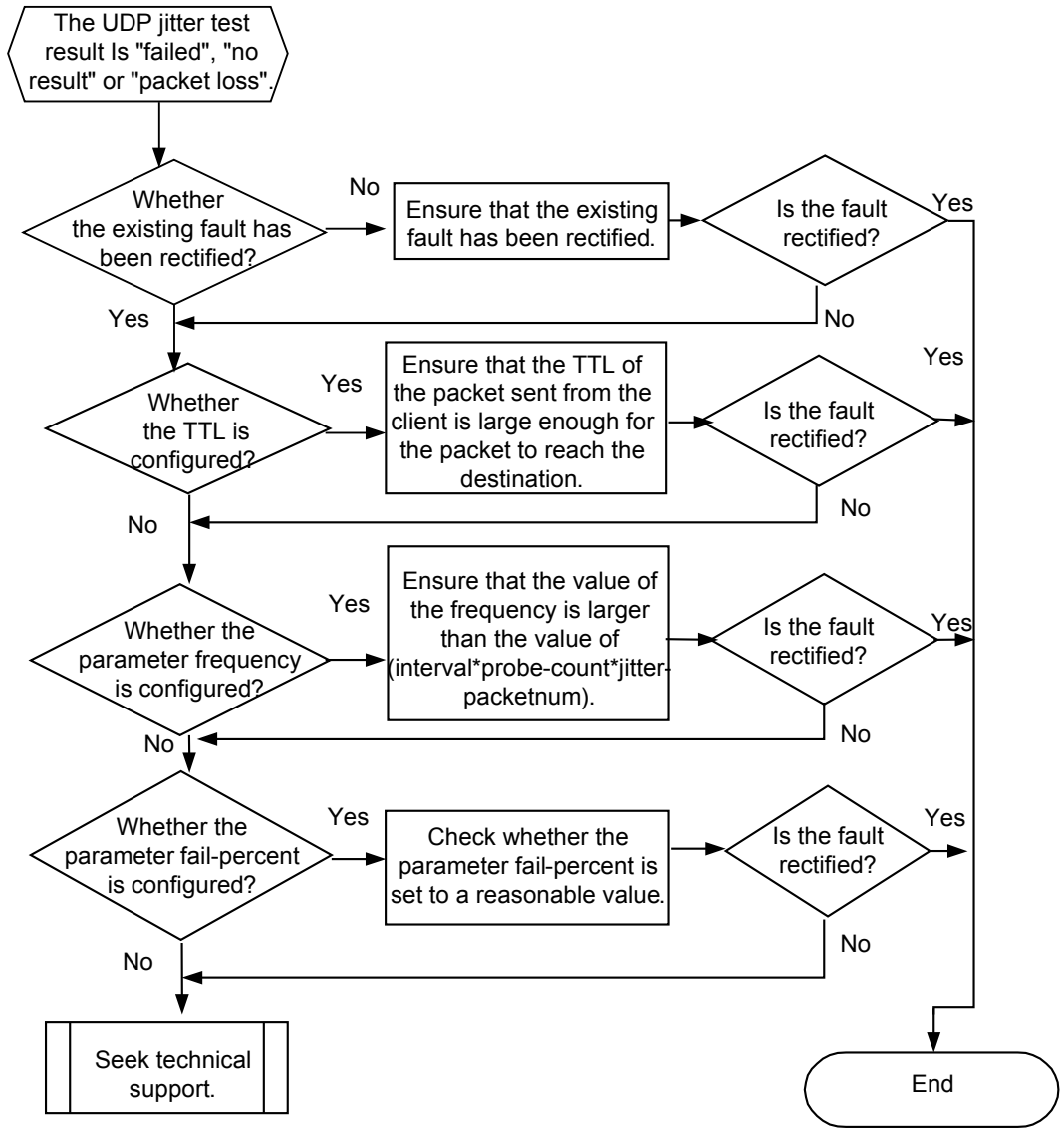
- If the "Completion" field is displayed as "failed", it indicates that the test fails.
- If the "Completion" field is displayed as "no result", it indicates that the test has no result.
- If the "lost packet ratio" field is not 0%, it indicates that packet loss occurs.

This fault is commonly caused by one of the following:

- A drop record exists in the UDP jitter test result.
- A busy record exists in the UDP jitter test result.
- A timeout record exists in the UDP jitter test result.
- The TTL expires.
- The parameter frequency is incorrect.
- The parameter fail-percent is incorrect.

Troubleshooting Flowchart

Figure 3-21 Troubleshooting flowchart for the fault that the UDP Jitter test result is "failed", "no result", or "packet loss"



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Unless otherwise stated, all the following commands, except display commands that can be run in all views, need to be run in the NQA test instance view.

Procedure

Step 1 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA client or the **display this** command in the NQA test instance view to check whether the TTL is configured.

- If the TTL is configured, you can run the **ttl number** command in the NQA test instance view to set the value of the TTL to 255. If the fault persists after the TTL is set to 255, go to Step 2.
- If the TTL is not configured, you can run the **ttl number** command in the NQA test instance view to set the value of the TTL to 255. If the fault persists after the TTL is set to 255, go to Step 2.

Step 2 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA agent or the **display this** command in the NQA test instance view to check whether the parameter **frequency** is configured.

- If the parameter **frequency** is configured, compare the value of the **frequency** and that of the (interval*probe-count*jitter-packetnum). To ensure that the UDP Jitter test instance can be complete normally, the value of the **frequency** must be greater than that of the (interval*probe-count*jitter-packetnum). If the value of the **frequency** is smaller than that of the (interval*probe-count*jitter-packetnum), you need to run the **frequency** *interval* command in the NQA test instance view to increase the value of the **frequency**.
- If the **frequency** is not configured or the fault persists after the **frequency** is set to proper value, go to Step 3.

Step 3 Run the **display nqa-agent** *admin-name test-name* [**verbose**] command on the NQA agent or the **display this** command in the NQA test instance view to check whether the parameter **fail-percent** is configured.

- If the **fail-percent** is configured, run the **undo fail-percent** command in the NQA test instance view to delete the **fail-percent**. If the fault persists after the **fail-percent** is deleted, go to Step 4.
- If the **fail-percent** is not configured, go to Step 4.

Step 4 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Copyright © Huawei Technologies Co., Ltd.

Relevant Logs

None.

3.10 NTP Troubleshooting

3.10.1 The Clock Is Not Synchronized

Common Causes

This fault is commonly caused by one of the following:

- The link flaps.
- The link is faulty.

Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check the NTP status.

```
[Quidway] display ntp-service status
 clock status: unsynchronized
 clock stratum: 16
 reference clock ID: none
 nominal frequency: 100.0000 Hz
 actual frequency: 99.9995 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 0.00 ms
 reference time: 14:25:55.477 UTC Jun 9 2010(CFBA22F3.7A4B76F6)
```

The "clock status" field is displayed as "unsynchronized", indicating that the local system clock is not synchronized with any NTP server or a reference clock.

Step 2 Check the status of the NTP connection.

```
[Quidway] display ntp-service sessions
        source          reference       stra reach poll  now offset delay disper
******************************************************************************
     [5] 20.1.14.1        0.0.0.0          16    0   64    -      -    0.0    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

The value of the "reference" is 0.0.0.0, indicating that the local system clock is not synchronized with any NTP server.

Step 3 Run the **ping** command on the NTP client to check the status of the link to the NTP server.

```
[Quidway] ping 20.1.14.1
  PING 20.1.14.1: 56  data bytes, press CTRL_C to break
```


Copyright © Huawei Technologies Co., Ltd.

```
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out
--- 20.1.14.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

- The displayed information "100.00% packetloss" indicates that the link is faulty. To locate the fault, refer to A Ping Operation Fails.
- If the packet loss percentage is not 100.00%, it indicates that the link flaps. To locate the fault, refer to A Ping Operation Fails.
- If the packet loss percentage is 0.00%, it indicates that the link is normal. Then proceed to step 4.

Step 4 If the fault persists, collect the following information and contact Huawei technical support engineers.

- Execution results of the preceding steps
- Configuration files, logs, and alarms about the device

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

The following log information indicates that the clock source with which the local device synchronizes is lost.

NTP/4/SOURCE_LOST

The following log information indicates that the local clock has synchronized with a clock source.

NTP/4/LEAP_CHANGE
NTP/4/STRATUM_CHANGE
NTP/4/PEER_SELE

3.11 HGMP Troubleshooting

3.11.1 A Candidate Switch Directly Connected to the Administrator Switch Cannot Be Added to the Cluster

Common Causes

Two switches are directly connected. A cluster is created on one switch. The other switch, that is, a candidate switch, cannot be added to the cluster, and there is no prompt on the administrator switch.

Copyright © Huawei Technologies Co., Ltd.

This fault is commonly caused by one of the following:

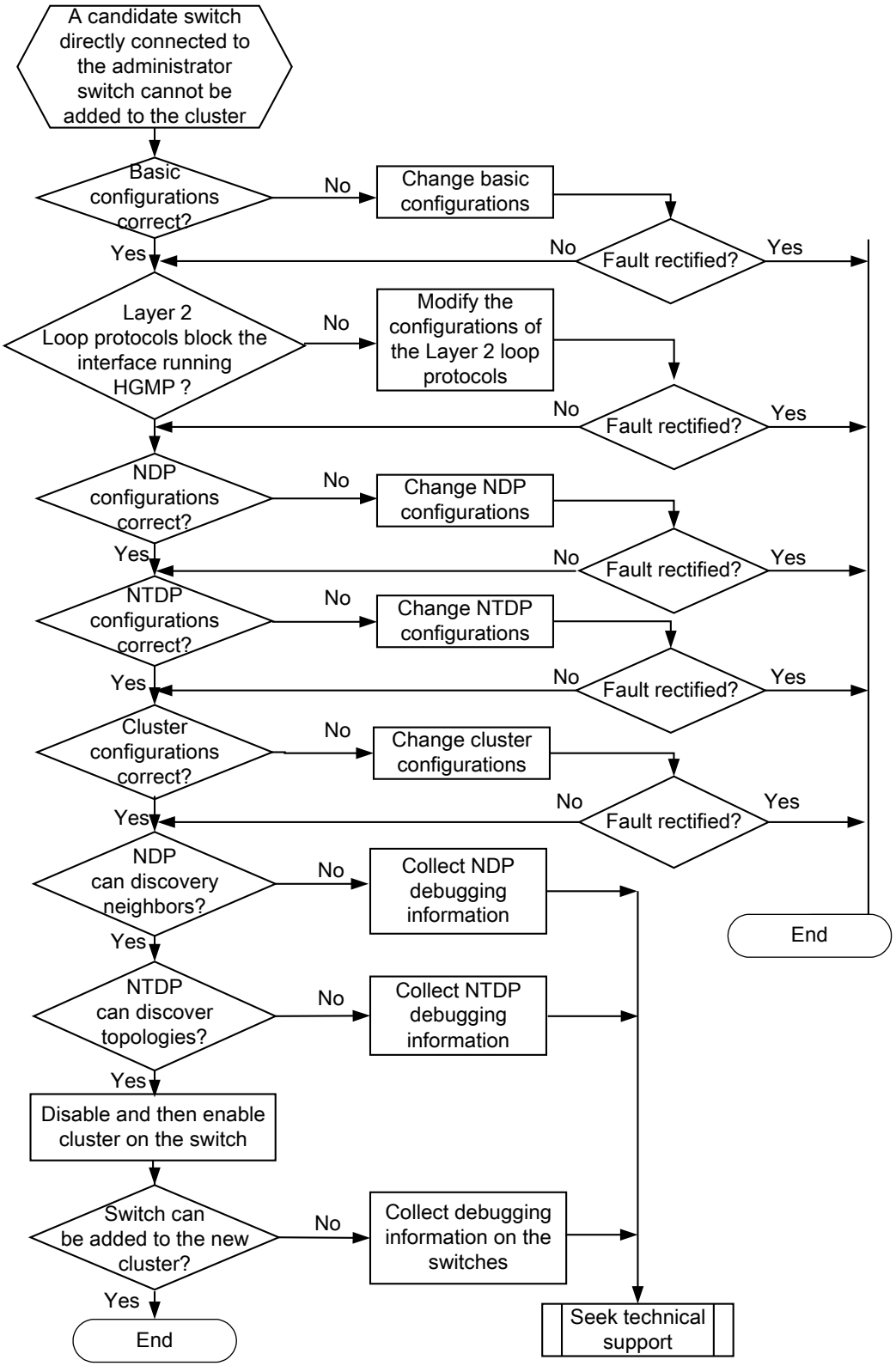
- Packets cannot be exchanged between the administrator switch and candidate switch because either of the interfaces connecting them is Down.
- The basic configuration of layer 2 forwarding is incorrectly configured.
- Layer 2 packet forwarding or transparent transmission of packets fails.
- Packets cannot be exchanged between the administrator switch and candidate switch because either of the interfaces that the packets pass through is blocked by a ring protocol.
- The cluster, NDP, or NTDP is incorrectly configured.
- The candidate switch has been added to the cluster and still remains in the cluster, and the new cluster to which the candidate switch is added has a different name from the current cluster.
- Authentication of the candidate switch fails due to inconsistent super passwords of the candidate switch and administrator switch.

Troubleshooting Flowchart

Figure 3-22 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-22 Troubleshooting flowchart for the fault that a candidate switch directly connected to the administrator switch cannot be added to the cluster



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that basic configurations of the administrator and candidate switches are correct.

HGMP packets can be exchanged only when Layer 2 forwarding is normal. You need to ensure that the administrator and candidate switches are correctly configured so that they can exchange Layer 2 packets.

Ensure that the two switches are configured as follows:

- The two directly connected interfaces are added to the same VLAN.
- The VLAN is the cluster management VLAN, which is specified by running the **mngvlanid** *vlan-id* command in the cluster view. In addition, *vlan-id* specifies the VLAN to which the interfaces belong.
- The two interfaces are added to the VLAN in the same manner. For example, the **port trunk allow-pass vlan** *vlan-id* command is run on both interfaces with *vlan-id* being the same.

If the preceding configurations are correct, run the **display vlan** *vlan-id* command on both the administrator and candidate switches to check whether interfaces in the VLAN are Up. For example,

```
[Quidway] display vlan 1000
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1000   common  TG:Eth0/0/1(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1000   enable  default       enable  disable    VLAN 01000
```

- If the interfaces are Down, the physical link may fail. In this case, rectify the physical link fault.
- If the interfaces are Up, Layer 2 protocol is normal. In the case where the fault still persists, either cluster configurations or packet processing at layers above Layer 2 may be incorrect. Go to **Step 2**.

Step 2 Check that the Layer 2 ring protocols on the interfaces of administrator and candidate switches run normally.

- If STP is enabled on administrator and candidate switches, check whether the interfaces running HGMP protocol are blocked by STP. Run the **display stp brief** command to check the interface status. For example,

```
[Quidway] display stp brief
MSTID      Port                  Role  STP State     Protection
   0        Ethernet0/0/1  ROOT  FORWARDING     NONE
   0        Ethernet0/0/2  DESI  FORWARDING     NONE
   0        Ethernet0/0/3  DESI  FORWARDING     NONE
```


Copyright © Huawei Technologies Co., Ltd.

If the packets can be normally forwarded, the "STP state" field is displayed as **FORWARDING** on the interfaces running HGMP protocol. If the "STP state" field is displayed as **DISCARDING**, it indicates that the interface is blocked by STP so that the interface cannot forward HGMP packets. You need to change the STP priority so that the interface can leave the **DISCARDING** state and the switch can be elected as the root bridge. by running the **stp priority** *priority-level* command in the system view. *priority-level* ranges from 0 to 61440. The smaller the value, the higher the priority. The device with a lower STP priority is elected as the root bridge of the ring.

If the interfaces running HGMP protocol are in the **FORWARDING** state, it indicates that STP on the interfaces runs normally.

- If RRPP is configured on both administrator and candidate switches, check whether the interfaces running HGMP protocol are blocked by RRPP. Run the **display rrpp verbose domain** *domain-index* command to check the interface status. For example,

```
[Quidway] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 1000    sub 1001
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Failed
Is Enabled     : Enable         Is Actived : Yes
Primary port   : Ethernet0/0/3         Port status: UP
Secondary port : Ethernet0/0/4         Port status: DOWN
```

If the "Port status" field is displayed as **BLOCK**, it indicates that cluster packets on the interfaces running HGMP protocol are blocked by RRPP. RRPP blocks secondary ports only. You need to change the blocked interface to be a non-secondary ports to ensure that the interface leave the blocked state.

If the interfaces running HGMP protocol are in the **Up**status, it indicates that RRPP on the interfaces runs normally. Go to **Step 3**.

NOTE

Only one ring protocol, in general, is configured on an interface. Check which ring protocol is configured on the interface before checking the interface status.

Step 3 Check that basic NDP functions are normal.

Run the **display ndp** command on both the administrator and candidate switches to check whether NDP can successfully discover neighbors. If NDP can discover neighbors, information about the directly connected neighbors can be displayed. For example,

```
<Quidway> display ndp
 Neighbor discovery protocol is enabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
 Interface: GigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 114, Packets Received: 108, Packets Error: 0
    Neighbor 1:  Aging Time: 174(s)
       MAC Address : 0018-8203-39d8
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.70 V100R005C00SPC001
       Device Name : Quidway
       Port Duplex : FULL
       Product Ver : S3700
```

If NDP cannot discover neighbors, check that NDP is configured as follows:

Copyright © Huawei Technologies Co., Ltd.

- NDP is globally enabled on both switches by running the **ndp enable** command in the system view.
- NDP is enabled on the two directly connected interfaces by running the **ndp enable** command in the interface view.

CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

If the NDP configurations are correct whereas NDP still cannot discover neighbors, collect the debugging information displayed by running the following commands and then contact Huawei technical support personnel.

- Run the **terminal monitor** and **terminal debugging** commands in the user view to enable monitoring debugging.
- Run the **debugging ndp packet interface** *interface-type interface-number* command in the user view to enable NDP debugging and collect the debugging information in three minutes.

If NDP can discover neighbors, go to **Step 4**.

Step 4 Check that basic NTDP functions are normal.

Check that NTDP is configured as follows:

- NTDP is globally enabled on both switches by running the **ntdp enable** command in the system view.
- NTDP is enabled on the two directly connected interfaces by running the **ntdp enable** command in the interface view.
- The cluster management VLAN is configured in the cluster view by running the **mngvlanid** *vlan-id* command in the cluster view. In addition, *vlan-id* specifies the VLAN to which the interface belongs.

If the NTDP configurations are incorrect, correctly configure NTDP.

If the NTDP configurations are correct, run the **ntdp explore** command on the administrator and candidate switches to discover topologies. After five seconds, run the **display ntdp device-list** command on the two switches to check whether NTDP can discover topologies. If NTDP can discover topologies, information about neighbors can be displayed. For example,

```
[Quidway] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 001c-2334-2312  1    1.1.1.2/24          S3700
 0018-82af-fc38  0    1.1.1.1/24          S3700
```

If NTDP cannot discover topologies, collect the debugging information displayed by running the following commands on the two switches and then contact Huawei technical support personnel.

- Run the **terminal monitor** and **terminal debugging** commands in the user view to enable monitoring debugging.

Copyright © Huawei Technologies Co., Ltd.

- Run the **debugging ntdp all** command in the use view to enable NTDP debugging.
- Run the **ntdp explore** command to discover topologies and the **display ntdp device-list** command to display the topologies.

If NTDP discovers topologies, go to **Step 5**.

NOTE

- A switch can be added to the cluster only if it has been discovered by NTDP on the administrator switch.
- Switches do not forward received NDP packets and therefore ring protocols cannot block NDP packets. NTDP packets are forwarded after being received and therefore NTDP packets may be blocked by ring protocols.

Step 5 Check that the basic cluster function is normal.

Check whether the cluster function is configured as follows:

- The cluster function is globally enabled on both switches by running the **cluster enable** command in the system view.
- VLANIF interfaces of the cluster management VLAN are configured on both switches by running the **interface vlanif** *vlan-id* command in the system view. *vlan-id* must be the same as that in the **mngvlanid** command configured in the cluster view.
- An available IP pool is configured on the administrator switch by running the **ip-pool** *administrator-ip-address mask* command in the cluster view.
- The IP addresses manually assigned to the VLANIF interfaces of the management VLAN do not reside in the IP pool configured by using the **ip-pool** command.
- No super password or the same super password is configured for the administrator and candidate switches.

If the cluster configurations are incorrect, correctly configure the cluster function.

If the cluster configurations are correct, disable cluster from the switch by running the **undo cluster enable** command, and then run the **cluster enable** command to ensure that the switch does not belong to any cluster. Then, delete the cluster on the administrator switch, and then create a new cluster. Check whether the candidate switch can be added to the new cluster.

- Run the **undo build** command in the cluster view to delete the existing cluster.
- Run the **auto-build** command to create a new cluster.

If the candidate switch still cannot be added to the cluster, collect the debugging information displayed by running the following commands on the two switches and then contact Huawei technical support personnel.

- Run the **terminal monitor** and **terminal debugging** commands in the user view to enable monitoring debugging.
- Run the **debugging cluster all** command in the use view to enable cluster debugging.
- Manually add the candidate switch to the cluster by running the **add-member mac-address** *mac-address* command in the cluster view and collect the command output displayed in 10 seconds.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the device

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

Relevant Alarms

HGMP/4/ClstMemStusChg:OID:[oid],DeviceID:[string], Role:[integer].

Relevant Logs

None.

3.12 LLDP Troubleshooting

This chapter describes common causes of the LLDP fault, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

3.12.1 An Interface Cannot Discover Neighbors

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the LLDP failure.

Common Causes

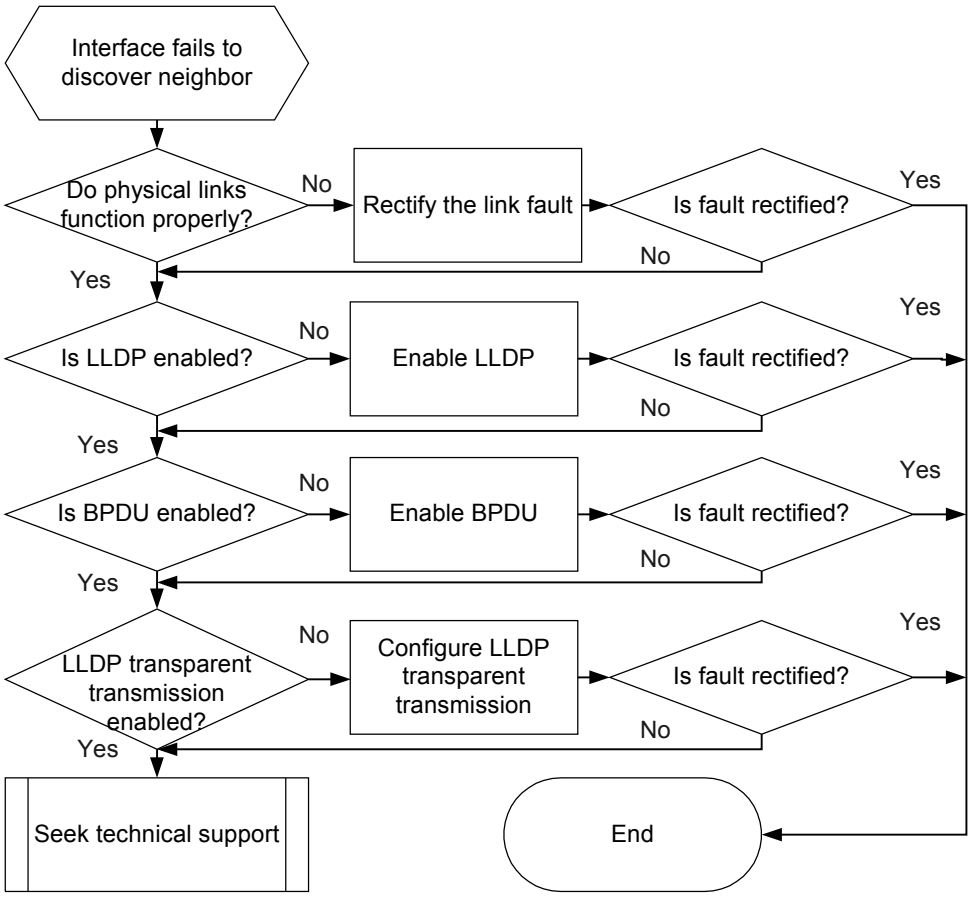
This fault is commonly caused by one of the following:

- The physical link is faulty.
- The LLDP function is not enabled.
- The BPDU function is not enabled on the interface.
- The LLDP transparent transmission function is not properly configured on the interface.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 3-23 LLDP troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

After you run the **display lldp neighbor brief** command, the output information shows that the device does not discover any neighbor.

Procedure

Step 1 Check that the physical links between devices function properly.

Run the **display interface** *interface-type interface-number* command to view the value of **current state**.

- If the value is DOWN, the link is faulty. Rectify the link faulty.
- If the value is UP, the link functions properly. Go to step 2.

Step 2 Check that LLDP is enabled.

By default, if global LLDP is enabled, LLDP is enabled on all interfaces. To disable LLDP on an interface, run the **undo lldp enable** on the interface.

Copyright © Huawei Technologies Co., Ltd.

1. Check that the global LLDP function is enabled.

   Run the **display current-configuration** command to check whether the output information contains the **lldp enable** command.

   - If the **lldp enable** command cannot be found, run the **lldp enable** to enable the global LLDP function.
   - If the **lldp enable** command is contained, go to step b.

2. Check whether LLDP is disabled on the interface.

   Run the **display this** command in the interface view to check whether the output information contains the **undo lldp enable** command.

   - If the **undo lldp enable** command is contained, run the **lldp enable** to enable the LLDP function. on the interface.
   - If the command is not found, go to step 3.

Step 3 Check whether BPDU is enabled on the interface.

Run the **display this** command in the interface view to check whether the output information contains the **bpdu enable** command.

- If not, LLDP packets are not sent to the CPU, and thus the interface cannot discover neighbors. Run the **bpdu enable** command to enable BPDU.
- If yes, go to step 4.

Step 4 Check whether LLDP transparent transmission is configured properly.

By default, LLDP transparent transmission is disabled on an interface. You can run the **display this** command in the interface view to check whether LLDP transparent transmission is enabled. If the output information contains **l2protocol-tunnel lldp enable**, LLDP transparent transmission is enabled on the interface.

- If the interface has only one neighbor, LLDP transparent transmission must be disabled on the LLDP-enabled device; otherwise, the interface cannot discover the neighbor.
- If the interface has multiple neighbors, LLDP transparent transmission must be disabled on the LLDP-enabled device, but enabled on the intermediate device; otherwise, the interface cannot discover neighbors.
  - To enable LLDP transparent transmission, run the **l2protocol-tunnel lldp enable** command in the interface view.
  - To disable LLDP transparent transmission, run the **l2protocol-tunnel lldp disable** command in the interface view.
- If the configuration is incorrect, modify the configuration.
- If the configuration is correct, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms

None.

Relevant Logs

None.

3.13 NAP-based Remote Deployment Troubleshooting

3.13.1 Fail to Log In to the Newly Deployed Device Through NAP

Common Causes

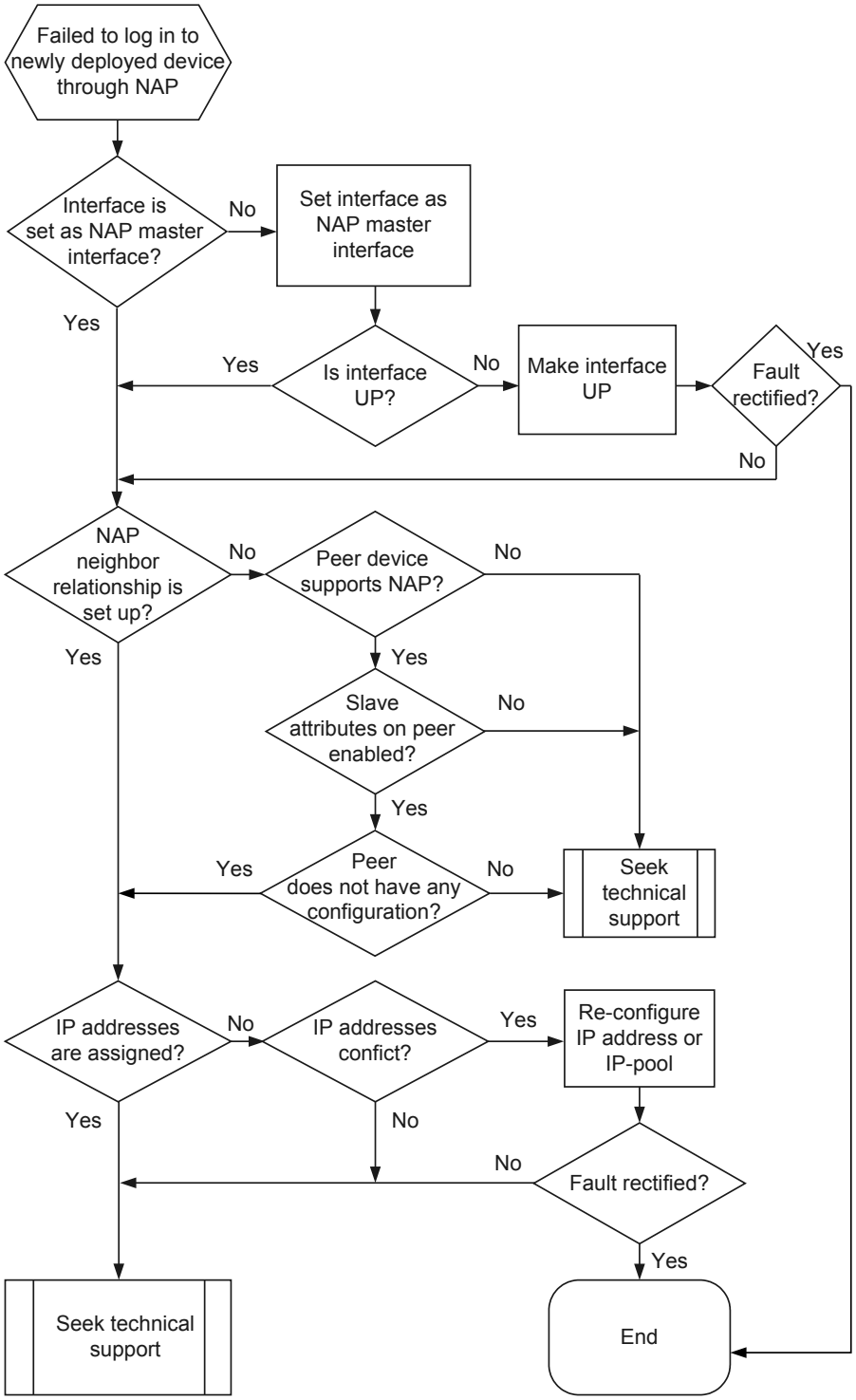
This fault is commonly caused by one of the following:

- The NAP configuration is error on the local device.
- The connection between the master and slave devices has not been established or is instable.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 3-24 Troubleshooting flowchart for the fault that log in to the newly deployed device through NAP fails



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

- Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.
- Before troubleshooting, ensure that the new device with empty configuration supports NAP.

  If you do not know whether the device to be logged in has configurations, contact the on-site Huawei technical support personnel to confirm that the device does not have any configuration.

Procedure

Step 1 Check that the current interface is the NAP master interface.

Run the **display nap interface** command in any view to check the **Port property** field.

- If **Master** is displayed in this field, go to **Step 2**.
- If the value displayed in this field is not **Master**, run the **nap port master** command in the corresponding interface view to configure the interface as the NAP master interface.

  If the interface cannot be configured with the **nap port master** command, the interface does not support NAP. Choose another interface of another type.

  NOTE

  Currently, Ethernet and Gigabit Ethernet interfaces support NAP.

Step 2 Check that the NAP master interface is in the DETECTING state.

Run the **display nap interface** command in any view to check the **Current status** field.

- If **DETECTING** is displayed in this field, run the **display interface** command to view the status of the NAP master interface.
  - If the NAP master interface is Down, check whether the new device is physically connected and whether the current NAP master interface is connected to the new device.
  - If the NAP master interface is Up, go to **Step 4**.
- If the value displayed in this field is not **DETECTING**, go to **Step 3**.

Step 3 Check that the NAP neighbor has obtained an IP address.

Run the **display nap interface** command in any view to check the **Current status** field.

- If **Established** is displayed in this field, and the IP addresses of the NAP master and slave interfaces keep changing, IP addresses allocated from the IP address pool conflict. Do as follows based on the number of master interfaces:
  - If only one master interface exists, run the **nap ip-pool** command in the system view to configure the IP address pool.
  - If two or more master interfaces exist, run the **nap local-ip** *mast-inter-mast-ip* **sub-ip** *mast-inter-sub-ip* **peer-ip** *sub-inter-mast-ip* **sub-ip** *sub-inter-sub-ip mask-length* command in the current master interface view to configure IP addresses for the master and slave interfaces.
- If **IP-ASSIGNED** is displayed in this field, an IP address has been allocated to the NAP neighbor. Then, go to **Step 4**.

Step 4 Collect the following information, and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures

Copyright © Huawei Technologies Co., Ltd.

- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

NAP/4/NAP_STATUSCHANGE:OID 1.3.6.1.4.1.2011.5.25.206.3.1 Index [integer], the status of the nap port [octet] has changed to [integer], and the AbnormalReason is [integer].

Relevant Logs

NAP/6/GOTONEIGHBOR:Connected to the device on the slave interface end through the main interface[STRING].

Copyright © Huawei Technologies Co., Ltd.

4 Physical Connection and Interfaces

About This Chapter

4.1 Ethernet Interface Troubleshooting
This chapter describes common causes of Ethernet interface faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

4.2 Eth-Trunk Interface Troubleshooting
This chapter describes common causes of Eth-Trunk interface faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

4.1 Ethernet Interface Troubleshooting

This chapter describes common causes of Ethernet interface faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

4.1.1 Connected Ethernet Interfaces Down

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when Ethernet interfaces between two devices cannot turn Up.

Common Causes

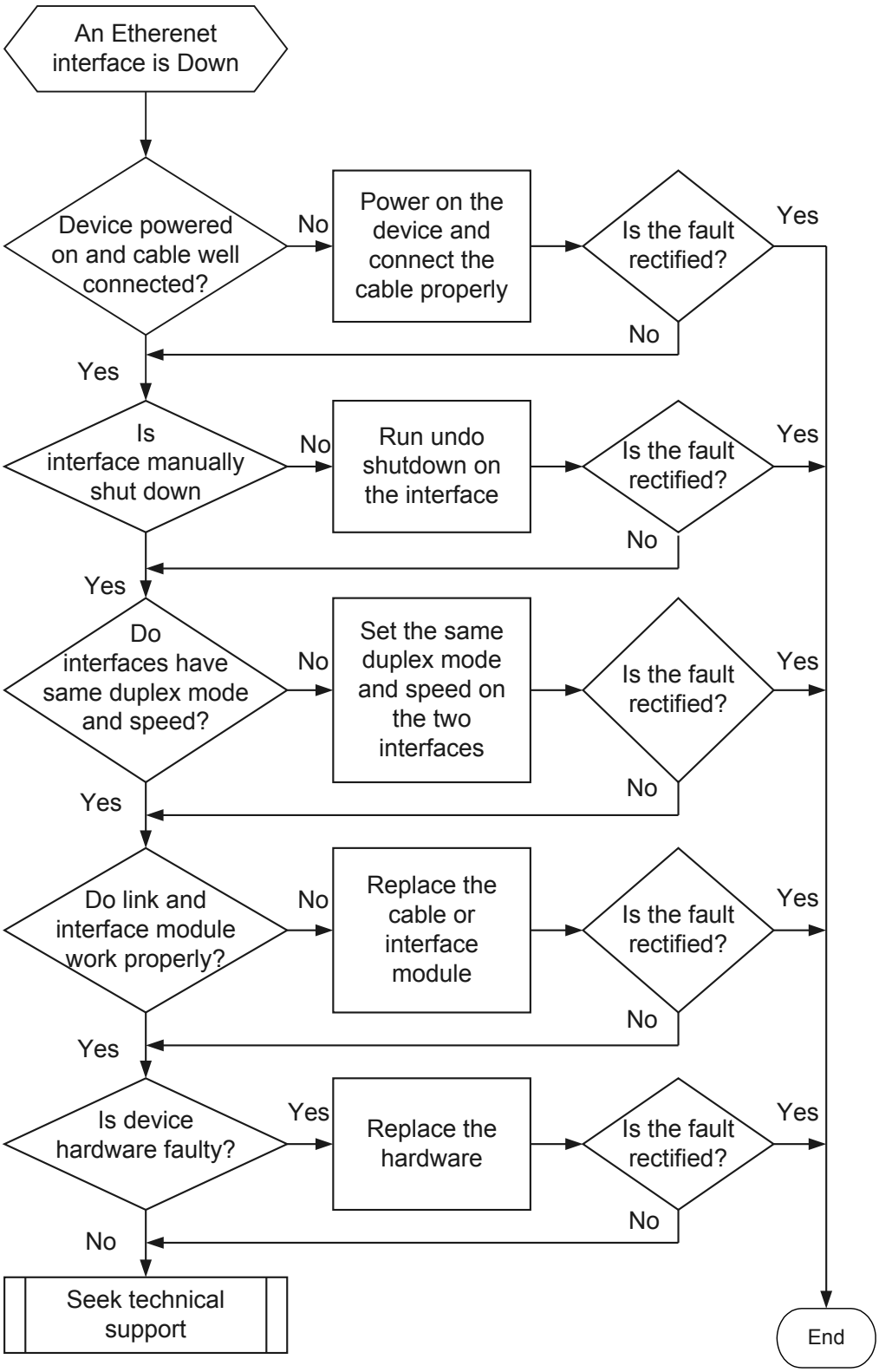
This fault is commonly caused by one of the following:

- The devices are powered off or the cable between the interfaces is not properly connected.
- The Ethernet interfaces are manually shut down.
- The twisted pair or fiber between the interfaces is too long or the attenuation is high.
- The duplex modes or the speeds of the local and remote interfaces are different.
- The interfaces, interface modules, or devices are faulty.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Troubleshooting flowchart for Ethernet interfaces in Down state



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the local and remote switches are powered on and that the cable and interface modules are installed properly.

If the fault persists, go to **Step 2**.

Step 2 Check that the interfaces are not manually shut down.

Run the **interface** *interface-type interface-number* command in the system view to enter the interface view, and then run the **display this** command to check the interface status.

If an interface was shut down by using the **shutdown** command, run the **undo shutdown** command in the interface view.

NOTE

If a Monitor Link group is configured on a switch, all downlink interfaces in the group are shut down when the uplink interface is deleted from the group or turns Down. If the uplink interface turns down, rectify the fault on the uplink interface.

If the fault persists, go to **Step 3**.

Step 3 Check that the two interfaces have the same duplex mode, speed, and negotiation mode.

Run the **display interface** command on the two interfaces to check the speeds, duplex modes, and negotiation modes of the interfaces.

Check Item	Description	Follow-Up Operation
Negotiation	Negotiation mode of an interface. ● ENABLE: indicates that the interface works in auto negotiation mode. ● DISABLE: indicates that the interface works in non-auto negotiation mode, that is, forced mode.	The two interfaces must work in the same negotiation mode. Run the **negotiation auto** command in the interface view to enable auto negotiation on the interfaces. If the interfaces are still Down, disable auto negotiation and forcibly set the same speed and duplex mode on the interfaces.
Speed	Current speed of an interface.	If the speeds of the interfaces are different, run the **speed** command in the interface view to set the same speed on the two interfaces.

Copyright © Huawei Technologies Co., Ltd.

Check Item	Description	Follow-Up Operation
Duplex	Duplex mode of an interface.	If the duplex modes of the interfaces are different, run the **duplex** command in the interface view to set the same duplex mode on the two interfaces.
Mdi	Network cable type supported by an interface. ● across: indicates that the interface can use a crossover cable. ● auto: indicates that an interface automatically identifies the network cable type. That is, the interface can use a straight-through cable or a crossover cable. ● normal: indicates that the interface can use a straight-through cable.	The two interfaces must support the same network cable type. By default, an interface works in auto mode. If the interfaces do not work in this mode, run the **mdi** command on the interfaces to change the mode to auto.

If the fault persists, go to **Step 4**.

Step 4 Check that the interface modules and the link between the interfaces work properly.

If the two interfaces are connected by a twisted pair, check the following items.

Check Item	Criteria	Follow-Up Operation
Twisted pair working status	The tester shows that the twisted pair works properly.	If the twisted pair is faulty, replace it.
Twisted pair length	The twisted pair length does not exceed 100 m. **NOTE** The 10/100/1000M electrical interfaces use RJ-45 connectors and category-5 twisted pairs or cables with higher specifications. The maximum transmission distance of such cables is 100 m.	If the twisted pair length exceeds 100 m, perform either of the following operations: ● Shorten the distance between the two switches and use a shorter twisted pair. ● If the distance between the two devices cannot be shortened, deploy a relay, hub, or switch between the devices.

Copyright © Huawei Technologies Co., Ltd.

Check Item	Criteria	Follow-Up Operation
Twisted pair type	Twisted pair cables are classified into straight-through cables and crossover cables. A straight-through cable connects Ethernet interfaces between the following devices: ● A router and a hub ● A router and an Ethernet switch ● A computer and an Ethernet switch ● A computer and a hub A crossover cable connects Ethernet interfaces between the following devices: ● Two routers ● A router and a computer ● Two hubs ● A hub and a switch ● Two switches ● Two computers	If the twisted pair type is incorrect, replace the twisted pair.
Electrical interface module	If electrical interface modules are installed, they work properly.	If an electrical interface module fails, replace it.

If the two interfaces are connected by fibers, check the following items.

Check Item	Criteria	Follow-Up Operation
Fiber working status	The tester shows that optical signals are sent and received successfully. In a loopback test, the two interfaces are Up.	If optical signals cannot be sent or received, replace the fibers. If the fault persists, replace the optical modules.
Types of optical modules and fibers	The fiber type matches the optical module type. For details about mappings between optical module types and fiber types, see "List of Optical Interface Attributes" in the hardware description.	If the fiber type does not match the optical module type, replace the optical modules or fibers.

Copyright © Huawei Technologies Co., Ltd.

Check Item	Criteria	Follow-Up Operation
Fiber length and maximum transmission distance of optical modules	The fiber length is smaller than the maximum transmission distance of the optical modules. For the maximum transmission distance supported by different optical modules, see "List of Optical Interface Attributes" in the hardware description.	If the fiber length exceeds the maximum transmission distance of the modules, shorten the distance between the devices or use optical modules with a larger transmission distance.
Optical signal attenuation	The tester shows that the optical signal attenuation is in the allowed range. For the attenuation range, see "List of Optical Interface Attributes" in the hardware description.	If the attenuation is high, replace the fibers. If the fault persists, shorten the distance between the devices and use shorter fibers.

If the fault persists, go to **Step 5**.

Step 5 Check whether the local or remote device has a hardware fault.

Connect the devices using other interfaces. If the fault persists, go to **Step 6**.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

4.1.2 An Ethernet Interface Frequently Alternates Between Up and Down

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when an Ethernet interface frequently alternates between Up and Down.

Common Causes

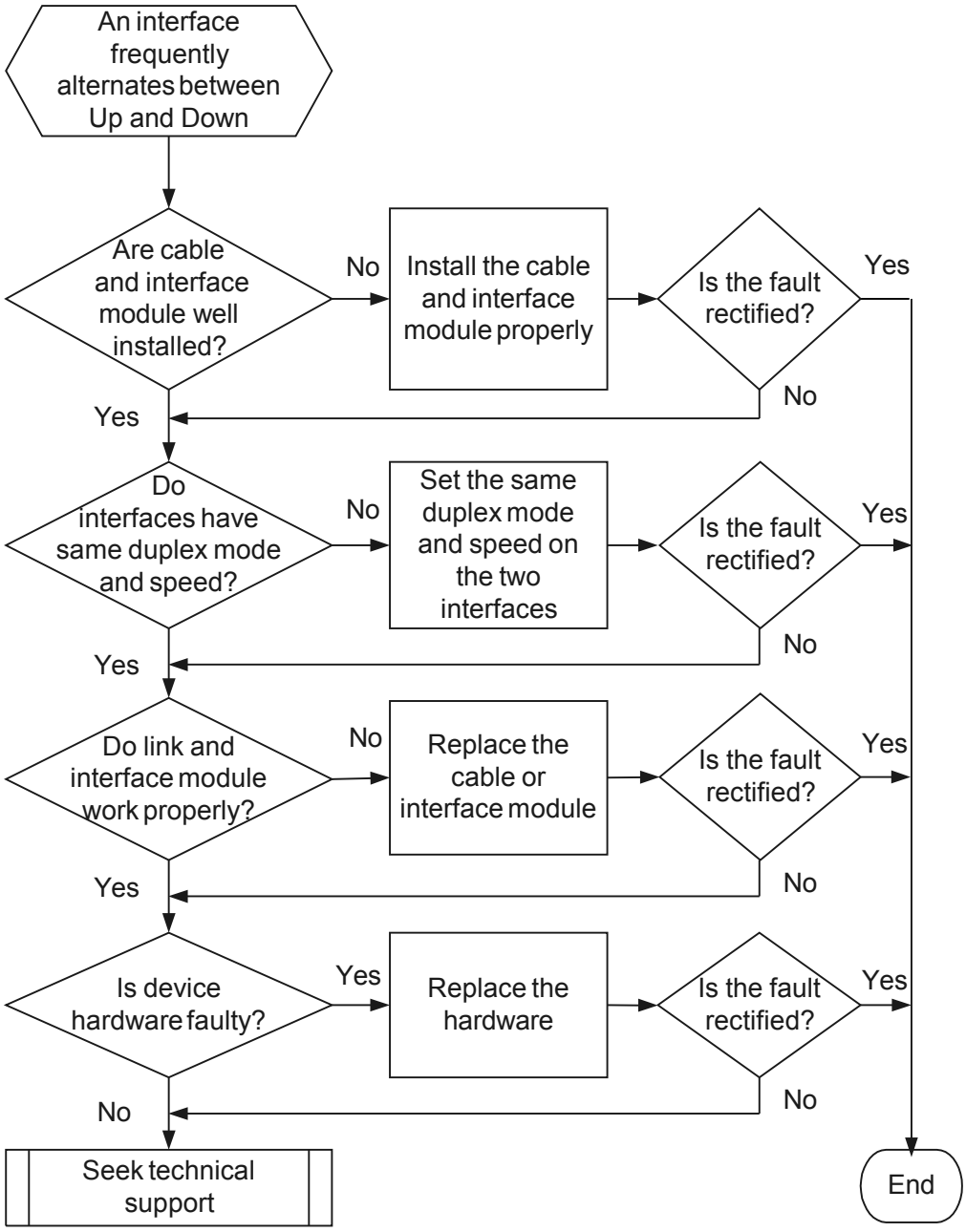
This fault is commonly caused by one of the following:

Copyright © Huawei Technologies Co., Ltd.

- The cable is not properly connected to the interface.
- The twisted pair or fiber connected to the interface is too long or the attenuation is high.
- The duplex modes or the speeds of the local and remote interfaces are different.
- The local and remote interfaces, interface modules, or devices are faulty.

Troubleshooting Flowchart

Figure 4-2 Troubleshooting flowchart for an Ethernet interface frequently alternating between Up and Down



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the cable and interface modules are properly installed on the local and remote devices.

If the fault persists, go to **Step 2**.

Step 2 Check that the two interfaces have the same duplex mode, speed, and negotiation mode.

Run the **display interface** command on the two interfaces to check the speeds, duplex modes, and negotiation modes of the interfaces.

Check Item	Description	Follow-Up Operation
Negotiation	Negotiation mode of an interface. ● ENABLE: indicates that the interface works in auto negotiation mode. ● DISABLE: indicates that the interface works in non-auto negotiation mode, that is, forced mode.	The two interfaces must work in the same negotiation mode. Run the **negotiation auto** command in the interface view to enable auto negotiation on the interfaces. If the fault persists, disable auto negotiation and forcibly set the same speed and duplex mode on the interfaces.
Speed	Current speed of an interface.	If the speeds of the interfaces are different, run the **speed** command in the interface view to set the same speed on the two interfaces.
Duplex	Duplex mode of an interface.	If the duplex modes of the interfaces are different, run the **duplex** command in the interface view to set the same duplex mode on the two interfaces.

If the fault persists, go to **Step 3**.

Step 3 Check that the interface modules and the link between the interfaces work properly.

If the two interfaces are connected by a twisted pair, check the following items.

Check Item	Criteria	Follow-Up Operation
Twisted pair working status	The tester shows that the twisted pair works properly.	If the twisted pair is faulty, replace it.

Copyright © Huawei Technologies Co., Ltd.

Check Item	Criteria	Follow-Up Operation
Twisted pair length	The twisted pair length does not exceed 100 m. **NOTE** The 10/100/1000M electrical interfaces use RJ-45 connectors and category-5 twisted pairs or cables with higher specifications. The maximum transmission distance of such cables is 100 m.	If the twisted pair length exceeds 100 m, perform either of the following operations: ● Shorten the distance between the two switches and use a shorter twisted pair. ● If the distance between the two devices cannot be shortened, deploy a relay, hub, or switch between the devices.
Electrical interface module	If electrical interface modules are installed, they work properly.	If an electrical interface module fails, replace it.

If the two interfaces are connected by fibers, check the following items.

Check Item	Criteria	Follow-Up Operation
Fiber working status	The tester shows that optical signals are sent and received successfully. In a loopback test, the two interfaces are Up.	If optical signals cannot be sent or received, replace the fibers. If the fault persists, replace the optical modules.
Types of optical modules and fibers	The fiber type matches the optical module type. For details about mappings between optical module types and fiber types, see "List of Optical Interface Attributes" in the hardware description.	If the fiber type does not match the optical module type, replace the optical modules or fibers.
Fiber length and maximum transmission distance of optical modules	The fiber length is smaller than the maximum transmission distance of the optical modules. For the maximum transmission distance supported by different optical modules, see "List of Optical Interface Attributes" in the hardware description.	If the fiber length exceeds the maximum transmission distance of the modules, shorten the distance between the devices or use optical modules with a larger transmission distance.
Optical signal attenuation	The tester shows that the optical signal attenuation is in the allowed range. For the attenuation range, see "List of Optical Interface Attributes" in the hardware description.	If the attenuation is high, replace the fibers. If the fault persists, shorten the distance between the devices and use shorter fibers.

Copyright © Huawei Technologies Co., Ltd.

If the fault persists, go to **Step 4**.

Step 4 Check whether the local or remote device has a hardware fault.

- Connect the twisted pair or fibers to another interface.
- If the remote device is a powered device (PD), check that the PD works properly and its power does not exceed the maximum power of the interface.

  NOTE

  When the instant power of the PD exceeds the maximum power of the interface, the local device powers off the PD. After a certain period, the device detects the PD and powers on it again. The PD is frequently powered on and off, so the interface alternates between Up and Down.

If the fault persists, go to **Step 5**.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

4.2 Eth-Trunk Interface Troubleshooting

This chapter describes common causes of Eth-Trunk interface faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

4.2.1 Eth-Trunk Interface Cannot Forward Traffic

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the fault that an Eth-Trunk interface cannot forward traffic.

Common Causes

After an Eth-Trunk interface is configured, it cannot forward traffic.

This fault is commonly caused by one of the following:

- Eth-Trunk member interfaces are faulty.
- Configurations of Eth-Trunk member interfaces on the two ends are inconsistent.
- The number of Up Eth-Trunk member interfaces is smaller than the lower threshold.

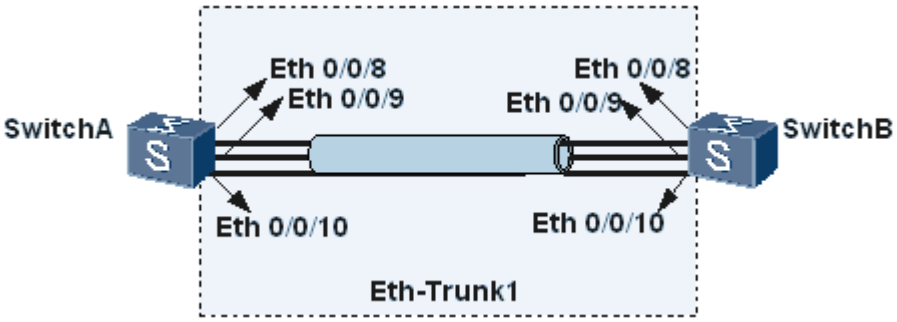
Copyright © Huawei Technologies Co., Ltd.

- Negotiation between member interfaces of the Eth-Trunk interface in static LACP mode fails.

Troubleshooting Flowchart

On the network shown in **Figure 4-3**, the Eth-Trunk interface cannot forward traffic.

Figure 4-3 Eth-Trunk network diagram



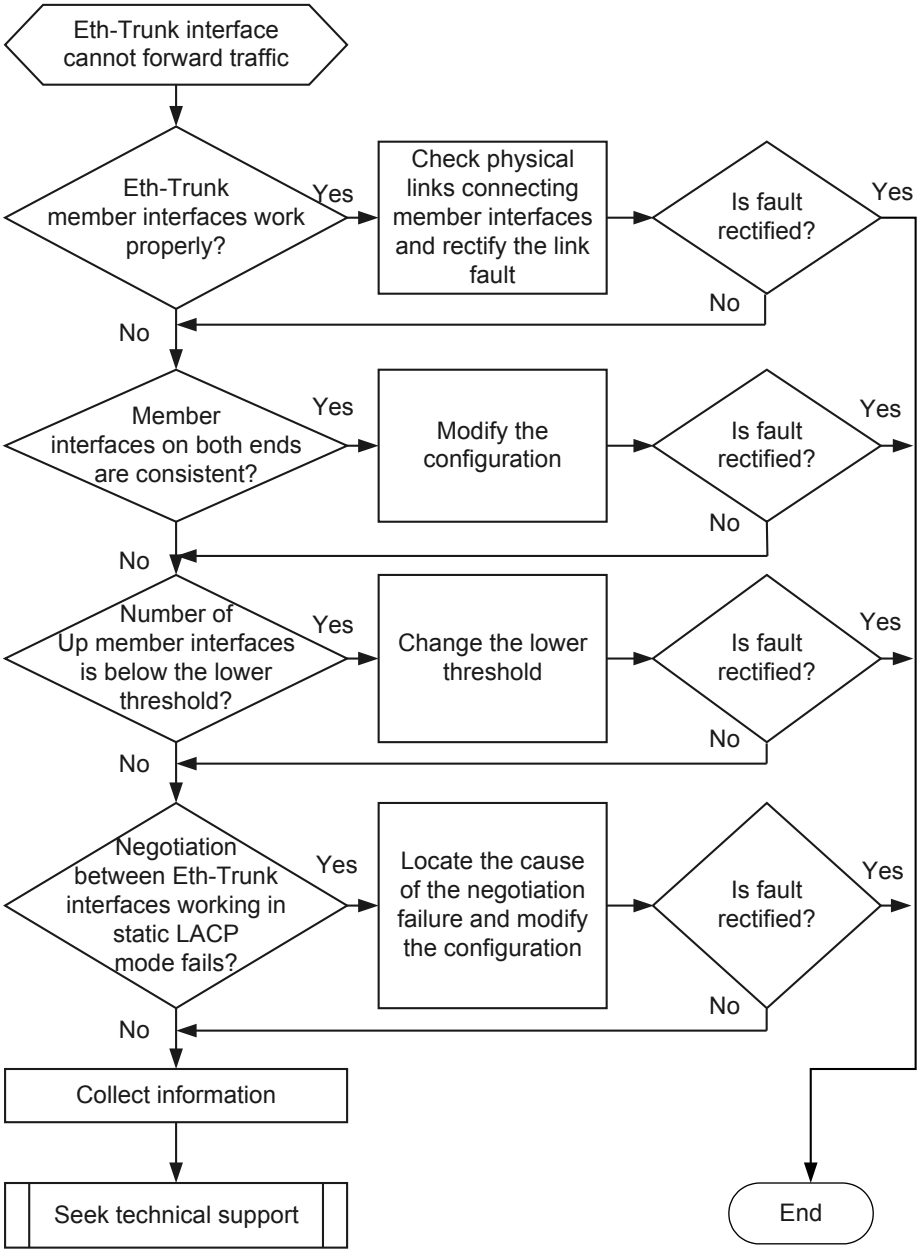
The troubleshooting roadmap is as follows:

- Check that Eth-Trunk member interfaces work properly.
- Check information about Eth-Trunk member interfaces on both ends.
- Check that the number of Up member interfaces is greater than the configured lower threshold.
- Check that LACP negotiation succeeds if the Eth-Trunk interface is in static LACP mode.

Figure 4-4 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-4 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that Eth-Trunk member interfaces work properly.

Run the **display eth-trunk 1** command in any view to check the status of the Eth-Trunk interface.

Copyright © Huawei Technologies Co., Ltd.

```
[Quidway] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic:According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 4
Operate status: down        Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------

PortName         Status      Weight
Ethernet0/0/8    Down        1
Ethernet0/0/9    Down        1
Ethernet0/0/10   Down        1
```

- If a member interface is Down, you need to troubleshoot the physical interface. For detailed troubleshooting procedures, see "**4.1.1 Connected Ethernet Interfaces Down**".
- If the member interface is Up, verify that each cable is correctly connected to interfaces. If the fault persists, go to **Step 2**.

Step 2 Check information about Eth-Trunk member interfaces on both ends.

Check information about member interfaces of the Eth-Trunk interface on Switch A and Switch B.

```
[SwitchA] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 4
Operate status: up          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------

PortName         Status      Weight
Ethernet0/0/8    up        1
Ethernet0/0/9    up        1
Ethernet0/0/10   up        1
[SwitchB] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 4
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName        Status      Weight
Ethernet0/0/8    up        1
Ethernet0/0/9    up        1
```

- Check information about member interfaces of the Eth-Trunk interface on Switch B.
- If the number of member interfaces of the Eth-Trunk interface on Switch A is different from that on Switch B, add the required physical interfaces to the Eth-Trunk interface.
- If the number of member interfaces of the Eth-Trunk interface on Switch A is the same as that on Switch B, go to **Step 3**.

Step 3 Check whether the Eth-Trunk interface is configured with a lower threshold of Up member interfaces.

Run the **display eth-trunk 1** command on Switch A and Switch B to view the configuration of the Eth-Trunk interface.

```
[SwitchA] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 4  Max Bandwidth-affected-linknumber: 4
Operate status: down        Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------

PortName         Status      Weight
Ethernet0/0/8    up        1
Ethernet0/0/9    up        1
Ethernet0/0/10   up        1
```


Copyright © Huawei Technologies Co., Ltd.

The preceding command output shows that the lower threshold of Up member interfaces of the Eth-Trunk interface has been set to 4. However, the number of Up member interfaces of the Eth-Trunk interface is actually 3, which causes the Eth-Trunk interface to go Down.

- If the Eth-Trunk interface is configured with a lower threshold of Up member interfaces and the configured lower threshold is greater than the actual number of Up member interfaces, set the lower threshold to a proper value.
- If the Eth-Trunk interface is not configured with a lower threshold of Up member interfaces, go to **Step 4**.

Step 4 Check whether Eth-Trunk interfaces work in static LACP mode.

Run the **display eth-trunk 1** command on Switch A and Switch B to view the configuration of the Eth-Trunk interface.

```
[SwitchA] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: STATIC
Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
System Priority: 32768      System ID: 0018-826f-fc7a
Least Active-linknumber: 1  Max Active-linknumber: 4
Operate status: down        Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName         Status     PortType  PortPri PortNo PortKey PortState Weight
Ethernet0/0/8  UnSelected 100M      32768   264    305     11100010  1
Ethernet0/0/9  UnSelected 100M      32768   265    305     11100010  1
Ethernet0/0/10 UnSelected 100M      32768   266    305     11100010  1
Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri SystemID        PortPri PortNo  PortKey   PortState
Ethernet0/0/8   32768  0018-823c-c473  32768   2056    305       11100010
Ethernet0/0/9   32768  0018-823c-c473  32768   2057    305       11100010
Ethernet0/0/10  32768  0018-823c-c473  32768   2058    305       11100010
```

- If the Eth-Trunk interface is configured to work in static LACP mode and no physical interface is selected, it indicates that LACP negotiation is unsuccessful. Possible causes for unsuccessful LACP negotiation are as follows:
  - Member interfaces fail, causing timeout of LACP protocol packets.

    Connect the cable to another idle interface and add the interface to the Eth-Trunk.
  - The Eth-Trunk interface on one end is configured to work in static LACP mode, whereas the Eth-Trunk interface on the other end is not.

    Correct the configurations of the two ends of the Eth-Trunk link to make them consistent.

  After the configurations are corrected and LACP negotiation succeeds, the output of the **display eth-trunk 1** command is as follows:

```
[SwitchB] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: STATIC
Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
System Priority: 32768      System ID: 0018-826f-fc7a
Least Active-linknumber: 1  Max Active-linknumber: 4
Operate status: up          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
--
ActorPortName          Status   PortType  PortPri PortNo PortKey PortState
Weight
Ethernet0/0/8   Selected 100M      32768   264    305     11111100  1
Ethernet0/0/9   Selected 100M      32768   265    305     11111100  1
Ethernet0/0/10  Selected 100M      32768   266    305     11111100  1
```


Copyright © Huawei Technologies Co., Ltd.

```
Partner:
------------------------------------------------------------------------------
--
ActorPortName          SysPri SystemID        PortPri PortNo  PortKey
PortState
Ethernet0/0/8   32768  0018-823c-c473  32768   2056    305       11111100
Ethernet0/0/9   32768  0018-823c-c473  32768   2057    305       11111100
Ethernet0/0/10  32768  0018-823c-c473  32768   2058    305       11111100
```

If LACP negotiation fails after the configurations are corrected, go to **Step 5**.

- If the Eth-Trunk interface is not configured to work in static LACP mode, go to **Step 5**.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

4.2.2 Troubleshooting Cases

Traffic Is Not Load Balanced Between Eth-Trunk Member Interfaces Due to the Incorrect Load Balancing Mode

Fault Symptom

As shown in **Figure 4-5**, SwitchA and SwitchB communicate by using an Eth-Trunk. All interfaces on SwitchA and SwitchB belong to the same VLAN. After the **display interface** command is run on SwitchA, the command output shows that the outgoing traffic rate on GE0/0/1is 800 Mbit/s and the outgoing traffic rate on GE0/0/2 is 200 Mbit/s. That is, outgoing traffic is not load balanced between GE0/0/1 and GE0/0/2.

Figure 4-5 Network diagram of Eth-Trunk load balancing

Copyright © Huawei Technologies Co., Ltd.

Fault Analysis

1. Run the **display current-configuration** command on the Switches to check the configuration of Eth-Trunk 1. The command outputs show that the load balancing mode of Eth-Trunk 1 is **src-dst-ip**. That is, load balancing is performed based on the Exclusive-Or result of source and destination IP addresses. SwitchA and SwitchB communicate at Layer 2; therefore, the load balancing mode is not applicable to this scenario.

   This fault is caused by the incorrect load balancing mode.

Procedure

Step 1 Run the **system-view** command on SwitchA to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the Eth-Trunk interface view.

Step 3 Run the **load-balance src-dst-mac** command to set the load balancing mode to **src-dst-mac** .

Run the **display interface** [*number* [*interface-type*]] command on SwitchA to check the traffic rates on GE0/0/1 and GE0/0/2. You can see that traffic is load balanced properly on the two interfaces.

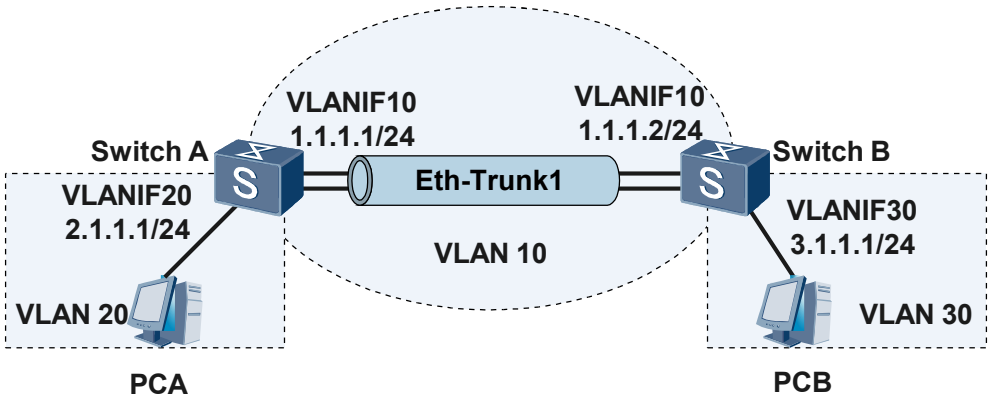
----End

Summary

The Switches can communicate at Layer 2 or Layer 3 by using Eth-Trunk 1.

Figure 4-6 shows the Layer 3 communication scenario. Eth-Trunk 1 belongs to VLAN 10. SwitchA functions as the gateway of PCA, and SwitchB functions as the gateway of PCB. IP addresses of PCA and PCB are in different network segments. To enable PCA to communicate with PCB, you must configure a route to the network segment 3.1.1.0 and set the next hop address of the route to 1.1.1.2 on SwitchA. In addition, configure a route to the network segment 2.1.1.0 and set the next hop address of the route to 1.1.1.1 on SwitchB. In the Layer 3 communication scenario, routes must be configured properly.

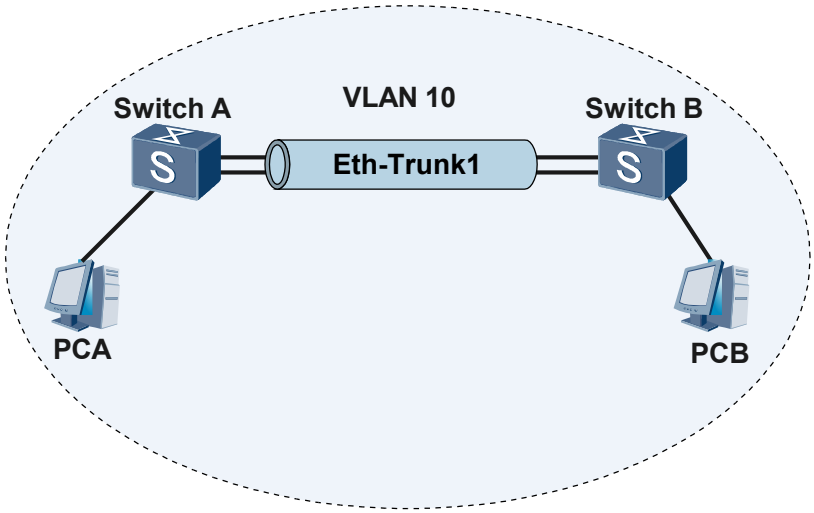
Figure 4-6 Layer 3 communication using Eth-Trunk 1



Copyright © Huawei Technologies Co., Ltd.

Figure 4-7 shows the Layer 2 communication scenario. All interfaces on SwitchA and SwitchB belong to VLAN 10. In the Layer 2 communication scenario, you do not need to configure routes.

Figure 4-7 Layer 2 communication using Eth-Trunk 1



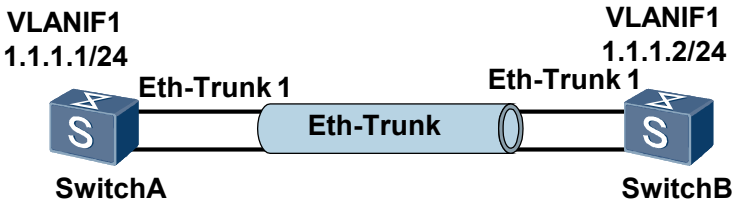
In the Layer 3 communication scenario, select the IP address-based load balancing modes. In the Layer 2 communication scenario, select the MAC address-based load balancing modes.

Devices at the Two Ends of an Eth-Trunk Cannot Ping Each Other Due to Inconsistent Aggregation Modes

Fault Symptom

As shown in Figure 4-8, SwitchA is an S3700, and SwitchB is a non-Huawei device. An Eth-Trunk consisting of two FE links is configured between the two devices. After the configuration, the devices cannot ping the management IP address of each other.

Figure 4-8 Network diagram of an Eth-Trunk



Fault Analysis

1. Run the **display current-configuration interface eth-trunk** command on SwitchA and SwitchB. The command outputs show that the Eth-Trunk interfaces on the two ends belong to the same VLAN.

Copyright © Huawei Technologies Co., Ltd.

2. Check the connection between the member interfaces. The member interfaces on SwitchA are correctly connected to the member interfaces on SwitchB.
3. Run the **display interface** command on SwitchA and SwitchB to check the status of the member interfaces. All the member interfaces are in Up state.
4. Run the **display trunkmembership eth-trunk** command on SwitchA and SwitchB to check the number of member interfaces in the Eth-Trunk. The two ends contain the same number of member interfaces.
5. Run the **display mac-address** command on SwitchA and SwitchB to check their MAC address tables. The command outputs show that SwitchA learns the MAC address of SwitchB, but SwitchB does not learn the MAC address of SwitchA. The negotiation between the two ends may fail. On the network, LACP is enabled on SwitchB, whereas SwitchA uses the manual aggregation mode. SwitchA does not respond to the LACP negotiation request sent by SwitchB; therefore, the Eth-Trunk is Down.

   NOTE

   - SwitchA receives the LACP negotiation request from SwitchB; therefore, SwitchA learns the MAC address of SwitchB.
   - SwitchA discards the LACP negotiation request because LACP is disabled. As a result, SwitchB cannot learn the MAC address of SwitchA.
   - LACP negotiation fails because SwitchA does not respond to the LACP packet sent from SwitchB. Therefore, the Eth-Trunk on SwitchB is in Block state, and the two devices cannot learn ARP entries of each other.

Procedure

Step 1 Disable LACP on SwitchB.

SwitchA and SwitchB can ping each other successfully.

----End

Summary

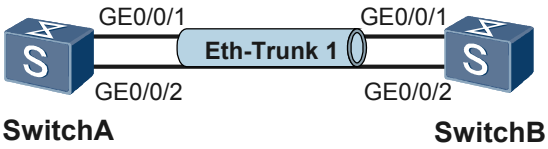
When connecting a Huawei switch to a non-Huawei switch by using an Eth-Trunk, ensure that the two switches use the same link aggregation mode.

Two Ends of an Eth-Trunk Cannot Communicate Because They Have Different Numbers of Member Interfaces

Fault Symptom

Figure 4-9 shows the network diagram of an Eth-Trunk.

Figure 4-9 Networking diagram of Eth-Trunk



Copyright © Huawei Technologies Co., Ltd.

SwitchA and SwitchB cannot communicate with each other.

Fault Analysis

1. Run the **display current-configuration interface eth-trunk** command on SwitchA and SwitchB to check the VLANs that the Eth-Trunk interfaces belong to. The command outputs show that the Eth-Trunk interfaces on the two ends belong to the same VLAN.
2. Check the connection between the member interfaces. The member interfaces on SwitchA are correctly connected to the member interfaces on SwitchB.
3. Run the **display interface** command on SwitchA and SwitchB to check the status of the member interfaces. All the member interfaces are in Up state.
4. Run the **display trunkmembership eth-trunk** command on SwitchA and SwitchB to check the number of member interfaces. The Eth-Trunk interface on SwitchA contains two member interfaces, but the Eth-Trunk interface on SwitchB contains only one member interface (GE0/0/1). The numbers of member interfaces on the two devices are different, so they cannot communicate with each other.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **eth-trunk** *trunk-id* command to add GE0/0/2 to Eth-Trunk 1.

Step 4 Run the **return** command to return to the user view, and then run the **save** command to save the configuration.

After the preceding operations are completed, SwitchA and SwitchB can communicate with each other.

----End

Summary

The two ends of an Eth-Trunk must have the same number of member interfaces; otherwise, the two ends cannot communicate with each other.

Copyright © Huawei Technologies Co., Ltd.

5 LAN

About This Chapter

5.1 VLAN Troubleshooting
This chapter describes common causes of VLAN faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

5.2 MAC Address Table Troubleshooting
This chapter describes common causes of MAC address table faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

5.3 QinQ Troubleshooting
This chapter describes common causes of QinQ faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

5.4 MSTP Troubleshooting

5.5 GVRP Troubleshooting
This chapter describes common causes of Generic VLAN Registration Protocol (GVRP) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

5.6 MAC Swap Loopback Troubleshooting
This chapter describes common causes of MAC swap loopback faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

5.7 VLAN Mapping Troubleshooting
This chapter describes common causes of VLAN mapping faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

5.8 Loop Troubleshooting
This chapter describes common causes of loops, and provides the corresponding troubleshooting procedures, alarms, and logs.

5.9 Loopback Detection Troubleshooting
This chapter describes common causes of Loopback Detection faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

5.1 VLAN Troubleshooting

This chapter describes common causes of VLAN faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

5.1.1 Users in a VLAN Cannot Communicate with Each Other

This section describes common causes of the communication failure between users in a port-based VLAN, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

Common Causes

This fault is commonly caused by one of the following:

- The link between users is faulty.
- The interfaces connected to the users are shut down manually or the physical interfaces are damaged.
- The switch learns incorrect MAC addresses.
- Port isolation is configured on the switch.
- Incorrect static Address Resolution Protocol (ARP) entries are configured on the user terminals.
- Incorrect mappings between interfaces and MAC addresses are configured on the switch.

NOTE

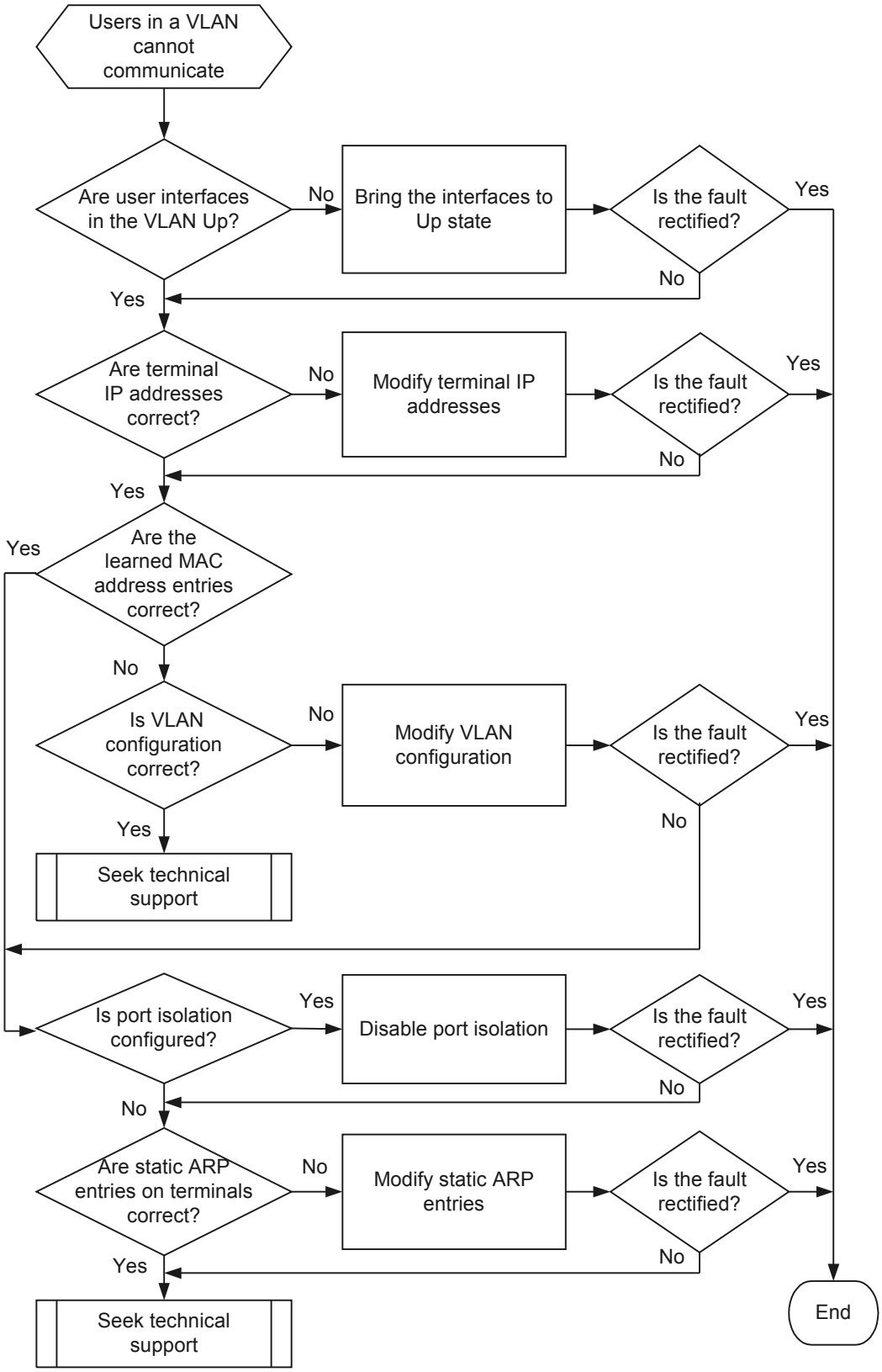
If users in different VLANs cannot communicate with each other, rectify the fault according to the IP Forwarding Troubleshooting.

Troubleshooting Flowchart

Figure 5-1 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Troubleshooting flowchart for communication failure between users in a port-based VLAN



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the interfaces connected to the user terminals are in Up state.

Run the **display interface** *interface-type interface-number* command in any view to check the status of the interfaces.

- If the interface is in Down state, rectify the fault according to **Connected Ethernet Interfaces Down**.
- If the interface is Up, go to 2.

Step 2 Check whether the IP addresses of user terminals are in the same network segment. .

- If they are in different network segments, change the IP addresses of the user terminals.
- If they are in the same network segment, go to **Step 3**

Step 3 Check that the MAC address entries on the Switch are correct.

Run the **display mac-address** command on the Switch to check whether the MAC addresses, interfaces, and VLANs in the learned MAC address entries are correct. If the learned MAC address entries are incorrect, run the **undo mac-address***mac-address* **vlan** *vlan-id* command on the interface to delete the current entries so that the Switch can learn MAC address entries again.

After the MAC address table is updated, check the MAC address entries again.

- If the MAC address entries are incorrect, go to 4.
- If the MAC address entries are correct, go to **Step 5**.

Step 4 Check that the VLAN is properly configured.

- Check the VLAN configuration according to the following table.

Check Item	Method
Whether the VLAN has been created	Run the **display vlan** *vlan-id* command in any view to check whether the VLAN has been created. If not, run the **vlan** command to create the VLAN.

Copyright © Huawei Technologies Co., Ltd.

Check Item	Method
Whether the interfaces are added to the VLAN	Run the **display vlan** *vlan-id* command in any view to check whether the VLAN contains the interfaces. If not, add the interfaces to the VLAN. **NOTE** If the interfaces are located on different switches, add the interfaces connecting the switches to the VLAN. ● Add an access interface to the VLAN by using either of the following methods: **NOTE** The default type of an Switch interface is hybrid. To change the interface type to access, run the **port link-type Access** command in the interface view. 1. Run the **port default vlan** command in the interface view. 2. Run the **port** command in the VLAN view. ● Add a trunk interface to the VLAN. **NOTE** The default type of an Switch interface is hybrid. To change the interface type to trunk, run the **port link-type trunk** command in the interface view. Run the **port trunk allow-pass vlan** command in the interface view. ● Add a hybrid interface to the VLAN by using either of the following methods: **NOTE** The default type of an Switch interface is hybrid. To change the interface type to hybrid, run the **port link-type Hybrid** command in the interface view. 1. Run the **port hybrid tagged vlan** command in the interface view. 2. Run the **port hybrid untagged vlan** command in the interface view.
Whether connections between interfaces and user terminals are correct	Check the connections between interfaces and user terminals according to the network plan. If any user terminal is connected to an incorrect interface, connect it to the correct interface.

After the preceding operations:

- If the MAC address entries are correct, go to **Step 5**.
- If the MAC address entries are incorrect, go to **Step 7**.

Step 5 Check whether port isolation is configured.

Run the **interface** *interface-type interface-number* command in the system view to enter the interface view, and then run the **display this** command to check whether port isolation is configured on the interface.

Copyright © Huawei Technologies Co., Ltd.

- If port isolation is configured, run the **undo port-isolate enable** command on the interface to disable port isolation.
- If port isolation is not configured, go to **Step 6**.

Step 6 Check whether correct static Address Resolution Protocol (ARP) entries are configured on the user terminals.

- If the static ARP entries are incorrect, modify them.
- If the static ARP entries are correct, go to **Step 7**.

Step 7 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

5.2 MAC Address Table Troubleshooting

This chapter describes common causes of MAC address table faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

5.2.1 Correct MAC Address Entries Cannot Be Generated

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the MAC address table fault.

Common Causes

This fault is commonly caused by one of the following:

- The device fails to learn correct MAC address entries because of incorrect configuration.
- The learned MAC addresses are updated frequently because of a loop on the network.
- The MAC address learning function on the interface is disabled.
- Blackhole MAC address entries and MAC address learning limit are configured on the interface.
- The number of learned MAC addresses exceeds the maximum.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

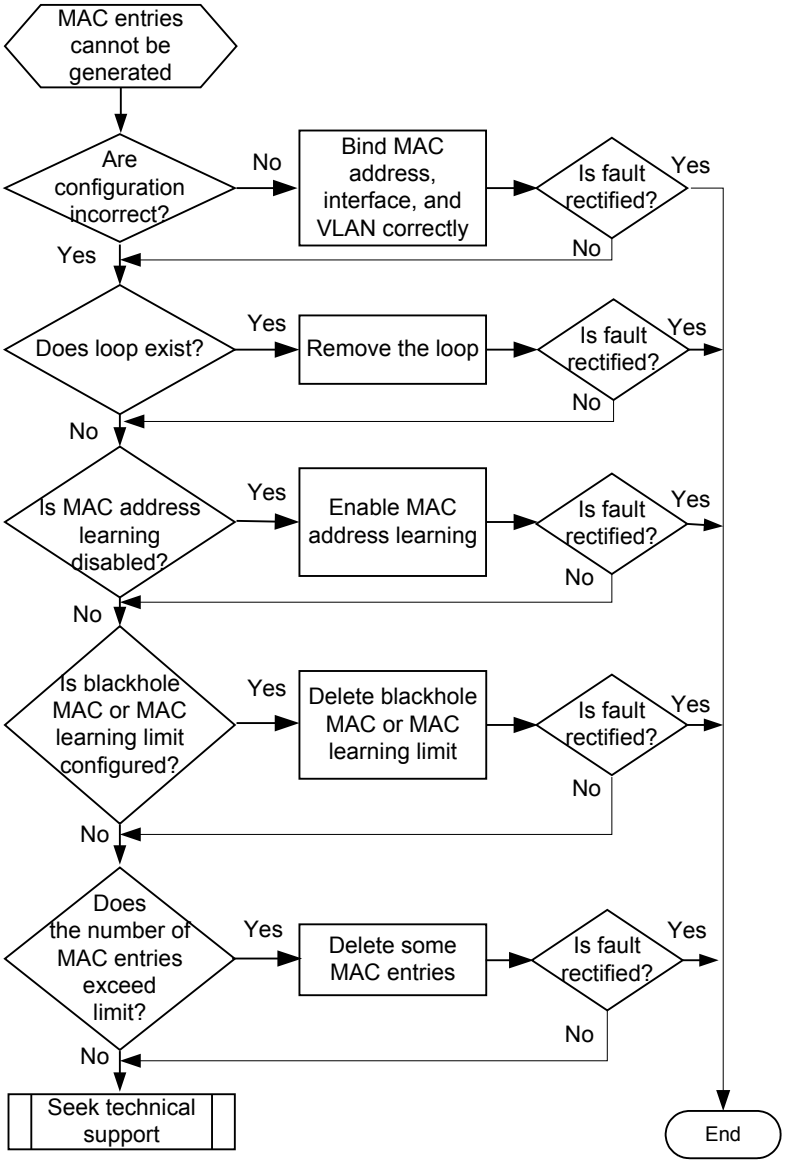
MAC address entries cannot be generated on the device, so Layer 2 forwarding fails.

The troubleshooting roadmap is as follows:

- Check the binding relationship between the outbound interface and the VLAN.
- Check whether a loop occurs on the network.
- Check whether the configurations on the interface conflict or MAC address learning limit is configured on the interface.
- Check whether the number of learned MAC addresses exceeds the limit.

Figure 5-2 shows the troubleshooting flowchart.

Figure 5-2 Troubleshooting flowchart



Troubleshooting Procedure

Copyright © Huawei Technologies Co., Ltd.

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the configurations on the interface are correct.

Run the **display mac-address** command in the system view to check whether the binding relationships between the MAC address, VLAN, and interface are correct.

```
<Quidway> display mac-address 000f-e207-f2e0
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI                          Learned-From        Type
--------------------------------------------------------------------------------
0025-9e80-2494 1/-                               GE0/0/1            dynamic

--------------------------------------------------------------------------------
Total items displayed = 1
```

If not, re-configure the binding relationships between the MAC address, VLAN, and interface.

If yes, go to step 2.

Step 2 Check whether a loop on the network causes MAC address flapping.

If a loop exists on the network, use either of the following methods to prevent MAC address flapping:

- Remove the loop from the network.
- Run the **loop-detect eth-loop** command in the VLAN view to enable the MAC flapping detection function. The S3700 checks whether a MAC address moves from one interface to another in the VLAN. If MAC address flapping occurs, the S3700 blocks the interface or MAC address.

If no loop exists, go to step 3.

Step 3 Check that MAC address learning is enabled.

Check whether MAC address learning is enabled in the interface view and the VLAN view.

```
[Quidway-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 mac-address learning disable
 port hybrid tagged vlan 10
 undo negotiation auto
#
return

[Quidway-vlan10] display this
 #
vlan 10
 mac-address learning disable
#
return
```

If the command output contains **mac-address learning disable**, MAC address learning is disabled on the interface or VLAN.

- If MAC address learning is disabled, run the **undo mac-address learning disable** command in the interface view or VLAN view to enable MAC address learning.

Copyright © Huawei Technologies Co., Ltd.

- If MAC address learning is enabled on the interface, go to step 4.

Step 4 Check whether any blackhole MAC address entry or MAC address limiting is configured.

If a blackhole MAC address entry or MAC address limiting is configured, the interface discards packets.

- Blackhole MAC address entry

  Run the **display mac-address blackhole** command to check whether any blackhole MAC address entry is configured.

```
[Quidway] display mac-address
blackhole
M-------------------------------------------------------------------------------
--
MAC Address    VLAN/VSI                          Learned-From
Type
-------------------------------------------------------------------------------
-
0001-0001-0001 3333/-                            -
blackhole

-------------------------------------------------------------------------------
-
Total items displayed = 1
```

  If a blackhole MAC address entry is displayed, run the **undo mac-address blackhole** command to delete it.

- MAC address limiting on the interface or VLAN
  - Run the **display this** command in the interface view or VLAN view. If the command output contains **mac-limit maximum**, the number of learned MAC addresses is limited. Run either of the following commands:
    - Run the **undo mac-limit** command in the interface view or VLAN view to disable MAC address limiting.
    - Run the **mac-limit** command in the interface view or VLAN view to increase the maximum number of learned MAC addresses.
  - Run the **display this** command in the interface view. If the command output contains **port-security max-mac-num** or **port-security enable**, the number of secure dynamic MAC addresses is limited on the interface. Run either of the following commands:

    NOTE

    By default, the limit on the number of secure dynamic MAC addresses is 1 after port security is enabled.
    - Run the **undo port-security enable** command in the interface view to disable port security.
    - Run the **port-security max-mac-num** command in the interface view to increase the maximum number of secure dynamic MAC addresses on the interface.

If the fault persists, go to step 5.

Step 5 Check whether the number of learned MAC addresses has reached the maximum supported by the S3700.

Run the **display mac-address summary** command to check the number of MAC addresses in the MAC address table.

- If the number of learned MAC addresses has reached the maximum supported by the S3700, no MAC address entry can be created. Run the **display mac-address** command to view MAC address entries.

Copyright © Huawei Technologies Co., Ltd.

- If the number of MAC addresses learned on an interface is much greater than the number of devices on the network connected to the interface, a user on the network may maliciously update the MAC address table. Check the device connected to the interface:
  - If the interface is connected to a switch, run the **display mac-address** command on the switch to view its MAC address table. Locate the interface connected to the malicious user according to the displayed MAC address entries. If the interface that you find is connected to another switch, repeat this step until you find the user of the malicious user.
  - If the interface is connected to a computer, perform either of the following operations after obtaining permission of the administrator:
    - Disconnect the computer. When the attack stops, connect the computer to the network again.
    - Run the **port-security enable** command on the interface to enable port security or run the **mac-limit** command to set the maximum number of MAC addresses that the interface can learn to 1.
  - If the interface is connected to a hub, perform either of the following operations:
    - Configure port mirroring and use a packet capture tool to observe packets received by the interface. Analyze the packet types to locate the attacking computer. Disconnect the computer after obtaining permission of the administrator. When the attack stops, connect the computer to the hub again.
    - Disconnect computers connected to the hub one by one after obtaining permission of the administrator. If the fault is rectified after a computer is disconnected, the computer is the attacker. After it stops the attack, connect it to the hub again.
- If the number of MAC addresses on the interface is equal to or smaller than the number of devices connected to the interface, the number of devices connected to the S3700 has exceeded the maximum supported by the S3700. Adjust network deployment.

- If the number of MAC addresses has not reached the maximum supported by the S3700, go to step 6.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

5.3 QinQ Troubleshooting

This chapter describes common causes of QinQ faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

5.3.1 Traffic Forwarding Fails on a QinQ Interface

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for a traffic forwarding failure on a QinQ interface of the S3700.

Common Causes

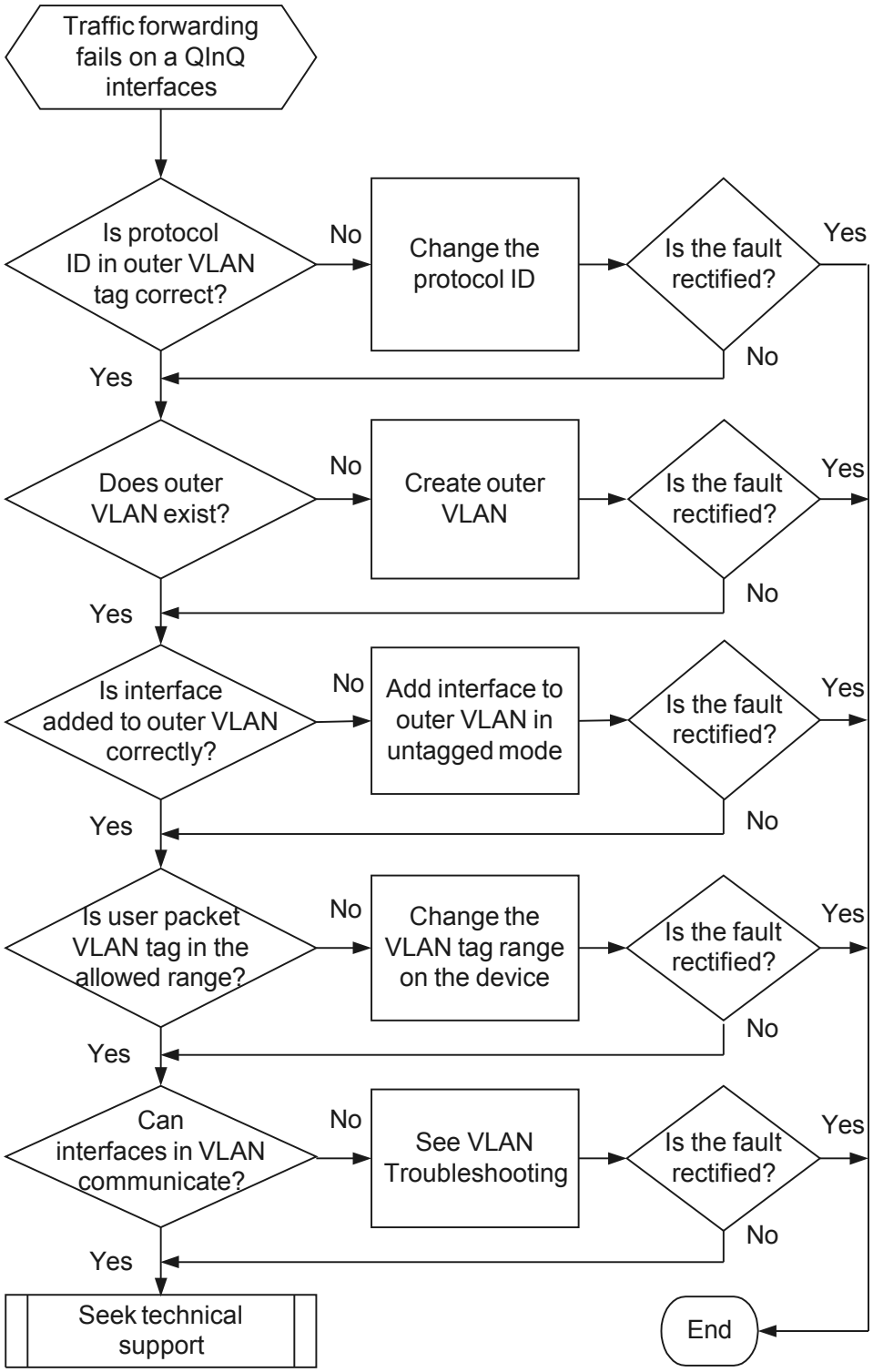
This fault is commonly caused by one of the following:

- The protocol ID in the QinQ outer VLAN tag configured on the S3700 interface cannot be identified by the device directly connected to the interface.
- The outer VLAN is not created, so the interface cannot be added to the VLAN.
- The S3700 interface is added to the outer VLAN not in untagged mode.
- The VLAN tag of received packets is not in the VLAN tag range set on the S3700, so the S3700 cannot identify the packets.
- The S3700 interface and the remote interface in the same VLAN cannot communicate with each other.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 5-3 Troubleshooting flowchart for a traffic forwarding failure on a QinQ interface



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 The protocol ID in the QinQ outer VLAN tag configured on the S3700 interface cannot be identified by the device directly connected to the interface.

NOTE

- The default protocol ID in the outer VLAN tag is 0x8100 on the S3700.
- If the protocol ID on the S3700 interface cannot be identified by the remote device directly connected to the interface, the remote device discards the QinQ packets sent from the S3700 interface.

Run the **display current-configuration interface** *interface-type interface-number* command on the S3700 interface to view the protocol ID in the outer VLAN tag.

- If **qinq protocol** *protocol-id* is displayed, the protocol ID has been changed to *protocol-id*.
- If **qinq protocol** *protocol-id* is not displayed, the default protocol ID 0x8100 is used.

Check the protocol ID in the outer VLAN tag on the remote interface.

- If the protocol ID on the remote interface is the same as that on the S3700 interface, go to step 2.
- If the protocol ID on the remote interface is different from that on the S3700 interface, run the **qinq protocol** *protocol-id* command in the interface view on the S3700 to set the protocol ID to be the same as that on the remote interface.

Step 2 Check that the specified outer VLAN exists.

NOTE

If the specified outer VLAN has not been created, the S3700 cannot add an outer VLAN tag to packets.

Run the **display vlan** *vlan-id* command on the S3700 to check whether the outer VLAN exists.

- If "Error: The VLAN does not exist" is displayed, the specified outer VLAN has not been created. Run the **vlan** *vlan-id* command to create the VLAN.
- If the outer VLAN exists, go to step 3.

Step 3 Check that the S3700 interface is added to the outer VLAN correctly.

NOTE

- By default, the type of an interface is hybrid.
- It is recommended that you retain the default interface type and add the interface to the outer VLAN in untagged mode. The trunk interface type is not recommended.

Run the **display current-configuration interface** command on the S3700 to check whether the S3700 interface is added to the outer VLAN correctly.

Copyright © Huawei Technologies Co., Ltd.

Field	Description	Follow-Up Operation
port hybrid untagged vlan *vlan-id*	The interface type is hybrid and the interface has been added to the outer VLAN in untagged mode.	Perform step 4.
port hybrid tagged vlan *vlan-id*	The interface is added to the outer VLAN in tagged mode.	Run the **port hybrid untagged vlan** *vlan-id* command to add the interface to the outer VLAN.
No preceding information displayed	The interface is not added to the outer VLAN.	

Step 4 Check that the VLAN tag of user packets is in the specified VLAN tag range specified on the S3700.

Run the **display current-configuration interface** command on the S3700 to check the configuration of the interface connected to the downstream device.

If **port vlan-stacking vlan** *vlan-id1* **to** *vlan-id2* **stack-vlan** *vlan-id3* is displayed, the S3700 adds outer VLAN tag *vlan-id3* to the packets carrying VLAN tags *vlan-id1* to *vlan-id2*.

- If the VLAN tag of user packets is in the range of *vlan-id1* and *vlan-id2*, go to step 5.
- If the VLAN tag of user packets is not in the specified range, run the **port vlan-stacking vlan** *vlan-id1* **to** *vlan-id2* **stack-vlan** *vlan-id3* command to change the VLAN tag range. Ensure that the VLAN tag range includes the VLAN tag of user packets.

Step 5 Check that the S3700 interface and the remote interface in the same VLAN can communicate with each other.

Perform ping operations on the two interfaces.

- If the interfaces cannot ping each other, rectify the fault according to **5.1 VLAN Troubleshooting**.
- If the interfaces can ping each other, go to step 6.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

5.4 MSTP Troubleshooting

5.4.1 MSTP Topology Change Leads to Service Interruption

Common Causes

After MSTP is configured on a device and the MSTP topology changes, services are interrupted.

This fault is commonly caused by one of the following:

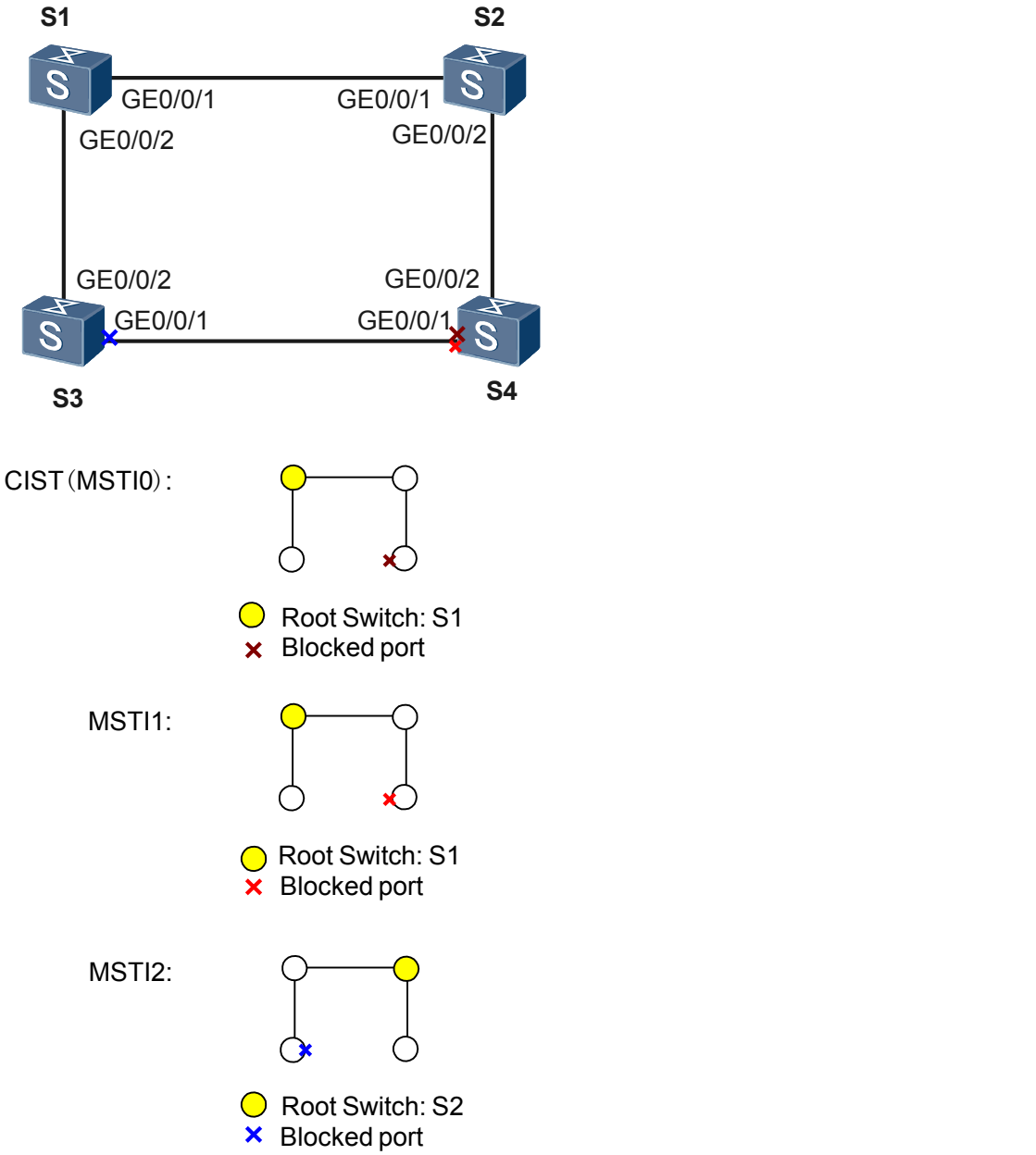
- MSTP is incorrectly configured.
- Physical links flap, causing a large number of TC messages to be sent.
- An MSTP-aware device receives MSTP TC messages from clients or transparently-transmitted MSTP TC messages.

Troubleshooting Flowchart

The troubleshooting of MSTP topology change leads to service interruption is based on the network shown in **Figure 5-4**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-4 Networking diagram of MSTP



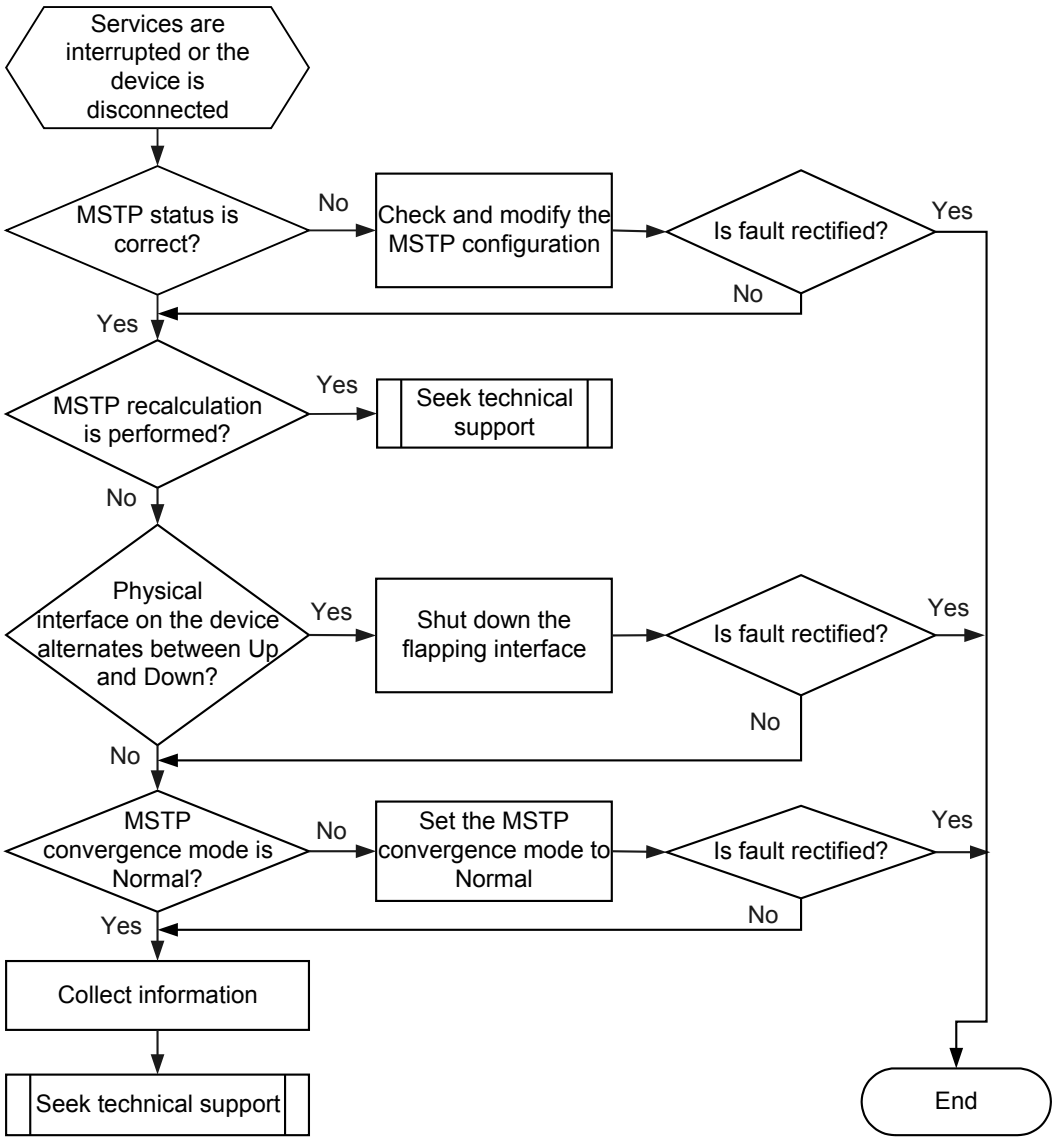
The troubleshooting roadmap is as follows:

- Check that the MSTP status is correct.
- Check whether the device has received TC messages.
- Check that no physical interface on the device alternates between Up and Down.
- Check that the MSTP convergence mode is Normal.

Figure 5-5 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-5 Troubleshooting flowchart for the fault that an MSTP topology change leads to service interruption



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check the status of interfaces on MSTP devices.

Check the role of each MSTP-enabled port in each instance.

On the network shown in **Figure 5-4**, there is only one MSTP ring, which means that each instance can have only one blocked interface.Run the **display stp brief** command on each device to check whether the status of each port is normal.

Copyright © Huawei Technologies Co., Ltd.

Run the **display stp brief** command in any view to check the MSTP status on S1.As shown in **Figure 5-4**, in instances 0 and 1, S1 functions as a root bridge and all ports on S1 are designated ports.In instance 2, one port on S1 is a designated port and the other port is a root port.Both ports are in the Forwarding state.

```
[S1] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   0        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   1        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   1        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/1  ROOT  FORWARDING      NONE
   2        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
```

Run the **display stp brief** command in any view to check the MSTP status on S2. As shown in **Figure 5-4**, in instances 2, S2 functions as a root bridge and all ports on S2 are designated ports.In other instances, one ports on S2 is a designated port and the other port is a root port. Both of them are in the Forwarding state.

```
[S2] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  ROOT  FORWARDING      NONE
   0        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   1        GigabitEthernet0/0/1  ROOT  FORWARDING      NONE
   1        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/2  DESI  FORWARDING      NONE
```

Run the **display stp brief** command in any view to check the MSTP status on S3. As shown in **Figure 5-4**, in instance 2, one port on S3 is an Alternate port and the other port is a root port. The Alternate port is blocked and in the Discarding state.In other instances, one port on S3 is a designated port and the other port is a root port. Both of them are in the Forwarding state.

```
[S3] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  DEST  FORWARDING      NONE
   0        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   1        GigabitEthernet0/0/1  DEST  FORWARDING      NONE
   1        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   2        GigabitEthernet0/0/1  ALTE  DISCARDING      NONE
   2        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
```

Run the **display stp brief** command in any view to check the MSTP status on S4. As shown in **Figure 5-4**, in instance 0, one port on S4 is an Alternate port and the other port is a root port. The Alternate port is blocked and in the Discarding state.In instance 2, one port on S4 is a designated port and the other port is a root port. Both of them are in the Forwarding state.

```
[S4] display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        GigabitEthernet0/0/1  ALTE  DISCARDING      NONE
   0        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   1        GigabitEthernet0/0/1  ALTE  DISCARDING      NONE
   1        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   2        GigabitEthernet0/0/1  DESI  FORWARDING      NONE
   2        GigabitEthernet0/0/2  ROOT  FORWARDING      NONE
```

- On the network shown in **Figure 5-4**, each instance has only one port in the Discarding state and the other port is in the Forwarding state.If several ports are in the Discarding state, an MSTP calculation error occurs. To solve this problem, go to **Step 6**.
- If the MSTP status is correct, go to **Step 2**.

Step 2 Check that the MSTP configuration is correct.

Run the **display stp region-configuration** command to view mappings between VLANs and instances.

Copyright © Huawei Technologies Co., Ltd.

```
[S1] display stp region-configuration
Oper Configuration:
   Format selector :0
   Region name     :huawei
   Revision level  :0

   Instance   Vlans Mapped
      0       21 to 4094
      1       1 to 10
      2       11 to 20
```

- Check whether mappings between VLANs and instances are correct.If the mapping between a VLAN and an instance is incorrect, run the **instance** command to map the VLAN to a specified spanning tree instance. Run the **active region-configuration** command to active the mapping between the VLAN and instance configured by using the **instance** command.

Run the **display current-configuration** command to view the MSTP configuration in the configuration file of the device.

- Check interface configurations to confirm that MSTP-enabled interfaces have been configured with the command (for example **bpdu enable**) to enable protocol packets to be sent to the CPU.
- Check whether MSTP is disabled on the interfaces connecting to user terminals or the interfaces are configured as edge interfaces.
- If an MSTP-enabled device is configured with a BPDU tunnel, check whether the BPDU tunnel configuration is correct. For BPDU tunnel configurations, see the chapter "BPDU Tunnel Configuration" in the *S3700 Configuration Guide - Ethernet*.
- Check whether a port is added to a VLAN correctly.For VLAN configurations, see the chapter "VLAN Configuration" in the *S3700 Configuration Guide - Ethernet*.
- If the MSTP configuration is correct, go to **Step 3**.

Step 3 Check that no MSTP recalculation is performed.

Run the **display stp** command in any view to check whether the device has received TC messages.

```
[S1] display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :57344.00e0-fc00-1597
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .0018-826f-fc7a / 20000
CIST RegRoot/IRPC   :57344.00e0-fc00-1597 / 0
CIST RootPortId     :128.2
BPDU-Protection     :disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Nomal
Time since last TC :2 days 14h:16m:15s

-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :4096.00e0-fc00-1597
MSTI RegRoot/IRPC   :4096.00e0-fc00-1597 / 0
MSTI RootPortId     :0.0
Master Bridge       :57344.00e0-fc00-1597
Cost to Master      :0
TC received         :0
TC count per hello  :2
```

- If values of the TC or TCN received, TC count per hello, TC received, and TC count per hello fields in the command output increase, the device has received TC messages and the network topology has changed. In this case, you need to view log messages MSTP/6/SET_PORT_DISCARDING and MSTP/6/SET_PORT_FORWARDING to check whether the role of an MSTP-enabled port changes.

Copyright © Huawei Technologies Co., Ltd.

- If the port role does not change, go to **Step 4**.
- If the port role changes, go to **Step 6**.

NOTE

If a multi-process has been created on the device and TC notification has been configured in the multi-process, when the topology of the multi-process changes, a TC message is sent to the process 0 for instructing devices in process 0 to refresh their MAC and ARP address tables. In this manner, devices on the network can re-select links to forward traffic, ensuring non-stop traffic.

- If the values in the TC or TCN received, TC count per hello, TC received, and TC count per hello fields in the command output are 0s, it indicates that the device does not receive any TC message. In this case, contact Huawei technical support personnel.

Step 4 Check that no interface on the device alternates between Up and Down.

View the log message IFNET/4/IF_STATE to check whether an MSTP-enabled port alternates between Up and Down.

- If an MSTP-enabled interface alternates between Up and Down, it indicates that the interface flaps. If a physical interface frequently alternates between Up and Down, the MSTP status of the device on the network will become unsteady. As a result, a large number of TC messages are generated; ARP entries and MAC entries are frequently deleted; services are interrupted. Run the **shutdown** command on the flapping interface. If services are not restored after the flapping interface is shut down, go to **Step 5**.
- If no interface flaps, go to **Step 5**.

Step 5 Check that the MSTP convergence mode is Normal.

Run the **display stp** command in any view to check the MSTP convergence mode of the device.

```
[S1] display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :57344.00e0-fc00-1597
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .0018-826f-fc7a / 20000
CIST RegRoot/IRPC   :57344.00e0-fc00-1597 / 0
CIST RootPortId     :128.2
BPDU-Protection     :disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC :2 days 14h:16m:15s

-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :4096.00e0-fc00-1597
MSTI RegRoot/IRPC   :4096.00e0-fc00-1597 / 0
MSTI RootPortId     :0.0
Master Bridge       :57344.00e0-fc00-1597
Cost to Master      :0
TC received         :0
TC count per hello  :2
```

- If the convergence mode is Normal, go to **Step 6**.
- If the convergence mode is Fast, run the **stp converge normal** command to change the convergence mode to Normal. If services are not restored after the convergence mode is changed, go to **Step 6**.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the device

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

Relevant Alarms

MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.1 hwMstpiPortStateForwarding

MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.2 hwMstpiPortStateDiscarding

MSTP_1.3.6.1.2.1.17.0.2 TOPOC

Relevant Logs

MSTP/6/RECEIVE_MSTITC

VOSCPU/4/CPU_USAGE_HIGH

5.5 GVRP Troubleshooting

This chapter describes common causes of Generic VLAN Registration Protocol (GVRP) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

5.5.1 No Dynamic VLAN Can Be Created on an Interface

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for a dynamic VLAN creation failure on an interface.

Common Causes

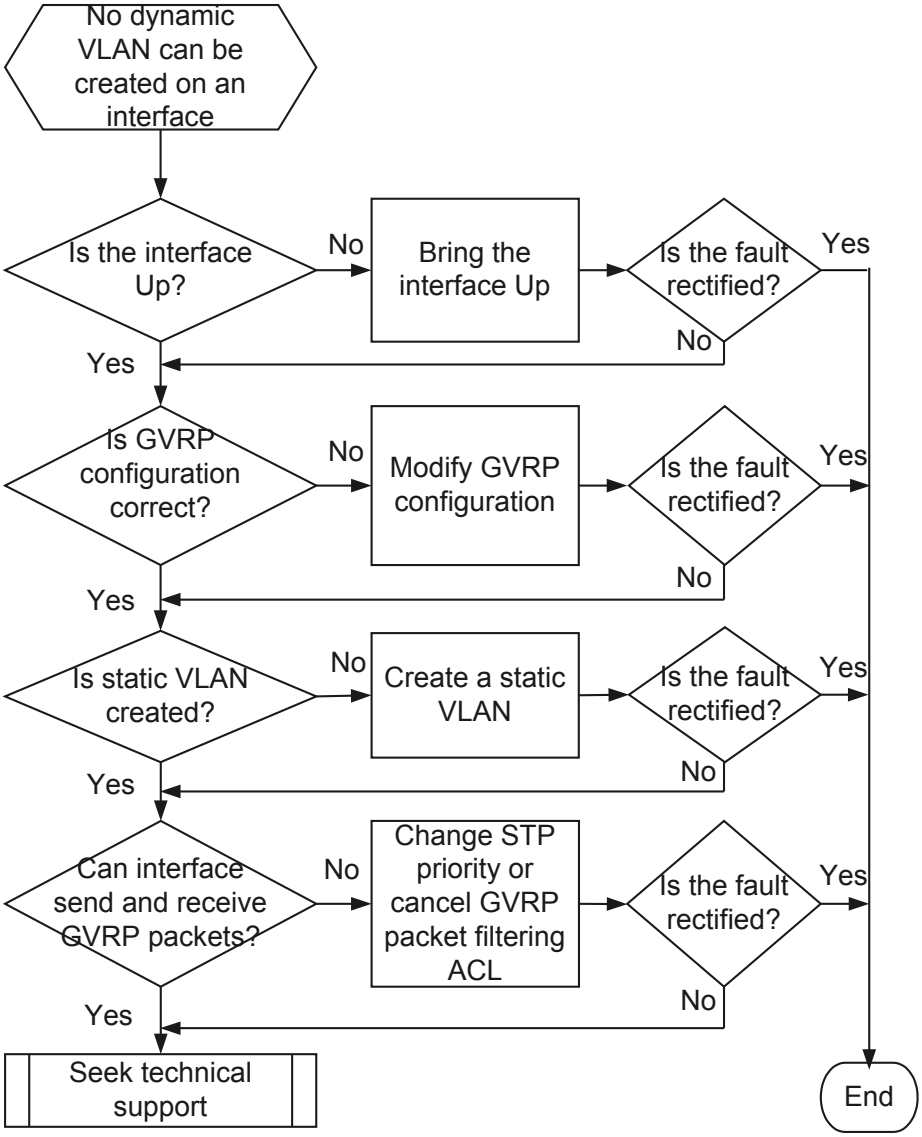
This fault is commonly caused by one of the following:

- The link between the GVRP-enabled devices is faulty.
- The interface registration mode is incorrect.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 5-6 Troubleshooting flowchart for a dynamic VLAN creation failure



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the GVRP-enabled interface is Up.

Run the **display interface** *interface-type interface-number* command in any view to check the interface status.

- If the interface is in Down state, rectify the fault according to **Connected Ethernet Interfaces Down**.

Copyright © Huawei Technologies Co., Ltd.

If the interface retains in Down state, go to **Step 5**.

- If the interface is Up, go to **Step 2**.

Step 2 Check that the GVRP configuration is correct.

Check the GVRP configuration according to the following table.

Check Item	Method

Whether the Bridge Protocol Data Unit (BPDU) function is enabled	Run the **display this** command in the interface view to check whether the BPDU function is enabled on the interface.
	`[Quidway-GigabitEthernet0/0/1] display this`
	`#`
	`interface GigabitEthernet0/0/1`
	`bpdu enable`
	`#`
	If the BPDU function is not enabled on the interface, run the **bpdu enable** command in the interface view to enable the BPDU function.

Whether GVRP is enabled	- Check whether global GVRP is enabled.
	By default, global GVRP is disabled. Run the **display gvrp status** command in the system view to check whether global GVRP is enabled.
	`<Quidway> display gvrp status`
	`GVRP is enabled`
	If global GVRP is not enabled, run the **gvrp** command in the system view to enable GVRP.
	- Check whether GVRP is enabled on the interface.
	Run the **display this** command in the interface view to check whether GVRP is enabled on the interface.
	`[Quidway-GigabitEthernet0/0/1] display this`
	`#`
	`interface GigabitEthernet0/0/1`
	`gvrp`
	`#`
	If GVRP is not enabled on the interface, run the **gvrp** command in the interface view to enable GVRP.

Whether the interface is added to VLANs by using the **port trunk allow-pass vlan** command	Run the **display this** command in the interface view to check the VLANs that the interface belongs to.
	`[Quidway-GigabitEthernet0/0/1] display this`
	`#`
	`interface GigabitEthernet0/0/1`
	`port link-type trunk`
	`port trunk allow-pass vlan 20 100`
	`gvrp`
	`#`
	NOTE
	The default type of an interface is hybrid. To change the interface type to trunk, run the **port link-type trunk** command in the interface view.
	If the interface is not added to VLANs as a trunk interface, run the **port trunk allow-pass vlan** command in the interface view to add the interface to correct VLANs.

Copyright © Huawei Technologies Co., Ltd.

Check Item	Method

Whether the interface registration mode is correct	Run the **display this** command in the interface view to check the interface registration mode.
	NOTE
	A GVRP interface supports three registration modes:
	● Normal: In this mode, the GVRP interface can register and deregister VLANs, and transmit dynamic VLAN registration information and static VLAN registration information.
	● Fixed: In this mode, the GVRP interface is disabled from registering and deregistering VLANs and can transmit only the static registration information. If a trunk interface works in fixed registration mode, it allows only the manually configured VLANs even if it is configured to allow all the VLANs.
	● Forbidden: In this mode, the GVRP interface is disabled from registering and deregistering VLANs and can transmit only information about VLAN 1. If a trunk interface works in forbidden registration mode, it allows only VLAN 1 even if it is configured to allow all the VLANs.
	The default registration mode of an interface is normal. If the registration mode is fixed or forbidden, run the **gvrp registration** command to change the registration mode to normal.
	`[Quidway-GigabitEthernet0/0/1] display this`
	`#`
	`interface GigabitEthernet0/0/1`
	`port link-type trunk`
	`port trunk allow-pass vlan 20 100`
	`gvrp`
	`gvrp registration forbidden`
	`#`

Step 3 Check that static VLANs are created.

Run the **display this** command in the system view to check whether static VLANs are created. If no static VLAN is created, dynamic VLAN cannot be created.

```
[Quidway]display this
#
vlan batch 1 to 10
#
```

- If no static VLAN is created, create static VLANs.
- If static VLANs are created, go to **Step 4**.

Step 4 Check the statistics on GVRP packets sent, received, and discarded on the interface.

Run the **display garp statistics** command in the user view to check whether there are statistics on GVRP packets sent, received, and discarded on the interface.

Run the **display garp statistics** command repeatedly to view the change of packet statistics.

NOTE

If the GVRP packets are sent and received by the interface and no GVRP packet is discarded, GVRP functions properly.

```
<Quidway> display garp statistics
  GARP statistics on port GigabitEthernet0/0/1
    Number of GVRP frames received       : 0
    Number of GVRP frames transmitted    : 0
    Number of frames discarded           : 0
```


Copyright © Huawei Technologies Co., Ltd.

- If GVRP functions properly, go to **Step 5**.
- If GVRP packets are discarded, check the following items.

Check Item	Method
The interface is blocked.	Run the **display stp brief** command to check whether the interface is blocked by the Spanning Tree Protocol (STP). If the STP state of the interface is DISCARDING, the interface is blocked. Dynamic VLANs cannot be created on a blocked interface. Run the **stp port priority** command to change the interface priority. After the spanning tree is recalculated, the interface will be unblocked.
GVRP packets are filtered out.	Check whether ACLs are configured on the local and remote devices to filter out GVRP packets. If such an ACL is configured, delete it.

If the fault persists, go to **Step 5**.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

5.5.2 Dynamic VLAN Flapping Occurs

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for dynamic VLAN flapping.

Common Causes

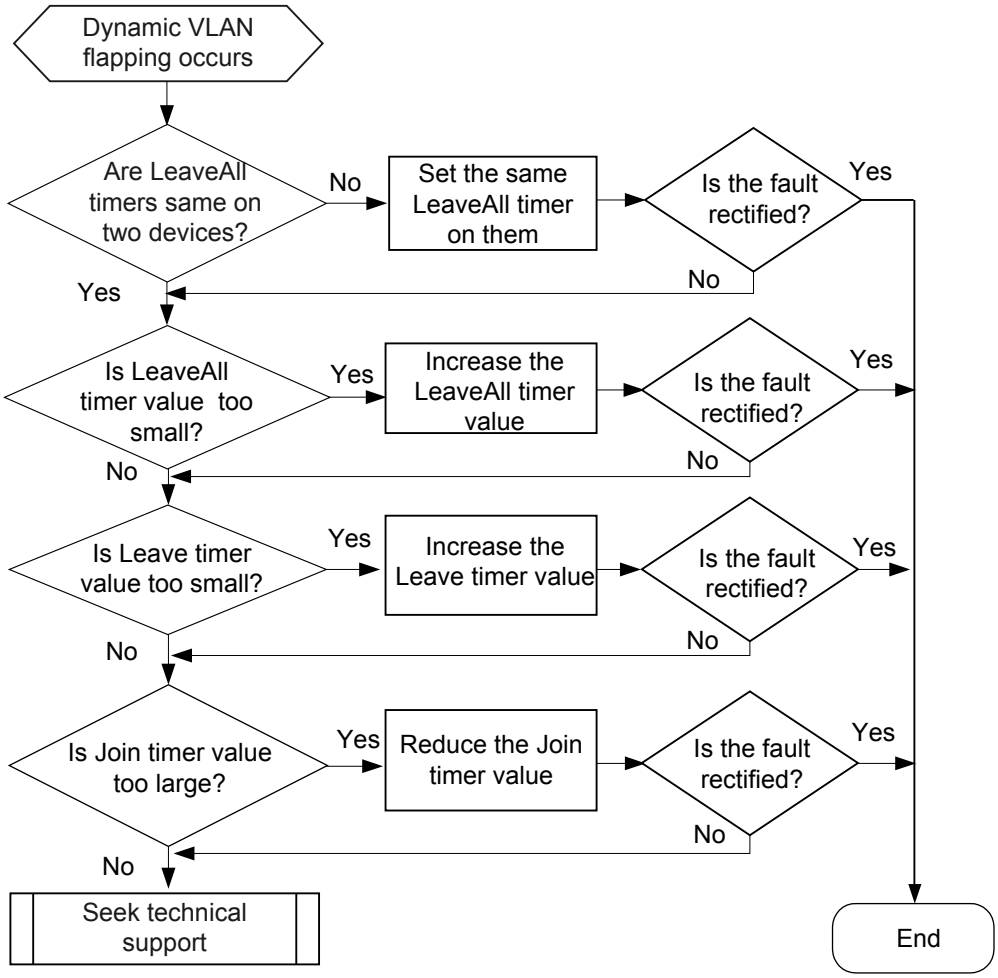
This fault is commonly caused by incorrect settings of Generic Attribute Registration Protocol (GARP) timers.

Troubleshooting Flowchart

If Layer 2 forwarding fails after GVRP is configured, dynamic VLAN flapping may occur. Rectify the fault according to the following flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-7 Troubleshooting flowchart for dynamic VLAN flapping



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that GARP timers are set properly.

After GVRP is enabled, a switch uses the default values of GARP timers. Improper GARP timer settings may cause dynamic VLAN flapping. When setting the GARP timers on a device, consider the timer values of other devices on the network.

Devices of different vendors have different performance. If many static VLANs are configured but the LeaveAll timer is small, dynamic VLAN flapping may occur.

Run the **display garp timer** command in the user view to check the values of GARP timers.

```
<Quidway> display garp timer
  GARP timers on port GigabitEthernet0/0/1
```

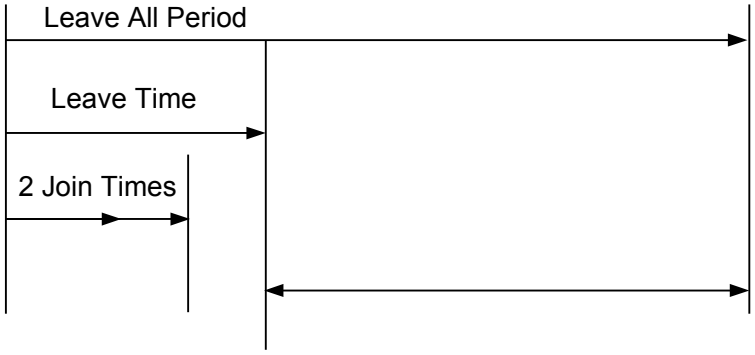

Copyright © Huawei Technologies Co., Ltd.

```
GARP JoinTime                : 20 centiseconds
GARP LeaveTime               : 60 centiseconds
GARP LeaveAllTime            : 1000 centiseconds
GARP HoldTime                : 10 centiseconds
```

The recommended values of the GARP timers are as follows:

- GARP Join timer: 600 centiseconds (6 seconds)
- GARP Leave timer: 3000 centiseconds (30 seconds)
- GARP LeaveAll timer: 12000 centiseconds (2 minutes)
- GARP Hold timer: 100 centiseconds (1 second)

If the GARP timers are not set properly, adjust the timer values according to the following figure.



Step 2 Run the **garp timer leaveall** command to set the global LeaveAll timer to be the same as that of other devices on the network.

Step 3 Run the **garp timer** command to adjust the values of the Leave timer and Join timer on interfaces.

Step 4 If the fault persists, contact Huawei technical personnel.

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

5.6 MAC Swap Loopback Troubleshooting

This chapter describes common causes of MAC swap loopback faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

NOTE

The S3700SI does not support MAC Swap Loopback.

Copyright © Huawei Technologies Co., Ltd.

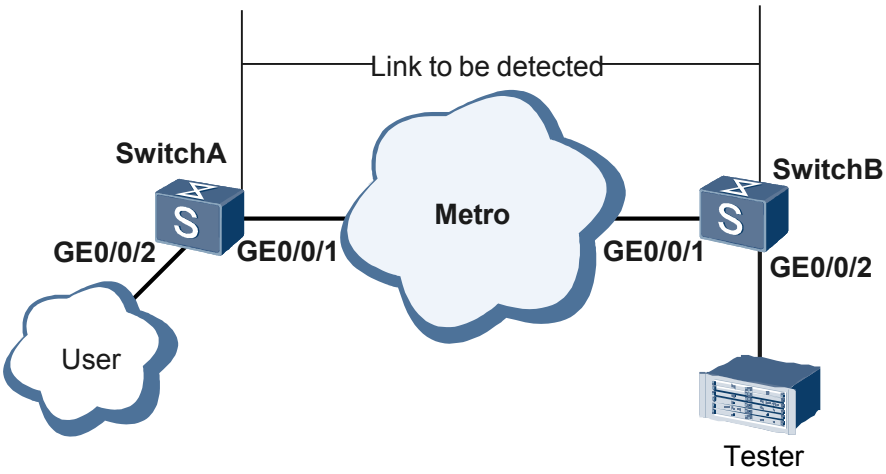
5.6.1 No Remote Loopback Traffic Is Received by the Tester

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when no remote loopback traffic is received by the tester.

Common Causes

As shown in **Figure 5-8**, remote loopback is configured on GE0/0/1 of SwitchA. Traffic is sent from a tester to check connectivity between GE0/0/2 of SwitchB and GE0/0/1 of SwitchA. The two interfaces are in the same VLAN.

Figure 5-8 Network diagram of remote loopback



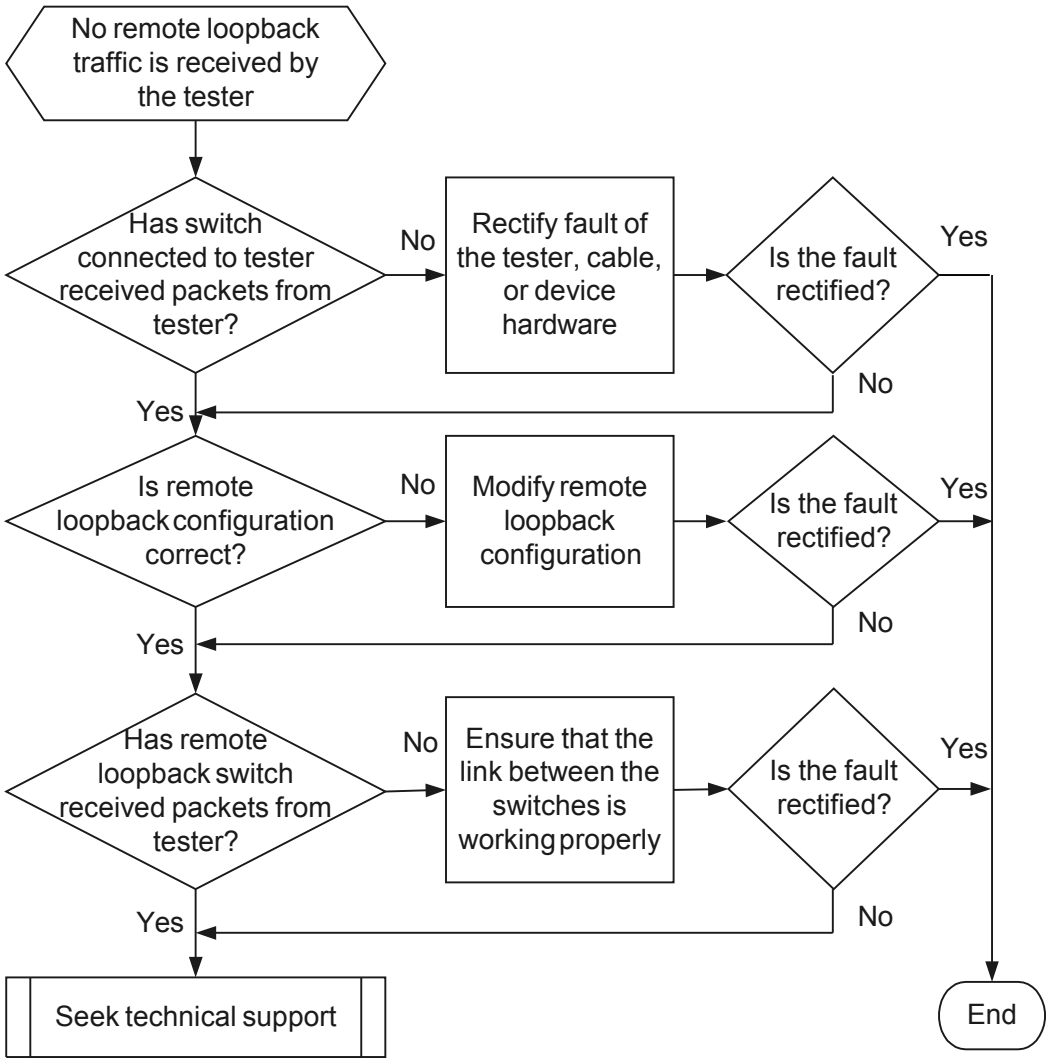
The tester does not receive the loopback traffic sent from SwitchA. This fault is commonly caused by one of the following:

- The remote loopback test has not started.
- The VLAN ID specified for loopback packets is different from the VLAN ID of the remote loopback interface.
- The source and destination MAC addresses of the packets sent from the tester are different from those configured on the remote loopback interface.
- The tester is faulty.
- Packets sent from the tester are not IP packets.
- The link between SwitchA and SwitchB are not functioning properly.
- SwitchA, SwitchB, or either interface module between SwitchA and SwitchB fails.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 5-9 Troubleshooting flowchart for a remote loopback failure



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether SwitchB has received the packets sent from the tester.

Run the **display mac-address** command on SwitchB to check whether SwitchB has learned the source MAC address of the packets sent from the tester and whether the source MAC address is learned on the interface connected to the tester.

- If SwitchB has not learned the source MAC address of the packets sent from the tester, check that:
  - The tester is configured correctly and packets constructed by the tester are IP packets.

Copyright © Huawei Technologies Co., Ltd.

- The cable between the tester and SwitchB is functioning properly.

If SwitchB still cannot learn the source MAC address of the packets sent from the tester, connect the tester to another interface of SwitchB. If the fault persists, go to step 4.

- If SwitchB has learned the source MAC address of the packets sent from the tester and the source MAC address is learned on the interface connected to the tester, go to step 2.

Step 2 Check the remote loopback configuration.

Run the **display loopback swap-mac information** command on SwitchA to check the remote loopback status and take actions accordingly.

Field	Description	Action
Loopback state	Remote loopback status. ● Running: indicates that the loopback test has started. ● stop: indicates that the loopback test has not started.	If this field is displayed as **stop**, run the **Loopback swap-mac start** command on the remote loopback interface to start the loopback test.
Loopback source MAC	Source MAC address of loopback packets.	If the value of this field is different from the source MAC address of the packets sent from the tester, run the **loopback remote swap-mac** command on the remote loopback interface to change the source MAC address. Alternatively, change the source MAC address of packets on the tester.
Loopback destination MAC	Destination MAC address of loopback packets.	If the value of this field is different from the destination MAC address of the packets sent from the tester, run the **loopback remote swap-mac** command on the remote loopback interface to change the destination MAC address. Alternatively, change the destination MAC address of packets on the tester.

Copyright © Huawei Technologies Co., Ltd.

Field	Description	Action
Loopback vlan	VLAN ID of loopback packets.	If the value of this field is different from the VLAN ID of the remote loopback interface, run the **loopback remote swap-mac** command on the remote loopback interface to change the VLAN ID of loopback packets.

If the fault persists, go to step 3.

Step 3 Check whether SwitchA has received the packets sent from the tester.

Run the **display mac-address** command on SwitchA to check whether SwitchA has learned the source MAC address of the packets sent from the tester and whether the source MAC address is learned on the remote loopback interface.

- If SwitchA has not learned the source MAC address of the packets sent from the tester, ensure that the link between SwitchA and SwitchB is functioning properly. If SwitchA still cannot learn the source MAC address of the packets sent from the tester, check whether packets of other services can be transmitted between SwitchA and SwitchB.
  - If packets of other services cannot be transmitted between SwitchA and SwitchB, interfaces between them may fail. Connect the cable to other interfaces of the Switches and add the interfaces to the VLAN. If the fault persists, go to step 4.
  - If packets of other services can be transmitted between SwitchA and SwitchB, go to step 4.
- If SwitchA has learned the source MAC address of the packets sent from the tester and the source MAC address is learned on the remote loopback interface, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the Switches

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

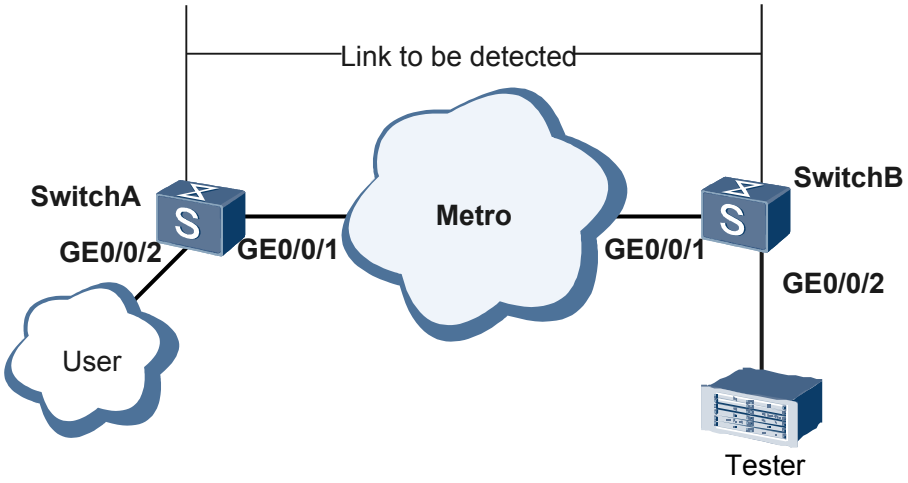
5.6.2 No Local Loopback Traffic Is Received by the Tester

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when no local loopback traffic is received by the tester.

Common Causes

As shown in **Figure 5-10**, local loopback is configured on GE0/0/2 of SwitchA. Traffic is sent from a tester to check connectivity between GE0/0/2 of SwitchB and GE0/0/1 of SwitchA. The two interfaces are in the same VLAN.

Figure 5-10 Network diagram of local loopback



The tester does not receive the loopback traffic sent from SwitchA. This fault is commonly caused by one of the following:

- The local loopback test has not started.
- The VLAN ID specified for loopback packets is different from the VLAN ID of the local loopback interface.
- The source and destination MAC addresses of the packets sent from the tester are different from those configured on the local loopback interface.
- The tester is faulty.
- Packets sent from the tester are not IP packets.
- The link between SwitchA and SwitchB are not functioning properly.
- SwitchA, SwitchB, or either interface module between SwitchA and SwitchB fails.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 5-11 Troubleshooting flowchart for a local loopback failure

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether SwitchB has received the packets sent from the tester.

Run the **display mac-address** command on SwitchB to check whether SwitchB has learned the source MAC address of the packets sent from the tester and whether the source MAC address is learned on the interface connected to the tester.

- If SwitchB has not learned the source MAC address of the packets sent from the tester, check that:
  - The tester is correctly configured.

Copyright © Huawei Technologies Co., Ltd.

- The cable between the tester and SwitchB is functioning properly.

If SwitchB still cannot learn the source MAC address of the packets sent from the tester, connect the tester to another interface of SwitchB. If the fault persists, go to step 4.

- If SwitchB has learned the source MAC address of the packets sent from the tester and the source MAC address is learned on the interface connected to the tester, go to step 2.

Step 2 Check the local loopback configuration.

Run the **display loopback swap-mac information** command on SwitchA to check the local loopback status and take actions accordingly.

Field	Description	Action
Loopback state	Local loopback status. ● Running: indicates that the loopback test has started. ● stop: indicates that the loopback test has not started.	If this field is displayed as **stop**, run the **loopback swap-mac start** command on the local loopback interface to start the loopback test.
Loopback source MAC	Source MAC address of loopback packets.	If the value of this field is different from the source MAC address of the packets sent from the tester, run the **loopback local swap-mac** command on the local loopback interface to change the source MAC address. Alternatively, change the source MAC address of packets on the tester.
Loopback destination MAC	Destination MAC address of loopback packets.	If the value of this field is different from the destination MAC address of the packets sent from the tester, run the **loopback local swap-mac** command on the local loopback interface to change the destination MAC address. Alternatively, change the destination MAC address of packets on the tester.

Copyright © Huawei Technologies Co., Ltd.

Field	Description	Action
Loopback vlan	VLAN ID of loopback packets.	If the value of this field is different from the VLAN ID of the local loopback interface, run the **loopback local swap-mac** command on the local loopback interface to change the VLAN ID of loopback packets.

If the fault persists, go to step 3.

Step 3 Check whether SwitchA has received the packets sent from the tester.

Run the **display mac-address** command on SwitchA to check whether SwitchA has learned the source MAC address of the packets sent from the tester and whether the source MAC address is learned on the local loopback interface.

- If SwitchA has not learned the source MAC address of the packets sent from the tester, ensure that the link between SwitchA and SwitchB is functioning properly. If SwitchA still cannot learn the source MAC address of the packets sent from the tester, check whether packets of other services can be transmitted between SwitchA and SwitchB.
  - If packets of other services cannot be transmitted between SwitchA and SwitchB, interfaces between them may fail. Connect the cable to other interfaces of the Switches and add the interfaces to the VLAN. If the fault persists, go to step 4.
  - If packets of other services can be transmitted between SwitchA and SwitchB, go to step 4.
- If SwitchA has learned the source MAC address of the packets sent from the tester and the source MAC address is learned on the remote loopback interface, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the Switches

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

5.7 VLAN Mapping Troubleshooting

This chapter describes common causes of VLAN mapping faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

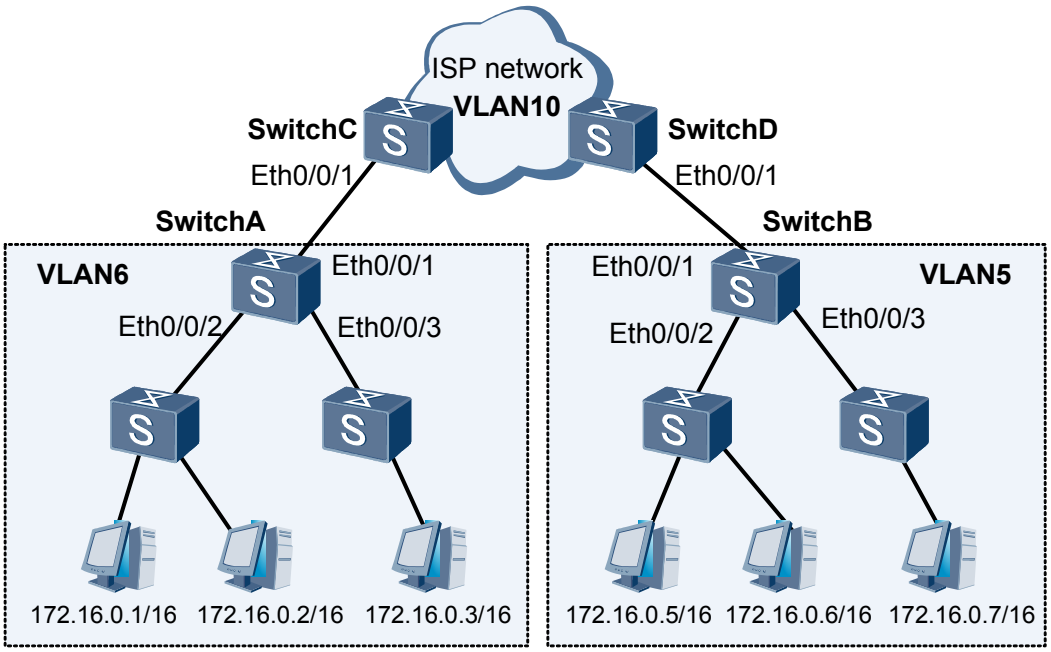
5.7.1 Users Cannot Communicate After VLAN Mapping Is Configured

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when users cannot communicate after VLAN mapping is configured.

Common Causes

As shown in **Figure 5-12**, users in VLAN 6 need to communicate with users in VLAN 5 over an ISP network. The carrier assigns VLAN 10 as the stack VLAN (S-VLAN). Single-tag VLAN mapping is configured on Eth0/0/1 of SwitchC and SwitchD to map customer VLANs (C-VLANs) 5 and 6 to S-VLAN 10.

Figure 5-12 VLAN mapping networking diagram



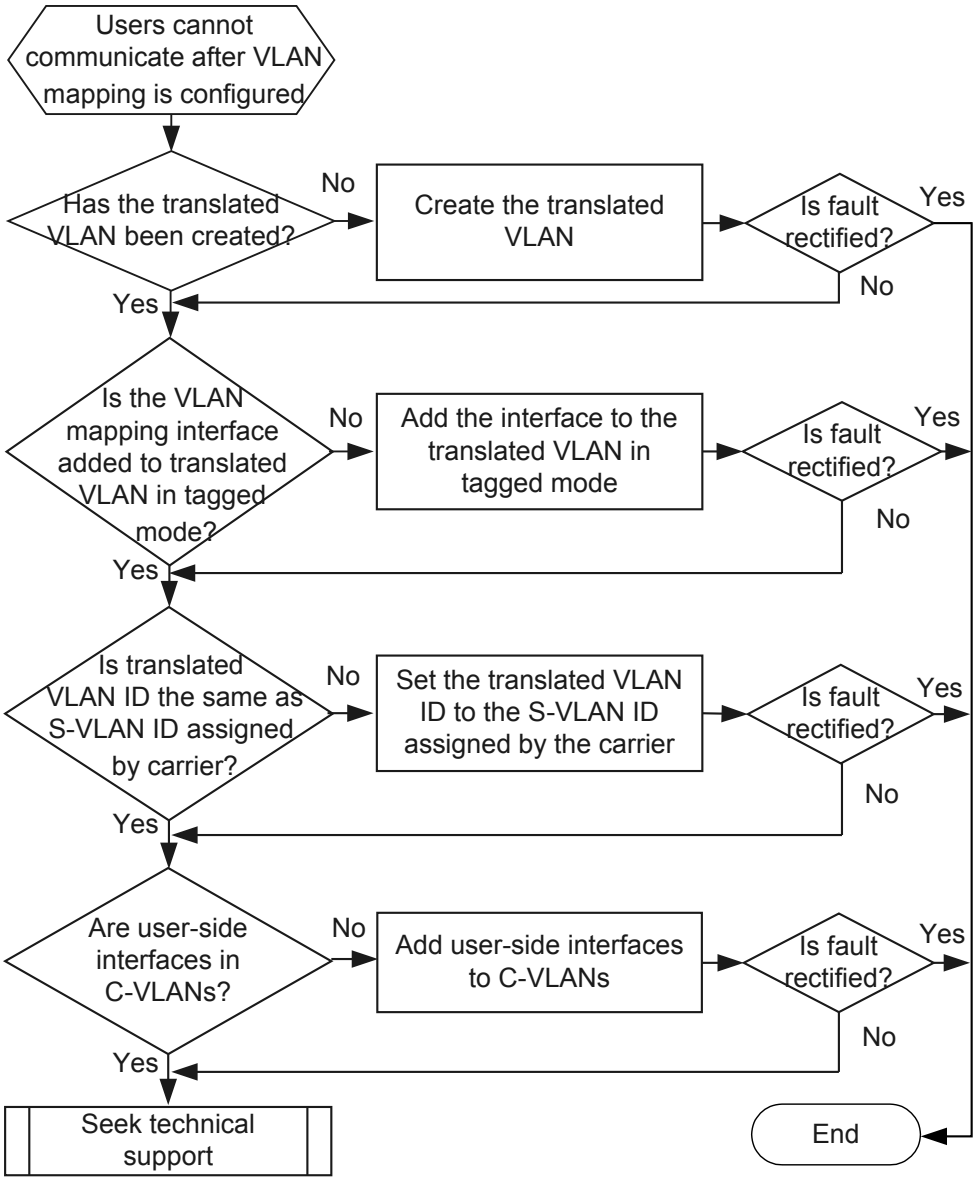
After VLAN mapping is configured on the interfaces, users in different VLANs cannot communicate with each other. This fault is commonly caused by one of the following:

- The translated VLAN (specified by **map-vlan**) has not been created.
- The interfaces configured with VLAN mapping are not added to the translated VLAN.
- The translated VLAN ID configured on SwitchC and SwitchD is different from the S-VLAN ID assigned by the carrier.
- The interfaces configured with VLAN mapping are faulty.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 5-13 VLAN mapping troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the translated VLAN (specified by **map-vlan**) has been created.

Copyright © Huawei Technologies Co., Ltd.

Run the **display vlan** command on SwitchC and SwitchD to check whether the translated VLAN has been created.

- If the translated VLAN has not been created, run the **vlan** command to create it.
- If the translated VLAN has been created, go to step 2.

Step 2 Check that the interfaces configured with VLAN mapping have been added to the translated VLAN in tagged mode.

Run the **display this** command on the interfaces configured with VLAN mapping to check whether the interfaces have been added to the translated VLAN in tagged mode.

NOTE

- VLAN mapping can only be configured on a trunk or hybrid interface, and the interface must be added to the translated VLAN in tagged mode.
- If a range of original VLANs is specified by *vlan-id1* to *vlan-id2* on an interface, the interface must be added to all the original VLANs in tagged mode, and the translated VLAN cannot have a VLANIF interface.
- Limiting MAC address learning on an interface may affect N:1 VLAN mapping on the interface.

- If the interfaces configured with VLAN mapping have not been added to the translated VLAN in tagged mode, run the **port trunk allow-pass vlan** or **port hybrid tagged vlan** command in the interface views to add the interfaces to the translated VLAN in tagged mode.
- If the interfaces have been added to the translated VLAN in tagged mode, go to step 3.

Step 3 Check that the translated VLAN ID configured on SwitchC and SwitchD is the same as the S-VLAN ID assigned by the carrier.

Run the **display this** command on the interfaces configured with VLAN mapping to check whether the translated VLAN ID is the same as the S-VLAN ID assigned by the carrier.

- If the translated VLAN ID on an interface is different from the S-VLAN ID assigned by the carrier, run the **undo port vlan-mapping vlan** command on the interface to delete the VLAN mapping configuration, and then run the **port vlan-mapping vlan** command to set the translated VLAN ID to the S-VLAN ID.
- If the translated VLAN ID is the same as the S-VLAN ID assigned by the carrier, go to step 4.

Step 4 Check that the user-side interfaces are in the C-VLANs.

Run the **display vlan** *vlan-id* command on SwitchA and SwitchB to check whether the user-side interfaces are in the C-VLANs.

- If the user-side interfaces are not in the C-VLANs, run the **port trunk allow-pass vlan**, **port hybrid tagged vlan**, or **port default vlan** command to add the interfaces to the C-VLANs.
- If the user-side interfaces are in the C-VLANs, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the Switches

----End

Relevant Alarms and Logs

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms

None.

Relevant Logs

None.

5.8 Loop Troubleshooting

This chapter describes common causes of loops, and provides the corresponding troubleshooting procedures, alarms, and logs.

5.8.1 Loops Cause Broadcast Storms

This section provides a step-by-step troubleshooting procedure for broadcast storms caused by loops.

Common Causes

Loops on a network cause broadcast storms and may also lead to the following problems:

- Users cannot log in to the switch remotely.
- The **display interface** command output shows a large number of broadcast packets received on one or more interfaces.
- It takes a long time to log in to the switch from the serial port.
- The switch CPU usage exceeds 70%.
- A large number of of ICMP packets are lost in ping tests.
- Interface indicators of interfaces in the VLAN where a loop has occurred blink at a higher frequency than usual.
- A large number of broadcast packets are captured on PCs on the network.
- Loop alarms are generated when loop detection is enabled.

This fault is commonly caused by one of the following:

- Cables are connected incorrectly.

  Figure 5-14 and **Figure 5-15** show loops caused by incorrect cable connections.

  - As shown in **Figure 5-14**, interfaces in the same VLAN on SwitchB are connected, causing a loop.

    In this scenario, locate the loop as follows:

    - Enable loopback detection on SwitchA and configure SwitchA to generate an alarm when detecting a loop. Locate the device, VLAN, and interface where the loop has occurred according to alarm messages. If a loop alarm is generated on the interface connected to SwitchB, the loop has occurred on SwitchB. If a loop alarm is generated on an interface not connecting SwitchB, the loop has occurred on SwitchA. On the Switch where the loop has occurred, view broadcast packet statistics on interfaces or observe interface indicators to locate the interface that may encounter a loop. Run the **shutdown** command on the interface or remove the cable from the interface and

Copyright © Huawei Technologies Co., Ltd.

check whether the broadcast storm disappears. If the broadcast storm disappears, the loop has occurred on this interface.

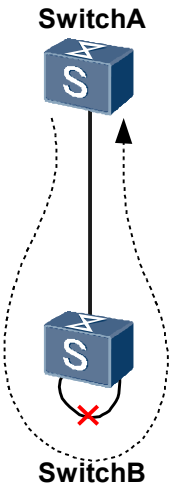
- On SwitchA, run the **shutdown** command on the interface connected to SwitchB or remove the cable from the interface. If the broadcast storm persists, the loop has occurred on SwitchA. If the broadcast storm disappears, the loop has occurred on SwitchB. On the Switch where the loop has occurred, view broadcast packet statistics on interfaces or observe interface indicators to locate the interface that may encounter a loop. Run the **shutdown** command on the interface or remove the cable from the interface and check whether the broadcast storm disappears. If the broadcast storm disappears, the loop has occurred on this interface.

- As shown in **Figure 5-15**, interfaces connecting SwitchD, SwitchE, and SwitchF belong to the same VLAN. SwitchE is mistakenly connected to SwitchF; therefore, a loop occurs.

  In this scenario, locate the loop as follows:

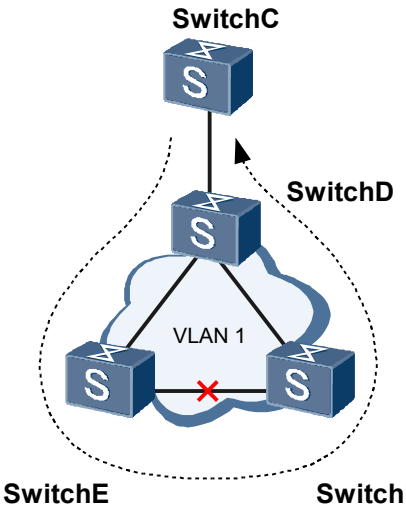
  - Enable loopback detection on SwitchC and configure SwitchC to generate an alarm when detecting a loop. Locate the Switch where the loop has occurred according to alarm messages. If a loop alarm is generated on the interface connected to SwitchD, the loop may have occurred on SwitchD, SwitchE, or SwitchF. If no loop alarm is generated, the loop has occurred on SwitchC. On the Switch where the loop has occurred, view broadcast packet statistics on interfaces or observe interface indicators to locate the interface that may encounter a loop. Run the **shutdown** command on the interface or remove the cable from the interface and check whether the broadcast storm disappears. If the broadcast storm disappears, the loop has occurred on this interface.

Figure 5-14 Loop on a switch caused by incorrect cable connections



Copyright © Huawei Technologies Co., Ltd.

Figure 5-15 Loop between switches caused by incorrect cable connections



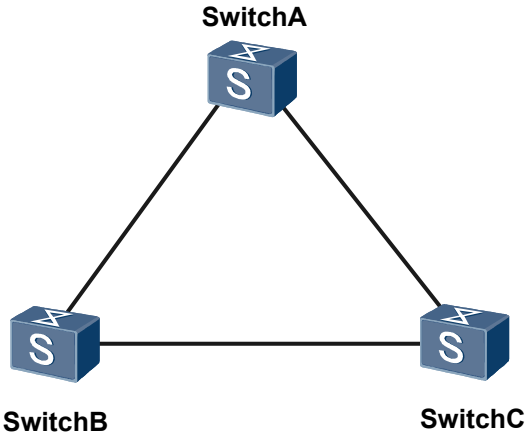
- Configurations of network devices are incorrect.

  Figure 5-16 shows a typical networking where incorrect configurations cause loops. As shown in **Figure 5-16**, interfaces connecting SwitchA and SwitchB and interfaces connecting SwitchA and SwitchC allow packets from VLAN *X* to pass through. Interfaces connecting SwitchB and SwitchC should not allow packets from VLAN *X* to pass through; however, a user incorrectly adds the two interfaces to VLAN *X*, causing a loop on the network.

  In this scenario, locate the loop as follows:

  - View broadcast packet statistics on interfaces or observe interface indicators to locate the interface that may encounter a broadcast storm. Run the **shutdown** command on the interface or remove the cable from the interface and check whether the broadcast storm disappears. If the broadcast storm disappears, the loop has occurred on this interface. Check whether the VLAN configuration on the interface is incorrect.

Figure 5-16 Incorrect configurations cause a loop



Loop Occurs Because of Incorrect Cable Connections

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Locate the interfaces where a broadcast storm has occurred.

Use either of the following methods:

- Check the indicator of each interface. If the indicator of an interface is blinking at a higher frequency than usual, a broadcast storm may have occurred on the interface.
- Run the **display interface brief** command to check the inbound and outbound bandwidth usages in a recent period of time on each interface.

  In the command output, **InUti** indicates the inbound bandwidth usage, and **OutUti** indicates the outbound bandwidth usage. If both the inbound and outbound bandwidth usages on an interface approximate to 100%, a broadcast storm may have occurred on the interface.

Step 2 Locate the device where a loop has occurred.

NOTE

To check whether a loop has occurred on a device, run the **shutdown** command on the interface where a broadcast storm has occurred or remove the cable from the interface. This operation will interrupt services on this interface and can be performed only after gaining the network administrator's permission. After the loop is removed, run the **undo shutdown** command to enable the interface.

- If broadcast storms occur on multiple interfaces and each of the interfaces is connected to a Switch, the loop may occur between Switches. Go to step 3.
- If a broadcast storm has occurred on a single interface and the interface is not connected to any Switch, the loop has occurred on the local Switch. Go to step 3.
- If the interface is connected to a Switch, the loop may have occurred on the local Switch or the Switch connected to the interface.
  - Use the loopback detection protocol to locate the device where the loop has occurred.

    NOTE

    Before configuring the loopback detection protocol, locate the VLAN where the loop has occurred in either of the following ways:

    - Check the VLAN to which the interface encountering a broadcast storm belongs.
    - Check the VLAN to which the PCs encountering a broadcast storm belong.

    - Enable loopback detection in the VLAN where the loop has occurred and configure the Switch to generate an alarm when a loop is detected. For details on how to configure loopback detection, see "loopback detection" in the *Quidway S3700 Series Ethernet Switches Configuration Guide - Ethernet*. If an **LDT 1.3.6.1.4.1.2011.5.25.174.3.3 hwLdtPortLoopDetect** alarm is generated, the interface indicated in the alarm message is the interface where the loop has occurred. If the interface indicated in the alarm message is the interface connected to a Switch, the loop has occurred on one of downstream Switches connected to the interface. In this case, repeat the preceding operations until the Switch where the loop has occurred is located. Go to step 3.

      If this alarm is not generated, the loop has occurred on the local Switch.
  - Run the **shutdown** command on the interface connected to the local Switch, and check whether the broadcast storm persists on the local Switch and the entire network.
    - If the broadcast storm persists on the local Switch but disappears on the downstream Switch, the loop has occurred on the local Switch. Go to step 3.
    - If the broadcast storm has occurred on an interface that is not connected to any Switch, the loop has occurred on the Switch where this interface resides. Go to step 3.

Copyright © Huawei Technologies Co., Ltd.

- If the broadcast storm disappears on the entire network, the loop has occurred between Switches. Go to step 3.

If the interface where a broadcast storm has occurred is connected to downstream Switches, and these Switches also encounter a broadcast storm, repeat the preceding operations on the Switches until the Switch where the loop has occurred is located.

Step 3 Locate the interfaces where the loop has occurred and remove the loop.

- If the loop has occurred on a single Switch, the loop is generated because two interfaces in the same VLAN on the Switch are directly connected. Remove the loop as follows:
  - Check whether the interface where a broadcast storm has occurred is connected to another interface on the local Switch. If yes, remove the network cable between the interfaces.
  - Run the **shutdown** command on the interface where a broadcast storm has occurred. If the broadcast storm disappears, and another interface on the local Switch goes Down, there is a loop between the two interfaces. Remove the network cable between the interfaces after gaining the network administrator's permission.
- If the loop exists between Switches, check for incorrect cable connections between Switches according to the network plan. Check the cable connection of each interface encountering a broadcast storm. If the connection between an interface and the remote device does not conform to the network plan, remove the cable from the interface.

If the fault persists after the preceding operations are complete , go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the Switches

----End

Loop Occurs Because of Incorrect Configuration

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Locate the interfaces where a broadcast storm has occurred.

Locate the interfaces where a broadcast storm has occurred on all the network devices encountering a broadcast storm.

- Check the indicator on each interface. If the indicator on an interface is blinking at a higher frequency than usual, a broadcast storm may have occurred on the interface.
- Run the **display interface brief** command to check the inbound and outbound bandwidth usages in a recent period of time on each interface.

  In the command output, **InUti** indicates the inbound bandwidth usage, and **OutUti** indicates the outbound bandwidth usage. If both inbound and outbound bandwidth usages on an interface approximate to 100%, a broadcast storm may have occurred on the interface.

Step 2 Identify and modify the incorrect configurations.

Copyright © Huawei Technologies Co., Ltd.

Check the VLANs to which the interfaces encountering a broadcast storm belong and confirm with the network administrator about the devices that should reject packets from these VLANs. Modify the VLAN configurations on the devices. If the fault persists, go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the Switches

----End

Relevant Alarms and Logs

Relevant Alarms

LDT_1.3.6.1.4.1.2011.5.25.174.3.3 hwLdtPortLoopDetect

Relevant Logs

None.

5.9 Loopback Detection Troubleshooting

This chapter describes common causes of Loopback Detection faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

5.9.1 Broadcast Storms Still Exist After Loopback Detection Is Configured

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when broadcast storms still exist after loopback detection is configured.

Common Causes

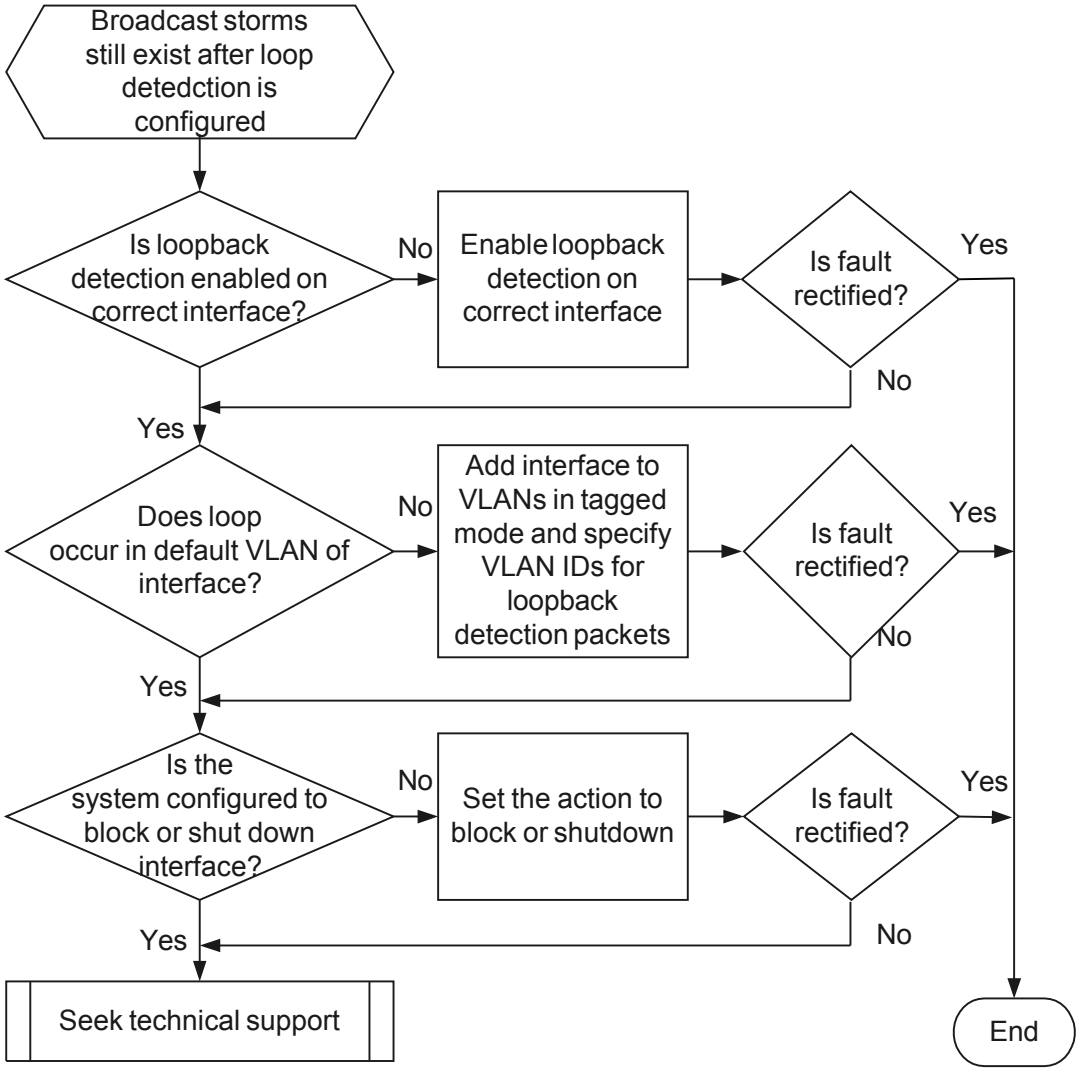
This fault is commonly caused by one of the following:

- Loopback detection is configured on an incorrect interface.
- The default VLAN of the loop detection interface is not the VLAN where a loop occurs.
- The system is not configured to block or shut down the interface when detecting a loop.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 5-17 Loopback detection troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that loopback detection is configured on the correct interface.

Run the **display this** command on the Switch interface connected to the network with a loop. If the command output contains **loopback-detect enable**, loopback detection is enabled on the interface.

- If the command output does not contain **loopback-detect enable**, run the **loopback-detect enable** command in the interface view or system view to enable loopback detection.
- If the command output contains **loopback-detect enable**, go to step 2.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Check whether the VLAN where the loop occurs is the default VLAN of the interface that receives broadcast packets.

- If the VLAN where the loop occurs is not the default VLAN of the interface, perform either of the following operations:
  - If the interface has been added to multiple VLANs in untagged mode, run the **port trunk allow-pass vlan** or **port hybrid tagged vlan** command on the local interface and remote interface to add the interfaces to these VLANs in tagged mode. Run the **loopback-detect packet vlan** *vlan-id* command on the local interface to specify these VLAN IDs for loopback detection packets.
  - If the interface has been added to multiple VLANs in tagged mode, run the **loopback-detect packet vlan** *vlan-id* command on the interface to specify these VLAN IDs for loopback detection packets.
- If the VLAN where the loop occurs is the default VLAN of the interface, go to step 3.

Step 3 Check whether the system is configured to block or shut down the interface when a loopback is detected.

Run the **display loopback-detect** command in the system view to check the loopback detection configuration. Check whether the value of the **Action** field is **block** or **shutdown**.

NOTE

If the action is set to **block**, the interface can recover automatically after the loop is removed. If the action is set to shutdown, the interface cannot recover automatically after the loop is removed.

- If the action is not block or shutdown, run the **loopback-detect action** command in the interface view to set the action to block or shutdown.
- If the action is block or shutdown, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

6 Multicast

About This Chapter

6.1 Layer 2 Multicast Troubleshooting
This chapter describes common causes of Layer 2 multicast faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

6.2 Layer 3 Multicast Troubleshooting
This chapter describes common causes of Layer 3 multicast faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

6.1 Layer 2 Multicast Troubleshooting

This chapter describes common causes of Layer 2 multicast faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

6.1.1 Users in User VLANs Fail to Receive Multicast Packets (IGMP snooping)

Common Causes

This fault is commonly caused by one of the following:

- The upstream link or downstream link of the S3700 is broken because the hardware (such as board, fiber, and network cable) is faulty.
- The Layer 2 multicast configuration of the system or the user VLAN is incorrect, for example, IGMP snooping is not enabled.
- The Layer 2 multicast configurations on the S3700 conflict, for example, the configuration of disabling dynamic multicast entry learning on interface, multicast group policy, interface fast leave, igmp-snooping require-router-alert and Layer 2 multicast filtering.
- The number of Layer 2 multicast entries on the S3700 reaches the limit.

Troubleshooting Flowchart

After the Layer 2 multicast is configured, multicast traffic cannot be transmitted to users.

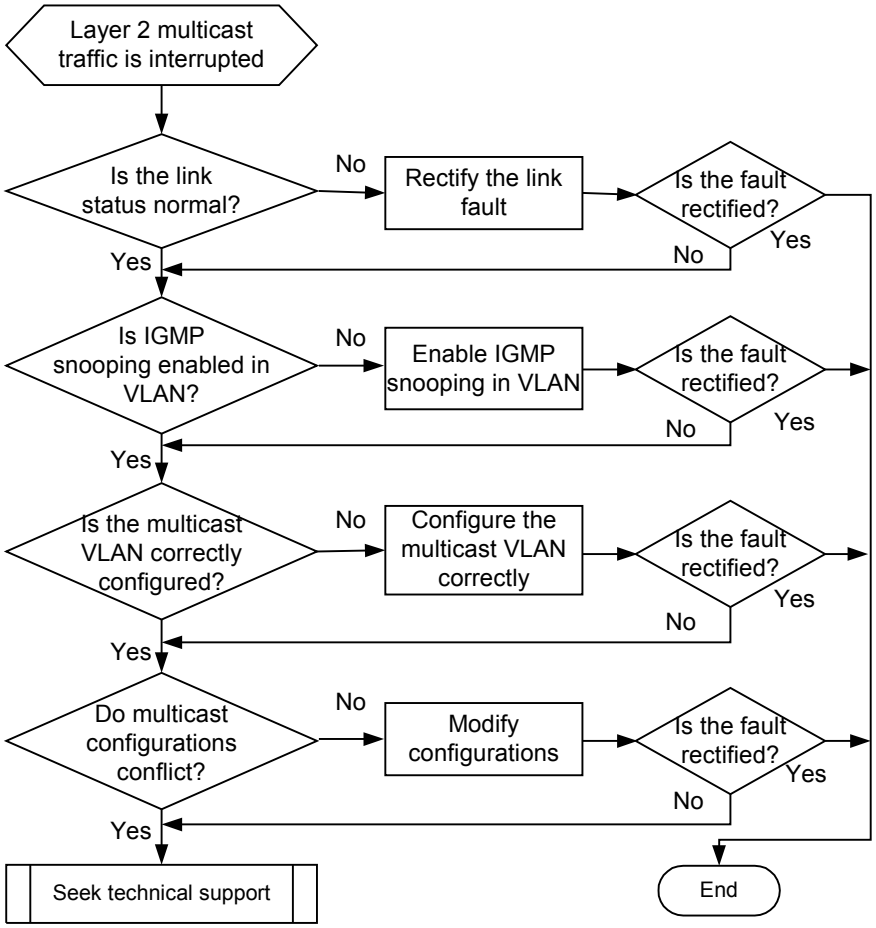
The troubleshooting roadmap is as follows:

- Check whether link failure occurs.
- Check whether the configurations are incorrect or conflict.

Figure 6-1 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-1 Troubleshooting flowchart for Layer 2 multicast



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the upstream and downstream links are Up.

Run the **display interface brief** command in the system view to check whether the Layer 2 multicast service interfaces are in Up state.

- If the *down status of an interface is Administratively Down, run the **undo shutdown** command in the interface view to enable the interface.
- If the physical status of the interfaces is Down, check the upstream and downstream physical links.
- If the physical status and protocol status of the interfaces are Up, go to step 2.

Step 2 Check whether IGMP snooping is enabled globally and in a VLAN.

Copyright © Huawei Technologies Co., Ltd.

If the output information contains **igmp-snooping enable**, global IGMP snooping is enabled.

Run the **display igmp-snooping configuration** command to check the IGMP snooping configuration of the VLAN.

- If the command output does not contain **igmp-snooping enable**, run the **igmp-snooping enable** command in the system view and VLAN view to enable IGMP snooping.
- If IGMP snooping has been enabled globally and in the VLAN, go to step 3.

Step 3 Check that the multicast VLAN is properly configured.

Run the **display multicast-vlan vlan** *vlan-id* command to check whether the user VLAN is bound to a correct multicast VLAN.

- If the user VLAN is not bound to a correct multicast VLAN, run the **multicast-vlan user-vlan** command to bind VLANs correctly. Check whether the igmp-snooping of the multicast vlan is enabled.
- If the user VLAN has been bound to a correct multicast VLAN, go to step 4.

  The following information shows that user VLANs 100 and 200 are bound to multicast VLAN 10.

```
[Quidway]display multicast-vlan vlan 10
 Multicast-vlan         :
10
 User-vlan Number       :
2
 IGMP snooping state    :
Enable
 MLD  snooping state    :
Disable
 User-vlan              Snooping-
state

---------------------------------------------
 100                     IGMP Enable /MLD
Disable
 200                    IGMP Enable /MLD Disable
```

Step 4 Check whether the multicast configurations conflict.

Check whether the following configurations exist on the device:

- Disabling dynamic learning of multicast entries on user interfaces or VLANs

  If the dynamic learning of router interfaces is disabled in a VLAN, the VLAN does not listen to IGMP Query messages. As a result, no multicast router port is generated. Run the **igmp-snooping router-learning** command in the VLAN view to enable the dynamic learning of router interfaces in the VLAN.

- Fast leave of member interfaces

  The fast leave function can be enabled in a VLAN only when each interface in the VLAN is connected to one host. If a member interface is connected to multiple hosts, the S3700 immediately deletes the forwarding entry of the member interface after receiving an IGMP Leave message from the member interface without sending a Group-Specific Query message.

  Run the **undo igmp-snooping prompt-leave** command in the VLAN view to disable the fast leave of member interfaces.

- igmp-snooping require-router-alert

  If igmp-snooping require-router-alert has been configured, the S3700 checks the Options field in IGMP packets, and discards the packets that do not contain the Options field.

Copyright © Huawei Technologies Co., Ltd.

Run the **undo igmp-snooping require-router-alert** command in the VLAN view to cancel the igmp-snooping require-router-alert configuration. The S3700 will not check the Options field in IGMP packets.

- Multicast group policy

  The multicast group policy limits the multicast groups that the hosts on a VLAN can join. You can run the **display igmp-snooping configuration** command in the VLAN view to verify the configuration of multicast group policy. If ACL is configured, verify the ACL configuration.

- Layer 2 multicast filtering on interface

  If this function is configured on the interface, the interface discards the UDP packets from certain VLANs.

  Run the **undo multicast-source-deny vlan** command in the interface view to disable the Layer 2 multicast filtering function.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

6.1.2 Troubleshooting Cases

This section presents several Layer 2 multicast troubleshooting cases.

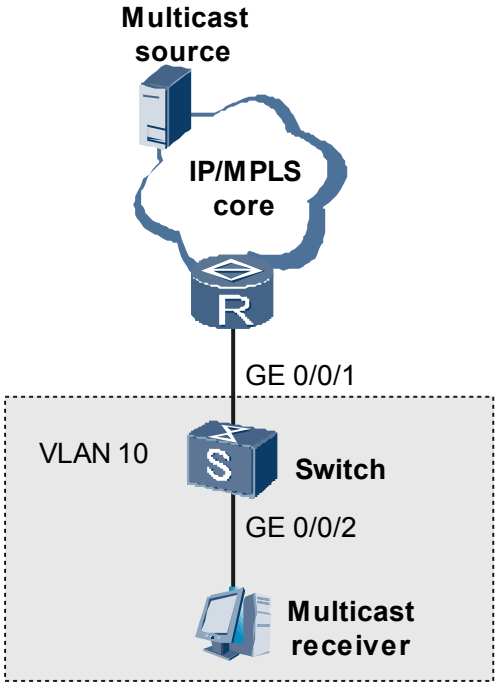
Multicast Forwarding Fails When IGMP Snooping Is Disabled

Fault Symptom

As shown in **Figure 6-2**, the Switch provides the Layer 2 multicast function. After IGMP snooping is configured on the Switch, clients can receive multicast traffic only for two minutes. When a client initiates a multicast-on-demand operation, a multicast entry is created on the Switch, but is deleted after two minutes. When the multicast entry is deleted, multicast traffic is interrupted.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Multicast forwarding fails when IGMP snooping is disabled



Fault Analysis

1. Only multicast traffic is interrupted, but other service traffic are forwarded normally; therefore, the links function properly.
2. On the network, the router is configured with a static multicast group, so it does not send IGMP Query packets. In addition, the Switch is not configured to send Query packets. Therefore, the client does not receive IGMP Query packets.

   When the client initiates the multicast-on-demand service, it sends an IGMP Report packet. Therefore, the Layer 2 multicast entry can be created. By default, IGMP Snooping does not update multicast entries; therefore, after the created multicast entry ages out, the multicast entry will not be created again unless the client re-initiates the multicast-on-demand service. The default aging time of multicast entries is 130 seconds. The formula is Query interval (60) x Robustness variable (2) + Maximum aging time (10). Therefore, the client keeps on receiving multicast traffic for only two minutes.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **vlan** *vlan-id* command to enter the VLAN view.

Step 3 Run the **igmp-snooping querier enable** command to enable IGMP snooping querier for the VLAN.

This command ensures that the Switch sends IGMP Query packets to update the multicast entries after IGMP snooping is enabled.

Copyright © Huawei Technologies Co., Ltd.

After the preceding configurations, the client receives multicast traffic and the traffic is not interrupted.

----End

Summary

When IGMP packets from the upstream router cannot reach the S3700 for some reasons, or when the upstream router only has static multicast forwarding entries, you can configure an IGMP querier on the S3700. The IGMP querier then sends IGMP Query packets for the upstream router.

6.2 Layer 3 Multicast Troubleshooting

This chapter describes common causes of Layer 3 multicast faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

6.2.1 Multicast Traffic Is Interrupted

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for Layer 3 multicast faults.

Common Causes

This fault is commonly caused by one of the following:

- Route configurations are incorrect.
- VLAN status is incorrect.
- PIM routing entries are not created.
- Multicast forwarding entries are not created.

Troubleshooting Flowchart

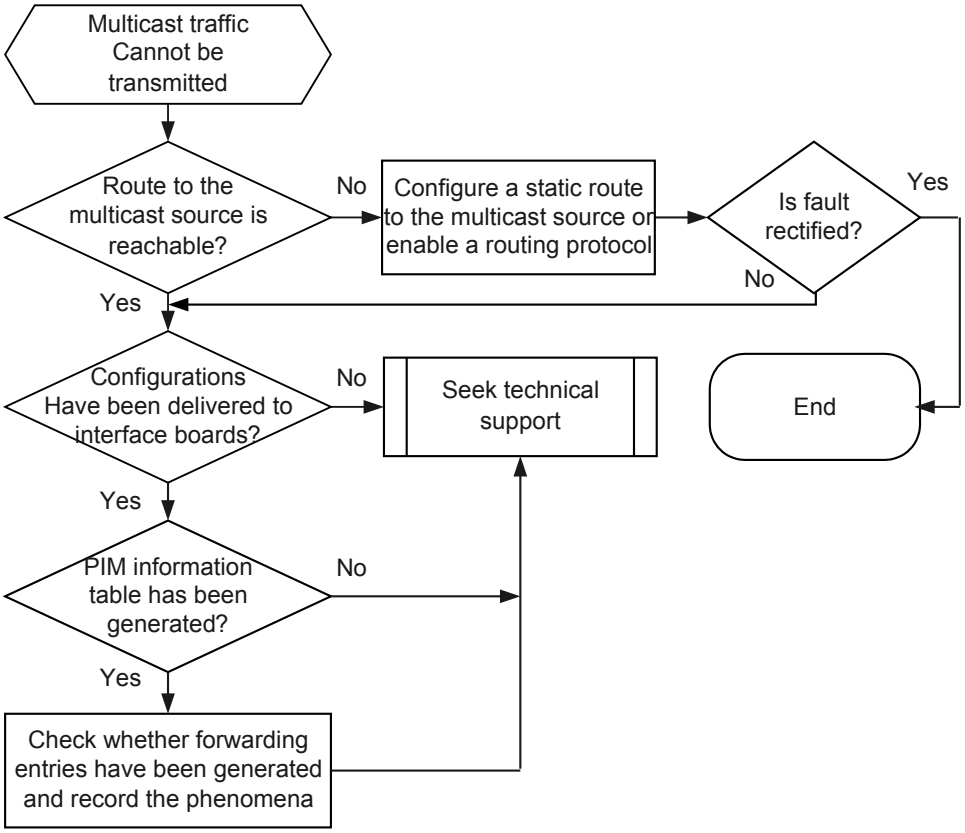
After the Layer 3 multicast is configured, multicast traffic cannot be transmitted to users.

The troubleshooting roadmap is as follows:

- Check that a route destined for the multicast source is available.
- Check that the VLANs on the inbound and outbound interfaces of the multicast route function properly.
- Check that the PIM routing entries are created.
- Check that the multicast forwarding entries are created.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that a route destined for the multicast source is available.

Run the **display ip routing-table** *ip-address* command to check whether the local routing table contains a route destined for the multicast source.

NOTE

ip-address specifies the multicast source address.

- If not, configure a route destined for the multicast source.
- If yes, go to step 2.

Step 2 Check that the VLANs on the inbound and outbound interfaces of the multicast forwarding entry function properly.

Run the **display interface vlanif** *vlan-id* command to view VLAN status.

Copyright © Huawei Technologies Co., Ltd.

- If the VLANs are abnormal, the multicast forwarding entry cannot be created. Rectify the fault according to **5.1 VLAN Troubleshooting**.

  In the following information, the status of VLANIF 90 is Down.

```
[Quidway] display interface Vlanif
90
Vlanif90 current state :
DOWN
Line protocol current state :
DOWN
Description:HUAWEI, Quidway Series, Vlanif90
Interface
Route Port,The Maximum Transmit Unit is
1500
Internet Address is
1.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
0018-2000-0140
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  :
--
    Output bandwidth utilization : --
```

- If the VLAN status is normal, go to step 3.

Step 3 Check that the PIM routing entries are created.

Run the **display pim routing-table** command to check whether PIM routing entries are created.

- If not, contact Huawei technical support personnel.
- If yes, go to step 4.

Step 4 Check whether the multicast forwarding entries are created.

Run the **display multicast forwarding-table** command to check that the multicast forwarding entries are created.

- If the fault persists, record the command output and contact Huawei technical support personnel.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

6.2.2 The PIM Neighbor Relationship Remains Down

Common Causes

This fault is commonly caused by one of the following causes:

- The interface is physically Down or the link-layer protocol status of the interface is Down.
- PIM is not enabled on the interface.
- PIM configurations on the interface are incorrect.

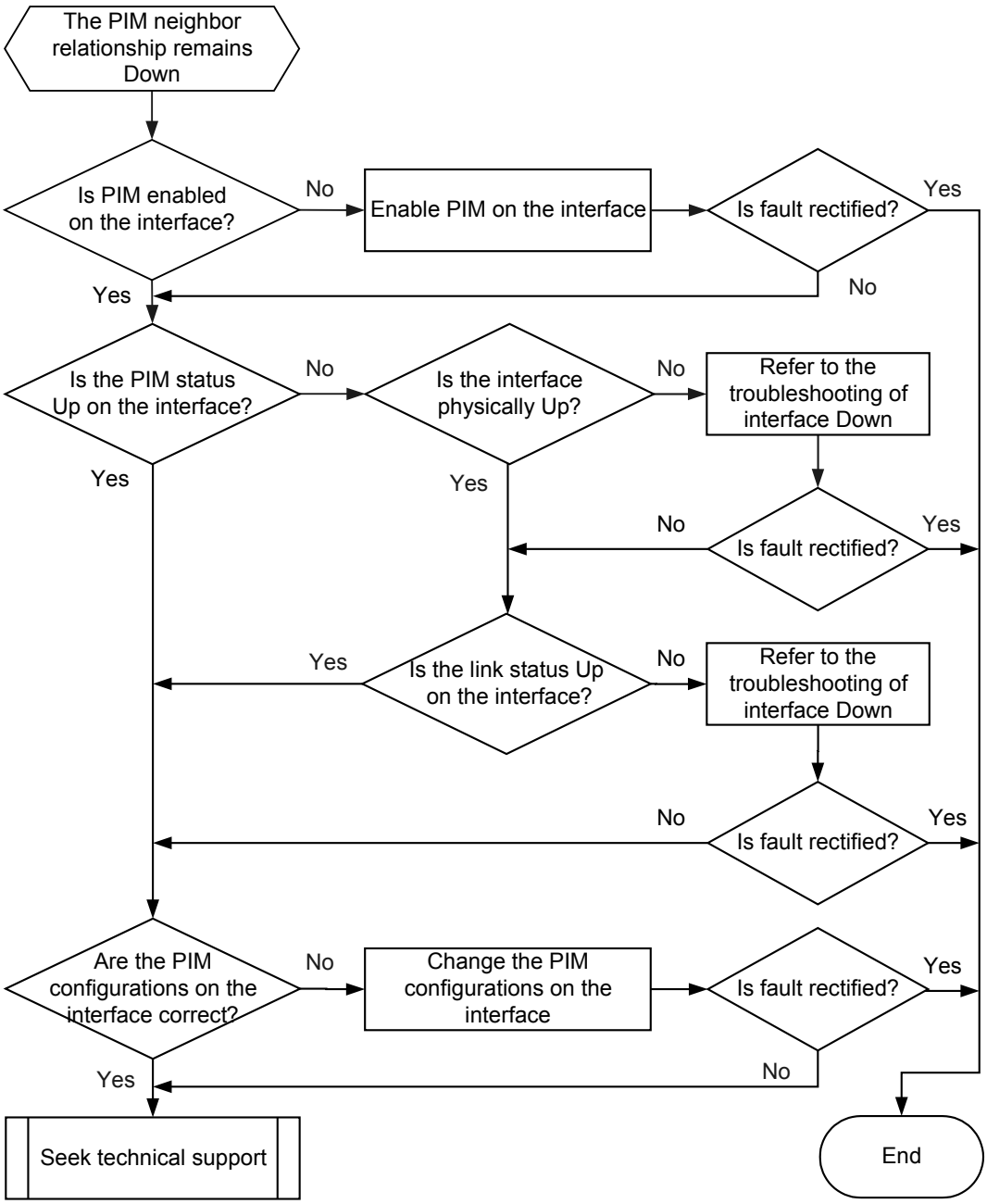
Troubleshooting Flowchart

After PIM network configuration is complete, the PIM neighbor relationship remains Down.

Figure 6-4 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-4 Troubleshooting flowchart for the fault that the PIM neighbor relationship remains Down



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check that PIM is enabled on the interface.

Run the **display current-configuration interface** *interface-type interface-number* command to check whether PIM is enabled on the interface.

- If PIM is not enabled, enable PIM on the interface.

  If "Warning: Please enable multicast routing in the system view first" is prompted when you enable PIM, you need to first run the **multicast routing-enable** command in the system view to enable the multicast function. Then, go on to enable PIM-SM or PIM-DM on the interface.
- If PIM has been enabled on the interface, go to **Step 2**.

Step 2 Check that the PIM status on the interface is Up.

Run the **display pim interface** *interface-type interface-number* command to check whether the PIM status on the interface is Up.

- If the PIM status is Down, run the **display interface** *interface-type interface-number* command to check whether the physical status and link status of the interface are both Up.
  1. If the physical status is not Up, make the physical status go Up.
  2. If the link status is not Up, make the link status go Up.
- If the PIM status of the interface is Up, go to **Step 3**.

Step 3 Check that PIM configurations on the interface are correct.

The fault may be caused by the following PIM configurations:

- The IP addresses of directly-connected interfaces are on different network segments.
- PIM silent is configured on the interface.
- A PIM neighbor filtering policy is configured on the interface and the address of the PIM neighbor is filtered out by the policy.
- If the interface is configured to deny the Hello messages without Generation IDs, the interface discards all the Hello messages received from the PIM neighbors without any Generation IDs and as a result, the PIM neighbor relationship cannot be set up. This case is applicable to the scenario of Huawei devices intercommunicating with non-Huawei devices.

Run the **display current-configuration interface** *interface-type interface-number* command to check whether any of the preceding PIM configurations exists on the interface.

- If any of the preceding PIM configurations exists, you need to correct it.
- If the fault persists after the preceding operations are complete, go to **Step 4**.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

PIM/4/NBR_DOWN

6.2.3 The RPT on a PIM-SM Network Fails to Forward Data

Common Causes

This fault is commonly caused by one of the following:

- The unicast route from the multicast device to the RP is unavailable.
- The RP addresses on multicast devices are inconsistent.
- The downstream interface of the multicast device does not receive any (*, G) Join messages.
- PIM-SM is not enabled on interfaces.
- The RPF route to RP is incorrect, for example, the unicast route has a loop.
- Configurations are incorrect, for example, the configurations of the TTL, MTU, or multicast boundary are improper.

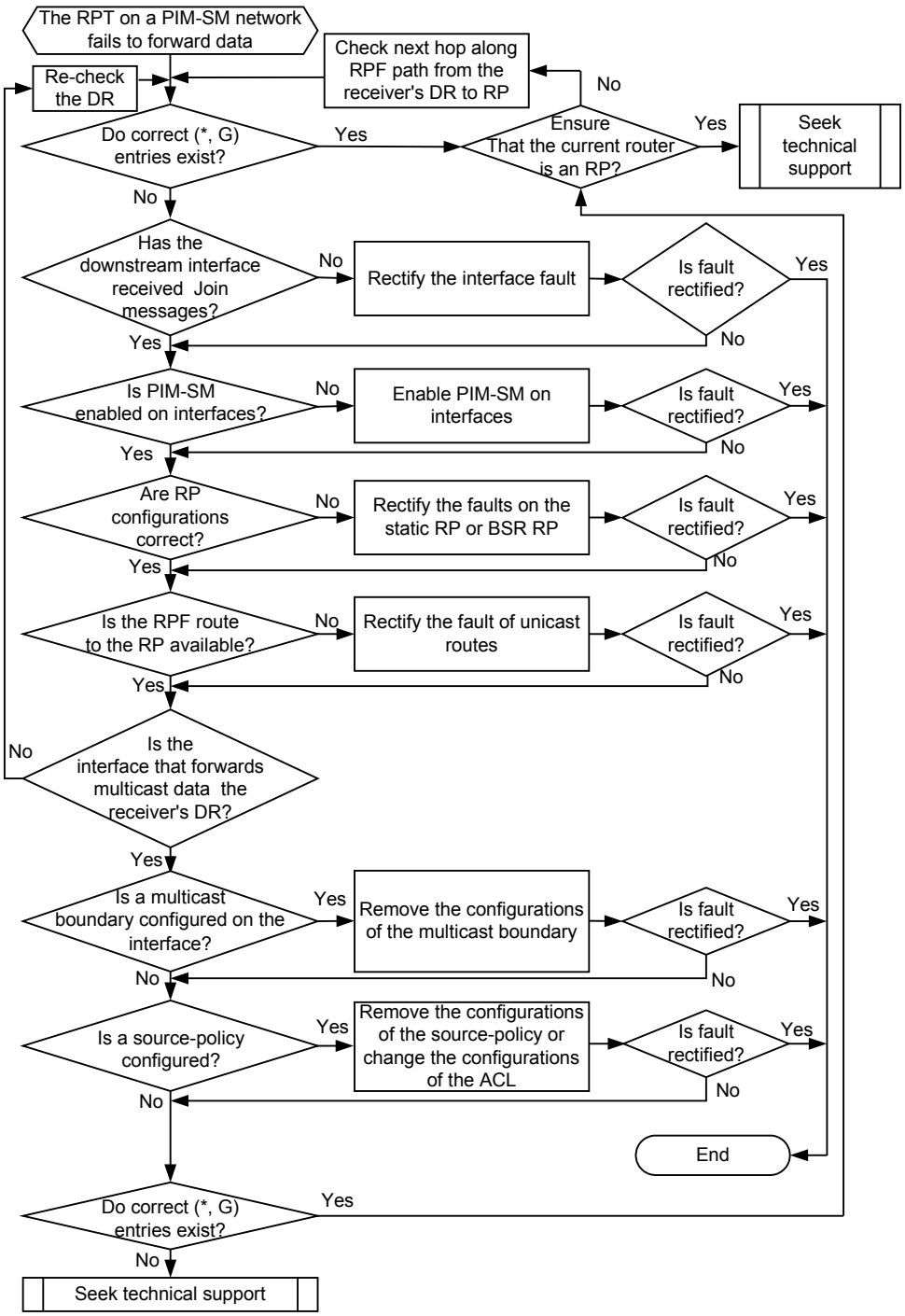
Troubleshooting Flowchart

After a PIM-SM network is configured, the RPT cannot forward data.

Figure 6-5 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-5 Troubleshooting flowchart for the fault that the RPT on a PIM-SM network fails to forward data



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check that the PIM routing table contains correct (*, G) entries.

Run the **display pim routing-table** *group-address* command on the device to check whether the PIM routing table contains correct (*, G) entries. Focus on checking whether the downstream interface list contains downstream interfaces to forward data to all (*, G) group members.

- If the (*, G) entries exist and are all correct in the PIM routing table, run the **display multicast forwarding-table** *group-address* command every 15 seconds to check whether the forwarding table contains (S, G) entries associated with the (*, G) entries and whether the value of the **Matched** field in the command output keeps increasing.
  - If the forwarding table contains associated (S, G) entries and the value of the **Matched** field keeps increasing, it indicates that the upstream device can normally forward multicast data to the current device but the current device fails to forward the data downstream, for example, a too small TTL value or a forwarding fault.
  - If the forwarding table does not contain associated (S, G) entries or the value of the **Matched** field remains unchanged, do as follows:
    - If the current device is not an RP, it indicates that the current device has not received any multicast data. The fault may be caused by the upstream device. Then check whether the PIM routing table on the upstream device contains correct (S, G) entries.
    - If the current device is already an RP, it indicates the RPT has been set up but the RP fails to receive the multicast data from the multicast source. The fault may be caused by a failure in source's DR registration. In such a case, go to Step 10.
- If the PIM routing table does not contain correct (*, G) entries, go to Step 2.

Step 2 Check that the downstream interface has received Join messages.

Run the **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** command to check whether the number of received Join/Prune messages on the downstream interface keeps increasing.

- If the number of received Join/Prune messages on the downstream interface does not increase, run the **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** command on the downstream device to check whether the downstream device has sent Join/Prune messages upstream.
  - If the command output shows that the number of sent Join/Prune messages keeps increasing, it indicates that the downstream device has sent Join/Prune messages. The fault may be caused by a failure in PIM neighbor communication. In such a case, go to Step 10.
  - If the command output shows that the number of sent Join/Prune messages does not increase, it indicates the downstream device experiences a fault. Then locate the fault.
- If the number of received Join/Prune messages on the downstream interface keeps increasing, go to Step 3.

Step 3 Check that PIM-SM is enabled on interfaces.

The following interfaces are easy to be ignored in enabling PIM-SM:

- RPF neighboring interface to the RP
- RPF interface to the RP
- Interface directly connected to shared network segment of user hosts, that is, downstream interface of the receiver's DR

Copyright © Huawei Technologies Co., Ltd.

Run the **display pim interface verbose** command to check PIM configurations on the interface. Focus on checking whether PIM-SM is enabled on the preceding interfaces.

- If the command output does not contain information about an interface of the device or the PIM mode of an interface is dense, you need to run the**pim sm** command on the interface.

  If the system prompts that "Warning: Please enable multicast routing first" when you configure PIM-SM on the interface, run the **multicast routing-enable** command in the system view to enable the multicast function first and enable PIM-SM on the interface.
- If PIM-SM has been enabled on all the interfaces on the device, go to Step 4.

Step 4 Check that the RP information is correct.

Run the **display pim rp-info** command on the device to check whether the device has learnt information about the RP serving a specific group and whether the RP information of the same group on all other devices is consistent.

- If no RP information is displayed or RP information on the devices are inconsistent, do as follows:
  - If the static RP is used on the network, run the **static-rp** command on all the devices to make information about the RP serving a specific group consistent.
  - If the dynamic RP is used, go to Step 10.
- If RP information of a specific group is consistent on all the devices, go to Step 5.

Step 5 Check that an RPF route to the RP is available.

Run the **display multicast rpf-info** *source-address* command on the device to check whether there is an RPF route to the RP.

- If the command output does not contain any RPF route to the RP, check the configurations of unicast routes. Run the **ping** command on the device and the RP to check whether they can ping each other successfully.
- If the command output contains an RPF route to the RP, do as follows:
  - If the command output shows that the RPF route is a static multicast route, run the **display current-configuration** command to check whether the static multicast route is properly configured.
  - If the command output shows that the RPF route is a unicast route, run the **display ip routing-table** command to check whether the unicast route is consistent with the RPF route.
- If the command output contains an RPF route to the RP and the route is properly configured, go to Step 6.

Step 6 Check that the interface that forwards multicast data is a receiver's DR.

Run the **display pim interface** *interface-type interface-number* command on the device to check whether the interface that forwards multicast data is a receiver's DR.

- If the DR information in the command output is not marked with **local**, troubleshoot the involved DR following the preceding steps.
- If the DR information in the command output is marked with **local**, go to Step 7.

Step 7 Check whether a multicast boundary is configured on the interface.

Run the **display current-configuration interface** *interface-type interface-number* command on the device to check whether a multicast boundary is configured on the interface.

Copyright © Huawei Technologies Co., Ltd.

- If the configuration of the interface contains **multicast boundary**, it indicates that a multicast boundary is configured on the interface. Then you need to run the **undo multicast boundary** { *group-address* { *mask* | *mask-length* } | **all** command to delete the configuration of the multicast boundary or re-plan the network to ensure that no multicast boundary is configured on the RPF interface or the RPF neighboring interface.
- If no multicast boundary is configured on the interface, go to Step 8.

Step 8 Check whether a source policy is configured.

Run the **display current-configuration configuration pim** command to view the current configurations in the PIM view.

- If the configuration contains **source-policy acl-number**, it indicates a source-based filtering rule is configured. If the received multicast data is denied by the ACL rule, the multicast data is discarded. Then you need to run the **undo source-policy** command to delete the configuration of the ACL rule or reconfigure an ACL rule to ensure that demanded multicast data can be normally forwarded.
- If no source policy is configured, go to Step 9.

Step 9 Check whether the PIM routing table contains correct (*, G) entries.

Run the **display pim routing-table** *group-address* command on the device to check whether the PIM routing table contains correct (*, G) entries. For details, see Step 1.

If the fault persists after the preceding troubleshooting procedures are complete, go to Step 10.

Step 10 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

6.2.4 The SPT on a PIM-SM Network Fails to Forward Data

Common Causes

This fault is commonly caused by one of the following:

- The downstream interface of the multicast device does not receive any (S, G) Join messages.
- PIM-SM is not enabled on the interface.
- The RPF route to the multicast source is incorrect, for example, the unicast route has a loop.

Copyright © Huawei Technologies Co., Ltd.

- Configurations are incorrect, for example, the configurations of the TTL, MTU, switchover threshold, or multicast boundary are improper.

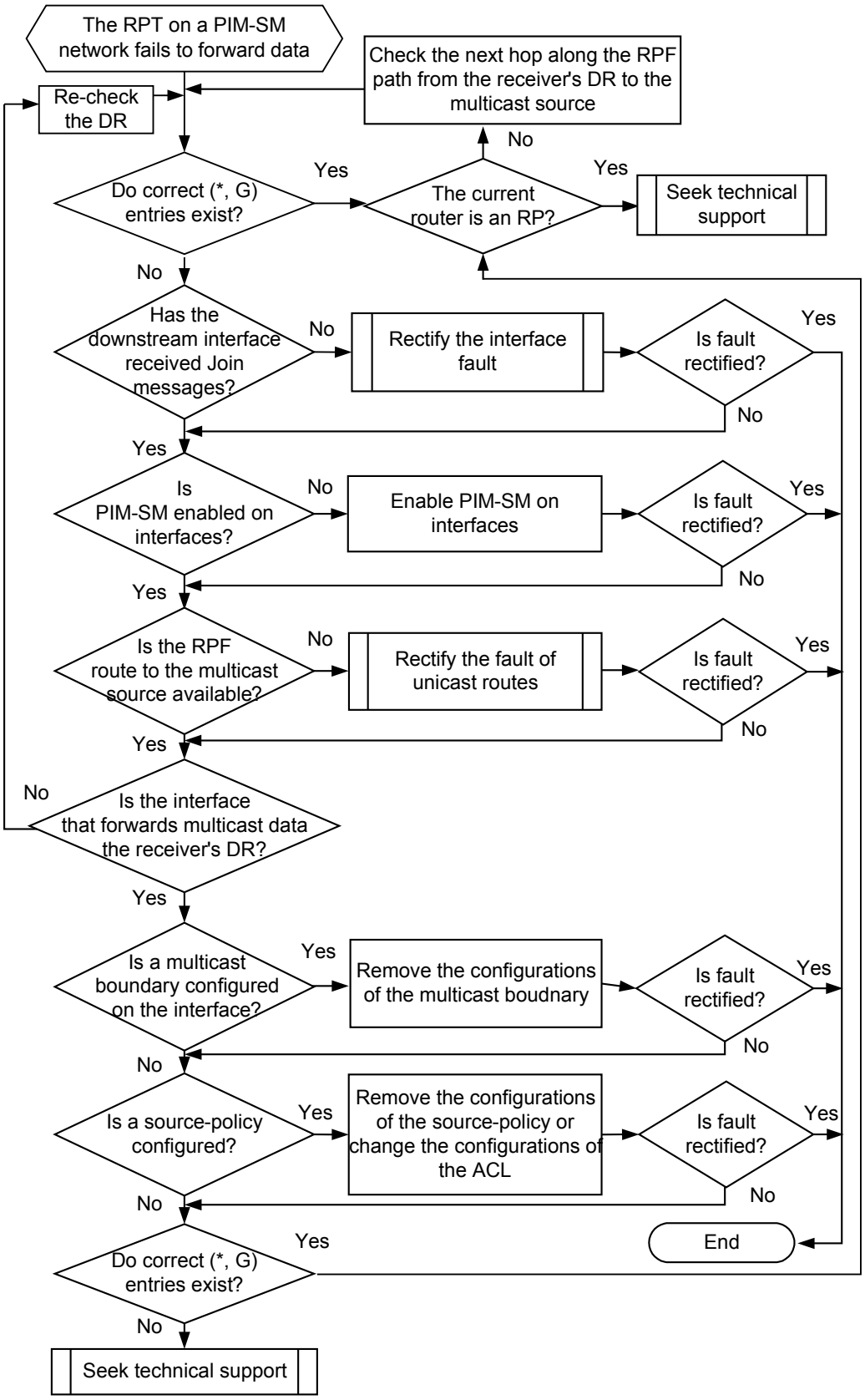
Troubleshooting Flowchart

After the PIM-SM network is configured, the SPT fails to forward data.

Figure 6-6 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-6 Troubleshooting flowchart for the fault that the SPT on a PIM-SM network fails to forward data



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the PIM routing table contains correct (S, G) entries.

Run the **display pim routing-table** command on the device to check whether the PIM routing table contains correct (S, G) entries.

- If the PIM routing table contains correct (S, G) entries, do as follows:
  - Check whether the entry has an SPT flag.
    - If the multicast group is in the ASM group address range, the SPT switchover is triggered by the RP, and the upstream interface of the RP is a register interface, it indicates that the RP has received the Register message from the source's DR but the SPT fails to be established. Then contact Huawei technical support personnel.
    - If the multicast group is in the ASM group address range, the SPT switchover is triggered by the receiver's DR, and the upstream interface is an RPF interface to the RP but not the SPT interface to the multicast source, it indicates that the SPT fails to be established.

      Then run the **display current-configuration configuration pim** command on the receiver's DR to view the current configurations in the PIM view. If the command output contains **spt-switch-threshold traffic-rate** or **spt-switch-threshold infinity**, run the **undo spt-switch-threshold** command to delete the configurations of the traffic rate or run the **spt-switch-threshold** *traffic-rate* command to reconfigure a proper traffic rate.
  - Check whether the downstream interface list contains downstream interfaces to forward data to all group members.
    - If the (S, G) entries exist and are all correct in the PIM routing table, run the **display multicast forwarding-table** command to view the (S, G) entries in the forwarding table and check whether the value of the **Forwarded** field in the command output keeps increasing. The value of the **Matched** field is not updated in time. Therefore, after running the **display multicast forwarding-table** command, you need to wait for several minutes.
      - If the value of the **Matched** field keeps increasing, it indicates that the upstream device can normally forward multicast data to the current device but the current device fails to forward the data downstream. Go to Step 9.
      - If the value of the **Matched** field remains unchanged, do as follows:
        - If the current device is not a source's DR, it indicates that the current device has not received any multicast data. The fault may be caused by the upstream device. Then check whether the PIM routing table on the upstream device contains correct (S, G) entries.

Copyright © Huawei Technologies Co., Ltd.

- If the PIM routing table on the upstream device does not contain correct (S, G) entries, troubleshoot the upstream device following the preceding steps.
- If the PIM routing table on the upstream device contains correct (S, G) entries, but the value of the **Matched** field still remains unchanged, go to Step 9.

- If the current device is already a source's DR, it indicates that SPT has been set up but the source's DR fails to forward the multicast data along the SPT. Go to Step 9.

- If the PIM routing table does not contain correct (S, G) entries, go to Step 2.

Step 2 Check that the downstream interface has received Join messages.

NOTE

If the current device is a receiver's DR, skip this step.

If the downstream interface does not receive any (S, G) Join messages, the possible causes may be as follows:

- A fault occurs on the downstream interface.
- PIM-SM is not enabled on the downstream interface.

Run the **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** command to check whether the number of received Join/Prune messages on the downstream interface keeps increasing.

- If the number of received Join/Prune messages on the downstream interface does not increase, run the **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** command on the downstream device to check whether it has sent Join/Prune messages upstream.
  - If the command output shows that the number of sent Join/Prune messages keeps increasing, it indicates that the downstream device has sent Join/Prune messages. The fault may be caused by a failure in PIM neighbor communication. In such a case, go to Step 9.
  - If the command output shows that the number of sent Join/Prune messages does not increase, it indicates the downstream device experiences a fault. Then locate the fault.
- If the number of received Join/Prune messages on the downstream interface keeps increasing, go to Step 3.

Step 3 Check that PIM-SM is enabled on interfaces.

The following interfaces are easy to be ignored in enabling PIM-SM:

- RPF neighboring interface to the multicast source
- RPF interface to the multicast source

NOTE

In PIM-SM network deployment, you are recommended to enable the multicast function on all the devices on the network and enable PIM-SM on all the interfaces.

Run the **display pim interface verbose** command to check PIM configurations on the interface. Focus on checking whether PIM-SM is enabled on the preceding interfaces.

- If the command output does not contain information about an interface of the device or the PIM mode of an interface is dense, you need to run the **pim sm** command on the interface.

Copyright © Huawei Technologies Co., Ltd.

If the system prompts that "Warning: Please enable multicast routing first" when you configure PIM-SM on the interface, run the **multicast routing-enable** command in the system view to enable the multicast function first and run the **pim sm** command in the interface view to enable PIM-SM on the interface.

- If PIM-SM has been enabled on all the interfaces on the device, go to Step 4.

Step 4 Check that an RPF route to the multicast source is available.

Run the **display multicast rpf-info** *source-address* command on the device to check whether there is an RPF route to the multicast source.

- If the command output does not contain any RPF route to the RP, check the configurations of unicast routes. Run the **ping** command on the device and the RP to check whether they can ping each other successfully.
- If the command output contains an RPF route to the multicast source, do as follows:
  - If the command output shows that the RPF route is a static multicast route, run the **display current-configuration** command to check whether the static multicast route is properly configured.
  - If the command output shows that the RPF route is a unicast route, run the **display ip routing-table** command to check whether the unicast route is consistent with the RPF route.
- If the command output contains an RPF route to the RP and the route is properly configured, go to Step 5.

Step 5 Check that the interface that forwards multicast data is the receiver's DR.

Run the **display pim interface** *interface-type interface-number* command on the device to check whether the interface that forwards multicast data is a receiver's DR.

- If the DR information in the command output is not marked with **local**, troubleshoot the involved DR following the preceding steps.
- If the DR information in the command output is marked with **local**, go to Step 6.

Step 6 Check whether a multicast boundary is configured on the interface.

Run the **display current-configuration interface** *interface-type interface-number* command on the device to check whether a multicast boundary is configured on the interface.

- If the configuration of the interface contains **multicast boundary**, it indicates that a multicast boundary is configured on the interface. Then you need to run the **undo multicast boundary** { *group-address* { *mask* | *mask-length* } | **all** command to delete the configuration of the multicast boundary or re-plan the network to ensure that no multicast boundary is configured on the RPF interface or the RPF neighboring interface.
- If no multicast boundary is configured on the interface, go to Step 7.

Step 7 Check whether a source policy is configured.

Run the **display current-configuration configuration pim** command to view the current configurations in the PIM view.

- If the configuration contains **source-policy acl-number**, it indicates that a source filtering rule is configured. If the received multicast data is denied by the ACL rule, the multicast data is discarded. Then you need to run the **undo source-policy** command to delete the configuration of the ACL rule or reconfigure an ACL rule to ensure that demanded multicast data can be normally forwarded.

Copyright © Huawei Technologies Co., Ltd.

- If no source policy is configured, go to Step 8.

Step 8 Check whether the PIM routing table contains correct (S, G) entries.

Run the **display pim routing-table** command on the device to check whether the PIM routing table contains (S, G) entries. For details, see Step 1.

Step 9 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

6.2.5 MSDP Peers Cannot Generate Correct (S, G) Entries

Common Causes

This fault is commonly caused by one of the following:

- The MSDP peer to initiate SA messages is not configured on the RP.
- The logical RP is not configured on the devices to be deployed with anycast RP or configurations of the logical RP are incorrect.
- MSDP peer relationships are not set up between every two members in a mesh group.
- The used intra-domain multicast protocol is not PIM-SM.
- The RPF route to the multicast source is incorrect, for example, the unicast route has a loop.
- Configurations are incorrect, for example, the configurations of the SA policy, import policy, TTL, switchover threshold, or multicast boundary are improper.
- SA message fails to pass RPF check.

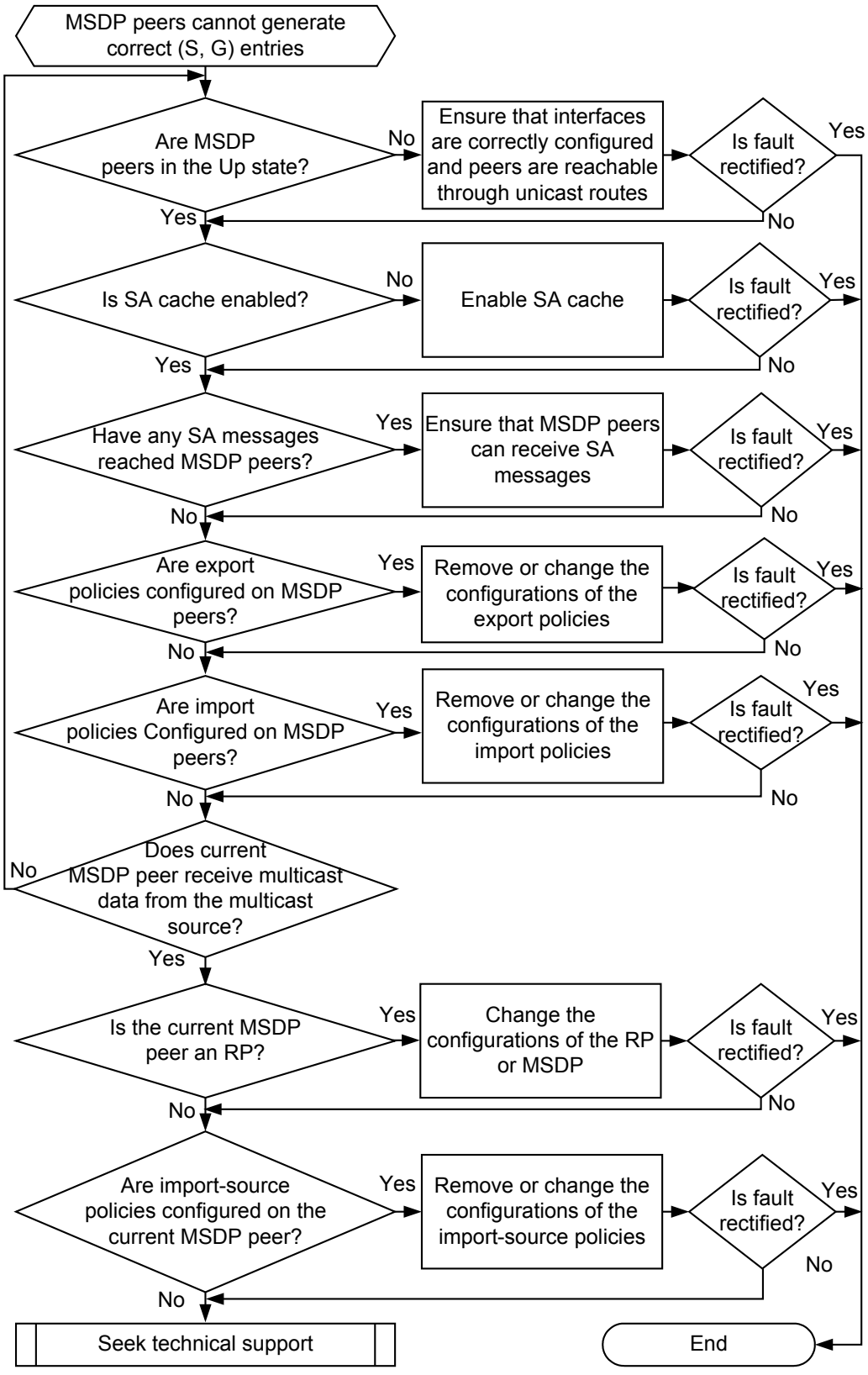
Troubleshooting Flowchart

After configurations are complete on a multicast network, MSDP peers cannot generate correct (S, G) entries.

Figure 6-7 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-7 Troubleshooting flowchart for the fault that MSDP peers cannot generate correct (S, G) entries



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the status of MSDP peers is Up.

Run the **display msdp brief** command on the devices setting up an MSDP peer relationship to check whether the status of MSDP peers is Up.

- If the command output shows that the status of MSDP peers is Down, check whether the MSDP peer interfaces are correctly configured and whether the MSDP peers can ping each other successfully. If the ping fails, perform troubleshooting based on The Ping Operation Fails.
- If the MSDP peers are both in the Up state, go to **Step 2**.

Step 2 Check that SA cache is enabled.

Run the **display current-configuration configuration msdp** command on MSDP peers to view the current configurations in the MSDP view.

- If the command output contains **undo cache-sa-enable**, it indicates that SA cache is disabled in the MSDP view. In this case, run the **cache-sa-enable** command in the MSDP view to enable SA cache.
- If SA cache has been enabled, go to **Step 3**.

Step 3 Check that SA messages have reached MSDP peers.

Run the **display msdp sa-count** command on MSDP peers to check the contents of the SA cache.

- If there is no command output, contact Huawei technical support personnel.
- If the value of the **Number of source** or **Number of group** field in the command output is non-zero, it indicates that SA messages have reached peers. Then go to **Step 4**.

Step 4 Check whether export policies are configured on MSDP peers.

Run the **display current-configuration configuration msdp** command on MSDP peers to view the current configurations in the MSDP view.

- If export policies are configured on MSDP peers, do as follows:
  - If the command output contains the configurations of the **peer peer-address sa-policy export** command without any parameter, it indicates that MSDP peers are disabled from forwarding messages received from the multicast source. Then run the **undo peer** *peer-address* **sa-policy export** command to delete the configurations of export policies.
  - If the command output contains the configurations of the **peer peer-address sa-policy export acl advanced-acl-number** or the **peer peer-address sa-policy export acl acl-name** command with an ACL specified, it indicates that MSDP peers can forward only the (S, G) entries permitted by the ACL. Then check whether ACL-related commands are run on the MSDP peers and whether (S, G) entries are permitted by the ACL. You can run the **undo peer** *peer-address* **sa-policy export** command to delete the configurations of the ACL or change the configurations of the ACL rules.

Copyright © Huawei Technologies Co., Ltd.

- If no export policies are configured on MSDP peers, go to **Step 5**.

Step 5 Check whether import policies are configured on MSDP peers.

Run the **display current-configuration configuration msdp** command on MSDP peers to view the current configurations in the MSDP view.

- If import policies are configured on MSDP peers, do as follows:
  - If the command output contains the configurations of the **peer peer-address sa-policy import** command without any parameter, it indicates that MSDP peers are disabled from receiving messages from the multicast source. Then run the **undo peer** *peer-address* **sa-policy import** command to delete the configurations of export policies.
  - If the command output contains the configurations of the **peer peer-address sa-policy import acl advanced-acl-number** or the **peer peer-address sa-policy import acl acl-name** command with an ACL specified, it indicates that MSDP peers can receive only the (S, G) entries permitted by the ACL. Then check whether ACL-related commands are run on the MSDP peers and whether (S, G) entries are permitted by the ACL. You can run the **undo peer** *peer-address* **sa-policy import** command to delete the configurations of the ACL or change the configurations of the ACL rule.
- If no import policies are configured on MSDP peers, go to **Step 6**.

Step 6 Check whether the current MSDP peer receives multicast data from the multicast source.

- If the current MSDP peer does not receive multicast data from the multicast source, troubleshoot the upstream device following the preceding steps.
- If the current MSDP peer receives multicast data from the multicast source, go to **Step 7**.

Step 7 Check whether the current MSDP peer is an RP.

Run the **display pim routing-table** command on the MSDP peer closest to the multicast source to view the routing table.

- If the (S, G) entry is without a **2MSDP** flag, it indicates that the MSDP peer is not an RP. Then change the configurations of the RP or MSDP peer on the PIM-SM network to ensure that the MSDP peer is an RP.
- If the MSDP peer is an RP, go to **Step 8**.

Step 8 Check whether import-source policies are configured on the current MSDP peer.

The **import-source** [**acl** { *acl-number* | *acl-name* }] command is used to enable an MSDP peer to filter the (S, G) entries to be advertised based on source addresses when creating SA messages. The MSDP peer can thus control the transmission of information about multicast sources. By default, SA messages can be used to advertise information about all known multicast sources.

Run the **display current-configuration configuration msdp** command on the MSDP peer closest to the multicast source to view the current configurations in the MSDP view.

- If import-source policies are configured on the MSDP peer, do as follows:
  - If the command output contains the configurations of the **import-source** command without any parameter, it indicates that the MSDP peer is disabled from advertising multicast source information. Then run the **undo import-source** command to delete the configurations of import-source policies.
  - If the command output contains the **import-source acl acl-number** or the **import-source acl acl-name** command with an ACL specified, it indicates that the MSDP peer advertises only (S, G) information matching the ACL. Then check whether ACL-related commands are run on the MSDP peer and whether (S, G) entries are permitted by the

Copyright © Huawei Technologies Co., Ltd.

ACL. Then run the **undo import-source** command to delete the configurations of the ACL or change the configurations of the ACL rule.

- If no import policies are configured on MSDP peers, go to **Step 9**.

Step 9 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding operation procedure
- Configuration files, log files, and alarm files of the device

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

6.2.6 Troubleshooting Cases

This section provides troubleshooting cases for Layer 3 multicast.

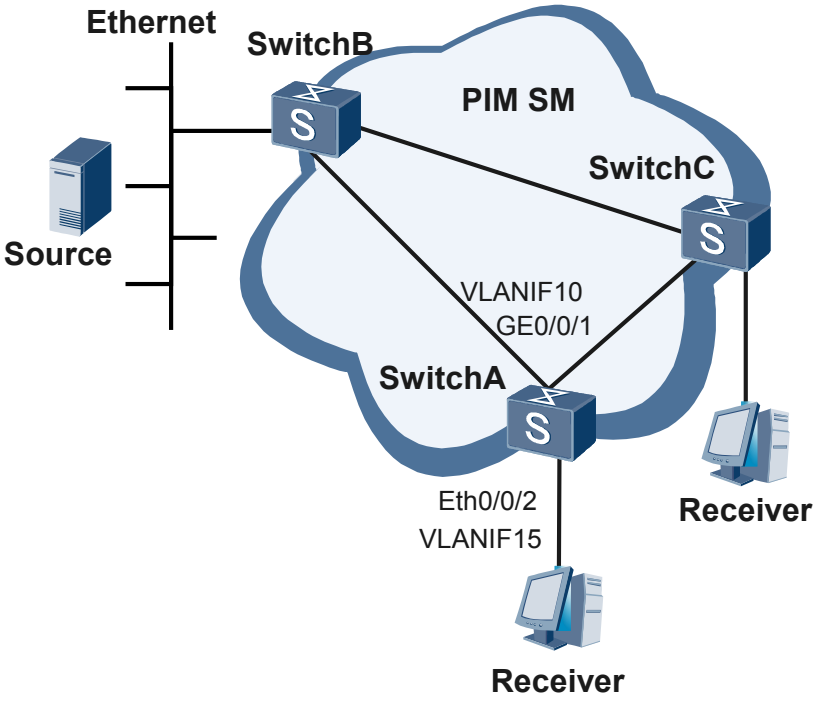
Receivers Attached to a Multicast Interface Experience Video Lagging

Fault Symptom

On the network shown in **Figure 6-8**, multicast services are deployed. Switch A and Switch C have Receivers attached to them. Receiver attached to Switch A experiences video lagging.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-8 Networking diagram of on-demand multicast programs on an interface



Fault Analysis

1. Check whether the multicast source works properly.

   Receiver attached to Switch C can properly receive multicast data. Therefore, it can be concluded that the multicast source is normal.

2. Check whether Receiver attached to Switch A has sent a Report message.

   On Switch A, run the **display igmp routing-table** command to check whether information about IGMP Report messages is displayed. Information about VLANIF 15 on Switch A is displayed:

   ```
   Total 1 entry

   00001. (*, 225.1.1.1)
         List of 1 downstream interface
          Vlanif15 (10.100.0.1),
                    Protocol: IGMP
   ```

   The command output indicates that Switch A has received a Report message.

3. Check whether multicast forwarding entries are correctly generated, that is, whether Switch A has a downstream interface to which Receiver attaches.

   Run the **display multicast forwarding-table** command on Switch A to check whether forwarding entries contain downstream interfaces. The multicast forwarding entry list contains the following information:

   ```
   1: Vlanif 15
   ```

   It indicates that Switch A has a downstream interface to which Receiver attaches.

4. Check the number of multicast packets sent and received by Switch A.

   - Run the **display this interface** command in the view of VLANIF 10 on Switch A to check the number of received multicast packets. The following information is displayed:

Copyright © Huawei Technologies Co., Ltd.

```
Input:  4161316 packets,  2562496780 bytes
   Unicast: 21839, Multicast: 4139477
```

- Run the **display this interface** command in the view of VLANIF 15 on Switch A to check the number of sent multicast packets. The following information is displayed:

```
Output:  366615 packets,  225759692 bytes
      Unicast: 3, Multicast: 366591
```

The preceding information shows that VLANIF 15 has received 4,139,477 multicast packets but VLANIF 15 has sent out only 366,591 multicast packets. This indicates that about 90% of the packets are lost.

Run the **display this** command in the view of VLANIF 15 on Switch A to check configurations of VLANIF 15. The following information is displayed:

```
igmp static-group 224.0.1.0
```

The preceding information shows that Receiver attached to Switch A has joined a multicast group whose address is in the reserved multicast group address range. (An interface board reserves the multicast group addresses 224.0.0.0 through 224.0.1.255 for protocol packets.)

Procedure

- Change the address of the multicast group that Receiver joins. Addresses 224.0.0.0 through 224.0.0.255 are reserved multicast group addresses that cannot be used for multicast data packet forwarding.

  After the preceding operations, multicast data packets can properly reach Receiver. The fault is rectified.

----End

Summary

Addresses 224.0.0.0 through 224.0.0.255 are reserved multicast group addresses that cannot be used for multicast data packet forwarding. Therefore, avoid using the addresses within this range as the group address of multicast data packets.

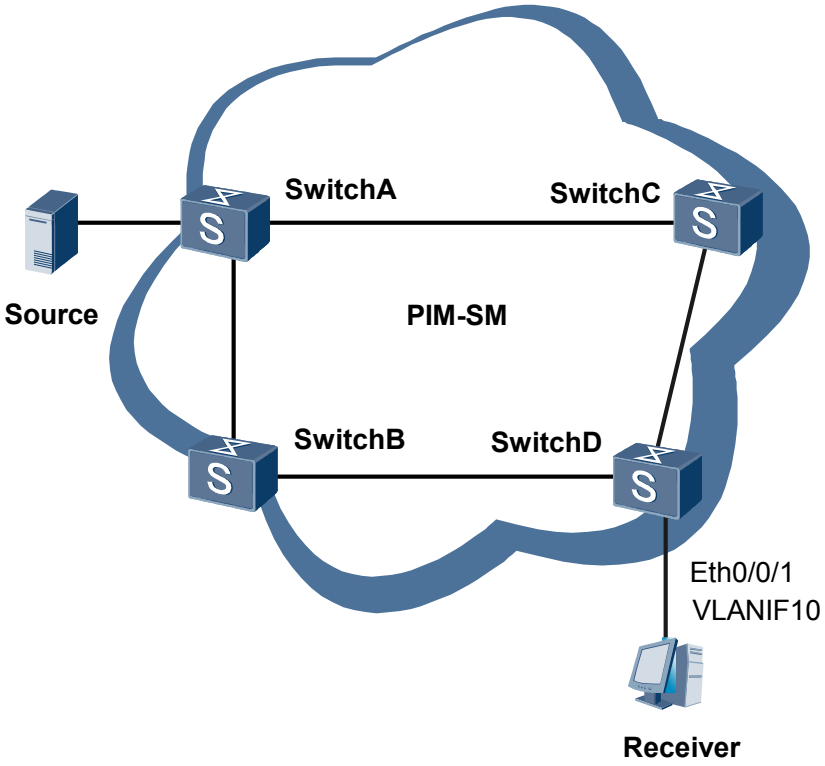
A Multicast Router Fails to Process BSR Messages Because the RPF Check Fails

Fault Symptom

On the network shown in **Figure 6-9**, multicast services are deployed. Switch A assumes the role of both BSR and RP. PIM-SM is configured on every Switch. Switch Switch D has an Receiver attached to it. After the configurations, Receiver cannot receive multicast traffic.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-9 Basic multicast networking



Fault Analysis

1. Run the **display pim neighbor** command on every switch to check whether PIM neighbor relationships are successfully set up.
2. On Switch D, run the **display igmp routing-table** command to check whether information about IGMP Report messages is displayed. Information about VLANIF 10 on Switch D is displayed:

```
Total 1 entry

00001. (*, 225.1.1.1)
      List of 1 downstream interface
       Vlanif10 (10.100.0.1),
                  Protocol: IGMP
```

   The preceding command output indicates that Switch D has received a Report message.
3. Run the **display pim rp-info** command on every switch to check whether RPs are successfully created. The command output shows that Switch D does not learn about the RP. A tester is then used to capture packets. Switch C is found to have sent a BSR message to Switch D.
4. On Switch D, run the **debugging pim event** command to locate the fault. The command output shows that Switch D ignores the BSR message sent by Switch C because the RPF check fails.
5. On Switch D, run the **display ip routing-table** command. The command output shows that the next hop of the route from Switch D to the BSR/RP is Switch B rather than Switch C.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Do as follows on Switch D:

Step 2 Run the **ip route-static** *ip-address* command to configure Switch C as the next hop of Switch D.

After the preceding operations, Switch D can normally learn the RP and Receiver can receive multicast data. The fault is cleared.

----End

Summary

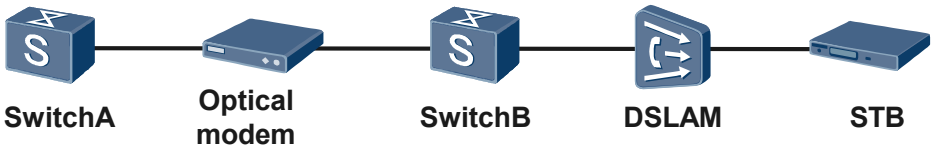
The RPF check failure will cause protocol packets unable to be processed. The RPF check affects the forwarding of both multicast data packets and protocol packets such as BSR packets. Therefore, in multicast service deployment, ensure that the unicast routing entries are correct to avoid the RPF check failure.

Users Cannot Watch IPTV Programs After QinQ Is Deployed

Fault Symptom

As shown in **Figure 6-10**, IPTV services are deployed. After QinQ is deployed on SwitchB, users cannot watch IPTV programs.

Figure 6-10 Network diagram



Fault Analysis

Compared with a common VLAN packet, a QinQ packet increases four bytes. That is, a QinQ packet has 1522 bytes. After QinQ is deployed on SwitchB, users cannot watch IPTV programs. A device along the link may not process packets with 1522 bytes.

1. Capture packets on the downlink interface of SwitchA and the uplink interface of SwitchB. The packets with 1522 bytes captured on the uplink interface of SwitchB are discarded on the downlink interface of SwitchA, indicating that packets with 1522 bytes are lost on the intermediate device.
2. Replace the optical modem with the tail fiber to connect SwitchA and SwitchB. Users can watch IPTV programs. The optical modem cannot process packets of 1522 or more bytes.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Replace the optical modem with the tail fiber to connect SwitchA and SwitchB.

After the preceding operation, users can watch IPTV programs. The fault is rectified.

----End

Summary

If packets cannot be captured onsite, configure a QinQ termination sub-interface on SwitchA and ping the packets with 1522 bytes destined for SwitchA on the DSLAM to check whether packets are lost on SwitchA.

If the QinQ configuration is incorrect, services cannot be forwarded after QinQ is configured.

Copyright © Huawei Technologies Co., Ltd.

7 Security

About This Chapter

7.1 AAA Troubleshooting
This chapter describes common causes of the authentication, authorization, and accounting (AAA) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.2 ARP Security Troubleshooting
This chapter describes common causes of ARP faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.3 NAC Troubleshooting
This chapter describes common causes of the network access control (NAC) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.4 DHCP Snooping Troubleshooting
This chapter describes common causes of Dynamic Host Configuration Protocol (DHCP) snooping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.5 Traffic Suppression Troubleshooting
This chapter describes common causes of traffic suppression faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

7.6 CPU Defense Troubleshooting
This chapter describes common causes of CPU defense faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.7 MFF Troubleshooting
This chapter describes common causes of MAC Forced Forwarding (MFF) faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

7.8 ACL Troubleshooting
This chapter describes common causes of ACL faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.9 PPPoE+ Troubleshooting

Copyright © Huawei Technologies Co., Ltd.

This chapter describes common causes of Point-to-Point Protocol over Ethernet (PPPoE) faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

7.1 AAA Troubleshooting

This chapter describes common causes of the authentication, authorization, and accounting (AAA) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.1.1 A User Fails in the RADIUS Authentication

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the Remote Authentication Dial In User Service (RADIUS) authentication failure.

Common Causes

This fault is commonly caused by one of the following:

- The user name or password is incorrect. For example, the user name does not exist, or the user name format (with or without the domain name) is different from the format configured on the Remote Authentication Dial In User Service (RADIUS) server.
- The RADIUS configuration on the S3700 is incorrect, including the authentication mode and the RADIUS server template.
- The port number and shared key configured on the S3700 are different from those on the RADIUS server.
- The number of online users reaches the maximum value.

Troubleshooting Flowchart

A user fails to pass the Authentication Dial In User Service (RADIUS) authentication.

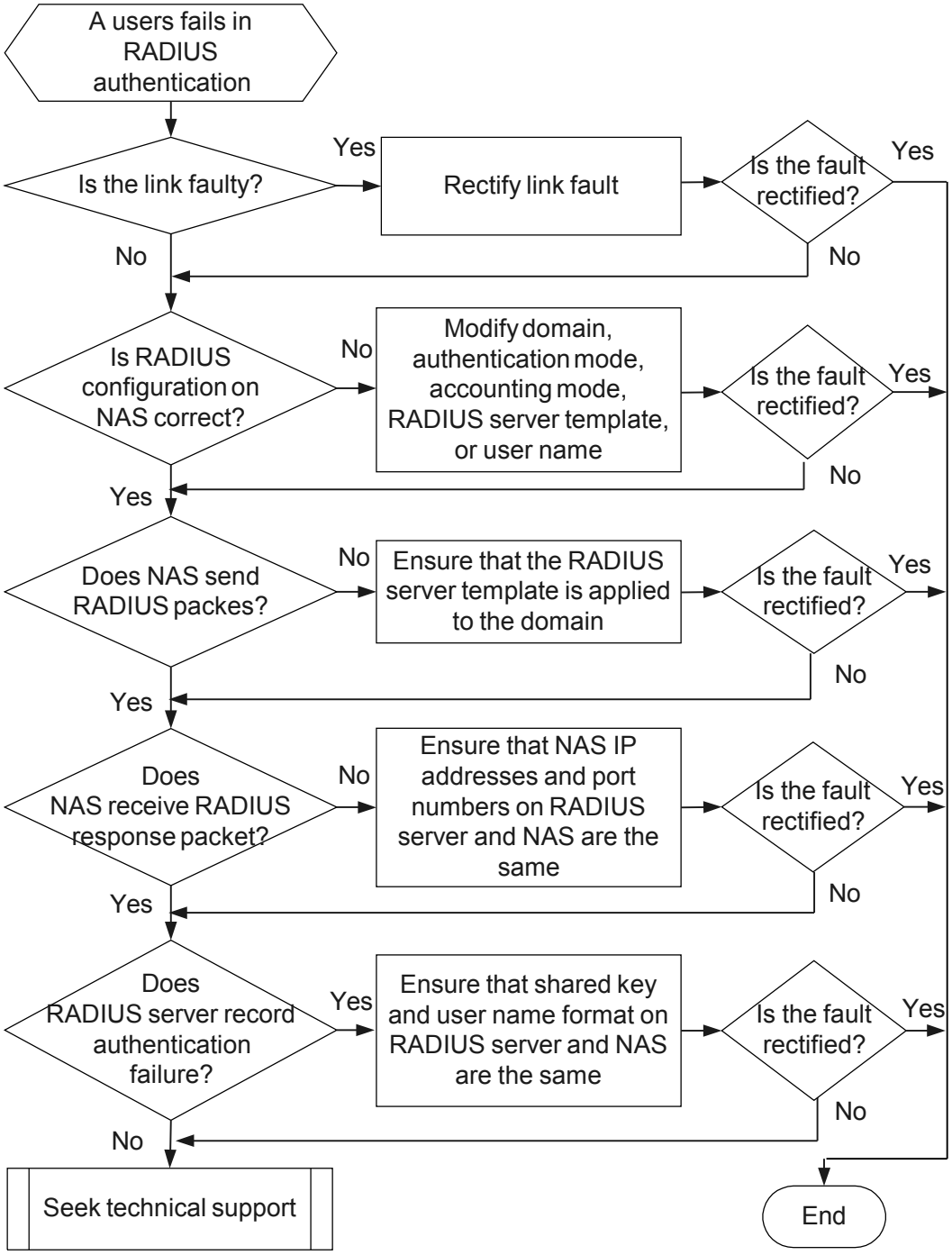
The troubleshooting roadmap is as follows:

- Check whether the link between the S3700 and the RADIUS server works properly.
- Check the RADIUS configuration on the S3700, including the domain name, RADIUS server template, authentication mode, and accounting mode.
- Check whether the network access server (NAS) IP address, port number, and shared key configured on the RADIUS server are the same as those configured on the S3700.

Figure 7-1 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-1 Troubleshooting flowchart for RADIUS authentication failure



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **ping** command to check whether the link between the network access server (NAS), namely, the S3700, and the RADIUS server works properly.

- If the ping operation fails, rectify the link fault according to A Ping Operation Fails.
- If the ping operation succeeds, go to step 2.

Step 2 Check that the RADIUS configuration on the S3700 is correct.

Check the RADIUS configuration to ensure that:

- The authentication scheme bound to the user domain is RADIUS authentication.
- The correct RADIUS server template is bound to the domain. The IP address and port of the authentication server and accounting server are set correctly in the template.
- The user name format and shared key specified in the template are the same as those on the RADIUS server.

Among the above three check items, the latter two items are required to check the configurations on the RADIUS server, go to step 3.

Action	Command
Check the domain configuration.	**display domain**
Check which RADIUS server template is bound to the domain.	**display domain name** *domain-name*
Check the authentication scheme bound to the domain.	**display authentication-scheme**
Check the accounting scheme bound to the domain.	**display accounting-scheme**
Check the configuration of the RADIUS server template.	**display radius-server configuration**

Step 3 Check information about the RADIUS packets sent and received by the S3700.

Run the **debugging radius packet** command in the user view to enable RADIUS packet debugging. Check whether any RADIUS packets are sent and received by the S3700.

```
<Quidway> debugging radius packet
<Quidway> terminal debugging
<Quidway> terminal monitor
```

CAUTION

Debugging affects the system performance. So, after debugging, run the **undo debugging all** command to disable the debugging immediately.

- If no debugging information is displayed, the NAS configuration is incorrect. Check that the RADIUS server template is bound to the domain.

Copyright © Huawei Technologies Co., Ltd.

The following configuration file shows that the RADIUS server template **radius** is bound to the domain **huawei**.

```
#
radius-server template radius
 radius-server authentication 1.1.1.1 1645
#
aaa
 authentication-scheme default
 authentication-scheme aaa
  authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme aaa
  radius-server  radius
```

- If debugging information is displayed, proceed according to the debugging information.

Debugging Information	Solution
Nov 10 2010 15:23:34.260.6 Quidway RDS/7/debug2: Radius Sent a Packet Server Template: 0 Server IP : 192.168.1.128 Protocol: Standard	The RADIUS module sent an authentication packet. This message indicates that the S3700 can send RADIUS authentication packets.
Nov 10 2010 15:23:34.260.6 Quidway %% 01RDS/4/RDAUTHDOWN(l): RADIUS authentication server (IP: 192.168.1.128) is down!	The RADIUS authentication server did not send any authentication response packet. This may because the link between the S3700 and the RADIUS server fails or the RADIUS server has not restarted. Check that the NAS IP address and RADIUS service port numbers configured on the RADIUS server are the same as those configured on the NAS, and that the RADIUS service is enabled.

Copyright © Huawei Technologies Co., Ltd.

Debugging Information	Solution
Nov 10 2010 15:23:34.260.6 Quidway RDS/7/debug2: [RDS (Evt):] Send a msg (Auth reject) Nov 10 2010 15:23:34.260.7 Quidway RDS/7/debug2: [RDS (Msg):]Msg type :Auth reject [RDS (Msg):]UserID :16005 [RDS (Msg):]Template no:88.99 [RDS (Msg):]Authmethod :(pap) [RDS (Msg):]ulSrcMsg :Auth req [RDS (Msg):]szBitmap :00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	The RADIUS authentication server returned an authentication failure packet. The possible causes of authentication failure are: ● The NAS IP address and the shared key are not configured on the RADIUS server. ● The shared key configured on the RADIUS server is different from the shared key configured on the NAS. ● The user account is not configured on the RADIUS server, or the user name format configured in the RADIUS server template is different from that on the RADIUS server. For example, the NAS sends the user name without the domain name but the RADIUS server requires the user name with the domain name. ● The password entered by the user is different from the password configured on the RADIUS server. If any of the preceding errors exist, modify the configuration on the RADIUS server. After configuration modification, check whether the user can pass the authentication. If the fault persists, go to step 4.

Step 4 Check whether the number of online users reaches the maximum.

Both the NAS and RADIUS server have a limit the number of online users. Run the **display access-user** command on the S3700 to check the number of online users.

- If the number of online users reaches the maximum, you do not need to take any action. The user can log in after the number of online users falls below the maximum.
- If the number of online users does not reach the maximum, check the maximum number of online users set on the RADIUS server. If the maximum number of online users set on the RADIUS server is not reached, go to step 5.

Step 5 Check the user type.

- If the user is a Telnet user or an FTP user, rectify the fault according to "**3.5.1 The User Fails to Log in to the Server Through Telnet**" or "**3.6.1 The User Fails to Log in to the Server Through FTP**."
- If the user is a network access user, rectify the fault according to "**7.3 NAC Troubleshooting**."

Step 6 If the fault persists, collect the following information and contact Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.1.2 A User Fails in the HWTACACS Authentication

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the Huawei Terminal Access Controller Access Control System (HWTACACS) authentication failure.

Common Causes

This fault is commonly caused by one of the following:

- The user name or password is incorrect. For example, the user name does not exist, or the user name format (with or without the domain name) is different from the format configured on the Huawei Terminal Access Controller Access Control System (HWTACACS) server.
- The HWTACACS configuration on the S3700 is incorrect, including the authentication mode and HWTACACS server template.
- The port number and shared key configured on the S3700 are different from those on the HWTACACS server.
- The number of online users reaches the maximum value.

Troubleshooting Flowchart

A user fails to pass the Huawei Terminal Access Controller Access Control System (HWTACACS) authentication.

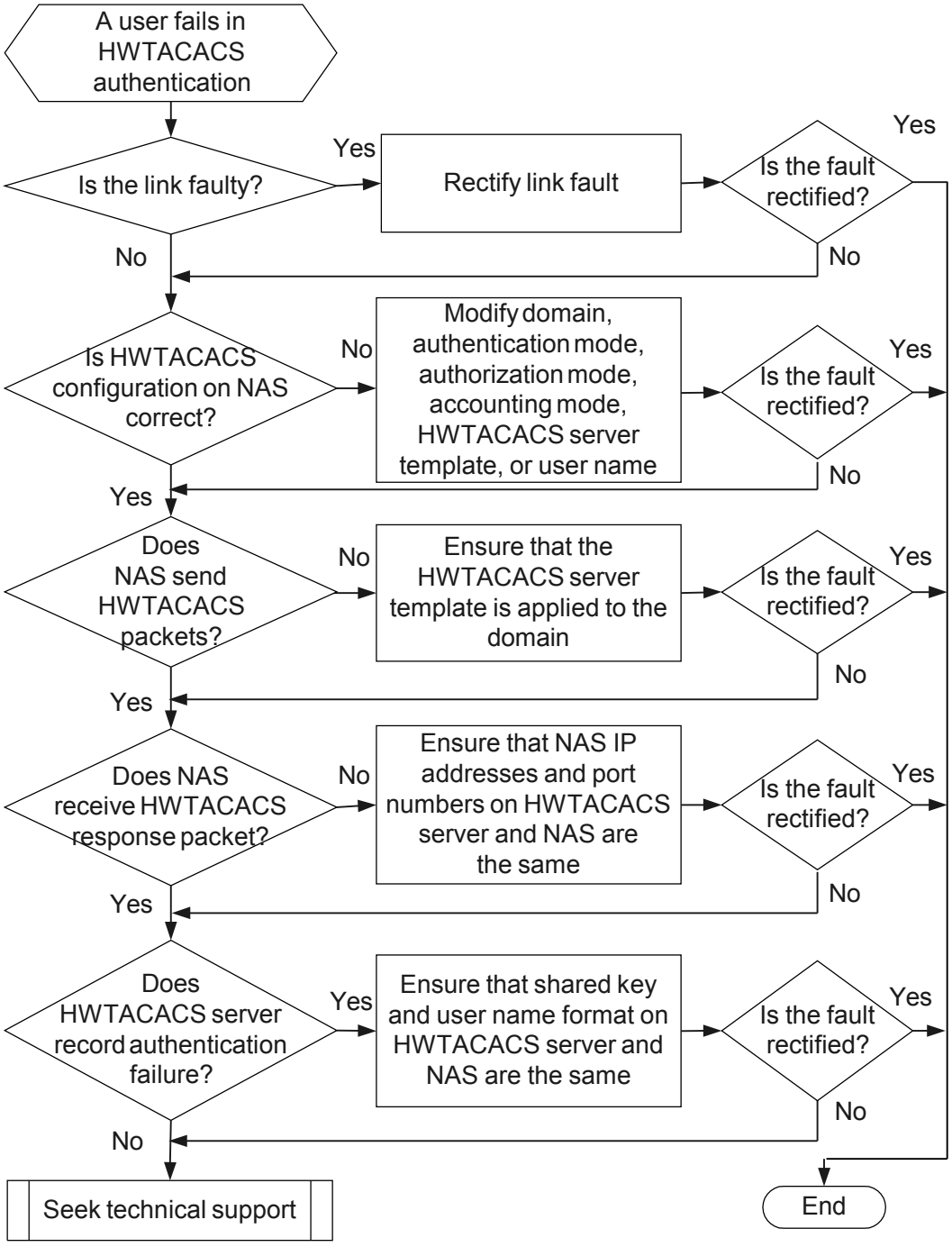
The troubleshooting roadmap is as follows:

- Check whether the link between the S3700 and the HWTACACS server works properly.
- Check the HWTACACS configuration on the S3700, including the domain name, HWTACACS server template, authentication mode, authorization mode, and accounting mode.
- Check whether the network access server (NAS) IP address, port number, and shared key configured on the HWTACACS server are the same as those configured on the S3700.

Figure 7-2 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-2 Troubleshooting flowchart for HWTACACS authentication failure



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **ping** command to check whether the link between the network access server (NAS), namely, the S3700, and the HWTACACS server works properly.

- If the ping operation fails, rectify the link fault according to A Ping Operation Fails.
- If the ping operation succeeds, go to step 2.

Step 2 Check the HWTACACS configuration on the S3700.

Check the HWTACACS configuration to ensure that:

- The authentication scheme bound to the user domain is HWTACACS authentication.
- The correct HWTACACS server template is bound to the domain. The IP address and port of the authentication server, authorization server, and accounting server are set correctly in the template.
- The user name format and shared key specified in the template are the same as those on the HWTACACS server.

Among the above three check items, the latter two items are required to check the configurations on the HWTACACS server, go to step 3.

Action	Command
Check the domain configuration.	**display domain**
Check which HWTACACS server template is bound to the domain.	**display domain name** *domain-name*
Check the authentication scheme bound to the domain.	**display authentication-scheme**
Check the authorization scheme bound to the domain.	**display authorization-scheme**
Check the accounting scheme bound to the domain.	**display accounting-scheme**
Check the configuration of the HWTACACS server template.	**display hwtacacs-server template**

Step 3 Check information about the HWTACACS packets sent and received by the S3700.

Run the **debugging hwtacacs all** command in the user view to enable HWTACACS packet debugging. Check whether any HWTACACS packets are sent and received by the S3700.

```
<Quidway> debugging hwtacacs all
<Quidway> terminal debugging
<Quidway> terminal monitor
```

CAUTION

Debugging affects the system performance. So, after debugging, run the **undo debugging all** command to disable the debugging immediately.

Copyright © Huawei Technologies Co., Ltd.

- If no debugging information is displayed, the NAS configuration is incorrect. Check that the HWTACACS server template is applied to the domain.

  The following configuration file shows that the HWTACACS server template **hwtacacs** is bound to the domain **huawei**.

```
#
hwtacacs-server template hwtacacs
 hwtacacs-server authentication 2.2.2.2
#
aaa
 authentication-scheme default
 authentication-scheme aaa
  authentication-mode hwtacacs
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme aaa
  hwtacacs-server hwtacacs
#
```

- If debugging information is displayed, proceed according to the debugging information.

Debugging Information	Solution
Nov 10 2010 15:43:35.500.6 Quidway TAC/7/Event:HandleReqMsg: Session status is not connect now. Nov 10 2010 15:43:35.500.7 Quidway TAC/7/Event:statistics: transmit flag: 1-SENDPACKET, server flag: 0-authentication, packet flag: 0xff Nov 10 2010 15:43:35.550.1 Quidway TAC/7/Event:HandleResp: Session status is connect now. Nov 10 2010 15:43:35.550.2 Quidway TAC/7/Event: Tac packet sending success! version:c0 type:1-authentication sequence:1 flag:1-UNENCRYPTED_FLAG session id:908 length:24 serverIP: 10.138.88.209 vrf:0	The HWTACACS module sent an authentication packet. This message indicates that the S3700 can send HWTACACS authentication packets.
Nov 10 2010 15:49:18.430.6 Quidway TAC/7/Event:HandleReqMsg: Session status is not connect now. Nov 10 2010 15:49:18.430.7 Quidway TAC/7/Event:statistics: transmit flag: 1-SENDPACKET, server flag: 0-authentication, packet flag: 0xff Nov 10 2010 15:49:18.480.2 Quidway TAC/7/Event:HandleResp: Session status is connect now. Nov 10 2010 15:49:18.480.3 Quidway TAC/7/Event: Tac send packet error!	The HWTACACS authentication server did not send any authentication response packet. This may because the link between the S3700 and the HWTACACS server is Down, the HWTACACS server has not restarted, or the HWTACACS server fails. In this case, check that the NAS IP address and HWTACACS service port numbers configured on the HWTACACS server are the same as those configured on the NAS, and that the HWTACACS service is enabled.

Copyright © Huawei Technologies Co., Ltd.

Debugging Information	Solution
Nov 10 2010 16:02:35.760.1 Quidway TAC/7/Event: version:c0 type:AUTHEN_REPLY seq_no:6 flag:UNENCRYPTED_FLAG session_id:0x4ff8 length:6 pstPacketAll->ulDataLen:6 pstAuthenReply:ucStatus=2 ucflags=0 usServerMsgLen=0 usDataLen=0 status:AUTHEN_STATUS_FAIL flag:REPLY_FLAG_ECHO server_msg len:0 data len:0 server_msg: data:	The HWTACACS server returned an authentication failure packet. The possible causes of authentication failure are: ● The NAS IP address and the shared key are not configured on the HWTACACS server. ● The shared key configured on the HWTACACS server is different from the shared key configured on the NAS. ● The user account is not configured on the HWTACACS server, or the user name format configured in the HWTACACS server template is different from that on the HWTACACS server. For example, the NAS sends the user name without the domain name but the HWTACACS server requires the user name with the domain name. ● The password entered by the user is different from the password configured on the HWTACACS server. If any of the preceding errors exist, modify the configuration on the HWTACACS server. After configuration modification, check whether the user can pass the authentication. If the fault persists, go to step 4.

Step 4 Check whether the number of online users reaches the maximum.

Both the NAS and HWTACACS server have a limit on the number of online users. Run the **display access-user** command on the S3700 to check the number of online users.

- If the number of online users reaches the maximum, you do not need to take any action. The user can log in after the number of online users falls below the maximum.
- If the number of online users does not reach the maximum, check the maximum number of online users set on the HWTACACS server. If the maximum number of online users set on the HWTACACS server is not reached, go to step 5.

Step 5 Check the user type.

- If the user is a Telnet user or an FTP user, rectify the fault according to "**3.5.1 The User Fails to Log in to the Server Through Telnet**" or "**3.6.1 The User Fails to Log in to the Server Through FTP**."
- If the user is a network access user, rectify the fault according to "**7.3 NAC Troubleshooting**."

Step 6 If the fault persists, collect the following information and contact Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.1.3 Troubleshooting Cases

This section presents several AAA troubleshooting cases.

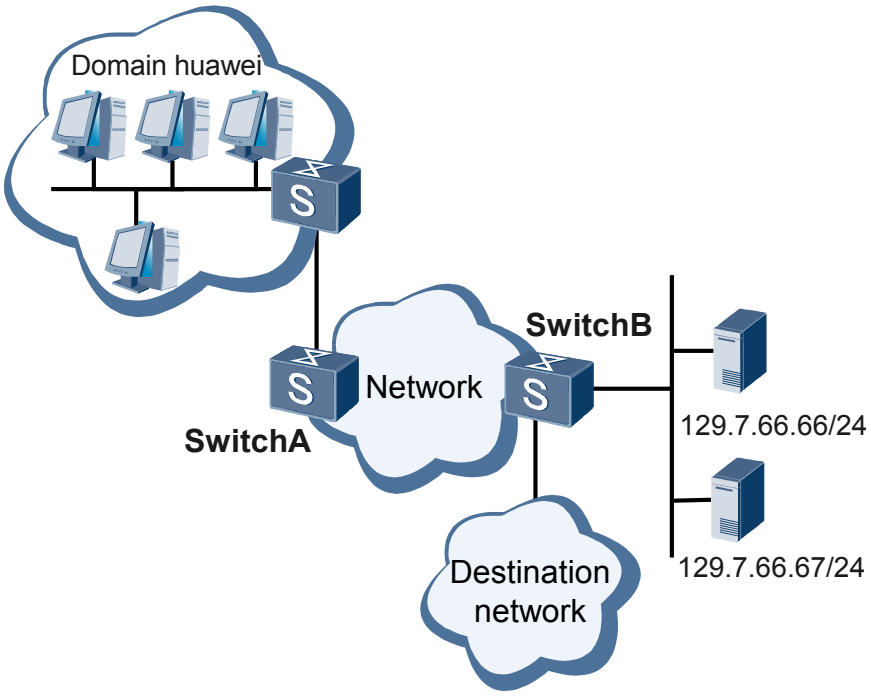
Users Are Forced Offline 10-plus Seconds After They Log In

Fault Symptom

On the network shown in **Figure 7-3**, users access the network through Switch B, which authenticates, authorizes, and charges the users.

Originally, Switch B uses the RADIUS protocol to perform authentication and accounting. After the RADIUS server fails, the administrator adopts local authentication temporarily.

Figure 7-3 Networking diagram of user access



Copyright © Huawei Technologies Co., Ltd.

After the configurations, users are forced offline 10-plus seconds after they log in.

Fault Analysis

1. Run the **display trapbuffer** and **display logbuffer** commands on Switch B to check whether a trap or a log indicating that users are forced offline is recorded. The following trap information is displayed:

   ```
   AAA cut user!
   ```

2. Run the **display current-configuration** command on Switch B to check the AAA configuration. The command output shows that local authentication and RADIUS accounting are adopted. Details are as follows:

   ```
   radius-server template provera
    radius-server shared-key xxxxxx
    radius-server authentication 129.7.66.66 1645
    radius-server accounting 129.7.66.66 1646
    undo radius-server user-name domain-included
   #
   aaa
    local-user telenor password cipher xxxxxxx
    authentication-scheme default
    #
    authentication-scheme provera
     authentication-mode  radius  local
    #
    authorization-scheme default
    #
    accounting-scheme default
    accounting-scheme provera
     accounting-mode radius
     accounting realtime 10
    #
    domain default
    #
    domain huawei
     authentication-scheme  provera
     accounting-scheme provera
     radius-server provera
    #
   user-interface vty 0 4
    authentication-mode aaa
    user privilege level 15
    set authentication password cipher xxxxxxx
    history-command max-size 256
    screen-length 15
   ```

   Because the RADIUS server is unavailable, real-time accounting fails. You can run the **accounting interim-fail** command to configure a real-time accounting failure policy to determine whether to keep users online or force users offline after the real-time accounting fails. If the **accounting interim-fail** command is not configured, Switch B adopts the default setting, that is, forcing users offline when real-time accounting fails.

   It can therefore be concluded that RADIUS accounting causes users to be forced offline. The period after which login users are forced offline is determined by the retransmission timeout period and retransmission times, which are configured by using the **radius-server timeout** and **radius-server retransmit** commands respectively. By default, data is retransmitted every 5 seconds for three consecutive times. If data fails to be retransmitted 15 seconds after login, users are forced offline.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **aaa** command to enter the AAA view.

Step 3 Run the **domain huawei** command to enter the Huawei domain view.

Step 4 Run the **undo accounting-scheme provera** command to configure the default accounting scheme for users in the domain, that is, non-accounting.

You can select any of the following methods to clear the fault:

- Run the **accounting-mode none** command to change the accounting mode to non-accounting.
  - Administrator users such as Telnet users and FTP users are not charged, and therefore you can change their accounting mode to non-accounting.
- Run the **accounting interim-fail online** command to configure to keep users online when real-time accounting fails.
- Run the **undo accounting-scheme provera** command to configure the default accounting scheme for the domain, that is, non-accounting.

In this troubleshooting case, Switch B mainly authenticates Telnet users that do not need to be charged, and therefore the non-accounting scheme is applicable. You can run the **undo accounting-scheme provera** command to configure the non-accounting scheme.

After the preceding configurations, users can log in without being forced offline. The fault is cleared.

----End

Summary

On the access network using AAA authentication, if the remote server is unavailable and local authentication is adopted, the accounting scheme must be non-accounting. Otherwise, users are forced offline.

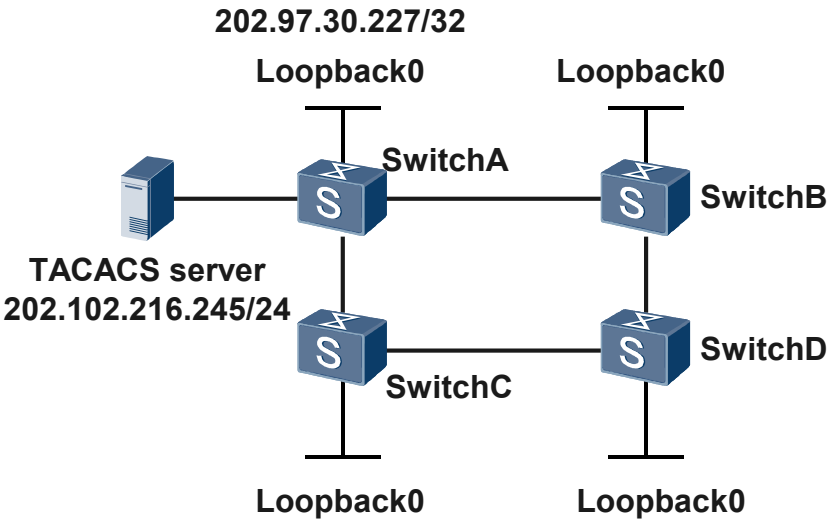
A User Cannot Pass the HWTACACS Authentication with Valid User Name and Password

Fault Symptom

As shown in **Figure 7-4**, the four switches at the core layer are in the same autonomous system (AS). They are configured with the Interior Border Gateway Protocol (IBGP), Intermediate System To Intermediate System (IS-IS), AAA, QoS, and the Simple Network Management Protocol (SNMP). The customer wants to configure a private AS number on the switches, replace IBGP with the Exterior Border Gateway Protocol (EBGP), and replace IS-IS with the Open Shortest Path First (OSPF). The IS-IS routing table contains only the routes to the IP addresses of connected interfaces and loopback interfaces.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-4 HWTACACS authentication at the core layer



After the configuration, the user fails to pass the Huawei Terminal Access Controller Access-Control System (HWTACACS) authentication by using the valid user name and password.

Fault Analysis

1. Check the user name and password configured on the HWTACACS server. The configured user name and password are the same as those entered by the user.
2. Run the **ping** command on SwitchA to ping the HWTACACS server. The ping operation is successful.
3. Run the **display current-configuration** command on SwitchA to check the HWTACACS configuration. The following configuration is displayed in the HWTACACS server template:

   ```
   hwtacacs-server source-ip 202.97.30.227
   ```

   In the preceding information, 202.97.30.227 is the IP address of the loopback interface on SwitchA.

   This IP address is contained in the IS-IS routing table and is used as the source IP address of HWTACACS packets sent by SwitchA. The IS-IS configuration has been deleted; therefore, SwitchA cannot receive the authentication response packet with the destination address 202.97.30.227 sent from the HWTACACS server. This may be the cause for the HWTACACS authentication failure.
4. Run the **ping -a 202.97.30.227 202.102.216.245** command on SwitchA to check whether the loopback interface address can ping the IP address of the HWTACACS server. Here, the IP address of the HWTACACS server is 202.102.216.245. The ping operation fails.
5. Run the **display ip routing-table** command on SwitchA. The command output shows that the IP address of this loopback interface is not advertised by the OSPF protocol.

   According to the preceding information, you can confirm that the authentication fails because the IS-IS configuration is deleted and the OSPF protocol does not advertise the loopback interface address.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** *process-id* command to enter the OSPF view.

Step 3 Run the **area** *area-id* command to enter the OSPF area view.

Step 4 Run the **network** *address wildcard-mask* command to advertise the IP address of loopback interface.

After the configuration is complete, the user can log in by using the user name and password.

----End

Summary

Before modifying the routing protocol configuration, record the current configuration. After modifying the configuration, check whether the new configuration meets the network requirements and whether the modification has impacts on other configurations.

A Telnet User Fails to Log In Because the User Account Is Not Configured on the RADIUS Server

Fault Symptom

On the S3700, 802.1x is enabled and the authentication mode is set to Remote Authentication Dial In User Service (RADIUS) authentication. After the configuration, 802.1x users pass the authentication successfully, but a Telnet user fails to log in to the S3700 by using the local user account.

Fault Analysis

1. The 802.1x users pass the authentication, indicating that the link between the S3700 and the RADIUS server works properly.
2. Run the **display current-configuration** command on the S3700 to check the current configuration.

```
.......
 dot1x enable
#
radius-server template remote
 radius-server shared-key 123456
 radius-server authentication 192.168.1.27 1645
 radius-server accounting 192.168.1.27 1646
#
.......
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 dot1x enable
 dot1x max-user 1
 dot1x port-method port
 dot1x reauthenticate
.......
aaa
 authentication-scheme default
 authentication-scheme cams
  authentication-mode  radius
 #
```


Copyright © Huawei Technologies Co., Ltd.

```
 authorization-scheme default
 authorization-scheme cams
  authorization-mode  none
 #
 accounting-scheme default
 accounting-scheme account
 #
 domain default
  authentication-scheme  cams
  authorization-scheme cams
  accounting-scheme cams
  radius-server remote
#
......
#
user-interface maximum-vty 15
user-interface con 0
user-interface vty 0 14
 authentication-mode aaa
 user privilege level 15
 idle-timeout 0 0
#
```

The preceding information indicates that the user domain is **default**, the authentication mode is RADIUS authentication, and the authorization mode is none. The 802.1x users use port-based 802.1x authentication. The Telnet user fails in the RADIUS authentication. The possible cause is that the user name and password of the Telnet user is not configured on the RADIUS server.

3. Check the configuration of the RADIUS server. The user name and password of the Telnet user is not found on the RADIUS server.

To rectify the fault, add the user name and password of the Telnet user to the RADIUS server or configure the authentication mode of the Telnet user to local authentication.

Procedure

- Add the user name and password of the Telnet user to the RADIUS server. For the configuration procedure, see the configuration guide of the RADIUS server.
- Configure the authentication mode of the Telnet user to local authentication on the S3700.

  Create a new domain for the Telnet user.

```
<Quidway> system-view
[Quidway] aaa
[Quidway-aaa] domain telnet
[Quidway-aaa-domain-telnet]
```

  Use the default authentication, authorization, and accounting schemes in the domain, that is, local authentication, local authorization, and no accounting.

```
<Quidway> display domain name telnet

  Domain-name                    : telnet
  Domain-state                   : Active
  Authentication-scheme-name     : default
  Accounting-scheme-name         : default
  Authorization-scheme-name      : -
  Service-scheme-name            : -
  RADIUS-server-template         : -
  HWTACACS-server-template       : -

<Quidway> display authentication-scheme default

  Authentication-scheme-name    : default
```


Copyright © Huawei Technologies Co., Ltd.

```
  Authentication-method         : Local
  Authentication-super method   : Super authentication-super
<Quidway> display authorization-scheme default
------------------------------------------------------------------------------
 Authorization-scheme-name   : default
 Authorization-method        : Local
......
<Quidway> display accounting-scheme default

  Accounting-scheme-name                : default
  Accounting-method                     : None
```

Create a local user whose user name contains the domain name. The Telnet user needs to enter the domain name for authentication.

```
<Quidway> system-view
[Quidway] aaa
[Quidway-aaa] local-user telnetuser@telnet password simple 123456
[Quidway-aaa] local-user telnetuser@telnet service-type telnet
```

----End

Summary

You are advised to use different authentication modes for access users (such as 802.1x user), Telnet users, and Secure Shell (SSH) users. When a Telnet user fails to log in to the S3700, the possible cause is that an incorrect authentication scheme is configured in the VTY user interface view and AAA view of the S3700, or on the remote authentication server.

7.2 ARP Security Troubleshooting

This chapter describes common causes of ARP faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.2.1 The ARP Entry of an Authorized User Is Modified Maliciously

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for malicious modification to the ARP entry of an authorized user.

Common Causes

This fault is commonly caused by the following:

- An attacker sends bogus ARP packets to modify the ARP entry of the authorized user.

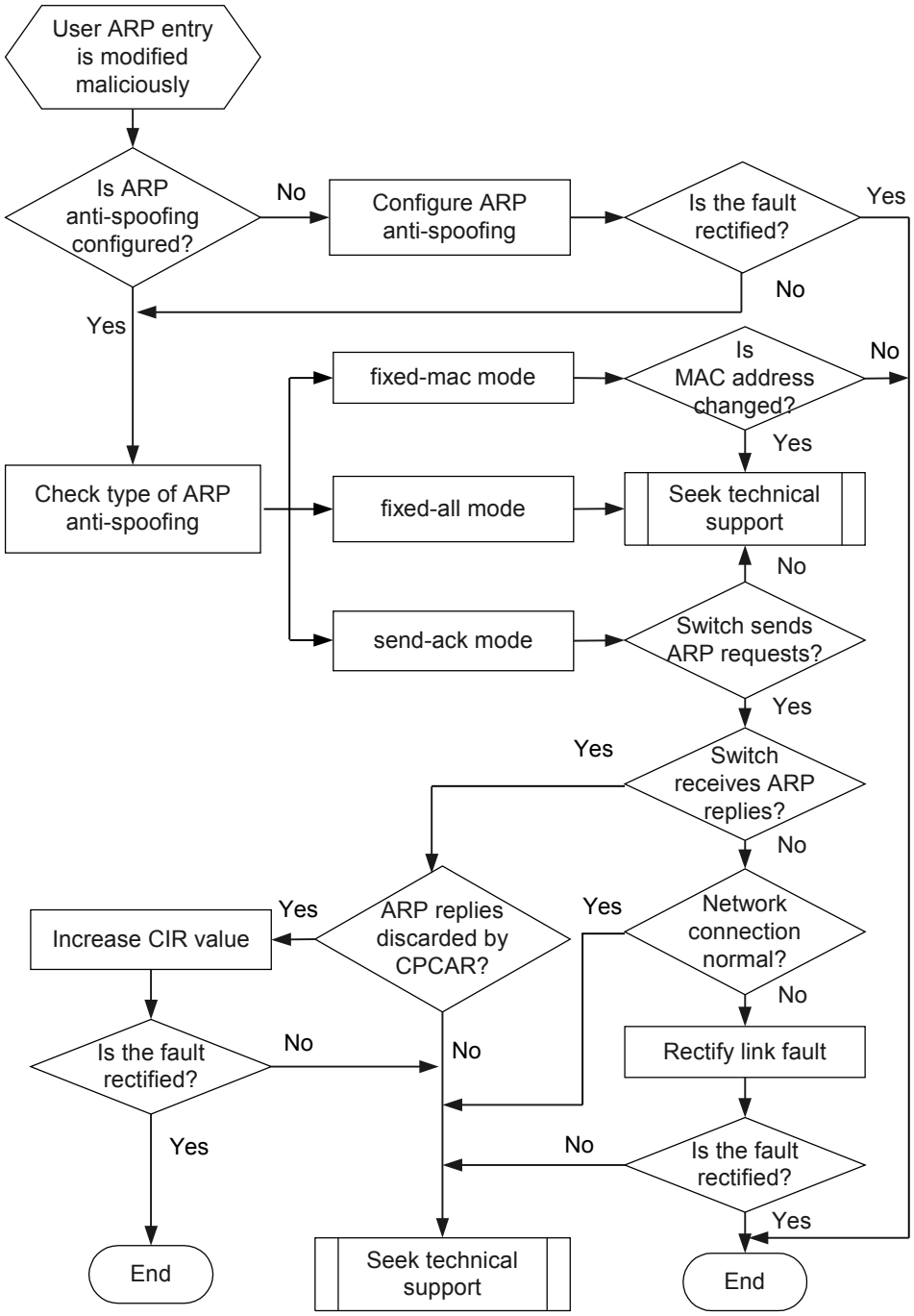
Troubleshooting Flowchart

An authorized user is disconnected from the Internet, but the links and routes are normal. The possible cause is that an attacker sends bogus ARP packets to modify the ARP entry of the user on the gateway. As a result, this user is disconnected from the network.

Figure 7-5 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-5 Troubleshooting flowchart for malicious modification to the ARP entry of an authorized user



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **display arp anti-attack configuration entry-check** command on the S3700 to check that ARP anti-spoofing is enabled.

- If the following information is displayed, ARP anti-spoofing is not enabled.
  ```
  ARP anti-attack entry-check mode: disabled
  ```
  Run the **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable** command to enable ARP anti-spoofing.

  NOTE

  Before enabling ARP anti-spoofing, run the **reset arp interface vlanif** *vlan-id* command to delete the ARP entries learned by the user-side interface.
- If the mode of ARP anti-spoofing is set to **send-ack**, go to step 2.
- If the mode of ARP anti-spoofing is set to **fixed-mac**, go to step 3.
- If the mode of ARP anti-spoofing is set to **fixed-all**, go to step 4.

Step 2 Perform the following steps to locate the fault in **send-ack** mode.

1. Capture packets on the user-side interface by configuring port mirroring. If the S3700 does not send any ARP request, go to step 4.
2. If the S3700 sends ARP requests but does not receive any ARP reply, check that the network connection between the S3700 and the user is normal.
3. If the S3700 receives ARP reply packets from the user, run the **display cpu-defend statistics packet-type arp-reply** command to check statistics about ARP reply packets. If the number of dropped ARP reply packets keeps increasing, the possible cause is that the rate of ARP reply packets exceeds the CPCAR. In this case, increase the committed information rate (CIR) by using the **car** command.
4. If the fault persists, go to step 4.

Step 3 Run the **display arp all | include** *ip-address* command to check the modified information in the ARP entry.

If the interface number or VLAN ID is changed, you do not need to take any action because it is normal in **fixed-mac** mode. If the MAC address is changed, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.2

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

7.2.2 The Gateway Address Is Changed Maliciously

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for gateway address spoofing attacks.

Common Causes

This fault is commonly caused by one of the following:

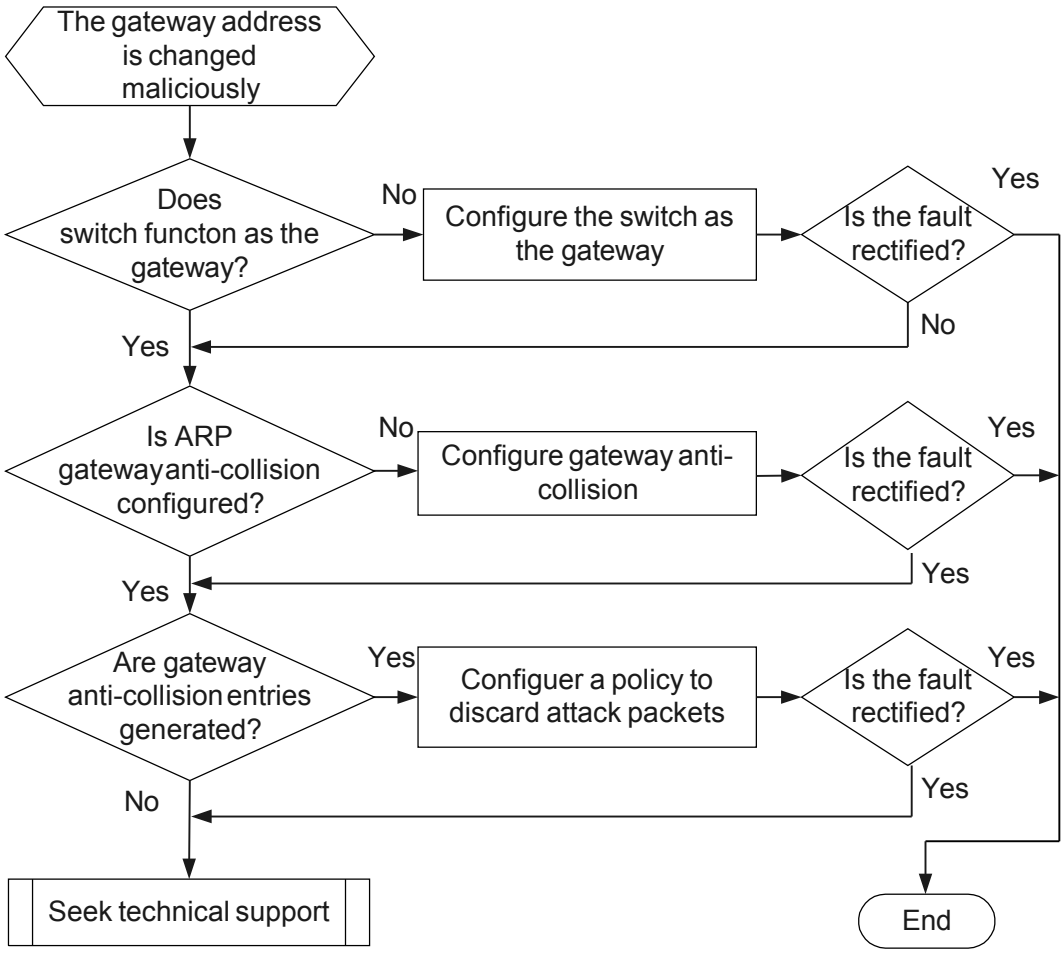
- An attacker sends bogus gratuitous ARP packets to users. Users change their gateway address after receiving the gratuitous ARP packets.
- An attacker sends bogus ICMP unreachable packets or ICMP redirect packets to users.

Troubleshooting Flowchart

An attacker sends gratuitous ARP packets with the source IP address being the IP address of the gateway on the LAN. After receiving the gratuitous ARP packets, hosts on the LAN change their gateway MAC address to the MAC address of the attacker. As a result, the hosts cannot access the network.

Figure 7-6 shows the troubleshooting flowchart.

Figure 7-6 Troubleshooting flowchart for gateway address spoofing



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the S3700 functions as the gateway. If the S3700 is not the gateway, the gateway anti-collision function does not take effect.

You can use either of the following methods to check whether the S3700 is the gateway:

- Run the **display arp all** command to view the type of the ARP entry corresponding to the gateway IP address.

  If the ARP entry type is displayed as **I-**, the gateway IP address is an interface address on the S3700.

```
<Quidway> display arp all
IP ADDRESS   MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                       VLAN
------------------------------------------------------------------------------
1.1.1.1      0022-0033-0044            I -         Vlanif10
```

- Run the **display ip routing-table** *gateway address* command to check whether a route to the gateway address exists.

  If a route to the gateway address is displayed in the command output, the S3700 is the gateway.

```
<Quidway> display ip routing-table 1.1.1.1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

1.1.1.1/24          Direct 0    0           D    127.0.0.1       InLoopback0
```

If the S3700 is not the gateway, configure it as the user gateway.

Step 2 Run the **display arp anti-attack configuration gateway-duplicate** command to check that ARP gateway anti-collision is enabled.

If ARP gateway anti-collision is not enabled, run the **arp anti-attack gateway-duplicate enable** command to enable this function.

Step 3 Run the **display arp anti-attack gateway-duplicate item** command to check the anti-collision entries.

- If an entry is displayed, you can find the IP address, MAC address, and source interface of the attacker from the entry. Add the attacker to the blacklist or configure a blackhole MAC entry according to attacker information. Subsequently, packets from the attacker will be discarded.
- If no entry is displayed, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure

Copyright © Huawei Technologies Co., Ltd.

- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.1

Relevant Logs

None.

7.2.3 User Traffic Is Interrupted by a Large Number of Bogus ARP Packets

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for traffic interruption caused by a large number of bogus ARP packets.

Common Causes

This fault is commonly caused by the following:

- An attacker sends a large number of bogus ARP requests, thus increasing the load of the destination network segment. If Layer 3 interfaces are configured on the S3700, the ARP requests are sent to the CPU, causing a high CPU usage. DoS attacks may also be initiated in this case.

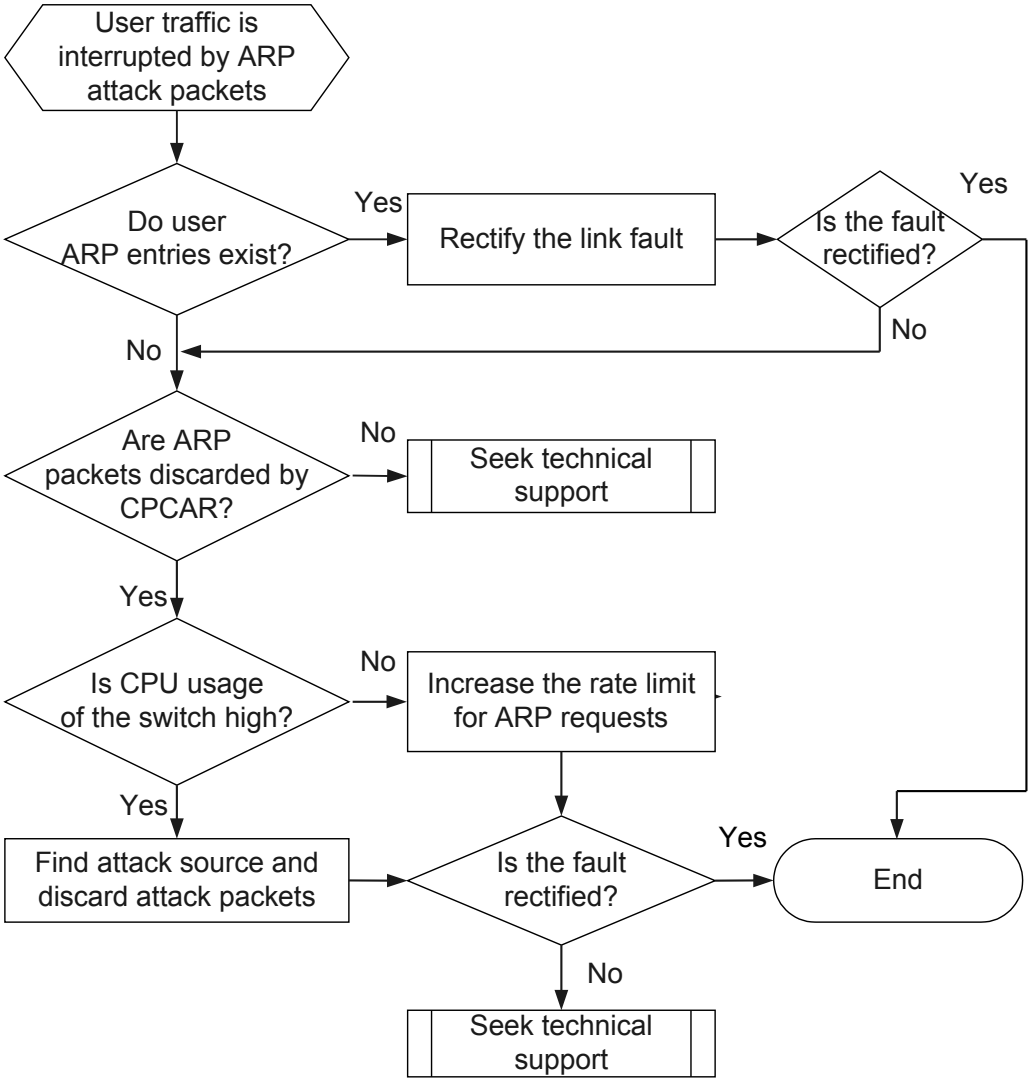
Troubleshooting Flowchart

The S3700 uses the CPCAR mechanism to limit the rate of ARP requests sent to the CPU. If an attacker sends a large number of bogus ARP requests, valid ARP requests are also discarded when the bandwidth limit is exceeded. Consequently, user traffic is interrupted.

Figure 7-7 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-7 Troubleshooting flowchart for traffic interruption caused by bogus ARP packets



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display arp all** command on the S3700 to view ARP entries of authorized users.

- If ARP entries of authorized users are displayed, the S3700 has learned the ARP entries, and traffic interruption is caused by a short link disconnection. In this case, rectify link faults.
- If no ARP entry is displayed, go to step 2.

Step 2 Run the **display cpu-defend statistics packet-type arp-request** command to view the statistics about ARP requests.

Copyright © Huawei Technologies Co., Ltd.

- If the count of dropped ARP requests is 0, go to step 8.
- If the count of dropped ARP requests is not 0, it indicates that the rate of ARP requests exceeds the CPCAR rate limit and excess ARP requests are discarded. Go to step 3.

Step 3 Run the **display cpu-usage** command to check the CPU usage of the main control board.

- If the CPU usage is smaller than 70% but ARP requests are discarded, the rate limit is too small. Go to step 4.
- If the CPU usage exceeds 70%, the CPU may be attacked by ARP packets. Go to step 5.

Step 4 Run the **car** command to increase the rate limit for ARP requests.

Run the **car** command in the attack defense policy view and apply the attack defense policy.

Step 5 Capture packets on the user-side interface, and find the attacker according to the source addresses of ARP requests.

If a lot of ARP requests are sent from a source address, the S3700 considers the source address as an attack source. Then add the source address to the blacklist or configure a blackhole MAC address entry to discard ARP requests sent by the attacker.

Step 6 Run the **arp speed-limit source-ip** [*ip-address*] **maximum** *maximum* command in the system view to set the rate limit for ARP packets from the attack source.

The **arp speed-limit source-mac** command can only be used on the S3700HI.

By default, ARP packet suppression based on source IP address is disabled.

Step 7 Run the **display arp anti-attack configuration log-trap-timer** command to check whether the ARP log and trap functions are enabled.

By default, the ARP log function is disabled. Run the **arp anti-attack log-trap-timer** *timer* command in the system view to enable the ARP log and trap functions. In this way, the S3700 will record logs and send traps when ARP attacks occur.

Step 8 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.3
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.4
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.5
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.6
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.7
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.11

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

7.2.4 IP Address Scanning Occurs

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for IP address scanning attacks.

Common Causes

This fault is commonly caused by the following:

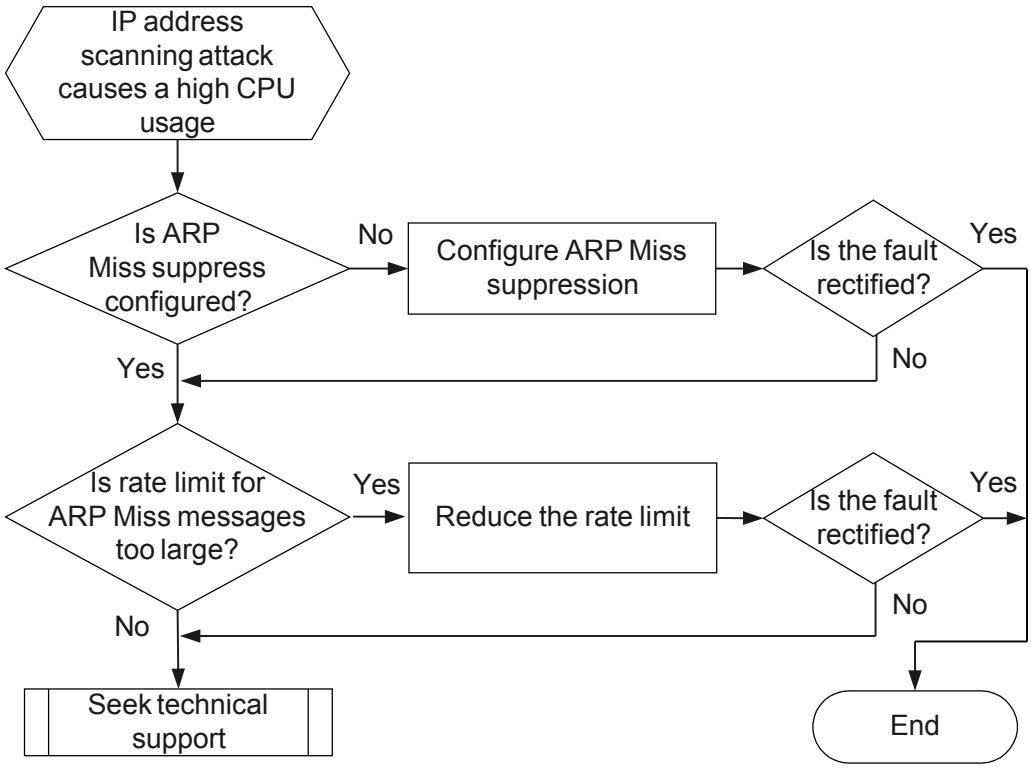
- An attacker sends a large number of destination unreachable packets to the S3700, and the packets trigger a large number of ARP Miss messages. In addition, the S3700 sends ARP requests to trigger ARP learning, causing a high CPU usage.

Troubleshooting Flowchart

An attacker sends a large number of destination unreachable packets to the S3700. The packets are sent to the CPU and trigger a large number of ARP Miss messages. In addition, the S3700 sends ARP requests to trigger ARP learning, causing a high CPU usage.

Figure 7-8 shows the troubleshooting flowchart.

Figure 7-8 Troubleshooting flowchart for IP address scanning



Troubleshooting Procedure

Copyright © Huawei Technologies Co., Ltd.

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display cpu-usage** command on the S3700 to check the CPU usage of the main control board.

In the command output, **ARQ** indicates the ARP packet processing task.

Step 2 Run the **display arp all** command to view the learned ARP entries.

If the MAC address in an ARP entry is in **Incomplete** state, the S3700 fails to learn the ARP entry.

```
<Quidway> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.10.10.12     0018-82d2-0e08            I -         Vlanif200
10.10.10.13     Incomplete      0         D-0         Vlanif200
                                          3004/-
10.10.10.14     Incomplete      0         D-0         Vlanif200
                                          3004/-
20.20.20.33     000c-76bd-43d6            I -         Vlanif300
20.20.20.55     0013-7227-842f  17        D-0         Vlanif300
...                                           3003/-
```

Generally, the possible causes are: the S3700 fails to send ARP requests, the ARP requests are discarded during transmission, or no ARP reply is received. If the CPU usage of the **ARQ** task is high, the S3700 fails to send ARP requests and generates ARP Miss messages. Go to step 3.

Step 3 Capture packets on the user-side interface and check the source addresses of IP packets.

Step 4 Run the **display arp anti-attack configuration arpmiss-speed-limit** command to view the configuration of ARP Miss suppression.

- If a source IP address is specified in the ARP Miss suppression command, the S3700 checks whether the specified IP address is the source address of the received IP packets. If so, the S3700 limits the rate of ARP Miss messages based on the rate limit configured in this command. If not, the S3700 limits the rate of the ARP Miss messages based on the limit set in the command without a source IP address specified.
- By default, ARP Miss suppression is enabled, and the maximum rate of ARP Miss messages is limited to 500 pps. When the rate of ARP Miss messages triggered by packets from the specified IP address exceeds the limit, the S3700 discards the packets sent from the IP address. You can change the rate limit for ARP Miss messages by running the **arp-miss speed-limit source-ip** [*ip-address*] **maximum** *maximum* command in the system view.

Step 5 Run the **display arp anti-attack configuration arpmiss-rate-limit** command on the S3700 to view the configuration of ARP Miss suppression.

- If many ARP Miss packets are triggered on an interface, in a VLAN, or on the entire device in a period, the S3700 is busy in broadcasting ARP request packets and its performance deteriorates. After ARP Miss suppression is configured, the S3700 counts ARP Miss packets generated within a specified period and discards excess ARP Miss packets.
- By default, the maximum rate of ARP Miss packets is 100 packets per second. To change the rate limit of ARP Miss packets, run the **arp-miss anti-attack rate-limit** *packet-number* [**interval-value**] command in the system view, VLAN view, or interface view.

Copyright © Huawei Technologies Co., Ltd.

Step 6 Run the **display arp anti-attack configuration log-trap-timer** command to check whether the ARP log and trap functions are enabled.

By default, the ARP log function is disabled. Run the **arp anti-attack log-trap-timer** *timer* command in the system view to enable the ARP log. In this way, the S3700 will record logs and send traps when ARP attacks occur.

Step 7 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.8
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.9
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.10
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.12

Relevant Logs

None.

7.2.5 ARP Learning Fails

This section provides a step-by-step for an ARP learning failure on the S3700.

Common Causes

The following table describes the possible causes of an ARP learning failure (assuming that the S3700 sends an ARP request to trigger ARP learning).

Condition	Possible Cause
The ARP request is not sent out.	A large number of ARP requests are triggered by ARP Miss messages, and the S3700 has not processed this ARP request.
The remote device does not receive the ARP request.	The link between the S3700 and the remote device is faulty, so the ARP request is discarded on the network.
The remote device receives the ARP request but discards it.	The remote device receives a large number of ARP packets. The rate of ARP packets exceeds the CAR, so the device discards the ARP request sent by the S3700.

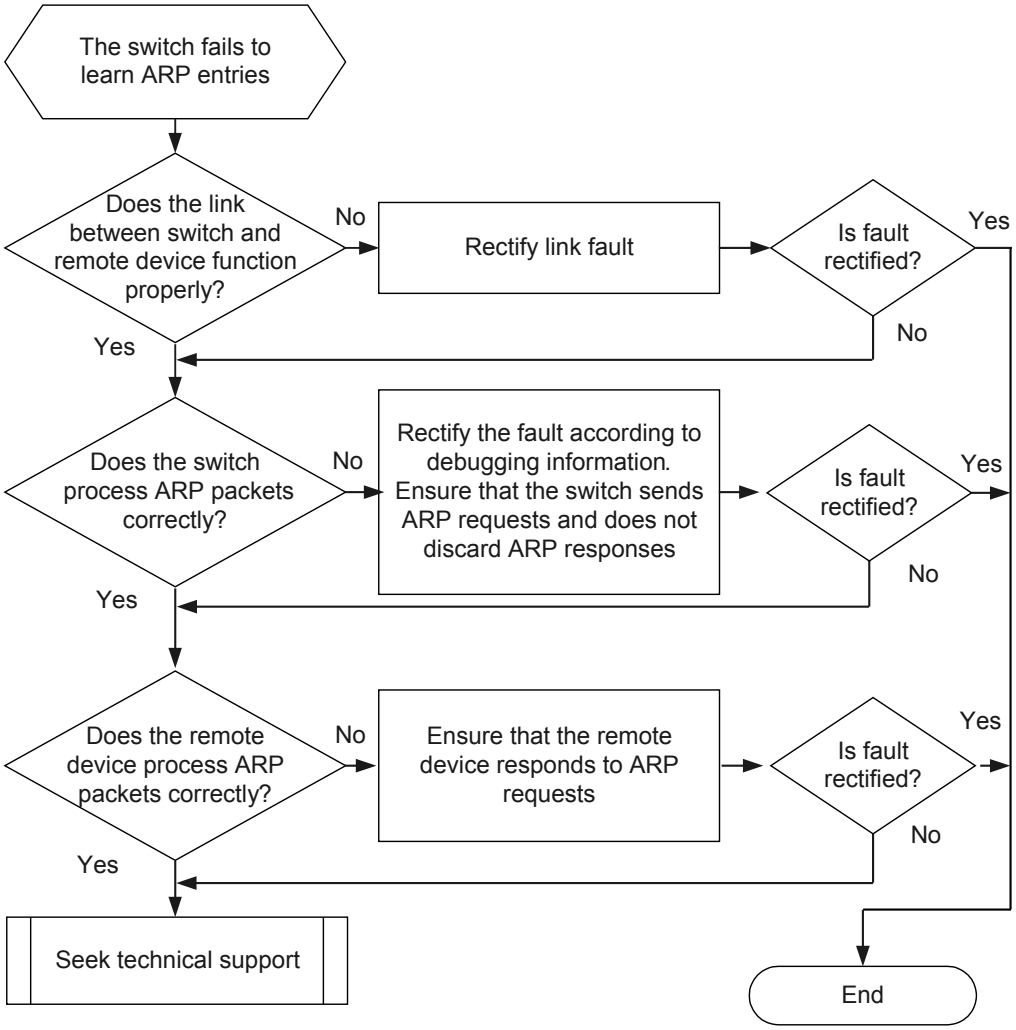
Copyright © Huawei Technologies Co., Ltd.

Condition	Possible Cause
The S3700 does not receive the ARP reply sent by the remote device.	The link between the S3700 and the remote device is faulty, so the ARP request is discarded on the network.
The S3700 receives the ARP reply but does not send it to the CPU.	The rate of ARP packets received by the S3700 exceeds the CPCAR or ARP packet rate limit, so the ARP reply is discarded.
The ARP reply is sent to the CPU but is discarded.	The ARP module of the S3700 is faulty.

Troubleshooting Flowchart

Figure 7-9 shows the troubleshooting flowchart.

Figure 7-9 Troubleshooting flowchart for ARP learning failure



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the link between the S3700 and the remote device works properly.

- Perform **ping** operations between the S3700 and the remote device. If the ping operations fail, check the routing configuration on the two devices.
- View traffic statistics on the two devices to check whether packets are discarded on the link. If any device on the link does not support the traffic statistics function, perform a ping test to check whether packets are discarded on the device. If packets are discarded on the link, rectify the link fault.

Step 2 Check that the S3700 processes ARP packets properly.

Run the **debugging arp packet interface** *interface-type interface-number* command in the user view to enable ARP debugging. Check whether information about ARP request and ARP reply packets is displayed.

NOTE

In the debugging information, the **operation** field indicates the ARP packet type. The value 1 indicates ARP request packets and the value 2 indicates ARP reply packets.

- If the S3700 does not send any ARP request packet, rectify the fault according to **7.2.4 IP Address Scanning Occurs**.
- If the S3700 does not receive any ARP reply packet, the ARP reply packets sent by the remote device may be discarded by the CPCAR mechanism. Go to step 3.
- If the S3700 receives ARP reply packets, go to step 5.

Step 3 Check whether ARP reply packets are discarded.

- Run the **display cpu-defend arp-reply statistics** command to view statistics about ARP reply packets.

  If the **Drop** value keeps increasing, the rate of ARP reply packets exceeds the CPCAR. Run the **car** command to increase the CPCAR for ARP reply packets.
- Run the **display this** command in the interface view, VLAN view, and system view to check whether a rate limit is set for ARP packets.

  If the rate limit is set and the rate of ARP packets is high, ARP reply packets may be discarded. Run the **arp anti-attack rate-limit** command to increase the rate limit.

Step 4 Check that the remote device processes ARP packets properly.

Check that the remote device receives the ARP request and sends the ARP reply.

If the remote device is a Huawei device, perform step 2 on the device. If the remote device is a non-Huawei device, see the manual of the device.

Step 5 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure

Copyright © Huawei Technologies Co., Ltd.

- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.3 NAC Troubleshooting

This chapter describes common causes of the network access control (NAC) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.3.1 802.1x Authentication of a User Fails

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the 802.1x authentication failure.

Common Causes

This fault is commonly caused by one of the following:

- Some parameters are set incorrectly or not set, such as the parameters of 802.1x authentication, AAA authentication domain, authentication server, and authentication server template.
- The user name or password entered by the user is incorrect.
- The number of online users reaches the maximum.

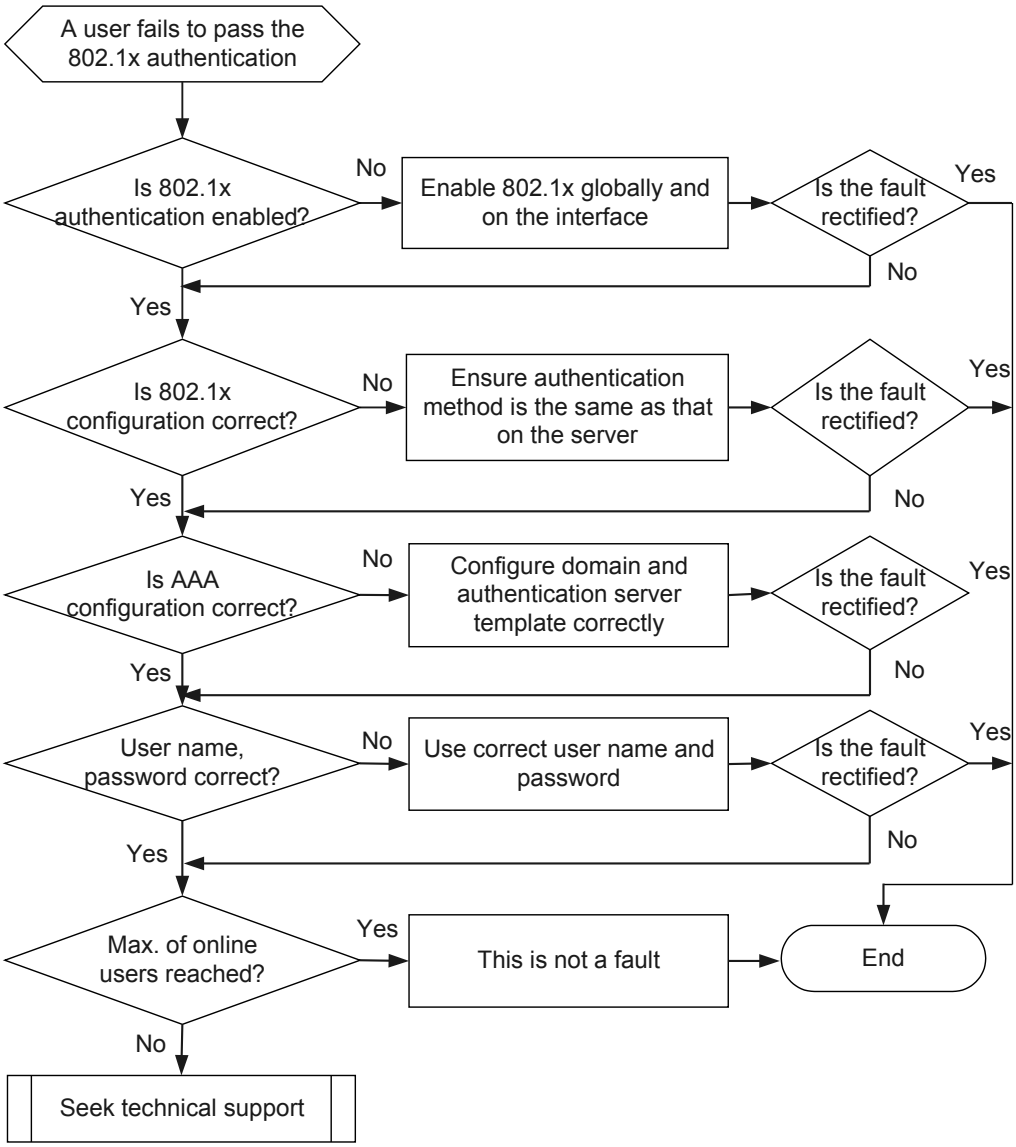
Troubleshooting Flowchart

A user fails to pass the 802.1x authentication.

Figure 7-10 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-10 Troubleshooting flowchart for 802.1x authentication failure



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that 802.1x authentication is enabled on the S3700.

Run the **display dot1x** command to check whether 802.1x authentication is enabled globally or on the user-side interface. If **Global 802.1x is Enabled** or **802.1x protocol is Enabled** is not displayed, 802.1x authentication is not enabled. Run the **dot1x enable** command to enable 802.1x authentication globally and on the user-side interface.

Copyright © Huawei Technologies Co., Ltd.

CAUTION

802.1x authentication and MAC address authentication cannot be enabled on the same interface. If MAC address authentication is enabled on the interface, the system displays an error message when you run the **dot1x enable** command.

Step 2 Check that 802.1x authentication is configured correctly.

Run the **display dot1x** command to check the 802.1x configuration.

The S3700 supports the following authentication methods for 802.1x: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Extensible Authentication Protocol (EAP). The authentication method is configured by using the **dot1x authentication-method** command.

- The authentication method on the S3700 must be the same as that on the authentication server.
- EAP authentication and local authentication cannot be configured simultaneously. If the authentication method for 802.1x users is EAP, go to step 3.
- If the authentication method for 802.1x users is PAP, check whether the client supports PAP authentication. If the client does not support PAP authentication, change the authentication method to CHAP or EAP.

Step 3 Check the AAA configuration.

1. Check whether the user name contains the domain name.
   - If user name does not contain the domain name, the user is authenticated in the default domain. In this case, check the authentication template bound to the default domain.
   - If the user name contains the domain name, the user should be authenticated in the specified domain. However, if the domain name is not found, the authentication fails. In this case, check the authentication template bound to the specified domain.
2. Check the authentication scheme applied to the user domain on the S3700.
   - If RADIUS or HWTACACS authentication is configured for the user domain, check whether the user account and the user attributes are created on the authentication server. For details on RADIUS troubleshooting and HWTACACS troubleshooting, see **7.1.1 A User Fails in the RADIUS Authentication** and **7.1.2 A User Fails in the HWTACACS Authentication**. For details on checking the authentication server, go to step 4.
   - If local authentication is configured for the user domain, run the **display local-user** command to check whether the local user name and password are created on the S3700. If not, run the **local-user** command to create the local user name and password.
   - If the authentication scheme is none, go to step 6.
3. Run the **display accounting-scheme** command to check the accounting scheme. If accounting is configured on the S3700 but the authentication server does not support accounting, the user will be forced offline after going online. To allow the user to go online, disable the accounting function in the user domain or run the **accounting start-fail online** command in the accounting scheme view to configure the S3700 to keep the user online after the accounting fails.

Step 4 Check the configuration of the authentication server.

Copyright © Huawei Technologies Co., Ltd.

- If the user information does not exist on the authentication server, create the user name and password on the authentication server.
- If user attributes on the authentication server contain VLAN authorization information but the VLAN is not created on the S3700, user authorization fails. To rectify the fault, create the VLAN.
- If user attributes on the authentication server contain ACL authorization information (ACL number or ACL content), but the ACL is not created on the S3700 or the ACL format is different from that required by the S3700, user authorization fails. To rectify the fault, create the ACL. Ensure that the ACL format used by the authentication server is the same that required by the S3700.

.

NOTE

The S3700 requires the following ACL format in the user attributes:
acl *acl-num* **key1** *key-value1...* **keyN** *key-valueN* **permit/deny**

Field	Description	Field	Description
acl	Delivers the ACL content.	*acl-num*	Specifies the ACL number. The value ranges from 10000 to 10999.
permit	Allows users matching the rules to access the network.	**deny**	Prohibits users matching the rules from accessing the network.
keyM (1 ⩽ M ⩽ N)	Indicates a keyword in the ACL, including src-ip (source IP address), src-ipmask (mask of source IP address), and tcp-srcport (source TCP port number).	*key-valueM* (1 < M < N)	Specifies the value of a keyword, which can be an IP address, a mask, or a port number.

If the **display access-user user-id** command output contains the user IP address and **Dynamic ACL desc (Effective)**, the ACL specified in the user attribute takes effect.

If the configurations of the S3700 and the authentication server are correct, go to step 5.

Step 5 Check that the user name and password entered by the user are correct.

If RADIUS authentication is used and the authentication method is CHAP or PAP, run the **test-aaa** command to check whether the user name and password can pass the RADIUS authentication.

- If the authentication fails, check the configuration of the RADIUS server and RADIUS configuration on the S3700. For details, see **Troubleshooting Procedure of RADIUS authentication failure**.
- If user passes the authentication, check the option settings on the client or capture packets on the network adapter of the client to check whether the client sends authentication packets correctly.

If preceding configurations are correct, go to step 6.

Step 6 Run the **display dot1x interface** *interface-type interface-number* command on the S3700 to check whether the number of online 802.1x users reaches the maximum.

Copyright © Huawei Technologies Co., Ltd.

If the number of online 802.1x users reaches the maximum, the S3700 does not trigger authentication for subsequent users, and subsequent users cannot go online.

Step 7 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

- 1.3.6.1.4.1.2011.5.25.40.4.2.1

Relevant Logs

None.

7.3.2 MAC Address Authentication of a User Fails

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the MAC address authentication failure.

Common Causes

This fault is commonly caused by one of the following:

- Some parameters are set incorrectly or not set, such as the parameters of MAC address authentication, authentication domain, authentication server, and authentication server template.
- The number of online users reaches the maximum.

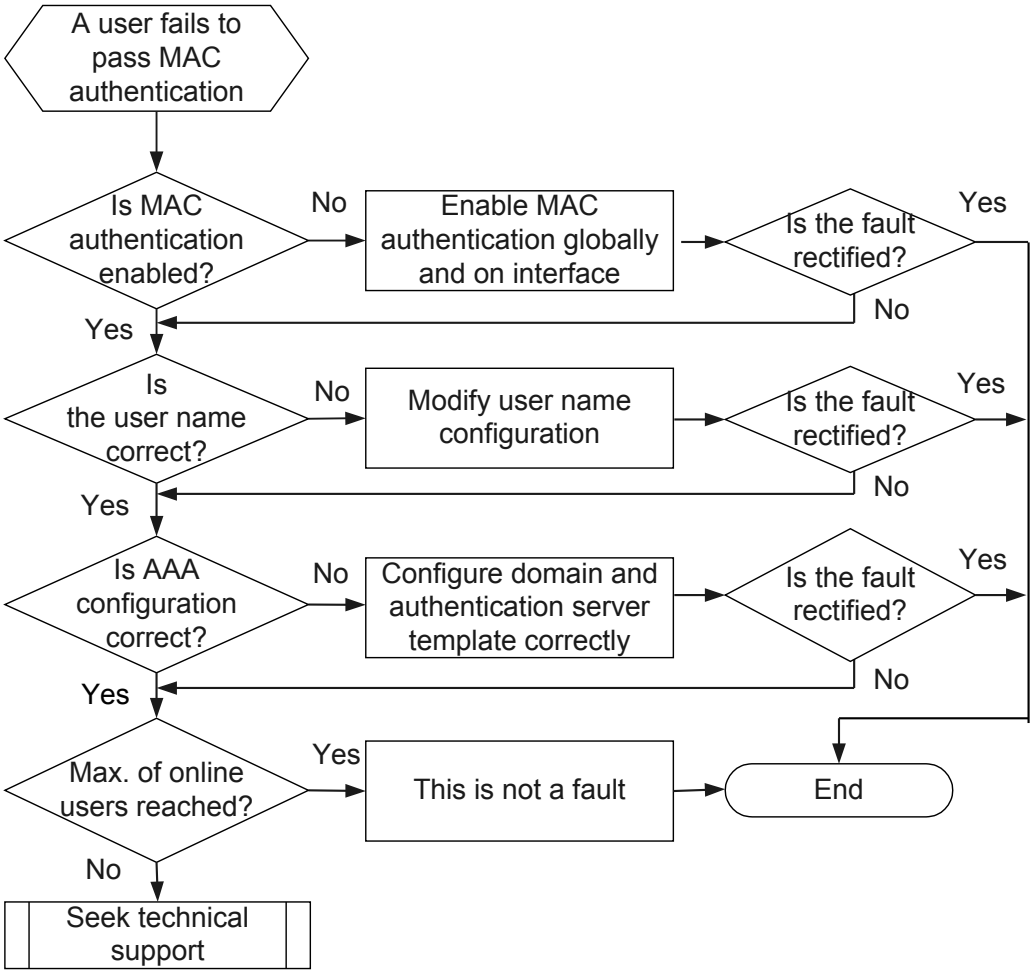
Troubleshooting Flowchart

A user fails to pass the MAC address authentication.

Figure 7-11 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-11 Troubleshooting flowchart for MAC address authentication failure



Troubleshooting Procedure

Context

When MAC address authentication is used, users do not need the dial-up software. The authentication information such as the user name and password is generated according to the MAC addresses of users. Similar to 802.1x authentication troubleshooting, when troubleshooting MAC address authentication, check whether the user name and password on the S3700 are same as those on the authentication server and whether the domain name in the user name is correct.

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that MAC address authentication is enabled on the S3700.

Copyright © Huawei Technologies Co., Ltd.

Run the **display mac-authen** command to check whether MAC address authentication is enabled globally or on the user-side interface. If **MAC address authentication is Enabled** is not displayed, MAC address authentication is not enabled. Run the **mac-authen** command to enable MAC address authentication globally and on the user-side interface.

CAUTION

802.1x authentication and MAC address authentication cannot be enabled on the same interface. If 802.1x authentication is enabled on the interface, the system displays an error message when you run the **mac-authen** command.

Step 2 Check the configuration of the user name for MAC address authentication.

Run the **display this** command in the interface view to check the configuration of MAC address authentication on the interface. If MAC address authentication is not configured on the interface, the global configuration is used. Run the **display mac-authen** command to check the configuration of global MAC address authentication.

MAC address authentication supports two user name formats: fixed user name and MAC address.

- If the user MAC address is used as the user name, the S3700 sends the MAC address of the user terminal as the user name and password to the authentication server. The authentication domain is configured by the **mac-authen domain** command. If no authentication domain is configured, the default domain is used.
- When the fixed user name contains a domain name, this domain is used as the authentication domain. If the fixed user name does not contain a domain name, the default domain is used as the authentication domain.

Check the authentication server template and AAA schemes bound to the authentication domain. Go to step 3.

Step 3 Check the AAA configuration.

1. Check the configuration of the authentication server template bound to the domain. Ensure that the IP address and port of the authentication server are set correctly in the template, and that the user name format and shared key specified in the template are the same as those on the authentication server.
2. Check the authentication scheme applied to the user domain on the S3700.
   - If RADIUS or HWTACACS authentication is configured for the user domain, check whether the user account and the user attributes are created on the authentication server. For details on RADIUS troubleshooting and HWTACACS troubleshooting, see **7.1.1 A User Fails in the RADIUS Authentication** and **7.1.2 A User Fails in the HWTACACS Authentication**. For details on checking the authentication server, go to step 4.
   - If local authentication is configured for the user domain, run the **display local-user** command to check whether the local user name and password are created on the S3700. If not, run the **local-user** command to create the local user name and password.
   - If the authentication scheme is none, go to step 5.
3. Run the **display accounting-scheme** command to check the accounting scheme. If accounting is configured on the S3700 but the authentication server does not support accounting, the user will be forced offline after going online. To allow the user to go online,

Copyright © Huawei Technologies Co., Ltd.

disable the accounting function in the user domain or run the **accounting start-fail online** command in the accounting scheme view to configure the S3700 to keep the user online after the accounting fails.

Step 4 Check the configuration of the authentication server.

- If the user information does not exist on the authentication server, create the user name and password on the authentication server.
- If user attributes on the authentication server contain VLAN authorization information but the VLAN is not created on the S3700, user authorization fails. To rectify the fault, create the VLAN.
- If user attributes on the authentication server contain ACL authorization information (ACL number or ACL content), but the ACL is not created on the S3700 or the ACL format is different from that required by the S3700, user authorization fails. To rectify the fault, create the ACL. Ensure that the ACL format used by the authentication server is the same that required by the S3700.

  NOTE

  The S3700 requires the following ACL format in the user attributes:
  acl *acl-num* **key1** *key-value1...* **keyN** *key-valueN* **permit**/**deny**

Field	Description	Field	Description
acl	Delivers the ACL content.	*acl-num*	Specifies the ACL number. The value ranges from 10000 to 10999.
permit	Allows users matching the rules to access the network.	**deny**	Prohibits users matching the rules from accessing the network.
keyM (1 ⩽ M ⩽ N)	Indicates a keyword in the ACL, including src-ip (source IP address), src-ipmask (mask of source IP address), and tcp-srcport (source TCP port number).	*key-valueM* (1 < M < N)	Specifies the value of a keyword, which can be an IP address, a mask, or a port number.

  If the **display access-user user-id** command output contains the user IP address and **Dynamic ACL desc (Effective)**, the ACL specified in the user attribute takes effect.

If the configurations of the S3700 and the authentication server are correct, go to step 5.

Step 5 Run the **display mac-authen interface** *interface-type interface-number* command on the S3700 to check whether the number of online MAC address authentication users reaches the maximum.

If the number of online MAC address authentication users reaches the maximum, the S3700 does not trigger authentication for subsequent users, and subsequent users cannot go online.

Step 6 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

Relevant Alarms

- 1.3.6.1.4.1.2011.5.25.171.2.1

Relevant Logs

None.

7.3.3 MAC Address Bypass Authentication of a User Fails

This section describes the method of MAC address bypass authentication troubleshooting.

In MAC address bypass authentication, a user terminal first sends an Address Resolution Protocol (ARP) packet or a Dynamic Host Control Protocol (DHCP) packet to the S3700 to trigger 802.1x authentication. If the S3700 does not receive any 802.1x packet from the terminal within 30 seconds, the S3700 sends the MAC address of the terminal as the user name and password to the authentication server.

After MAC address bypass authentication is configured, the S3700 starts MAC address authentication automatically after a user fails to pass the 802.1x authentication. 802.1x authentication and MAC address authentication cannot be enabled on the same interface. If 802.1x authentication is enabled on the interface, the system displays an error message when you attempt to enable MAC address authentication. You can enable MAC address bypass authentication by using the **dot1x mac-bypass** command. In MAC address bypass authentication, the terminal MAC address is used as the user name and password. The process of MAC address bypass authentication is the same as the process of MAC address authentication. The troubleshooting procedure for MAC address bypass authentication failure is similar to the troubleshooting procedure for MAC address authentication failure. For details, see **7.3.2 MAC Address Authentication of a User Fails**.

7.3.4 Web Authentication of a User Fails

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the Web authentication failure.

Common Causes

This fault is commonly caused by one of the following:

- Some parameters are set incorrectly or not set, such as the parameters of Web address authentication, authentication domain, authentication server, and authentication server template.
- The Web authentication server is unreachable or unavailable.
- The user name or password entered by the user is incorrect.

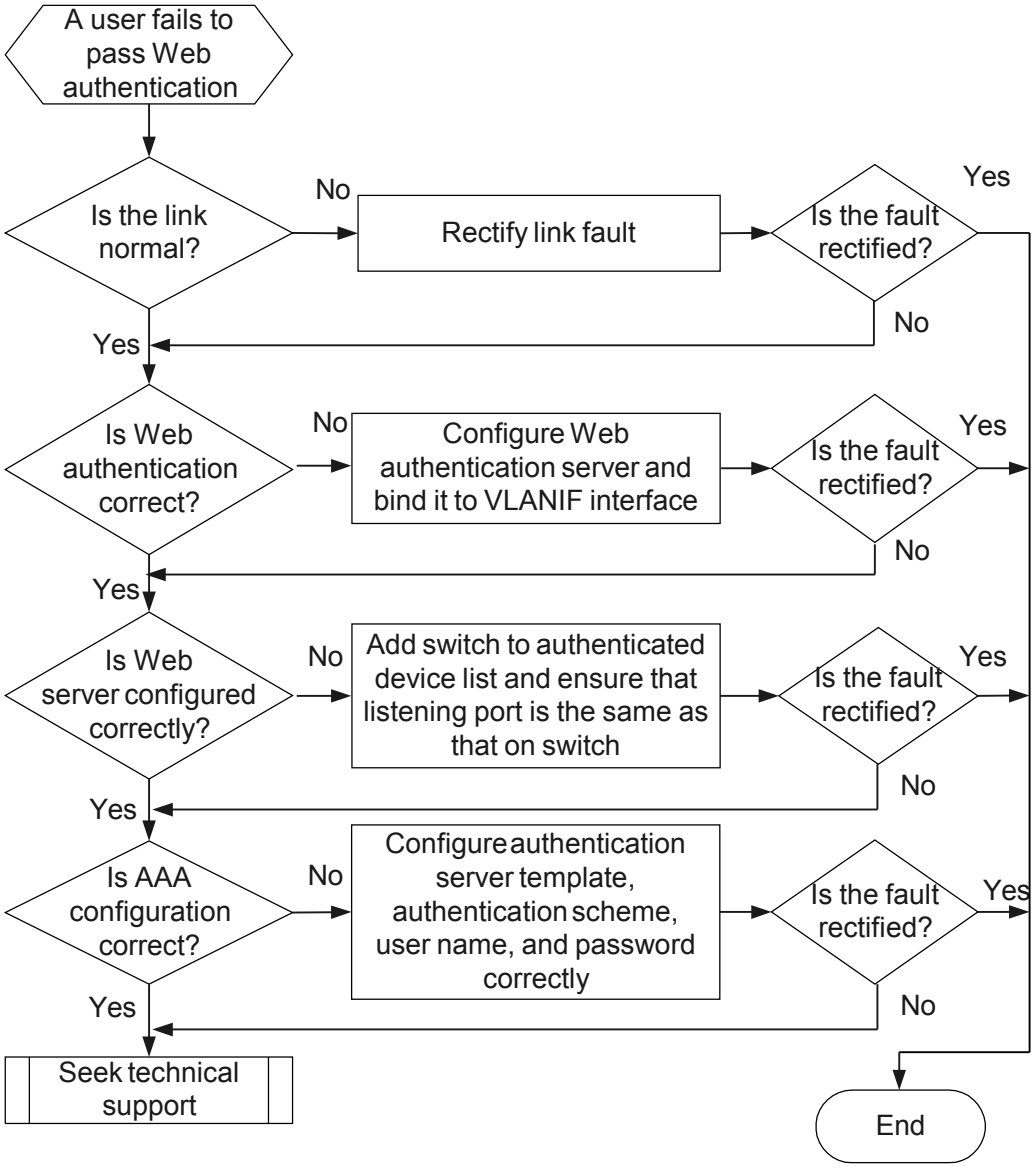
Troubleshooting Flowchart

A user fails to pass the Web authentication.

Figure 7-12 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-12 Troubleshooting flowchart for Web authentication failure



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **ping** command to check whether the link between the S3700 and the Web authentication server and the link between the S3700 and the RADIUS or HWTACACS authentication server work properly.

Copyright © Huawei Technologies Co., Ltd.

- If the ping operation fails on any link, rectify the fault on the link according to A Ping Operation Fails.
- If the ping operation succeeds, go to step 2.

Step 2 Check that Web authentication is configured correctly on the S3700.

- Run the **display web-auth-server configuration** command to check whether the Web authentication server is configured. If not, run the **web-auth-server** command in the system view to configure a Web authentication server. Run the **server-ip** command in the web-auth-server view to configure an IP address for the Web authentication server.

  You can also run the **port**, **shared-key**, and **url** commands in the web-auth-server view to configure the port number, shared key, and URL of the Web authentication server. If these parameters are configured on the S3700, ensure that the parameter settings are the same as those configured on the Web authentication server. If they are not configured on the S3700, the default port number is 50100, and there is no default shared key or URL.
- Run the **display this** command in the VLANIF interface view to check whether the Web authentication server is bound to the VLANIF interface. If not, run the **web-auth-server** command in the VLANIF interface view to bind the Web authentication server to the VLANIF interface.
- Run the **display web-auth-server configuration** command to check the listening port of Portal packets. Go to step 3.

Step 3 Check the configuration of the Web authentication server.

- Check whether the S3700 is in the authenticated device list.
- Check whether the listening port of Portal packets is the same as that configured on the S3700.
- Check whether the IP address of the user is in the IP address group of the S3700.

Ensure that the S3700 is in the authenticated device list, the listening port of Portal packets on the S3700 is the same as that configured on the Web authentication server, and the IP address of the user is in the IP address group of the S3700.

Step 4 Check the AAA configuration.

1. Check the configuration of the authentication server template bound to the domain. Ensure that the IP address and port of the authentication server are set correctly in the template and that the user name format and shared key specified in the template are the same as those on the authentication server.
2. Check the authentication scheme applied to the user domain on the S3700.
   - If RADIUS or HWTACACS authentication is configured for the user domain, check that the user name and password are configured on the authentication server. Ensure that the user enters the correct user name and password. For details on RADIUS troubleshooting and HWTACACS troubleshooting, see **7.1.1 A User Fails in the RADIUS Authentication** and **7.1.2 A User Fails in the HWTACACS Authentication**.
   - If local authentication is configured for the user domain, run the **display local-user** command to check whether the local user name and password are created on the S3700. If not, run the **local-user** command to create the local user name and password.
   - If the authentication scheme is none, go to step 5.
3. Run the **display accounting-scheme** command to check the accounting scheme. If accounting is configured on the S3700 but the authentication server does not support accounting, the user will be forced offline after going online. To allow the user to go online,

Copyright © Huawei Technologies Co., Ltd.

disable the accounting function in the user domain or run the **accounting start-fail online** command in the accounting scheme view to configure the S3700 to keep the user online after the accounting fails.

Step 5 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.4 DHCP Snooping Troubleshooting

This chapter describes common causes of Dynamic Host Configuration Protocol (DHCP) snooping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.4.1 Users Fail to Go Online After DHCP Snooping Is Configured

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the DHCP snooping fault.

Common Causes

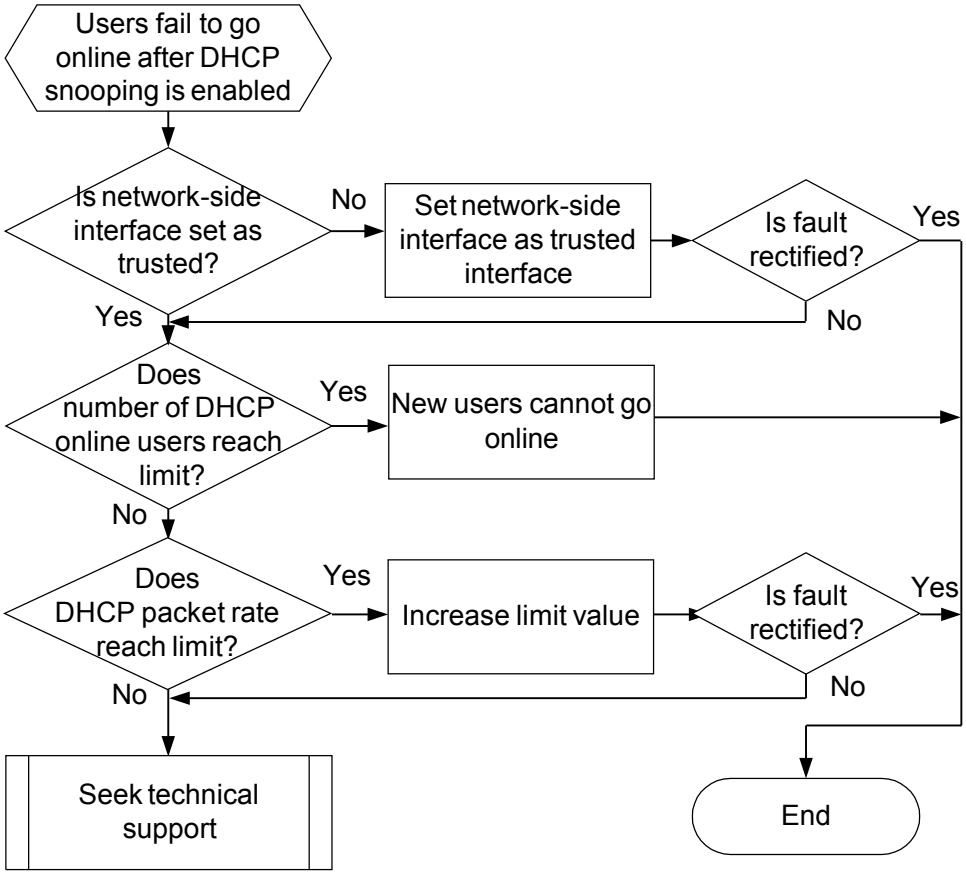
This fault is commonly caused by one of the following:

- The network-side interface connected to the DHCP server is not configured as a trusted interface.
- The number of DHCP users connected to the user-side interface reaches the upper limit.
- The transmission rate of DHCP packets exceeds the upper limit, so the DHCP packets of new users are discarded.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 7-13 DHCP snooping troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the trusted interface is correctly configured.

- Run the **display dhcp snooping global** command to check the VLANs and interfaces enabled with DHCP snooping.
- Run the **display dhcp snooping interface** command to check whether "dhcp snooping trusted" is displayed under the network-side interface.
- Run the **display this** command in the VLAN view to check whether "dhcp snooping trusted interface xxx" is displayed.

After DHCP snooping is enabled on an interface, the interface is an untrusted interface by default. When receiving packets from network-side interfaces, the S3700 processes only the DHCP Reply packets received by the trusted interface and discards DHCP Reply packets received by untrusted interfaces. When receiving packets from user-side interfaces, the S3700 forwards the packets only to the trusted interface.

Copyright © Huawei Technologies Co., Ltd.

- The network-side interface of the DHCP server must be configured as a trusted interface. If the network-side interface is not a trusted interface, run the **dhcp snooping trusted** command in the interface view or run the **dhcp snooping trusted interface** command in the VLAN view to configure the interface as a trusted interface.
- If the trusted interface is correctly configured, go to step 2.

Step 2 Check whether the number of DHCP online users reaches the upper limit.

- Run the **display dhcp snooping interface** command to check whether "dhcp snooping max-user-number xxx" is displayed under the user-side interface.
- Run the **display this** command in the VLAN view to check whether "dhcp snooping max-user-number xxx" is displayed.
- Run the **display this** command in the system view to check whether "dhcp snooping global max-user-number xxx" is displayed.

In the command outputs, max-user-number indicates the maximum number of DHCP users. If this field is not displayed, the default value 512 (For S3700HI, the number is 1024) is used. If max-user-number is displayed in all the preceding command outputs, the smallest one among the displayed values is used.

Run the **display dhcp snooping user-bind all** command to view the number of DHCP users on the DHCP snooping-enabled interface. If the number of DHCP users on the interface reaches the upper limit, new users cannot go online.

If the number of DHCP users on the interface is lower than the upper limit, go to step 3.

Step 3 Check whether the transmission rate of DHCP packets exceeds the upper limit.

Run the **display this** command in the interface view, VLAN view, and system view to check whether a limit is set for DHCP packet rate. If the output information does not contain **dhcp snooping check dhcp-rate xx**, the DHCP packet rate is the default value 100.

The DHCP snooping rate limit can be set in the system view, interface view, and VLAN view. After a rate limit is set, the number of packets sent to the protocol stack within a certain period of time cannot exceed the limit; otherwise, the excess packets are discarded. The smallest value among the rate limits set in the system view, interface view, and VLAN view takes effect. If users cannot go online because the DHCP snooping rate limit is small, run the **dhcp snooping check dhcp-rate** command in the system view, interface view, and VLAN view to increase the rate limit values.

If the fault persists after the rate limit values are increased, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Copyright © Huawei Technologies Co., Ltd.

Relevant Logs

None.

7.4.2 Troubleshooting Cases

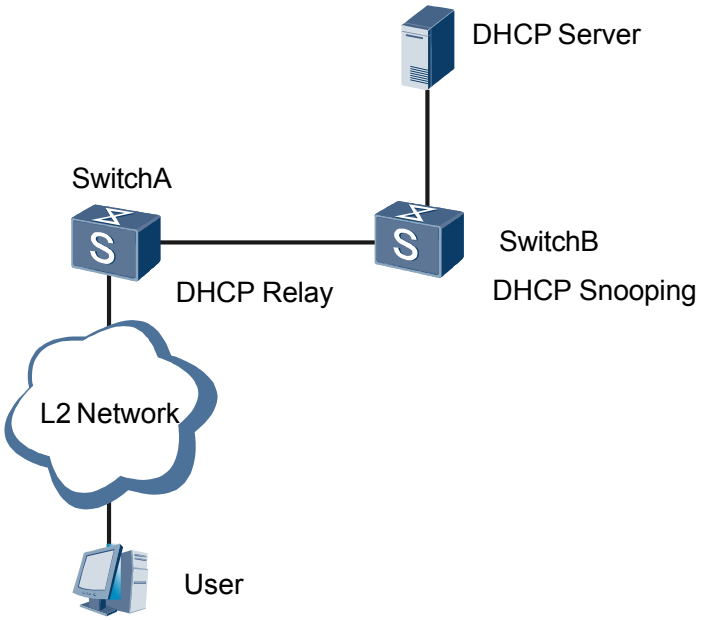
This section provides a DHCP snooping troubleshooting case.

Users Fail to Obtain IP Addresses After DHCP Snooping Is Enabled

Fault Symptom

As shown in **Figure 7-14**, DHCP relay is enabled on SwitchA, SwitchB is a non-Huawei device, and DHCP snooping is enabled on SwitchB. Users cannot obtain IP addresses.

Figure 7-14 Network diagram



Fault Analysis

1. Check the DHCP configurations on SwitchA and SwitchB. The configurations are correct; therefore, DHCP packets may be discarded.
2. Check whether SwitchB correctly processes DHCP Discover packets.

   Capture and analyze the packets on SwitchB. The DHCP Discover packets with the source port and destination port being port 67 are discarded before they enter DHCP snooping queues.
3. Check the network. The DHCP snooping-enabled device (SwitchB) is between the DHCP relay and the DHCP server, and the source and destination ports of the DHCP Discover packets sent by the DHCP relay are port 67.

Copyright © Huawei Technologies Co., Ltd.

4. Check the packet processing mechanism of SwitchB. SwitchB considers the packets with the source and destination ports being port 67 as invalid DHCP Discover packets, so it discards them.

Procedure

Step 1 Contact the vendor of SwitchB to modify the software codes to make SwitchB support the DHCP Discover packets with the source and destination ports being port 67. The fault is then rectified.

----End

Summary

A typical DHCP network structure is client-relay-server and DHCP snooping is usually enabled on the relay or between the relay and the client. If DHCP snooping is enabled on a network using another structure, consider whether DHCP packet forwarding is affected.

7.5 Traffic Suppression Troubleshooting

This chapter describes common causes of traffic suppression faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

7.5.1 Broadcast Suppression Fails to Take Effect on an Interface

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when broadcast suppression fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

- Broadcast suppression is not configured on interfaces, or the broadcast suppression threshold is set too high.
- Broadcast packets are not discarded on the inbound interface.

Troubleshooting Flowchart

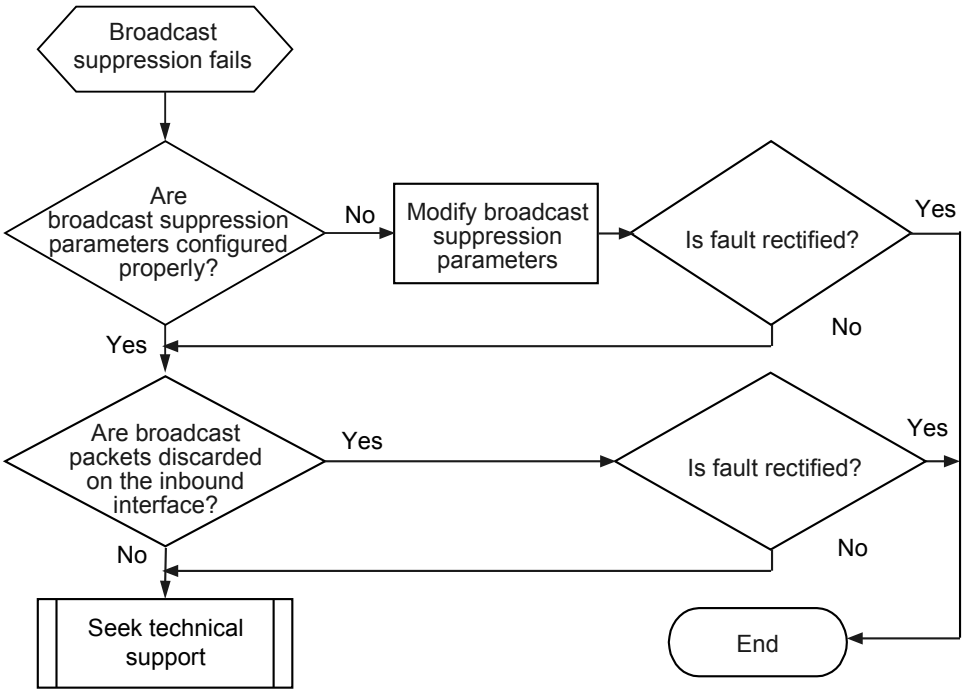
When a broadcast storm occurs on an interface and broadcast suppression fails to take effect on the interface, see **Figure 7-15** to rectify the fault.

NOTE

- Run the **display interface** *interface-type interface-number* command to check the packets sent and received on the interface. If the rate of incoming or outgoing packets reaches several Mbit/s and most packets are broadcast packets, a broadcast storm occurs on the interface.
- Generally, only ARP packets and DHCP packets are broadcast on a network. If a broadcast storm occurs, the network may have a loop. When many physical loops exist on the network, loop prevention protocols such as the Spanning Tree Protocol (STP) and the Rapid Ring Protection Protocol (RRPP) must be enabled to prevent network loops. When loop prevention is ineffective and network loops occur, broadcast suppression can restore the network. Broadcast suppression is a remedy for broadcast storms. An effective prevention measure for broadcast storms is to eliminate network loops. For details about loop prevention measures, see **MSTP Troubleshooting** and **RRPP Troubleshooting**.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-15 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

- Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.
- The troubleshooting procedures for multicast suppression and unknown unicast suppression are similar to that for broadcast suppression.

Procedure

Step 1 Check that traffic suppression is correctly configured on the related interface.

NOTE

The traffic suppression function controls the traffic entering the S3700 from an interface. Traffic suppression must be configured on both the user-side and network-side interfaces on the S3700. If broadcast suppression is configured only on the user-side or network-side interface, the S3700 can only control the broadcast traffic in one direction. When a downstream device sends a large number of broadcast packets to the S3700, broadcast storms still occur if broadcast suppression is not configured on the interface connected to the downstream device.

Normally, broadcast packets are transmitted at a rate less than 1000 kbit/s. Therefore, setting the broadcast suppression threshold to less than 1000 kbit/s is recommended. The formula for calculating the PPS rate is as follows: PPS = CIR x 1000/(84 x 8). The value 84 is the average packet length, including a 60-byte packet body, a 20-byte inter-frame gap and a 4-byte CRC. The value 8 is the number of bits in a byte.

Run the **display flow-suppression interface** *interface-type interface-number* command in the user view to check whether the values of **rate mode** and **set rate value** in the **broadcast** field are proper.

Copyright © Huawei Technologies Co., Ltd.

- If these values are improper, run the **broadcast-suppression** { *percent-value* | **packets** *packets-per-second* } command in the user view to modify broadcast suppression parameters.
- If these values are proper, go to step 2.

Step 2 Check whether broadcast packets are discarded in the inbound direction of the interface.

You can check whether broadcast packets are discarded in the inbound direction of the interface by using the following methods:

- Run the **display interface** *interface-type interface-number* command in the user view to check whether the value of **Input bandwidth utilization** changes greatly after traffic suppression is configured. Normally, after traffic suppression is configured, the interface bandwidth usage decreases if the interface discards excess packets. If the value of **Input bandwidth utilization** does not change or changes a little, go to step 3.
- Configure another interface (interface B), and add it and the interface configured with traffic suppression (interface A) to the same VLAN. Then check whether the volume of the outgoing traffic on interface B is the same as the volume of the traffic on interface A. If they are different, no packet is discarded in the inbound direction of interface A. Go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.6 CPU Defense Troubleshooting

This chapter describes common causes of CPU defense faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.6.1 Protocol Packets Fail to Be Sent to the CPU

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when protocol packets fail to be sent to the CPU.

Common Causes

This fault is commonly caused by one of the following:

- The inbound interface does not receive any protocol packet.

Copyright © Huawei Technologies Co., Ltd.

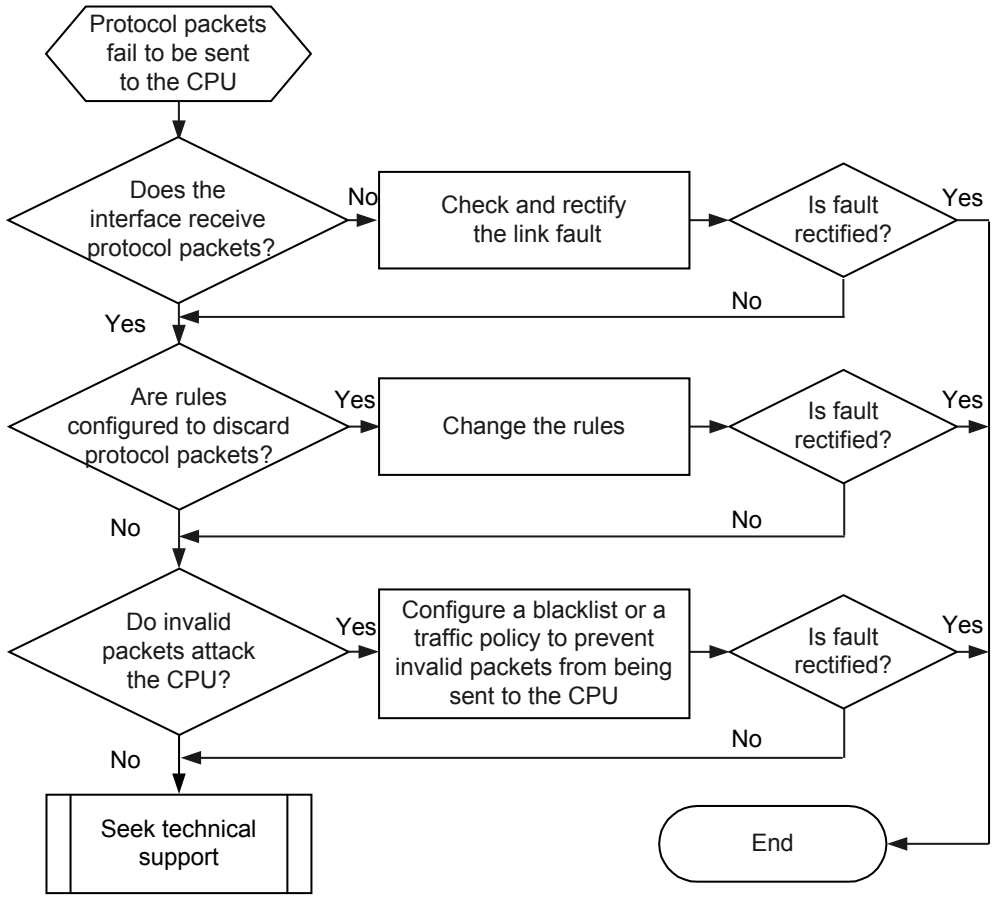
- A policy is configured on the S3700 to discard protocol packets. For example, a blacklist is configured, or the action taken on the protocol packets to be sent to the CPU is **deny**.
- Invalid packets attack the CPU.

Troubleshooting Flowchart

If a certain function does not work because protocol packets fail to be sent to the CPU, rectify the fault according to **Figure 7-16**.

Run the **display cpu-defend statistics** command to check the value of the Pass field to determine whether protocol packets are sent to the CPU.

Figure 7-16 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the interface receives protocol packets.

Copyright © Huawei Technologies Co., Ltd.

Capture packets on the interface to check whether the interface receives protocol packets.

- If the interface does not receive any protocol packet, run the **display interface** *interface-type interface-number* command to check whether the interface is physically Up.
  - If the interface is physically Down, see **4.1.1 Connected Ethernet Interfaces Down** to rectify the interface fault.
  - If the interface is physically Up, go to step 3.
- If the interface receives protocol packets, go to step 2.

Step 2 Check whether a policy is configured to discard protocol packets on the S3700.

NOTE

On the S3700, protocol packets will be discarded and fail to be sent to the CPU in the following situations:

- A blacklist is configured, and protocol packets match the ACL rule of the blacklist.
- The action taken on the protocol packets to be sent to the CPU is **deny**.

Run the **display this** command in the system view to check the configured attack defense policy. Then run the **display cpu-defend policy** command to check whether a blacklist is configured or whether the action taken on the protocol packets to be sent to the CPU is **deny**.

- If a blacklist is configured, run the **display acl** command to check whether protocol packets match rules of the blacklist.
  - If protocol packets match the rules, change the rules according to the service plan.
  - If no protocol packet matches the rules, go to step 3.
- If the action taken on the protocol packets to be sent to the CPU is **deny**, run the **car** command to set the CAR.
- If no blacklist is configured, and the action taken on the protocol packets to be sent to the CPU is not **deny**, go to step 3.

Step 3 Check statistics about the packets sent to the CPU.

NOTE

If there are excessive packets of a certain protocol, for example, invalid packets attack the CPU, other protocol packets cannot be sent to the CPU.

Run the **display cpu-defend statistics** command to check whether a large number of protocol packets are discarded.

- If a large number of protocol packets are discarded, check whether these packets are invalid attack packets by using the attack source tracing function. If they are invalid attack packets, use the configured blacklist or traffic policy to prevent these packets from being sent to the CPU.

  NOTE

  - For the configuration of the attack source tracing function, see "Configuring Attack Source Tracing" in the *Quidway S3700 Series Ethernet Switches Configuration Guide - Security*.
  - For the configuration of a blacklist, see "Configuring Attack Defense Policies" in the *Quidway S3700 Series Ethernet Switches Configuration Guide - Security*.
  - For the configuration of a traffic policy, see "Configuring Attack Defense Policies" in the *Quidway S3700 Series Ethernet Switches Configuration Guide - Security*.
- If no protocol packet is discarded, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure

Copyright © Huawei Technologies Co., Ltd.

- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.6.2 Blacklist Function Fails to Take Effect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when the blacklist function fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

- The configured blacklist fails to be applied.
- Packets do not match rules of the blacklist.

Troubleshooting Flowchart

None.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the configured blacklist is applied to the corresponding board successfully.

Run the **display cpu-defend policy** *policy-name* command to check whether the blacklist in the attack defense policy has been applied successfully.

```
<Quidway> display cpu-defend policy 1
 Related slot : <0>
 Configuration :
   Blacklist 1 ACL number : 2001
```

- If "Related slot : <0>" is displayed in the command output, the attack defense policy has been applied successfully.
- If "Blacklist 1 ACL number : 2001" is displayed in the command output, a blacklist has been configured in the attack defense policy.

Step 2 Check whether packets match rules of the blacklist.

Check the ACL of the blacklist in the displayed attack defense policy information, and then run the **display acl** *acl-number* command to check whether service packets match the ACL rule.

Copyright © Huawei Technologies Co., Ltd.

- If service packets do not match the ACL rule, run the **rule** command in the ACL view to modify the ACL rule.
- If service packets match the ACL rule, the blacklist may fail to be applied because ACL resources are insufficient. Go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.6.3 Attack Source Tracing Fails to Take Effect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when attack source tracing fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

- The attack defense policy configured with attack source tracing is not applied.
- The threshold for attack source tracing is set too high, so the attack source tracing function fails to identify attack packets.

Troubleshooting Flowchart

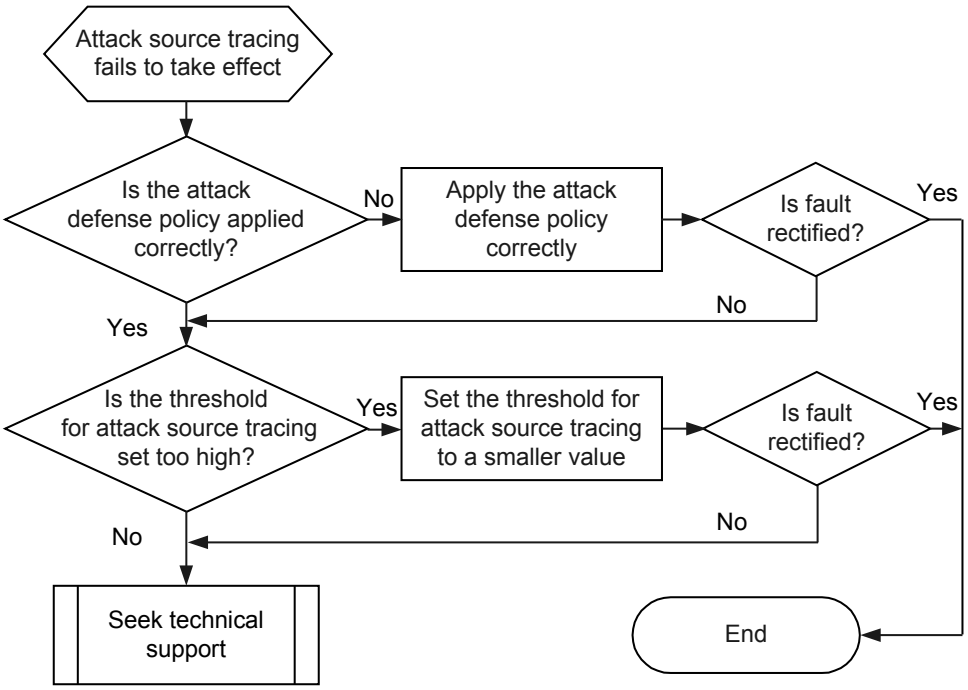
If attack source tracing is configured, but the source of attack packets sent to the CPU cannot be found by using the **display auto-defend attack-source** command, see **Figure 7-17** to rectify the fault.

NOTE

The attack source tracing function can collect statistics about only DHCP, ICMP, IGMP, TCP, Telnet, and ARP packets as well as packets with the TTL being 1.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-17 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the attack defense policy configured with attack source tracing is applied correctly.

Run the **display this** command in the system view to check whether the **cpu-defend-policy global** command has been executed.

- If no attack defense policy is applied successfully, run the **cpu-defend-policy global** command in the system view to apply an attack defense policy.
- If the attack defense policy has been applied successfully, go to step 2.

Step 2 Check whether the threshold for attack source tracing is set too high.

NOTE

If the threshold for attack source tracing is set too high, attack source tracing cannot identify attack packets or collect attack packet statistics.

Run the **auto-defend threshold** command to set a smaller threshold for attack source tracing.

NOTE

Only the S3700HI supports the **auto-defend action** command.

Copyright © Huawei Technologies Co., Ltd.

After a specified period, run the **display auto-defend attack-source** command to check whether the attack source list is displayed. If no attack source list is displayed, go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

- 1.3.6.1.4.1.2011.5.25.165.2.2.1.1
- 1.3.6.1.4.1.2011.5.25.165.2.2.1.2

Relevant Logs

None

7.7 MFF Troubleshooting

This chapter describes common causes of MAC Forced Forwarding (MFF) faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

7.7.1 Users Fail to Access the Internet After MFF Is Configured

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when users fail to access the Internet after MFF is configured.

Common Causes

This fault is commonly caused by one of the following:

- No binding table is generated for users.
- User access configurations are incorrect. For example, DHCP snooping is not enabled on the user-side interface; the network-side interface is not configured as a trusted interface; the user address is on a different network segment than the gateway address.
- MFF configurations are incorrect. For example, the user-side interface is not added to the MFF-enabled VLAN, or no network-side interface is configured.
- The S3700 does not receive any ARP reply packet from the gateway because the route from the S3700 to the gateway is unreachable or the link between them is busy.

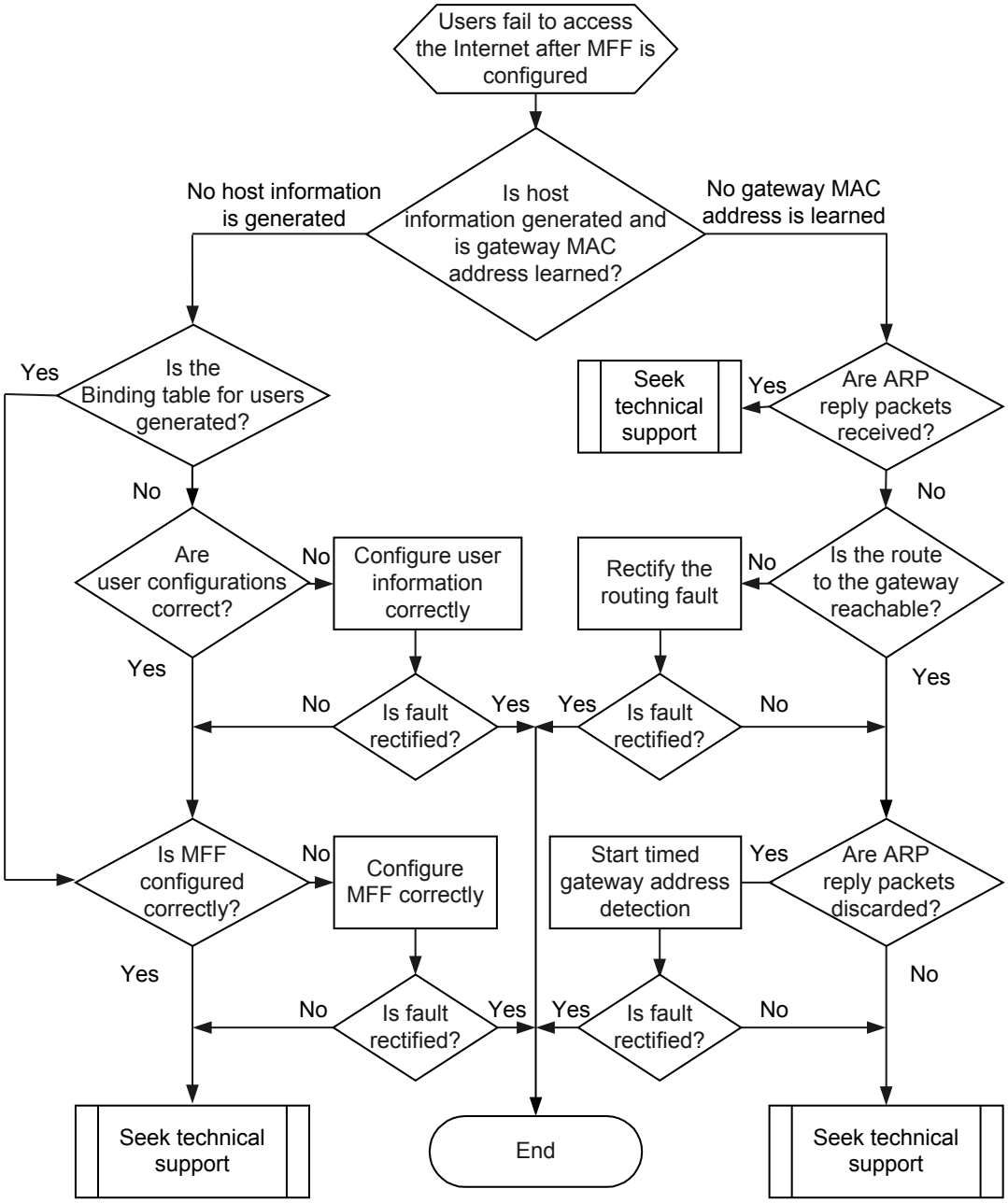
Troubleshooting Flowchart

The troubleshooting roadmap is as follows:

- Check whether MFF host information is generated.
- Check whether the gateway MAC address is learned by the S3700.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-18 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display mac-forced-forwarding vlan** *vlan-id* command to check generated MFF information.

Copyright © Huawei Technologies Co., Ltd.

- If the **User IP** and **User MAC** fields are empty, no host information is generated. Go to step 2.
- If the **Gateway MAC** field is empty, no gateway MAC address is learned. Go to step 3.

Step 2 Check configurations to ensure that MFF host information is generated.

1. Check that user access configurations are correct.

User Type	Check Item	Method	Solution
Dynamic user	DHCP snooping is enabled on the user-side interface.	Run the **display this** command in the user-side interface view to check whether the **dhcp snooping enable** command has been executed.	If the **dhcp snooping enable** command has not been executed, run this command in the interface view. You can also run this command in the VLAN view if the user-side interface has been added to the VLAN.
	The network-side interface is configured as a trusted interface.	Run the **display this** command in the network-side interface view to check whether the **dhcp snooping trusted** command has been executed.	If the **dhcp snooping trusted** command has not been executed, run this command in the interface view. You can also run the **dhcp snooping trusted interface** command in the VLAN view if the network-side interface has been added to the VLAN.
	Users can get online.	Run the **display dhcp snooping user-bind vlan** *vlan-id* command to check whether DHCP snooping entries exist.	If there is no DHCP snooping entry for the user IP address, the user cannot get online. Rectify the fault according to **7.4.1 Users Fail to Go Online After DHCP Snooping Is Configured**.

Copyright © Huawei Technologies Co., Ltd.

User Type	Check Item	Method	Solution
Static user	A correct static gateway address is configured.	Run the **display this** command in the MFF-enabled VLAN view to check whether the **mac-forced-forwarding static-gateway** *ip-address* command has been executed and whether the static gateway address is on the same network segment as the static user address.	If the **mac-forced-forwarding static-gateway** *ip-address* command is not run or the static gateway address is on a different network segment than the static user address, run the **mac-forced-forwarding static-gateway** *ip-address* command to configure a static gateway, which resides on the same network segment as the static user.

If the fault persists, go to step b.

2. Check that MFF configurations are correct.
   - Run the **display this** command in the user-side interface view to check whether the interface is added to the MFF-enabled VLAN. If not, add it to the MFF-enabled VLAN by using commands.
   - Run the **display this** command in the network-side interface view to check whether the **mac-forced-forwarding network-port** command is run. If it is not run, run this command.

   If MFF configurations of both the user-side and network-side interfaces are correct, go to step 3.

Step 3 Ensure that the S3700 can learn the gateway address.

1. Check whether the S3700 receives an ARP reply packet from the gateway.

   Run the **debugging ethernet packet arp interface** *interface-type interface-number* command in the user view to check whether the S3700 receives an ARP reply packet from the gateway.
   - If the S3700 does not receive any ARP reply packet from the gateway, go to step c for dynamic users, and go to step b for static users.
   - If the S3700 receives the ARP reply packet from the gateway, but the gateway MAC address still cannot be learned, go to step 4.
2. Check that the link between the S3700 and the gateway works properly.

   Ping the gateway from the S3700 to check whether the route between them is reachable.
   - If the ping fails, rectify the link fault according to A Ping Operation Fails.
   - If the ping succeeds, go to step c.

Copyright © Huawei Technologies Co., Ltd.

3. Check whether ARP reply packets are discarded.
   - Run the **display this** command in the interface view, VLAN view, and system view to check whether a rate limit is set for ARP packets.

     If the rate limit is set to a low value, ARP reply packets may be discarded. Run the **arp anti-attack rate-limit** command to increase the rate limit.
   - Run the **mac-forced-forwarding gateway-detect** command in the MFF-enabled VLAN view to enable timed gateway address detection and obtain the gateway MAC address by retransmitting an ARP request packet.

   If the gateway MAC address still cannot be learned, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.8 ACL Troubleshooting

This chapter describes common causes of ACL faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

7.8.1 A User-Defined ACL Fails to Take Effect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when a user-defined ACL fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

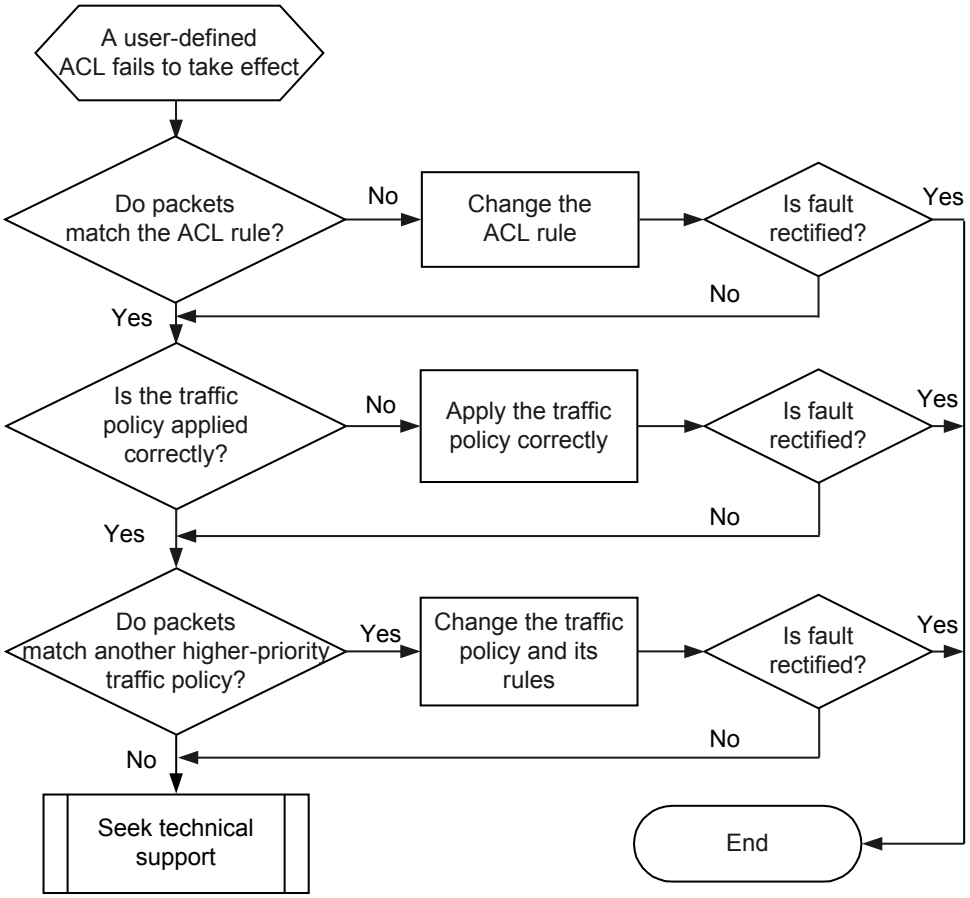
- Packets do not match user-defined ACL rules.
- The traffic policy configured with the user-defined ACL is applied incorrectly. For example, the traffic policy is applied to an incorrect object or applied in an incorrect direction.
- Packets match another traffic policy with a higher priority.

Troubleshooting Flowchart

If a user-defined ACL fails to take effect, see **Figure 7-19** to rectify the fault.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-19 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether packets match user-defined ACL rules.

CAUTION

User-defined ACLs match 4-byte information each time. Therefore, configuring 4-byte user-defined ACLs is recommended. If only 2 bytes are specified, the 2 bytes are used as the lower 2 bytes of 4 bytes to match information.

Run the **display acl** command to view user-defined ACL rules and then capture packets to check whether information in the packets (including the IP address, MAC address, DSCP priority, VLAN ID, and 802.1p priority) matches the user-defined ACL rules.

Copyright © Huawei Technologies Co., Ltd.

- If information in the packets does not match the user-defined ACL rules, run the **rule** command to modify the ACL rules to match the information.
- If information in the packets matches the user-defined ACL rules, go to step 2.

Step 2 Check that the traffic policy configured with the user-defined ACL is applied correctly.

1. Determine the traffic policy configured with the user-defined ACL.

   Run the **display current-configuration** command to view the current configuration file. Search the traffic classifier containing the **if-match acl** *acl-number* command, and then determine the traffic policy bound to this traffic classifier.

2. Check whether the traffic policy configured with the user-defined ACL is applied correctly.

   Run the **display traffic-policy applied-record** command to check whether the traffic policy is applied to the correct VLAN, LPU, or interface and whether the traffic policy is applied in the correct direction. On the S3700, when a user-defined ACL is applied, the traffic policy can be applied only in the inbound direction to match incoming packets.

   - If the traffic policy is applied to an incorrect object, run the **traffic-policy** command to apply the traffic policy to a correct object.
   - If the traffic policy is applied to an incorrect direction, run the **undo traffic-policy** command to delete the traffic policy, and then run the **traffic-policy** command to apply the traffic policy in the correct direction.
   - If the fault persists, go to step 3.

Step 3 Check whether packets match another traffic policy with a higher priority.

For details, see step 2 of **Troubleshooting Procedure** in **8.1.1 Traffic Policy Fails to Take Effect**.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the devices

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

7.8.2 Troubleshooting Cases

This section provides user-defined ACL troubleshooting cases.

A User-Defined ACL Fails to Limit the Packet Rate

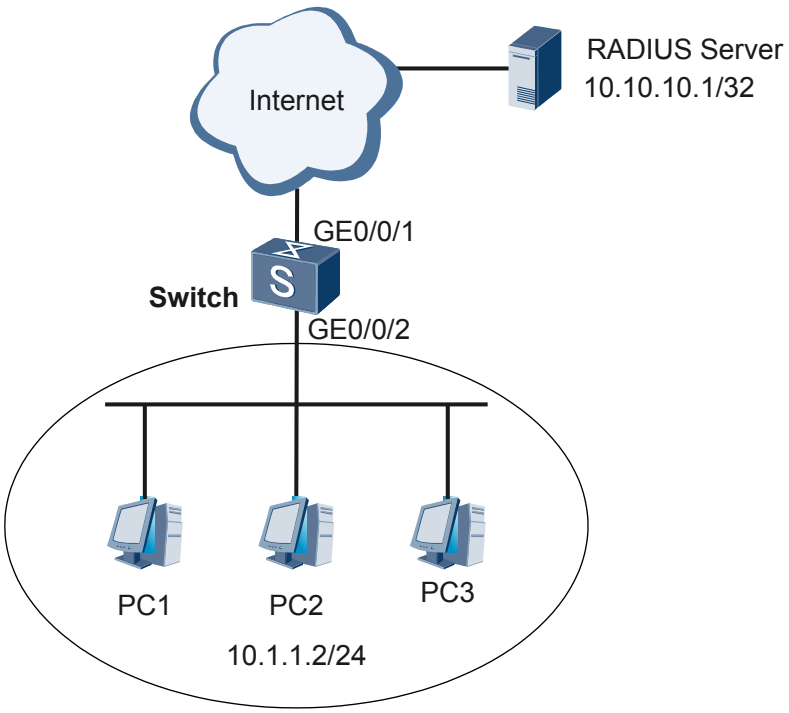
Fault Symptom

As shown in **Figure 7-20**, PCs access the network from GE 0/0/1 by using a PPPoE dialer and are authenticated by a RADIUS server. If too many user packets are sent to the RADIUS server,

Copyright © Huawei Technologies Co., Ltd.

the RADIUS server will stop responding. To solve this problem, the Switch needs to limit the rate of UDP packets from users by using a user-defined ACL. Assume that a user-defined ACL (ACL 5000) containing ACL rule of rule 5 permit l2-head 0x0011 0x00ff 30 is configured. The traffic behavior is to limit the packet rate to 20 Mbit/s and to collect traffic statistics, and the traffic policy name is specified as **udp**. After these configurations are complete, traffic is not limited and no traffic statistics are collected.

Figure 7-20 Network diagram



Configure the Switch.

```
<Quidway> system-view
[Quidway] acl 5000
[Quidway-acl-user-5000] rule permit l2-head 0x0011 0x00ff 30
[Quidway] traffic classifier udp
[Quidway-classifier-udp] if-match acl 5000
[Quidway-classifier-udp] quit
[Quidway] traffic behavior udp
[Quidway-behavior-udp] statistic  enable
[Quidway-behavior-udp] car cir 20000
[Quidway-behavior-udp] quit
[Quidway] traffic policy udp
[Quidway-trafficpolicy-udp] classifier udp behavior udp
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] traffic-policy udp inbound
```

After the preceding configurations are complete, use a tester to simulate login for a large number of users and observe outgoing traffic on GE 0/0/2. Traffic information shows that the traffic rate is still greater than 20 Mbit/s. That is, rate limit fails to take effect. Then run the **display traffic policy statistics interface** *interface-type interface-number* **inbound** command. The following command output is displayed.

```
[Quidway-GigabitEthernet0/0/2] display traffic policy statistics interface
gigabitethernet0/0/2 inbound

 Interface: GigabitEthernet0/0/2
```


Copyright © Huawei Technologies Co., Ltd.

```
 Traffic policy inbound: udp
 Rule number: 1
 Current status: OK!
 Board : 3
Item                                Packets                          Bytes
------------------------------------------------------------------------------
Matched                                   0                              0
  +--Passed                               0                              0
  +--Dropped                              0                              0
    +--Filter                             0                              0
    +--URPF                               -                              -
    +--CAR                                0                              0
```

The preceding command output shows that no traffic statistics are collected. This is, packets do not match the traffic policy **udp** configured with ACL 5000.

Fault Analysis

1. Check whether packets match the ACL rule.

   Run the **display acl 5000** command on the Switch. The following command output is displayed.

   ```
   [Switch] display acl 5000
   User ACL 5000, 1 rule
   Acl's step is 5
    rule 5 permit 0x00000011 0x000000ff 30
   ```

   Capture packets on GE 0/0/2 and analyze the packets sent from the Switch to the RADIUS server. Packet information shows that the UDP protocol number is 0x11, and the offset from the Layer 2 header is 30. 0x11 should match higher 16 bits, but the ACL rule is configured to match lower 16 bits. As a result, packets fail to match the ACL rule.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **acl 5000** command to enter the user-defined ACL view.

Step 3 Run the **undo rule 5** command to delete ACL rule 5.

Step 4 Run the **rule permit l2-head 0x00110000 0x00ff0000 30** command to re-define an ACL rule.

After the preceding configurations are complete, use a tester to simulate login for a large number of users, and observe outgoing traffic on GE 0/0/2. Traffic information shows that the traffic rate is smaller than 20 Mbit/s. The fault is rectified.

----End

Summary

On the S3700, user-defined ACLs match 4-byte information each time. Therefore, configuring 4-byte user-defined ACLs is recommended. If only 2 bytes are specified, the S3700 uses the 2 bytes as the lower 2 bytes of 4 bytes to match information.

7.9 PPPoE+ Troubleshooting

This chapter describes common causes of Point-to-Point Protocol over Ethernet (PPPoE) faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

7.9.1 PPPoE Users Fail to Access the Internet

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when PPPoE users fail to access the Internet.

Common Causes

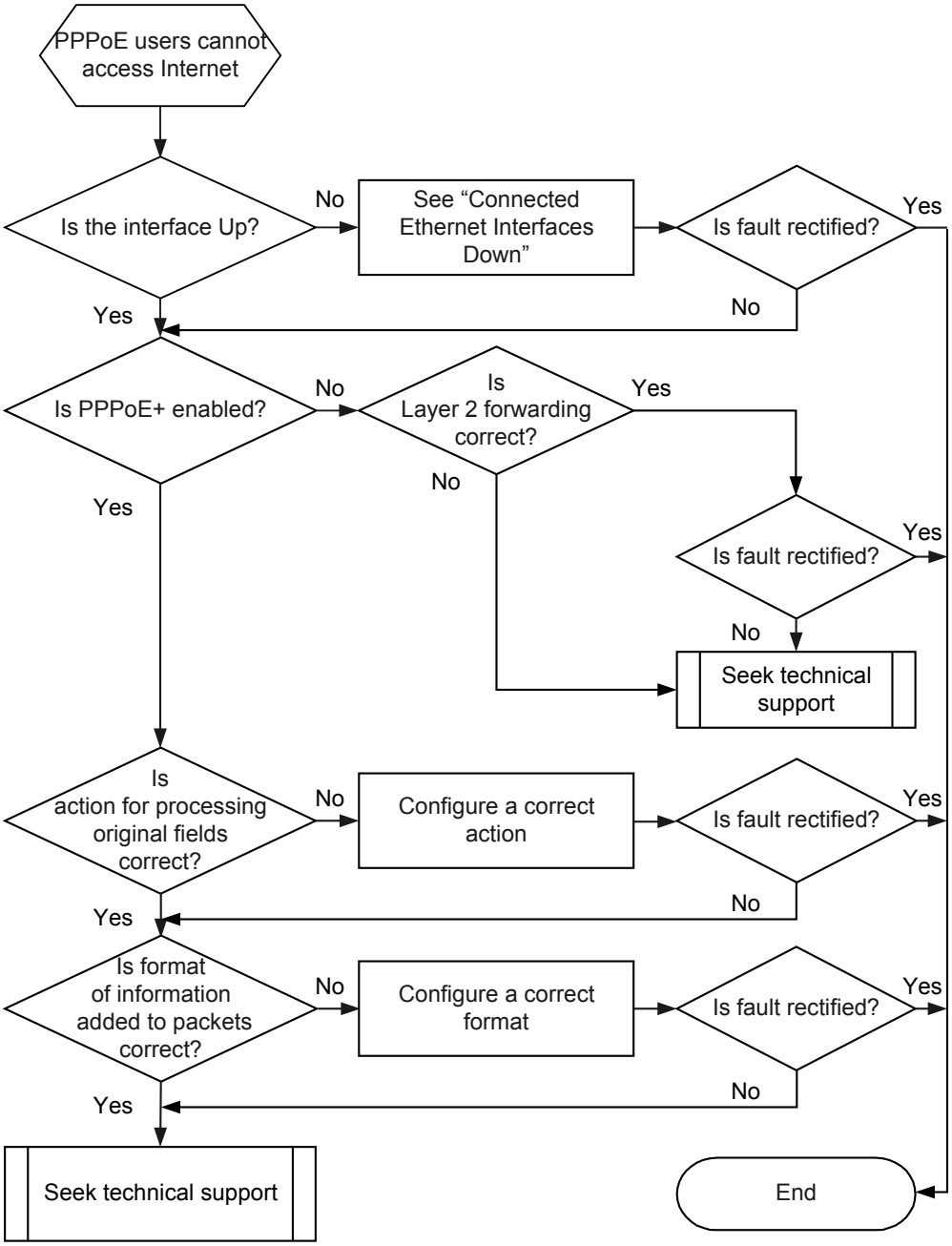
This fault is commonly caused by one of the following:

- The link between the PPPoE client and the PPPoE server is faulty.
- This PPPoE+ configuration is incorrect. For example, an uplink interface is an untrusted interface, or the action for processing original fields in PPPoE packets or the format of information added to PPPoE packets is incorrect.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 7-21 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the connected interfaces of the user device, S3700, and PPPoE server are Up.

Copyright © Huawei Technologies Co., Ltd.

- If some interfaces are Down, rectify the fault according to **4.1.1 Connected Ethernet Interfaces Down**.
- If these interfaces are Up, go to step 2.

Step 2 Check that PPPoE+ is enabled.

Run the **display this** command in the system view to check whether the **pppoe intermediate-agent information enable** command was executed. If not, PPPoE+ is disabled.

- If PPPoE+ is disabled, the S3700 directly forwards PPPoE packets at Layer 2. If PPPoE packets are not forwarded from the S3700, or if packets are forwarded at Layer 2 but PPPoE users cannot access the Internet, go to step 4.
- If PPPoE+ is enabled, go to step 3.

Step 3 Check that the PPPoE+ configuration is correct.

1. Check whether the network-side interface connected to the PPPoE server is the trusted interface.

   If the network-side interface is not the trusted interface, PPPoE server spoofing may occur or PPPoE packets are forwarded to non-PPPoE interfaces. As a result, authorized PPPoE users cannot access the Internet.

   Run the **display this** command in the view of the network-side interface to check whether the **pppoe uplink-port trusted** command was executed.

   - If no, the network-side interface is an untrusted interface. Run the **pppoe uplink-port trusted** command to configure the network-side interface as the trusted interface.
   - If yes, the network-side interface is the trusted interface. Go to step b.

2. Check whether the action for processing original fields in PPPoE packets is correct.

   Run the **display this** command in the system view and in the view of the user-side interface to check whether the **pppoe intermediate-agent information policy** command was executed in the system and on the interface. If the actions for processing original information fields in PPPoE packets are configured on the interface and in the system, the action configured on the interface takes effect. If the action for processing original fields in PPPoE packets is not configured on the interface or in the system, the system replaces the original fields in PPPoE packets according to the configured field format by default.

   Check whether the action for processing original fields in PPPoE packets is correct.

   - If the action is incorrect, run the **pppoe intermediate-agent information policy** command to configure a correct action.
   - If the action is correct, go to step c.

3. Check that the format of information added to PPPoE packets is correct.

   Run the **display pppoe intermediate-agent information format** command to check whether the format of information added to PPPoE packets is supported by the PPPoE server.

   - If the format is not supported by the PPPoE server, run the **pppoe intermediate-agent information format** command to configure a format supported by the PPPoE server.
   - If the format is supported by the PPPoE server, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure

Copyright © Huawei Technologies Co., Ltd.

- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

8 QoS

About This Chapter

8.1 Traffic Policy Troubleshooting
This chapter describes common causes of traffic policy faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.2 Priority Mapping Troubleshooting (S3700SI or S3700EI)
This chapter describes common causes of priority mapping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.3 Priority Mapping Troubleshooting (S3700HI)
This chapter describes common causes of priority mapping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.4 Traffic Policing Troubleshooting
This chapter describes common causes of traffic policing faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.5 Traffic Shaping Troubleshooting
This chapter describes common causes of traffic shaping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.6 Congestion Avoidance Troubleshooting
This chapter describes common causes of congestion avoidance faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.7 Congestion Management Troubleshooting
This chapter describes common causes of congestion management faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

8.1 Traffic Policy Troubleshooting

This chapter describes common causes of traffic policy faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.1.1 Traffic Policy Fails to Take Effect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when the traffic policy fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

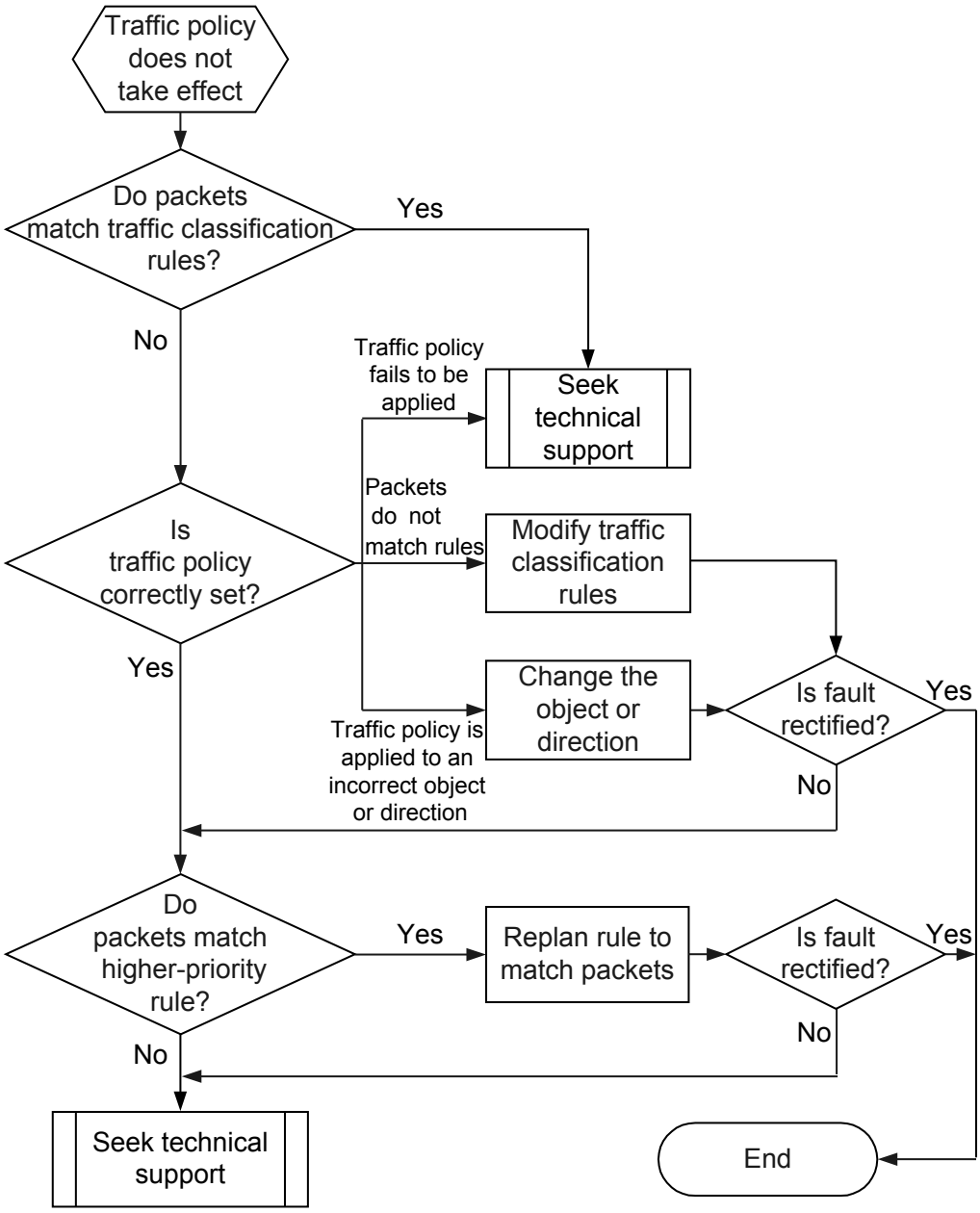
- The packets do not match rules of the traffic classifier in the traffic policy.
- The traffic behavior associated with the traffic classifier in the traffic policy is configured incorrectly.
- The traffic policy is applied to an incorrect object.
- The traffic policy is also applied to another object with a higher priority. A traffic policy can be applied to an interface, a VLAN, and the entire system. The traffic policy has the highest priority if applied to an interface, and the lowest priority if applied to the entire system.
- The traffic policy conflicts with another applied traffic policy and the packets match rules in the applied traffic policy.

Troubleshooting Flowchart

Figure 8-1 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-1 Troubleshooting flowchart for ineffective traffic policy



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether packets match traffic classification rules.

Copyright © Huawei Technologies Co., Ltd.

Run the **display traffic policy statistics** command to check the traffic statistics in the system, on an interface, or in a VLAN to which a traffic policy is applied. If the corresponding field is empty, packets do not match traffic classification rules.

NOTE

Before viewing the traffic statistics, you must run the **statistic enable** command in the traffic behavior view to configure the traffic statistics function.

- If packets match traffic classification rules, go to step 4.
- If packets do not match traffic classification rules, go to step 2.

Step 2 Check that the traffic policy is configured correctly.

1. Check whether the information in the packets matches traffic classification rules.

   Check the information in the packets such as the IP address, MAC address, DSCP priority, VLAN ID, and 802.1p priority, run the **display traffic policy user-defined** command to view the traffic classifier bound to the traffic policy, and then run the **display traffic classifier user-defined** command to view the rules in the traffic classifier. Capture the packets on the inbound interface. Check whether packet characteristics match traffic classification rules.

   - If not, modify the rules to match the information in the packets.
   - If yes, go to step b.

2. Run the **display traffic policy user-defined** *policy-name* **classifier** *classifier-name* command to check whether the traffic behavior associated with the traffic classifier is configured correctly.

   - If not, run the **traffic behavior** command to enter the traffic behavior view and correctly configure the traffic behavior.
   - If yes, go to step c.

3. Check whether the traffic policy is applied correctly.

   Run the **display traffic-policy applied-record** command to check whether the traffic policy is applied successfully, whether the traffic policy is applied to the correct VLAN, LPU, or interface and whether the traffic policy is applied to the correct direction. On the S3700, when the traffic policy is applied to incoming packets, the displayed traffic policy direction should be **inbound**; when it is applied to outgoing packets, the displayed traffic policy should be **outbound**.

   NOTE

   On the S3700SI and S3700EI, a traffic policy cannot be applied to an LPU or in the outbound direction.

   - If the traffic policy is applied to an incorrect object or direction, run the **undo traffic-policy** command to unbind the traffic policy from the incorrect object or direction, and then run the **traffic-policy** command to re-apply the traffic policy.
   - If the traffic policy is applied to an incorrect object or direction, run the **traffic-policy** command to re-apply the traffic policy.

     NOTE

     On the S3700SI or S3700EI, run the **undo traffic-policy** command to unbind the traffic policy from an incorrect object before running the **traffic-policy** command to re-apply the traffic policy.

   - If the traffic policy fails to be applied, go to step 4.
   - If yes, go to step 3.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Check whether packets match another rule that has a higher priority.

Run the **display current-configuration** command to check whether packets match another rule on the S3700.

NOTE

On the S3700HI, check the matching order of traffic classifiers in a traffic policy.

- If not, go to step 4.
- If there is another matching rule check the rule that takes effect:

1. Check the types of traffic classifiers.

   The S3700 supports four types of traffic classifiers, which are based on Layer 2 information, Layer 3 information, User-defined Flow (UDF), and Layer 2 and Layer 3 information. The rule priorities of the traffic classifiers in descending order are UDF, Layer 2 and Layer 3 information, Layer 3 information, and Layer 2 information.

   The rules in traffic classifiers are defined as follows:

   - Layer 2: The traffic classifier contains only Layer 2 rules.
   - Layer 3: The traffic classifier contains only Layer 3 rules.
   - Layer 2 and Layer 3: The traffic classifier contains Layer 2 and Layer 3 rules. The logical relationship between the rules is OR.
   - UDF: The traffic classifier contains only user-defined rules.

   Table 8-1 describes the classification of rules in traffic classifiers.

Table 8-1 Classification of rules in traffic classifiers

Type	Rule
Layer 2	• **if-match acl 4000-4999** • **if-match any** • **if-match cvlan-8021p** • **if-match cvlan-id** • **if-match 8021p** • **if-match vlan-id** • **if-match destination-mac** • **if-match source-mac** • **if-match inbound-interface** • **if-match outbound-interface** • **if-match discard** • **if-match double-tag** • **if-match l2-protocol**

Copyright © Huawei Technologies Co., Ltd.

Type	Rule
Layer 3	● **if-match acl 2000-2999** ● **if-match acl 3000-3999** ● **if-match dscp** ● **if-match ip-precedence** ● **if-match protocol** ● **if-match tcp**
UDF	● **if-match acl 5000-5999**

2. Check the object where the traffic policy is applied.

   On the S3700, the traffic policy can be applied to the entire system a VLAN, or an interface. When rules in traffic classifiers are of the same type and the traffic policy is applied to different objects, the traffic policies applied to an interface, a VLAN, and the entire system take effect in descending order of priority.

If the rule takes precedence over the current rule, the traffic action corresponding to the rule takes effect. Replan the rule so that the current rule takes effect and other services are not affected. Otherwise, go to step 4.

- If there is another matching rule and the configuration order is used for traffic classifiers in a traffic policy on the S3700HI, check the rule that take effect as follows:

  1. Compare the objects to which the traffic policies are applied if the rule and the current rule are bound to different traffic policies. On the S3700, the traffic policies applied to an interface, a VLAN, and the system take effect in descending order of priority. The rule that is bound to the traffic policy with a higher priority takes effect.
  2. Determine the sequence in which traffic classifiers were bound to a traffic policy. If the rule and the current rule are bound to the same traffic policy but are in different traffic classifiers, the rule in the traffic classifier that is bound to the traffic policy first takes effect.
  3. Determine the sequence in which rules were configured in an ACL. If the rule and the current rule are bound to the same traffic policy, traffic classifier, and ACL, the rule that was configured in the ACL first takes effect.

  If another rule takes effect, modify the rule so that the current rule takes effect and other services are not affected. Otherwise, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Copyright © Huawei Technologies Co., Ltd.

Relevant Logs

None.

8.1.2 Troubleshooting Cases

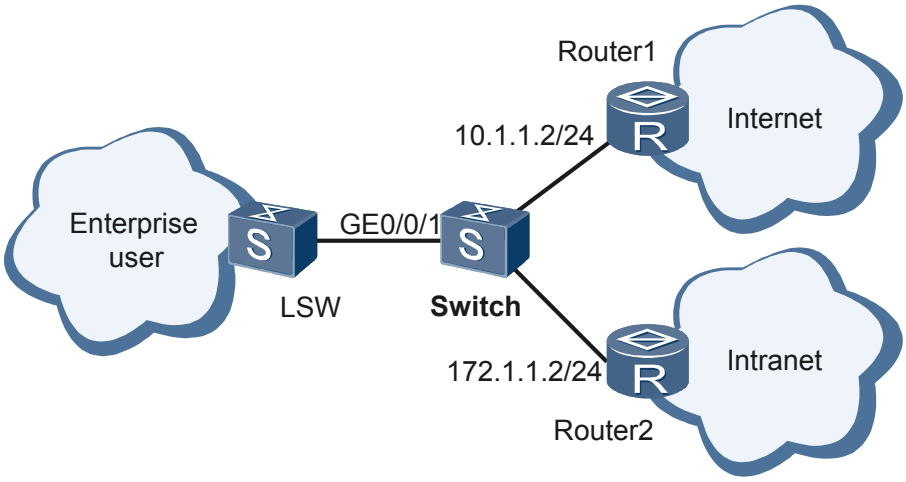
This section provides traffic policy troubleshooting cases.

PBR Based on Traffic Policies Fails to Take Effect (S3700SI or S3700EI)

Fault Symptom

As shown in **Figure 8-2**, policy-based routing (PBR) based on traffic policies is configured on the Switch so that data flows are redirected to the next hop 10.1.1.2/24 when enterprise users access the Web service.

Figure 8-2 Network diagram



After the configuration, data flows are not redirected to the next hop 10.1.1.2 when enterprise users access the Web service.

Fault Analysis

1. Capture packets on the inbound interface GE 0/0/1 of the Switch when enterprise users access the Web service. Data flows for enterprise users' access to the Web service can be captured.
2. Run the **display ip routing-table** command to view the routing table. There is a route to 10.1.1.2/24.
3. Check whether the data flows match another rule with a higher priority.
   (1) Run the **display this** command in the view of the inbound interface GE 0/0/1 to view the traffic policy configuration.

```
[Switch-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
```


Copyright © Huawei Technologies Co., Ltd.

```
 port trunk allow-pass vlan 100
 traffic-policy tp1 inbound
#
return
```

(2) Run the **display traffic policy user-defined** command to view the detailed traffic policy configuration.

```
[Switch] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
     Operator: AND
     Behavior: tb1
      Deny
   Classifier: tc2
     Operator: AND
     Behavior: tb2
      Redirect:
        Redirect ip-nexthop
        10.1.1.2
```

(3) Run the **display traffic classifier user-defined** command to check the configurations of traffic classifiers **tc1** and **tc2**. The system displays the following information:

```
[Switch] display traffic classifier user-defined tc1
  User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match any
              if-match dscp 6
[Switch] display traffic classifier user-defined tc2
  User Defined Classifier Information:
   Classifier: tc2
    Operator: AND
    Rule(s) : if-match acl 3000
```

(4) Run the **display acl 3000** command to view the content of ACL 3000.

```
[Switch] display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit tcp destination-port eq www
```

The preceding information indicates that the traffic policy is bound to two traffic classifiers **tc1** and **tc2**. The matching rule of **tc1** is **if-match any** and **if-match dscp 6**, which is a Layer 2 and Layer 3 rule. The matching rule of **tc2** is **if-match acl 3000**, which is a Layer 3 rule. On the S3700, a Layer 2 and Layer 3 rule takes precedence over a Layer 3 rule. Therefore, the data flows match **tc1** and contain the **deny** action. Such data flows are discarded and cannot be redirected to 10.1.1.2/24.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the GE 0/0/1 interface view.

Step 3 Run the **undo traffic-policy inbound** command to delete the traffic policy from the interface.

Step 4 Run the **quit** command to exit the interface view.

Step 5 Run the **traffic policy tp1** command to enter the view of the traffic policy **tp1**.

Step 6 Run the **undo traffic classifier tc1** command to unbind the traffic classifier tc1 from the traffic policy.

Copyright © Huawei Technologies Co., Ltd.

Step 7 Run the **quit** command to exit the traffic policy view.

Step 8 Run the **interface** *interface-type interface-number* command to enter the GE 0/0/1 interface view.

Step 9 Run the **traffic-policy tp1 inbound** command to re-apply the traffic policy to GE 0/0/1.

After the preceding operations, when enterprise users access the Web service, data flows are redirected to the next hop 10.1.1.2. The fault is rectified.

NOTE

On the S3700HI, only steps 1, 5, and 6 need to be performed.

Before unbinding the traffic classifier **tc1** from the traffic policy, ensure that **tc1** is not in use. You may need to replan the rule priorities according to the network requirements.

----End

Summary

If PBR based on traffic policies fails to take effect, the possible causes are as follows:

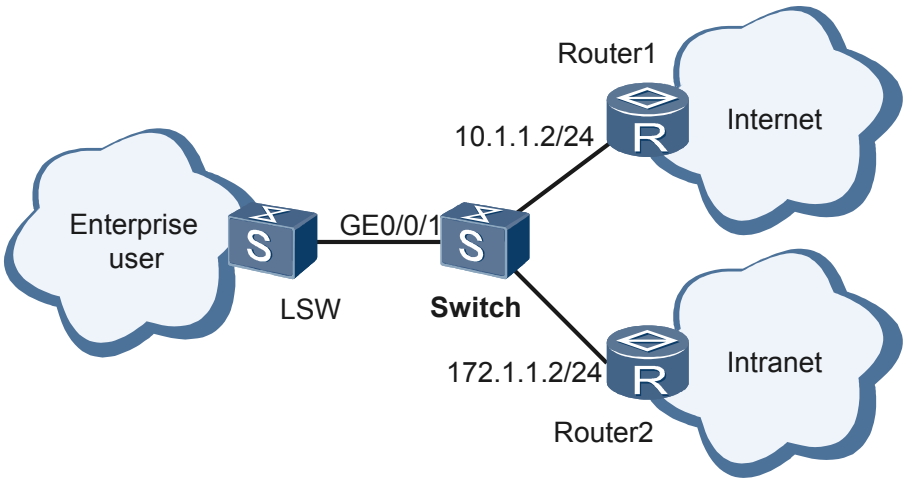
- The data flows do not match rules in the traffic policy.
- The route destined for the next hop does not exist in the routing table.
- The data flows match a rule with a higher priority. For details on how to determine priorities of rules, see **Troubleshooting Procedure** in **8.1.1 Traffic Policy Fails to Take Effect**.

PBR Based on Traffic Policies Fails to Take Effect (S3700HI)

Fault Symptom

As shown in **Figure 8-3**, policy-based routing (PBR) based on traffic policies is configured on the Switch so that data flows are redirected to the next hop 10.1.1.2/24 when enterprise users access the Web service.

Figure 8-3 Network diagram



Copyright © Huawei Technologies Co., Ltd.

After the configuration, data flows are not redirected to the next hop 10.1.1.2 when enterprise users access the Web service.

Fault Analysis

1. Capture packets on the inbound interface GE 0/0/1 of the Switch when enterprise users access the Web service. Data flows for enterprise users' access to the Web service can be captured.
2. Run the **display ip routing-table** command to view the routing table. There is a route to 10.1.1.2/24.
3. Check whether the data flows match another rule with a higher priority.

   (1) Run the **display this** command in the view of the inbound interface GE 0/0/1 to view the traffic policy configuration.

   ```
   [Switch-GigabitEthernet0/0/1] display this
   #
   interface GigabitEthernet0/0/1
    port link-type trunk
    port trunk allow-pass vlan 100
    traffic-policy tp1 inbound
   #
   return
   ```

   (2) Run the **display traffic policy user-defined** command to view the detailed traffic policy configuration.

   ```
   [Switch] display traffic policy user-defined tp1
     User Defined Traffic Policy Information:
     Policy: tp1
      Classifier: tc1
        Operator: AND
        Behavior: tb1
         Deny
      Classifier: tc2
        Operator: AND
        Behavior: tb2
         Redirect:
           Redirect ip-nexthop 10.1.1.2
   ```

   (3) Run the **display current-configuration** command to check the matching order of traffic classifiers in the traffic policy.

   Two traffic classifiers are bound to the traffic policy **tp1**; therefore, you need to check the matching order of traffic classifiers in the traffic policy.

   ```
   <Quidway> display current-configuration
   #
   traffic policy tp1
    classifier tc1 behavior tb1
    classifier tc2 behavior tb2
   ```

   The preceding information indicates that the automatic order is used.

   NOTE

   The automatic order is used by default and is not displayed in the configuration file.

   (4) Run the **display traffic classifier user-defined** command to check the configurations of traffic classifiers **tc1** and **tc2**. The system displays the following information:

   ```
   [Switch] display traffic classifier user-defined tc1
     User Defined Classifier Information:
      Classifier: tc1
       Operator: AND
       Rule(s) : if-match any
                 if-match dscp 6
   [Switch] display traffic classifier user-defined tc2
   ```


Copyright © Huawei Technologies Co., Ltd.

```
  User Defined Classifier Information:
   Classifier: tc2
    Operator: AND
    Rule(s) : if-match acl 3000
```

(5) Run the **display acl 3000** command to view the content of ACL 3000.

```
[Switch] display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit tcp destination-port eq www
```

The preceding information indicates that the matching order of traffic classifiers in the traffic policy is **auto** and the traffic policy is bound to two traffic classifiers **tc1** and **tc2**. The matching rule of **tc1** is **if-match any** and **if-match dscp 6**, which is a Layer 2 and Layer 3 rule. The matching rule of **tc2** is **if-match acl 3000**, which is a Layer 3 rule. On the S3700, if the matching order of traffic classifiers in the traffic policy is **auto**, a Layer 2 and Layer 3 rule takes precedence over a Layer 3 rule. Therefore, the data flows match **tc1** and contain the **deny** action. Such data flows are discarded and cannot be redirected to 10.1.1.2/24.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **traffic policy tp1** command to enter the view of the traffic policy **tp1**.

Step 3 Run the **undo traffic classifier tc1** command to unbind the traffic classifier tc1 from the traffic policy.

After the preceding operations, when enterprise users access the Web service, data flows are redirected to the next hop 10.1.1.2. The fault is rectified.

NOTE

Before unbinding the traffic classifier **tc1** from the traffic policy, ensure that **tc1** is not in use. You may need to replan the rule priorities according to the network requirements.

----End

Summary

If PBR based on traffic policies fails to take effect, the possible causes are as follows:

- The data flows do not match rules in the traffic policy.
- The route destined for the next hop does not exist in the routing table.
- The data flows match a rule with a higher priority. For details on how to determine priorities of rules, see **Troubleshooting Procedure** in **8.1.1 Traffic Policy Fails to Take Effect**.

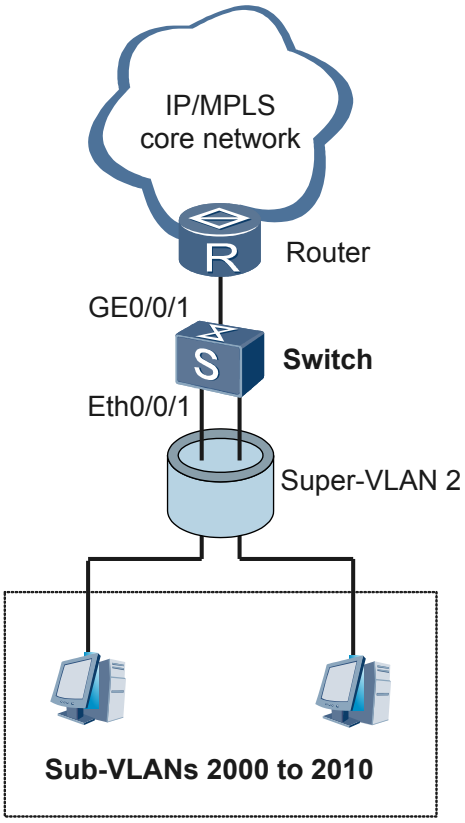
Re-marking Fails to Take Effect After the Traffic Policy Is Applied to the Super-VLAN

Fault Symptom

As shown in **Figure 8-4**, the re-marking function is configured on the Switch to re-mark DSCP priorities of user packets. The upstream router then performs unified QoS control of user packets according to the re-marked priorities.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-4 Network diagram



After the configuration is complete, packets are captured on the inbound interface Eth 0/0/1 and the outbound interface GE 0/0/1. The captured packets show that their DSCP priorities remain unchanged, which means that the re-marking function fails to take effect.

Fault Analysis

1. Run the **display current-configuration** command to check the configuration of the Switch.

   The command output is as follows:

```
<Switch> display current-configuration
traffic classifier temp operator and
 if-match any
traffic behavior temp
 statistic enable
 remark dscp af23
traffic policy temp
 classifier temp behavior temp
vlan 2
 traffic-policy temp inbound
 aggregate-vlan
 access-vlan 2000 to 2010

#
interface Ethernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2000 to 2010
#
interface GigabitEthernet0/0/1
```


Copyright © Huawei Technologies Co., Ltd.

```
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2000 to 2010
```

The preceding information indicates that a traffic policy (the only traffic policy) on the Switch re-marks AF23 on all packets and is applied to the inbound direction in super-VLAN 2. Such a configuration of the Switch is correct.

2. Run the **display traffic policy statistics vlan 2** command on the Switch to check whether the traffic policy is matched.

   The command output is as follows:

```
<Switch> display traffic policy statistics vlan 2 inbound verbose classifier-
base
 Vlan: 2
 Traffic policy inbound: temp
 Rule number: 1
 Current status: OK!
-------------------------------------------------------------------------
 Classifier: temp operator and
 Behavior: temp
 Board : 0
Item                                Packets                         Bytes
-------------------------------------------------------------------------
Matched                                   0                             0
  +--Passed                               0                             0
  +--Dropped                              0                             0
    +--Filter                             0                             0
    +--URPF                               -                             -
    +--CAR                                0                             0
```

   The preceding information indicates that the traffic policy in super-VLAN 2 is not matched.

3. Analyze the packets captured on Eth0/0/1. The packets carry VLAN 2000, different from super-VLAN 2 to which the traffic policy is applied.

   When a traffic policy is applied to the super-VLAN, the traffic policy matches only the packets carrying the super-VLAN ID and it is ineffective for packets in sub-VLANs.

Procedure

Step 1 Run the **system-view** command on the Switch to enter the system view.

Step 2 Run the **vlan 2** command to enter the VLAN view.

Step 3 Run the **undo traffic-policy inbound** command to unbind a traffic policy from VLAN 2.

Step 4 Run the **quit** command to exit the VLAN view.

Step 5 Run the **traffic classifier temp** command to enter the traffic classifier view.

Step 6 Run the **if-match vlan-id 2000 to 2010** command to change the rule of the traffic classifier to match all packets in sub-VLANs.

Step 7 Run the **interface ethernet 0/0/1** command to enter the inbound interface view.

Step 8 Run the **traffic-policy temp inbound** command to apply the traffic policy to the inbound direction of the inbound interface.

After the preceding steps, packets captured on Eth 0/0/1 and GE 0/0/1 show that the DSCP priorities are re-marked with AF23. The fault is rectified.

Copyright © Huawei Technologies Co., Ltd.

NOTE

On the S3700HI, traffic polices can be changed dynamically. You need to perform step 1, step 5, and step 6.

----End

Summary

When a traffic policy is applied to the super-VLAN, the traffic policy matches only the packets carrying the super-VLAN ID but not the sub-VLAN ID. To match the traffic policy with the packets in the super-VLAN, you need to configure the traffic policy to match all the packets in sub-VLANs and apply the traffic policy to interfaces of sub-VLANs.

8.2 Priority Mapping Troubleshooting (S3700SI or S3700EI)

This chapter describes common causes of priority mapping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.2.1 Packets Enter Incorrect Queues

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when packets enter incorrect queues.

Common Causes

This fault is commonly caused by one of the following:

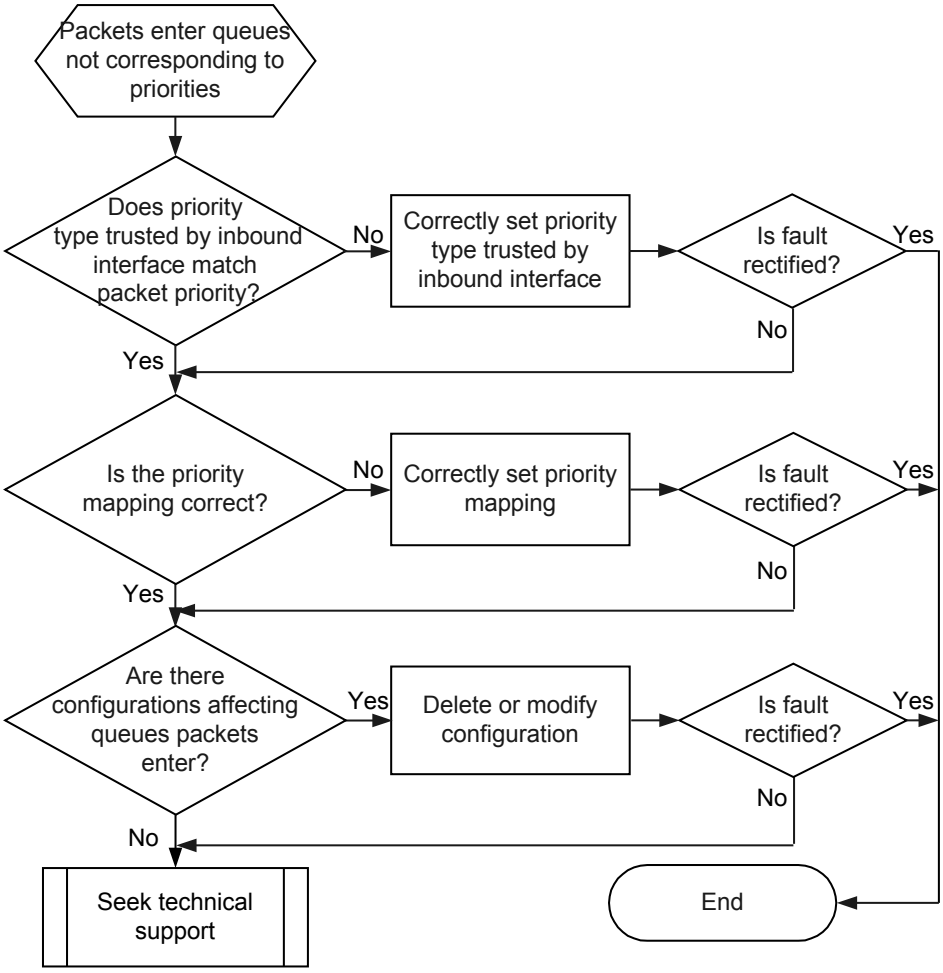
- The priority type of packets is different from the priority type trusted by the inbound interface.
- Priority mapping in the priority mapping table is incorrect.
- There are configurations affecting the queues that packets enter on the inbound interface, including:
  - **port vlan-stacking**
  - **port vlan-mapping vlan inner-vlan**, or **port vlan-mapping vlan map-vlan**
  - **port link-type dot1q-tunnel**
  - **traffic-policy** containing the **remark 8021p**, **remark dscp**, **remark local-precedence**, or **remark ip-precedence** action
- **traffic-policy** containing the **remark 8021p**, **remark dscp**, **remark local-precedence**, or **remark ip-precedence** action in the VLAN that packets belong to.
- There are configurations affecting the queues that packets enter in the system, including:
  - **qos local-precedence-queue-map**
  - **traffic-policy** where **remark 8021p**, **remark dscp**, **remark local-precedence**, or **remark ip-precedence** action is defined

Troubleshooting Flowchart

Figure 8-5 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-5 Troubleshooting flowchart for packets entering incorrect queues



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the priority type of packets is the same as the priority type trusted by the inbound interface.

Run the **display this** command in the inbound interface view to check the configuration of the **trust** command on the inbound interface (if the **trust** command is not used, the system does not trust any priority by default). Then, capture packets on the inbound interface, and check whether the priority type of the captured packets is the same as the priority type trusted by the inbound interface.

- If not, run the **trust** command to modify the priority type trusted by the inbound interface to be the same as the priority type of the captured packets.
- If yes, go to step 2.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Check whether priority mapping is correct.

Enter the priority mapping table view and run the **display this** command to check whether priority mapping is configured correctly.

- If priority mapping is configured incorrectly, run the **input** command in the DSCP priority mapping table view or the **input** command in the IP mapping table view.
- If priority mapping is configured correctly, go to step 3.

Step 3 Check whether there are configurations affecting the queues that packets enter on the device.

1. Check whether there are configurations affecting the queues that packets enter on the inbound interface.

   The following configurations affect the queues that packets enter on the inbound interface:

   - If the **port vlan-stacking** command is used with **remark-8021p** specified, the priorities of packets are re-marked. The mapping between 802.1p priorities and local priorities may be incorrect and packets may enter incorrect queues.
   - If the **port vlan-mapping vlan inner-vlan**, or **port vlan-mapping vlan map-vlan** command is used with **remark-8021p** specified, the priorities of packets are re-marked. The mapping between 802.1p priorities and local priorities may be incorrect and packets may enter incorrect queues.
   - If the **traffic-policy** command where **remark local-precedence** is defined is used for incoming packets, the system sends packets to queues based on the re-marked priority.
   - If the **traffic-policy** command where **remark 8021p**, **remark ip-precedence** or **remark dscp** is defined is used, the system maps the re-marked priorities of packets to 802.1p priorities and sends the packets to queues based on the mapped priorities.
   - If the **port link-type dot1q-tunnel** command is used, all the packets reaching the interface enter queues based on the default 802.1p priority of the interface. The default 802.1p priority of an interface is set by using the **port priority** command. The default 802.1p priority of an interface is 0.

   Run the **display this** command in the inbound interface view to check whether there are configurations affecting the packets enqueuing on the inbound interface.

   - If yes, delete or modify the configurations as required.
   - If not, go to step b.

2. Check whether there are configurations affecting the queues that packets enter in the VLAN that the inbound interface of the packets belong to.

   The following configurations affect the queues that packets enter:

   - If the **traffic-policy** command where **remark local-precedence** is defined is used, the system sends packets to queues based on the re-marked priorities.
   - If the **traffic-policy** command where **remark 8021p**, **remark ip-precedence** or **remark dscp** is defined is used, the system maps the re-marked priorities of packets to 802.1p priorities and sends the packets to queues based on the mapped priorities.

   Run the **display this** command in the view of the VLAN that the inbound interface of the packets belongs to and check whether there are configurations affecting the queues that packets enter in the VLAN.

   - If yes, delete or modify the configurations as required.
   - If not, go to step c.

3. Check whether there are configurations affecting the queues that packets enter in the system.

Copyright © Huawei Technologies Co., Ltd.

The following configurations affect the queues that packets enter:

- If the **qos local-precedence-queue-map** command is used, the system sends packets to queues based on the mapping between local priorities and queues specified by this command.
- If the **traffic-policy** command where **remark local-precedence** is defined is used, the system sends packets to queues based on the re-marked priority.
- If the **traffic-policy** command where **remark 8021p**, **remark ip-precedence** or **remark dscp** is defined is used, the system maps the re-marked priorities of packets to 802.1p priorities and sends the packets to queues based on the mapped priorities.

Run the **display current-configuration** command to check whether the configurations affecting the packets enqueuing are performed in the system.

- If yes, delete or modify the configurations as required.
- If not, go to step 4.

NOTE

If the packets match traffic classifiers in two or all traffic policies applied to an interface, a VLAN, and the system, the traffic policies applied to the interface, VLAN, and system take effect in descending order of priorities.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

8.2.2 Priority Mapping Results Are Incorrect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when priority mapping results are incorrect.

Common Causes

This fault is commonly caused by one of the following:

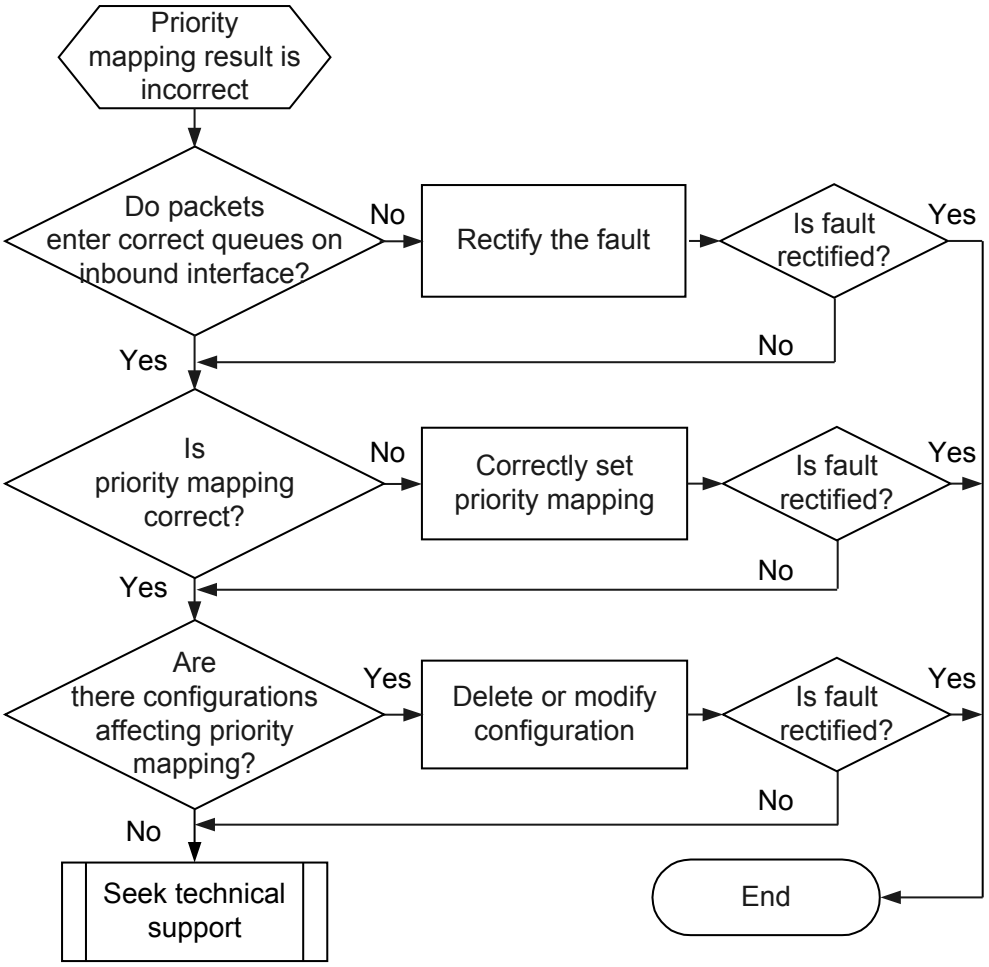
- On the inbound interface, packets enter incorrect queues.
- The type of the priority trusted by the outbound interface is incorrect.
- Priority mapping in the priority mapping table is incorrect.
- There are configurations affecting the priority mapping on the outbound interface. For example: **traffic-policy** containing the **remark 8021p**, **remark ip-precedence** or **remark dscp** action.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 8-6 shows the troubleshooting flowchart.

Figure 8-6 Troubleshooting flowchart for incorrect priority mapping



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that packets enter correct queues on the inbound interface.

Run the **display qos queue statistics** command to check whether packets enter correct queues on the inbound interface.

- If not, rectify the fault according to **8.2.1 Packets Enter Incorrect Queues**.
- If yes, go to step 2.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Check whether priority mapping is correct.

Enter the priority mapping table view and run the **display this** command to check whether priority mapping is configured correctly.

- If priority mapping is configured incorrectly, run the **input** command in the DSCP priority mapping table view or the **input** command in the IP mapping table view.
- If priority mapping is configured correctly, go to step 3.

Step 3 Check whether the configurations affecting priority mapping are performed on the outbound interface.

The following configurations affect priority mapping on the outbound interface:

- If the **traffic-policy** command where **remark 8021p**, **remark ip-precedence** or **remark dscp** is defined is used on the outbound interface, the re-marked priority is the packet priority.

Run the **display this** command in the view of the outbound interface to check whether the configurations affecting priority mapping are performed on the outbound interface.

- If yes, delete or modify the configurations as required.
- If not, go to step 5.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

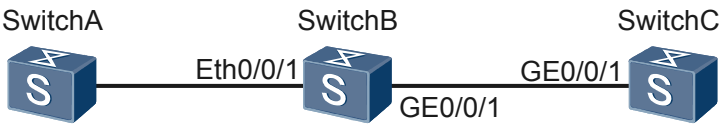
8.2.3 Troubleshooting Cases

This section provides priority mapping troubleshooting cases.

Packets Cannot Enter Correct Queues

Fault Symptom

Figure 8-7 Network Diagram



Copyright © Huawei Technologies Co., Ltd.

As shown in **Figure 8-7**, packets from SwitchA carry VLAN 100 and priorities 0 to 7.

When you run the **display qos port statistics** command on SwitchB to view the traffic statistics on GE0/0/1, packets do not enter correct queues. The command output is as follows:

```
<SwitchB> system-view
[SwitchB] qos port statistics enable interface gigabitethernet0/0/1
[SwitchB] display qos port statistics interface
gigabitethernet0/0/1
 Port: GigabitEthernet0/0/1
--------------------------------------------------------------------------------
Queue                    Passed(Packet)                 Dropped(Packet)
--------------------------------------------------------------------------------
0                        116,975                                0
--------------------------------------------------------------------------------
1                        0                                      0
--------------------------------------------------------------------------------
2                        116,975                                0
--------------------------------------------------------------------------------
3                        116,975                                0
--------------------------------------------------------------------------------
4                        116,975                                0
--------------------------------------------------------------------------------
5                        116,975                                0
--------------------------------------------------------------------------------
6                        116,975                                0
--------------------------------------------------------------------------------
7                        233950                                 0
--------------------------------------------------------------------------------
```

The preceding information indicates that packets with 802.1p priority 1 do not enter the AF1 queue.

Fault Analysis

Packets enter incorrect queues because the mappings between priorities and queues are incorrect.

1. Check the configuration of the inbound interface on SwitchB and check whether there are configurations affecting the queues that packets enter.

   (1) Run the **display this** command on Eth0/0/1 of SwitchB to check the configuration.

   ```
   [SwitchB-Eth0/0/1] display this
   #
   interface Eth0/0/1
    port link-type trunk
    port trunk allow-pass vlan 100
    trust 8021p
   #
   return
   ```

   The preceding information indicates that Eth0/0/1 allows packets from VLAN 100 to pass through and trusts 802.1p priorities; therefore, the mappings in the priority mapping table **dscp-dot1p** or **ip-pre-dot1p** do not affect the queues that packets enter.

2. Run the **display current-configuration configuration system** command to check whether there are other configurations affecting the queues that packets enter on SwitchB.

   ```
   <SwitchB> display current-configuration configuration system
   #
    sysname SwitchB
   #
    vlan batch 1
   100
   #
    qos car car1 cir 10000 cbs
   1880000
   #
   ```


Copyright © Huawei Technologies Co., Ltd.

```
 qos local-precedence-queue-map  af1  7
return
```

The preceding information indicates that the mappings between local priorities and queues are configured on SwitchB, so packets with 802.1p priority 1 enter queue 7.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **undo qos local-precedence-queue-map af1** command to cancel the mapping between local priority AF1 and queue 7.

After the preceding configurations are complete, run the **display qos port statistics gigabitethernet0/0/1** command. You can see that packets with 802.1p priorities 0 to 7 enter queues based on priorities.

----End

Summary

When packets enter incorrect queues, check whether there are configurations affecting the queues that packets enter, including the configurations of **port vlan-stacking**, **port vlan-mapping**, **qos local-precedence-queue-map**, **trust upstream none**, **port link-type dot1q-tunnel**, **dei enable**, or **traffic-policy** containing the **remark** action.

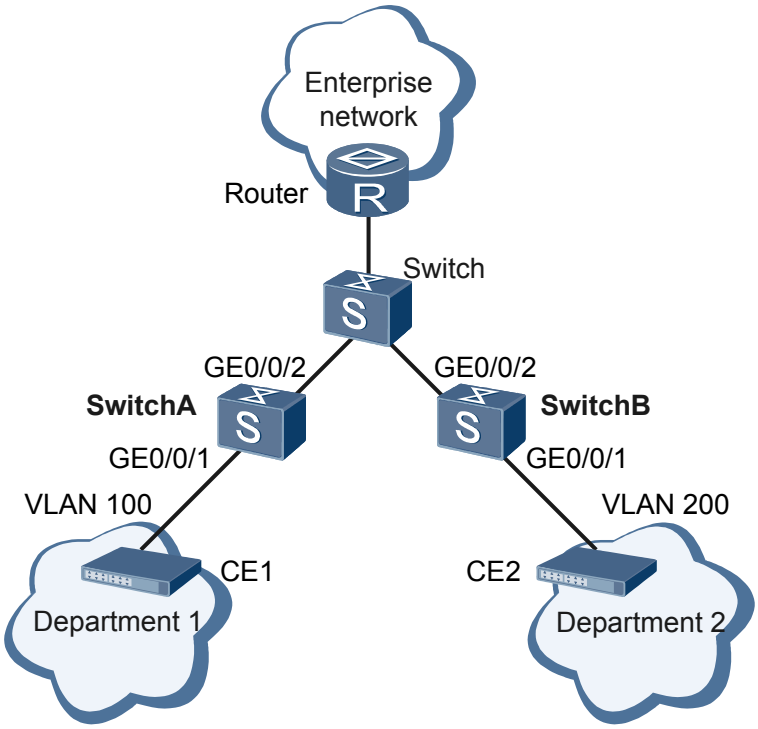
Priority Mapping Is Incorrect Because the Trusted Priority Is Not Set

Fault Symptom

As shown in **Figure 8-8**, department 1 and department 2 are connected to the enterprise network through the Switch. Packets from department 1 and department 2 carry 802.1p priorities, whereas devices on the enterprise network process packets based on Differentiated Services Code Point (DSCP) priorities. Therefore, you need to configure priority mapping on SwitchA and SwitchB to set the DSCP priority of packets from department 1 to 10 and the DSCP priority of packets from department 2 to 63. In this way, the upstream device can provide different QoS services for packets based on their DSCP priorities.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-8 Network diagram



After the configuration, DSCP priorities of packets from department 1 and department 2 received on the router are different from the actual values.

Fault Analysis

1. Check the priority mapping and the trusted priority of packets.

   (1) Capture packets on access interfaces of department 1 and department 2 and analyze packet priorities. You can see that DSCP priorities of packets are 0.

   (2) Run the **display this** command in the interface view to check the priority mapping configuration.

   ```
   <SwitchA> system-view
   [SwitchA] qos map-table dscp-dscp
   [SwitchA-dscp-dscp] display this
   #
   qos map-table dscp-dscp
     input 0 to 9 output 10
     input 11 to 63 output 10
   <SwitchB> system-view
   [SwitchB] qos map-table dscp-dscp
   [SwitchB-dscp-dscp] display this
   #
   qos map-table dscp-dscp
     input 0 to 62 output 63
   ```

   The preceding information indicates that SwitchA and SwitchB are configured with DSCP priority mapping.

2. Check the trusted type of priority on the incoming interface.

   Run the **display this** command in the interface view to check the interface configuration.

   ```
   <SwitchA> system-view
   [SwitchA] interface gigabitethernet 0/0/1
   ```


Copyright © Huawei Technologies Co., Ltd.

```
[SwitchA-GigabitEthernet0/0/1] display this
#
trust 8021p
<SwitchB> system-view
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] display this
#
trust 8021p
```

The preceding information indicates that GE 0/0/1 interfaces of SwitchA and SwitchB are configured to trust 802.1p priorities instead of DSCP priorities. Therefore, SwitchA and SwitchB do not mark packets sent from GE 0/0/1 interfaces based on the DSCP priority mapping. That is, SwitchA and SwitchB do not mark DSCP priorities of packets from department 1 with 10 or DSCP priorities of packets from department 2 with 63.

Procedure

Step 1 Run the **interface gigabitethernet 0/0/1** command to enter the interface view.

Step 2 Run the **trust dscp** command to configure the interface to trust the DSCP priority of packets.

After the fault is rectified, simulate users on department 1 to send packets to SwitchA and simulate users on department 2 to send packets to SwitchB. Then capture packets on outbound interfaces GE 0/0/2 of SwitchA and SwitchB. The captured packets show that the DSCP priorities of the packets meet requirements.

----End

Summary

If the priority mapping is incorrect, check the priority mapping configuration on the inbound and outbound interfaces and the trusted priority in packets. These may cause the failure to map the priorities of packets.

8.3 Priority Mapping Troubleshooting (S3700HI)

This chapter describes common causes of priority mapping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.3.1 Packets Enter Incorrect Queues

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when packets enter incorrect queues.

Common Causes

This fault is commonly caused by one of the following:

- The priority type of packets is different from the priority type trusted by the inbound interface.
- The priority mapping configured in the DiffServ domain trusted by the inbound interface is incorrect.
- There are configurations affecting the queues that packets enter on the inbound interface, including:
  - **port vlan-stacking**

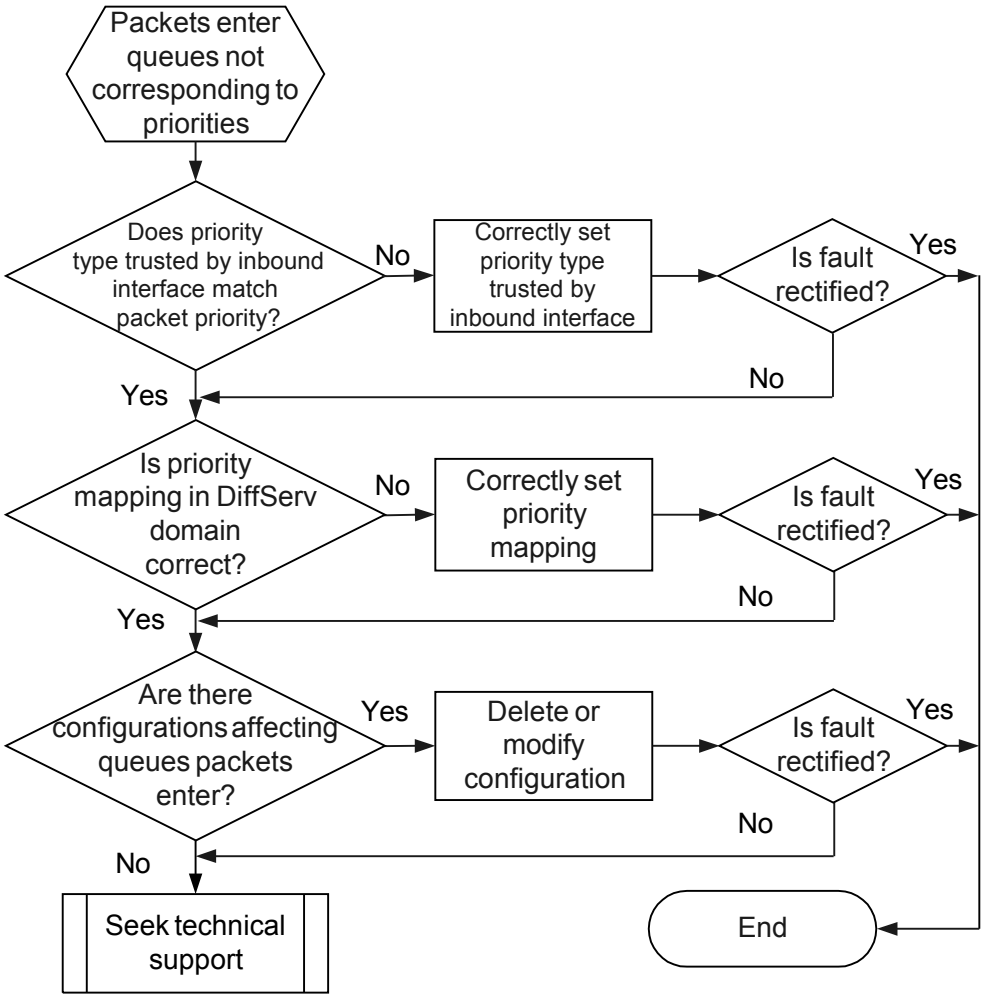
Copyright © Huawei Technologies Co., Ltd.

  - **port vlan-mapping vlan inner-vlan**, or **port vlan-mapping vlan map-vlan**
  - **trust upstream none**
  - **port link-type dot1q-tunnel**
  - **traffic-policy** containing the **remark 8021p**, **remark dscp**, **remark local-precedence**, or **remark ip-precedence** action
- **traffic-policy** containing the **remark 8021p**, **remark dscp**, **remark local-precedence**, or **remark ip-precedence** action in the VLAN that packets belong to.
- There are configurations affecting the queues that packets enter in the system, including:
  - **qos local-precedence-queue-map**
  - **traffic-policy** where **remark 8021p**, **remark dscp**, **remark local-precedence**, or **remark ip-precedence** action is defined

Troubleshooting Flowchart

Figure 8-9 shows the troubleshooting flowchart.

Figure 8-9 Troubleshooting flowchart for packets entering incorrect queues



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the priority type of packets is the same as the priority type trusted by the inbound interface.

Run the **display this** command in the inbound interface view to check the configuration of the **trust** command on the inbound interface (if the **trust** command is not used, the system trusts the 802.1p priority in the outer VLAN tag by default). Then, capture packets on the inbound interface, and check whether the priority type of the captured packets is the same as the priority type trusted by the inbound interface.

- If not, run the **trust** command to modify the priority type trusted by the inbound interface to be the same as the priority type of the captured packets.
- If yes, go to step 2.

Step 2 Check whether the configured priority mapping is correct.

Run the **display this** command in the inbound interface view and check the configuration of the **trust upstream** command (If the **trust upstream** command is not used, the system trusts the **default** DiffServ domain). Then, run the **display diffserv domain name** *domain-name* command to check whether the priority mapping configured in the DiffServ domain trusted by the inbound interface is correct.

- If not, run the **ip-dscp-inbound**, **ip-dscp-outbound**, **8021p-inbound**, or **8021p-outbound** command to correctly configure the priority mapping.
- If yes, go to step 3.

Step 3 Check whether there are configurations affecting the queues that packets enter on the device.

1. Check whether there are configurations affecting the queues that packets enter on the inbound interface.

   The following configurations affect the queues that packets enter on the inbound interface:

   - If the **port vlan-stacking** command is used with **remark-8021p** specified, the priorities of packets are re-marked. The mapping between 802.1p priorities and local priorities may be incorrect and packets may enter incorrect queues.
   - If the **port vlan-mapping vlan inner-vlan**, or **port vlan-mapping vlan map-vlan** command is used with **remark-8021p** specified, the priorities of packets are re-marked. The mapping between 802.1p priorities and local priorities may be incorrect and packets may enter incorrect queues.
   - If the **traffic-policy** command where **remark local-precedence** is defined is used for incoming packets, the system sends packets to queues based on the re-marked priority.
   - If the **traffic-policy** command where **remark 8021p** , **remark ip-precedence**or **remark dscp** is defined is used, the system maps the re-marked priorities of packets to the local priorities and sends the packets to queues based on the mapped priorities.
   - If the **trust upstream none** command is used, priorities of all the incoming packets are not mapped and the packets enter queues based on the default priority of the interface.

Copyright © Huawei Technologies Co., Ltd.

- If the **port link-type dot1q-tunnel** command is used but the **trust 8021p inner** command is not used on the interface, all the incoming packets enter queues based on the default priority of the interface.

Run the **display this** command in the inbound interface view to check whether there are configurations affecting the packets enqueuing on the inbound interface.

- If yes, delete or modify the configurations as required.
- If not, go to step b.

2. Check whether there are configurations affecting the queues that packets enter in the VLAN that packets belong to.

   The following configurations affect the queues that packets enter:

   - If the **traffic-policy** command where **remark local-precedence** is defined is used, the system sends packets to queues based on the re-marked priorities.
   - If the **traffic-policy** command where **remark 8021p** , **remark ip-precedence** or **remark dscp** is defined is used, the system maps the re-marked priorities of packets to the local priorities and sends the packets to queues based on the mapped priorities.

   Run the **display this** command in the view of the VLAN that packets belong to and check whether the configurations affecting the packets enqueuing are performed in the VLAN.

   - If yes, delete or modify the configurations as required.
   - If not, go to step c.

3. Check whether there are configurations affecting the queues that packets enter in the system.

   The following configurations affect the queues that packets enter:

   - If the **qos local-precedence-queue-map** command is used, the system sends packets to queues based on the mapping between local priorities and queues specified by this command.
   - If the **traffic-policy** command where **remark local-precedence** is defined is used, the system sends packets to queues based on the re-marked priority.
   - If the **traffic-policy** command where **remark 8021p**, **remark ip-precedence**, or **remark dscp** is defined is used, the system maps the re-marked priorities of packets to the local priorities and sends the packets to queues based on the mapped priorities.

   Run the **display current-configuration** command to check whether the configurations affecting the packets enqueuing are performed in the system.

   - If yes, delete or modify the configurations as required.
   - If not, go to step 4.

NOTE

The traffic policy is applied to an interface, a VLAN, and the system in descending order of priorities.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

8.3.2 Priority Mapping Results Are Incorrect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when priority mapping results are incorrect.

Common Causes

This fault is commonly caused by one of the following:

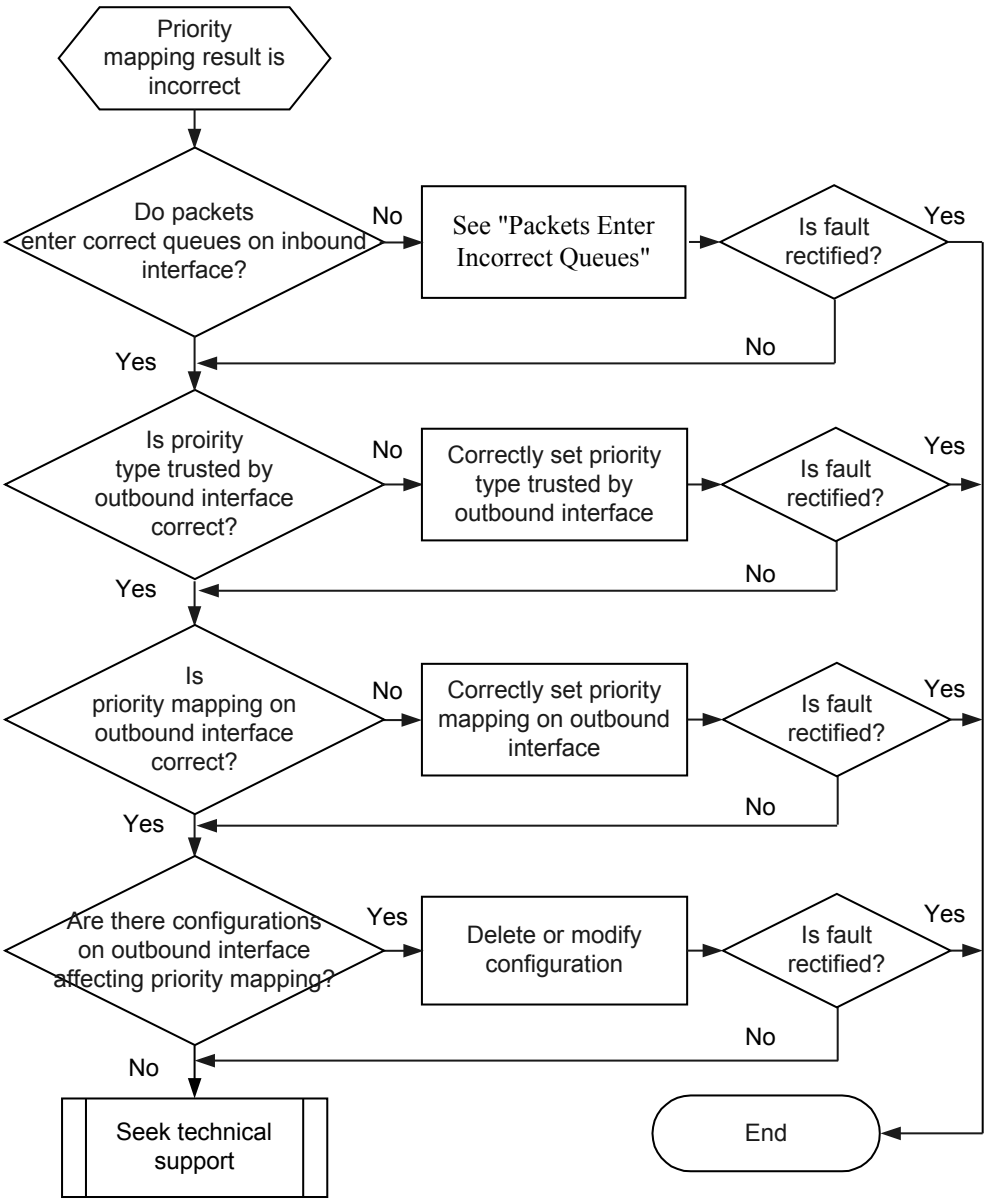
- On the inbound interface, packets enter incorrect queues.
- The type of the priority trusted by the outbound interface is incorrect.
- The priority mapping configured in the DiffServ domain trusted by the outbound interface is incorrect.
- There are configurations affecting the priority mapping on the outbound interface. For example:
  - **undo qos phb marking enable**
  - **trust upstream none**
  - **traffic-policy** containing the **remark 8021p**, **remark ip-precedence** or **remark dscp** action

Troubleshooting Flowchart

Figure 8-10 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-10 Troubleshooting flowchart for incorrect priority mapping



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that packets enter correct queues on the outbound interface.

Run the **display qos queue statistics interface** *interface-type interface-number* command to check whether packets enter correct queues on the outbound interface.

- If not, rectify the fault according to **8.3.1 Packets Enter Incorrect Queues**.

Copyright © Huawei Technologies Co., Ltd.

- If yes, go to step 2.

Step 2 Check that the priority type trusted by the outbound interface is correct.

Run the **display this** command in the view of the outbound interface to check whether the trusted priority type set by using the **trust** command on the outbound interface is correct. (If the **trust** command is not used, the system trusts the 802.1p priority in the outer VLAN tag by default.)

- If not, run the **trust** command to correctly configure the priority type trusted by the outbound interface.
- If yes, go to step 3.

Step 3 Check that the priority mapping configured in the DiffServ domain trusted by the outbound interface is correct.

Run the **display this** command in the view of the outbound interface to check whether the **trust upstream** command is used. If the **trust upstream** command is not used, the system trusts the **default** DiffServ domain by default.

Run the **display diffserv domain name** *domain-name* command to check whether the mapping between local priorities and packet priorities complies with service planning.

NOTE

The local priority refers to the mapped priority of the inbound interface.

- If not, run the **ip-dscp-outbound** or **8021p-outbound** command to correctly configure the mapping between local priorities and packet priorities.
- If yes, go to step 3.

Step 4 Check whether the configurations affecting priority mapping are performed on the outbound interface.

The following configurations affect priority mapping on the outbound interface:

- If the **undo qos phb marking enable** command is used, the system does not perform PHB mapping for outgoing packets on an interface.
- If the **trust upstream none** command is used, the system does not perform PHB mapping for outgoing packets on an interface.
- If the **traffic-policy** command where **remark 8021p**, **remark ip-precedence** or **remark dscp** is defined is used on the outbound interface, the re-marked priority is the packet priority.

Run the **display this** command in the view of the outbound interface to check whether the configurations affecting priority mapping are performed on the outbound interface.

- If yes, delete or modify the configurations as required.
- If not, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Copyright © Huawei Technologies Co., Ltd.

Relevant Logs

None.

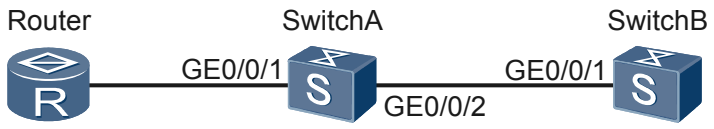
8.3.3 Troubleshooting Cases

This section provides priority mapping troubleshooting cases.

Packets Enter Incorrect Queues

Fault Symptom

Figure 8-11 Network diagram



As shown in **Figure 8-11**, the packets from the router carry VLAN 100 and priorities 0 to 7, run the **display qos queue statistics** command on SwitchA to view the traffic statistics on the outbound interface GE 0/0/2, packets enter incorrect queues. The following information is displayed:

```
<SwitchA> display qos queue statistics interface gigabitethernet
0/0/2
 Queue  CIR/PIR(kbps)          Passed(Packet/Byte)        Dropped(Packet/Byte)
  ------------------------------------------------------------------------------
    0             0                  58,489,690                          0
               1000000               5,848,935,830                       0
  ------------------------------------------------------------------------------
    1             0                           0                          0
               1000000                        0                          0
  ------------------------------------------------------------------------------
    2             0                  58,487,970                          0
               1000000               5,848,797,000                       0
  ------------------------------------------------------------------------------
    3             0                  58,487,969                          0
               1000000               5,848,796,900                       0
  ------------------------------------------------------------------------------
    4             0                  58,487,968                          0
               1000000               5,848,796,800                       0
  ------------------------------------------------------------------------------
    5             0                  58,487,967                          0
               1000000               5,848,796,700                       0
  ------------------------------------------------------------------------------
    6             0                  58,487,967                          0
               1000000               5,848,796,600                       0
  ------------------------------------------------------------------------------
    7             0                 116,975,932                          0
               1000000              11,697,593,000                       0
  ------------------------------------------------------------------------------
```

The preceding information indicates that packets whose priority is 1 are not entering the AF1 queue.

Fault Analysis

This fault is generally caused by incorrect mapping between priorities and queues.

Copyright © Huawei Technologies Co., Ltd.

1. Check the DiffServ domain on the inbound interface of SwitchA and check whether priority mapping is correct.

   (1) Run the **display this** command on the inbound interface GE 0/0/1 of SwitchA to view the priority mapping.

   ```
   [SwitchA-GigabitEthernet0/0/1] display this
   #
   interface
   GigabitEthernet0/0/1
    port link-type
   trunk
    port trunk allow-pass vlan
   100
   #
   return
   ```

   The preceding information indicates that the **default** DiffServ domain is applied to GE 0/0/1 and the outer 802.1p priority is trusted by default.

   (2) Run the **display diffserv domain name default** command to view priority mapping in the **default** DiffServ domain.

   ```
   <SwitchA> display diffserv domain name default
   diffserv domain name:default
    8021p-inbound 0 phb be
   green
    8021p-inbound 1 phb af1
   green
    8021p-inbound 2 phb af2
   green
    8021p-inbound 3 phb af3
   green
    8021p-inbound 4 phb af4
   green
    8021p-inbound 5 phb ef
   green
    8021p-inbound 6 phb cs6
   green
    8021p-inbound 7 phb cs7
   green
    8021p-outbound be green map
   0
    8021p-outbound be yellow map
   0
    8021p-outbound be red map
   0
    8021p-outbound af1 green map
   1
    8021p-outbound af1 yellow map
   1
    8021p-outbound af1 red map
   1
    8021p-outbound af2 green map
   2
    8021p-outbound af2 yellow map
   2
    8021p-outbound af2 red map
   2
    ......
   ```

   The preceding information indicates that priority mapping in the inbound interface is correct.

2. Check the DiffServ domain on the outbound interface of SwitchA and check whether priority mapping is correct.

   Run the **display this** command on the outbound interface GE 0/0/2 of SwitchA to view the priority mapping.

   ```
   [SwitchA-GigabitEthernet0/0/2] display this
   #
   ```


Copyright © Huawei Technologies Co., Ltd.

```
interface
GigabitEthernet0/0/2
 port link-type
trunk
 port trunk allow-pass vlan
100
#
return
```

The preceding information indicates that the **default** DiffServ domain is applied to GE 0/0/2 and the outer 802.1p prioritiy is trusted by default. According to the configuration of the **default** DiffServ domain, priority mappings on the outbound interface are correct.

3. Run the **display current-configuration configuration system** command to check whether there are configurations affecting the queues that packets enter on SwitchA.

```
<SwitchA> display current-configuration configuration system
#
 sysname SwitchA
#
 vlan batch 1
100
#
 qos car car1 cir 10000 cbs
1880000
#
 qos local-precedence-queue-map  af1  7
return
```

The preceding information indicates that mappings between local priorities and queues are configured on SwitchA. Packets with 802.1p priority 1 enter queue 7.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **undo qos local-precedence-queue-map af1 7** command to cancel the mapping between local priority AF1 and queue 7.

After the configuration, run the **display qos queue statistics interface gigabitethernet0/0/2** command. You can see that packets with 802.1p priorities 0 to 7 enter queues based on priorities.

----End

Summary

When packets enter incorrect queues, check whether the configurations affecting the packets enqueuing are performed, including the configurations of **port vlan-stacking**, **port vlan-mapping**, **qos local-precedence-queue-map**, **trust upstream none**, **port link-type dot1q-tunnel**, **dei enable**, or **traffic-policy** containing the **remark** action.

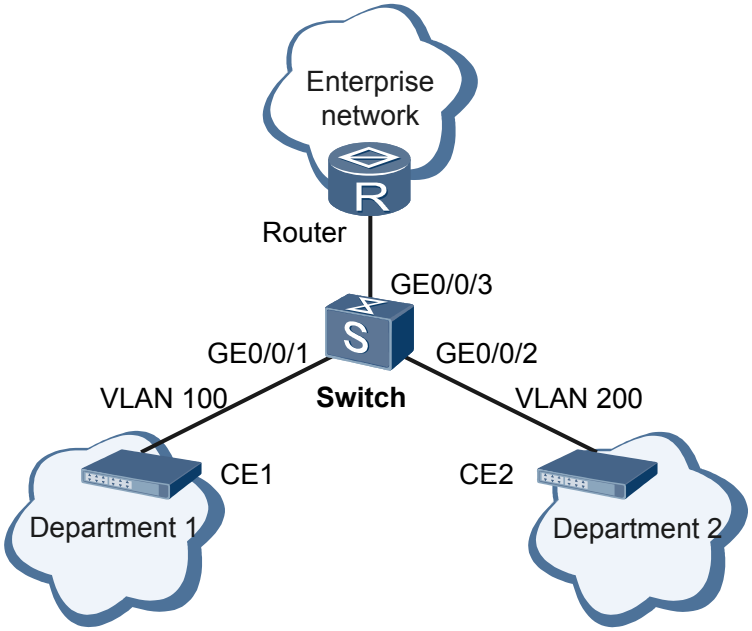
Priority Mapping Is Incorrect Because the Trusted Priority Is Not Set

Fault Symptom

As shown in **Figure 8-12**, department 1 and department 2 are connected to the through the Switch. Packets from department 1 and department 2 carry 802.1p priorities, whereas devices on the process packets based on Differentiated Services Code Point (DSCP) priorities. Therefore, you need to configure priority mapping on Switch to set the DSCP priority of packets from department 1 to 10 and the DSCP priority of packets from department 2 to 63. In this way, the device can provide different QoS services for packets based on their DSCP priorities.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-12 Network diagram



After the configuration, DSCP priorities of packets from department 1 and department 2 received on the router are different from the actual values.

Fault Analysis

1. Check the priority mapping and the trusted priority of packets on the inbound interface.

   (1) Capture packets on access interfaces of department 1 and department 2 and analyze packet priorities. It is found that 802.1p priorities of packets are 0.

   (2) Run the **display this** command in the views of inbound interfaces GE 0/0/1 and GE 0/0/2 to check the configuration of the interfaces.

```
[Switch-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
 trust upstream out-ds
#
return
<Quidway> display diffserv domain name out-ds
ip-dscp-outbound be green map 0
 ip-dscp-outbound be yellow map 0
 ip-dscp-outbound be red map 0
 ip-dscp-outbound af1 green map 10
 ip-dscp-outbound af1 yellow map 12
 ip-dscp-outbound af1 red map 14
 ip-dscp-outbound af2 green map 10
 ip-dscp-outbound af2 yellow map 10
 ip-dscp-outbound af2 red map 10
 ip-dscp-outbound af3 green map 26
 ip-dscp-outbound af3 yellow map 28
 ip-dscp-outbound af3 red map 30
 ip-dscp-outbound af4 green map 34
 ip-dscp-outbound af4 yellow map 36
 ip-dscp-outbound af4 red map 38
 ip-dscp-outbound ef green map 46
```


Copyright © Huawei Technologies Co., Ltd.

```
 ip-dscp-outbound ef yellow map 46
 ip-dscp-outbound ef red map 46
 ip-dscp-outbound cs6 green map 48
 ip-dscp-outbound cs6 yellow map 48
 ip-dscp-outbound cs6 red map 48
 ip-dscp-outbound cs7 green map 63
 ip-dscp-outbound cs7 yellow map 63
 ip-dscp-outbound cs7 red map 63
```

The preceding information indicates thatGE 0/0/1 is configured with DiffServ domain **ds1** and GE 0/0/2 is configured with DiffServ domain **ds2**. The interfaces trust the 802.1p priority in the outer VLAN tag by default. Run the **display diffserv domain name** command to check the configurations of **ds1** and **ds2**.

```
<Switch> display diffserv domain name ds1
diffserv domain name:ds1
 8021p-inbound 0 phb af2 green
 8021p-inbound 1 phb af2 green
 8021p-inbound 2 phb af2 green
 8021p-inbound 3 phb af2 green
 8021p-inbound 4 phb af2 green
 8021p-inbound 5 phb af2 green
 8021p-inbound 6 phb af2 green
 8021p-inbound 7 phb af2 green
......
<Switch> display diffserv domain name ds2
diffserv domain name:ds2
 8021p-inbound 0 phb cs7 green
 8021p-inbound 1 phb cs7 green
 8021p-inbound 2 phb cs7 green
 8021p-inbound 3 phb cs7 green
 8021p-inbound 4 phb cs7 green
 8021p-inbound 5 phb cs7 green
 8021p-inbound 6 phb cs7 green
 8021p-inbound 7 phb cs7 green
......
```

2. Check the priority mapping and the trusted type of priority on the outgoing interface.

   Run the **display this** command in the GE0/0/3 interface view to check the interface configuration.

```
[Switch-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
 trust upstream out-ds
#
return
<Quidway> display diffserv domain name out-ds
ip-dscp-outbound be green map 0
 ip-dscp-outbound be yellow map 0
 ip-dscp-outbound be red map 0
 ip-dscp-outbound af1 green map 10
 ip-dscp-outbound af1 yellow map 12
 ip-dscp-outbound af1 red map 14
 ip-dscp-outbound af2 green map 10
 ip-dscp-outbound af2 yellow map 10
 ip-dscp-outbound af2 red map 10
 ip-dscp-outbound af3 green map 26
 ip-dscp-outbound af3 yellow map 28
 ip-dscp-outbound af3 red map 30
 ip-dscp-outbound af4 green map 34
 ip-dscp-outbound af4 yellow map 36
 ip-dscp-outbound af4 red map 38
 ip-dscp-outbound ef green map 46
 ip-dscp-outbound ef yellow map 46
 ip-dscp-outbound ef red map 46
 ip-dscp-outbound cs6 green map 48
 ip-dscp-outbound cs6 yellow map 48
```


Copyright © Huawei Technologies Co., Ltd.

```
ip-dscp-outbound cs6 red map 48
ip-dscp-outbound cs7 green map 63
ip-dscp-outbound cs7 yellow map 63
ip-dscp-outbound cs7 red map 63
```

The preceding information indicates that GE 0/0/3 is configured with the DiffServ domain **out-ds**. In **out-ds**, AF2 is mapped to DSCP 10 and CS7 is mapped to DSCP 63. The mappings are correct.

The interface is not configured to trust the priority of packets. That is, GE 0/0/3 trusts only the 802.1p priority in the outer VLAN tag. Therefore, the outbound interface GE 0/0/3 of the Switch does not mark the outgoing packets based on the priority mapping configured in the **out-ds** domain. DSCP priorities of packets from department 1 should be marked with 10 and DSCP priorities of packets from department 2 should be marked with 63.

Procedure

Step 1 Run the **interface** gigabitethernet 0/0/3 command to enter the interface view.

Step 2 Run the **trust dscp** command to configure the interface to trust the DSCP priority of packets.

After the preceding configurations are complete, simulate users on department 1 and department 2 to send packets to the Switch, capture packets on outbound interface gigabitethernet 0/0/3. The captured packets show that the DSCP priorities of the packets meet requirements. The fault is rectified.

----End

Summary

If the priority mapping is incorrect, check the configuration of priority mapping on the inbound and outbound interfaces and the trusted priority in packets. These may cause the failure to map the priorities of packets.

8.4 Traffic Policing Troubleshooting

This chapter describes common causes of traffic policing faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.4.1 Traffic Policing Based on Traffic Classifiers Fails to Take Effect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when traffic policing based on traffic classifiers fails to take effect.

Traffic policing applies the traffic policy's Committed Access Rate (CAR) or aggregated CAR action to packet flows. Its troubleshooting roadmap is the same as that for the traffic policy. For details, see **8.1.1 Traffic Policy Fails to Take Effect**.

8.4.2 Interface-based Traffic Policing Results Are Incorrect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when interface-based traffic policing results are incorrect.

Copyright © Huawei Technologies Co., Ltd.

Common Causes

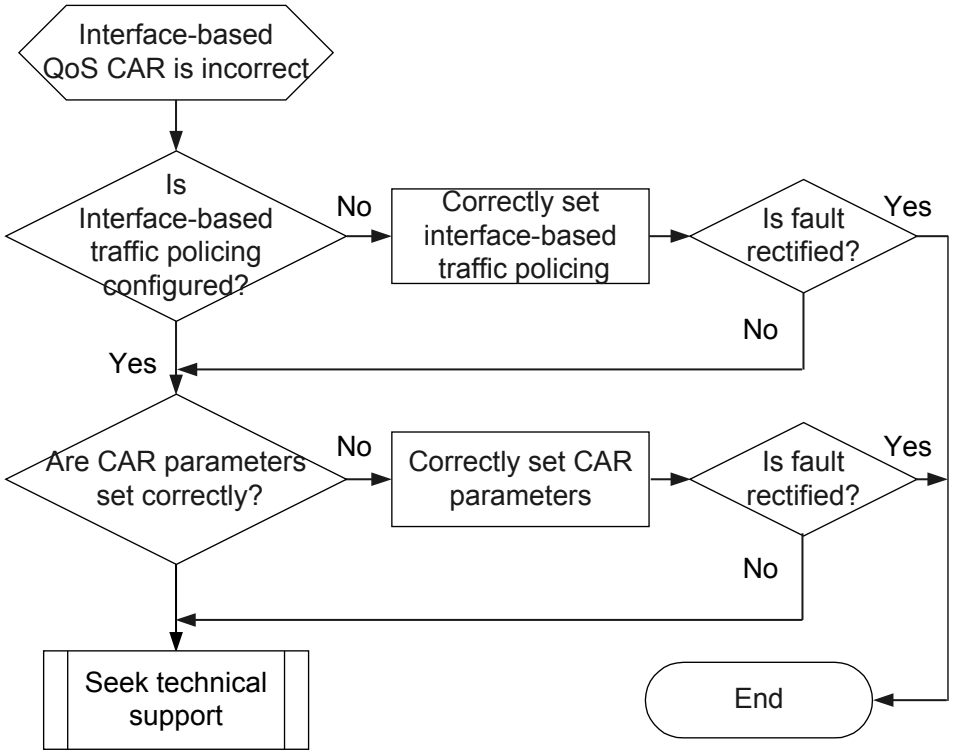
This fault is commonly caused by one of the following:

- The **qos lr inbound** command is not used on the interface.
- The CAR parameters are set incorrectly.

Troubleshooting Flowchart

Figure 8-13 shows the troubleshooting flowchart.

Figure 8-13 Troubleshooting flowchart for incorrect interface-based traffic policing results



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the interface-based traffic policing is configured on the interface.

Run the **display this** command in the interface view to check whether the **qos lr inbound** command is used.

- If not, run the **qos lr inbound** command to configure the interface-based traffic policing correctly.

Copyright © Huawei Technologies Co., Ltd.

- If yes, go to step 2.

Step 2 Check whether the CAR parameters are set correctly.

Run the **display qos lr** command to check whether the CAR parameters are set correctly.

NOTE

On the S3700SI and S3700EI, the granularity of interface-based traffic policing is 64 kbit/s. If the CIR value divided by 64 is greater than or equal to 1 but is smaller than 2, the traffic policing rate is (64+64) kbit/s. If the CIR value divided by 64 is greater than or equal to 2 but is smaller than 3, the traffic policing rate is (64+64*2) kbit/s, and so on.

On the S3700HI, the granularity of interface-based traffic policing is 8 kbit/s. If the CIR value divided by 8 is greater than or equal to 1 but is smaller than 2, the traffic policing rate is (64+8) kbit/s. If the CIR value divided by 8 is greater than or equal to 2 but is smaller than 3, the traffic policing rate is (64+8*2) kbit/s, and so on.

- If not, run the **qos lr inbound** command to set the CAR parameters correctly.
- If yes, go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

8.4.3 Troubleshooting Cases

This section provides QoS CAR troubleshooting cases.

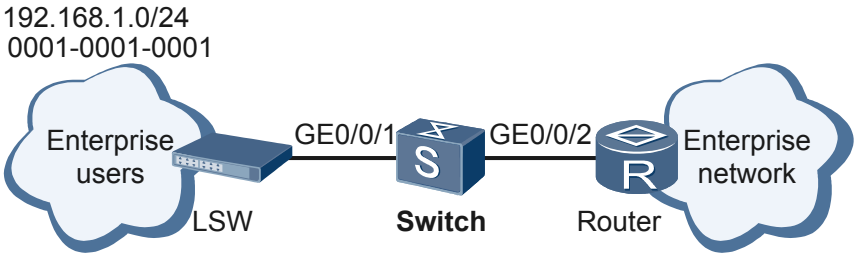
Traffic Policing Based on Traffic Classifiers Fails to Take Effect

Fault Symptom

As shown in **Figure 8-14**, a user accesses the Switch using the LSW. The user resides on the network segment 192.168.1.0/24 and the MAC address of the user is 0001-0001-0001. Traffic policing is configured on GE 0/0/1 of the Switch to limit the maximum transmission rate of incoming traffic to 50 Mbit/s. However, when traffic is transmitted from the LSW to the Switch at the rate of 100 Mbit/s, the Switch still forwards the traffic at the rate of 100 Mbit/s. That is, traffic policing fails to take effect.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-14 Network diagram



Fault Analysis

1. Check whether the traffic policy is configured for incoming packets on the interface.

   Run the **display this** command in the view of the GE 0/0/1 interface to view the traffic policy configuration on the interface.

   ```
   [Quidway-GigabitEthernet0/0/1] display this
   #
   interface GigabitEthernet0/0/1
    port link-type trunk
    port trunk allow-pass vlan 100
    traffic-policy tp1 inbound
   #
   return
   ```

   The preceding information indicates that the traffic policy **tp1** is configured for incoming packets on the GE0/0/1interface.

2. Check whether the traffic classifier and the traffic behavior bound to the traffic policy are correct.

   Run the **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]] command to check whether the traffic policy contains the traffic classifier and the traffic behavior, whether the CAR action is configured, and whether the CAR configuration is correct.

   ```
   [Quidway] display traffic policy user-defined tp1
     User Defined Traffic Policy Information:
     Policy: tp1
      Classifier: tc1
       Operator: AND
        Behavior: tb1
           Committed Access Rate:
           CIR 5000 (Kbps), CBS 625000 (Byte)
           PIR 5000 (Kbps), PBS 625000 (Byte)
           Green Action   : pass
           Yellow Action  : pass
           Red Action     : discard
   ```

   Run the **display traffic classifier user-defined** command to check whether the rule in the traffic classifier is correct.

   ```
   [Quidway] display traffic classifier user-defined tc1
     User Defined Classifier Information:
      Classifier: tc1
       Operator: AND
       Rule(s) : if-match acl 4000
   [Quidway] display acl 4000
   Advanced ACL 4000, 1 rule
   Acl's step is 5
    rule 5 permit source-mac 0001-0001-0001 ffff-ffff-0fff (0 times matched)
   ```


Copyright © Huawei Technologies Co., Ltd.

The preceding information indicates that the traffic classifier and the traffic behavior in the traffic policy **tp1** are correct.

3. Check whether the information in the packets matches traffic classification rules.

   Run the **display traffic policy statistics** command to check the traffic statistics on GE 0/0/1 to which the traffic policy is applied. The following information is displayed:

```
[Quidway] display traffic policy statistics interface gigabitethernet 0/0/1
 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: tp1
 Rule number: 1
 Current status: OK!
-------------------------------------------------------------------------
 Board : 0
Item                                Packets                         Bytes
-------------------------------------------------------------------------
Matched                                   0                             0
  +--Passed                               0                             0
  +--Dropped                              0                             0
    +--Filter                             0                             0
    +--URPF                               -                             -
    +--CAR                                0                             0
```

   The preceding information indicates that packets do not match the traffic classificarion rules.

4. Check whether another rule with a higher priority is configured for the packets.

   Run the **display current-configuration** command to check the traffic policy in the system.

```
[Quidway] display current-configuration
#
 sysname Quidway
#
acl number 3000
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
acl number 4000
 rule 5 permit rule 10 permit source-mac 0001-0001-0001 ffff-ffff-0fff
#
traffic classifier test operator or
 if-match acl 3000
traffic classifier tc1 operator or
 if-match acl 4000
#
traffic behavior test
 permit
traffic behavior tb1
 car cir 50000 pir 50000 cbs 6250000 pbs 6250000 green pass yellow pass red
discard
#
traffic policy test
 classifier test behavior test
traffic policy tp1
 classifier tc1 behavior tb1
#
 traffic-policy test global inbound
#
interface GigabitEthernet0/0/1 port link-type trunk
 port trunk allow-pass vlan 100
 traffic-policy tp1 inbound
#
return
```

   The preceding information indicates that the traffic policy **test** is configured on the Switch, which contains the traffic classifier **test** and the traffic behavior **test**. The traffic classifier references ACL 3000 that matches packets whose source IP address is 192.168.1.0. This is a Layer 3 rule. The action defined in the traffic behavior **test** is permit.

Copyright © Huawei Technologies Co., Ltd.

On the S3700, The traffic policy containing Layer 3 ACL rules takes precedence over the traffic policy containing Layer 2 rules. The packets with source MAC address 0001-0001-0001 from 192.168.1.0/24 match two rules, whereas only the traffic policy **test** containing ACL 3000 takes effect. As a result, the packets are directly forwarded and traffic policing fails to take effect.

Procedure

Step 1 Run the **undo traffic-policy global inbound** command in the system view to disable the traffic policy **test**.

After the traffic policy **test** is disabled, transmit traffic to the GE 0/0/1interface at the rate of 100 Mbit/s. The GE 0/0/2 interface forwards the packets at the rate of 50 Mbit/s. The fault is rectified.

----End

Summary

If traffic policing based on traffic classifiers fails to take effect, rectify the fault according to **Traffic Policy Fails to Take Effect**.

8.5 Traffic Shaping Troubleshooting

This chapter describes common causes of traffic shaping faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.5.1 Traffic Shaping Results of Queues Are Incorrect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when traffic shaping results of queues are incorrect.

Common Causes

The fault symptom may be any of the following:

- Traffic shaping does not take effect.
- The CIR value for traffic shaping in queues cannot be reached.

This fault is commonly caused by one of the following:

- Traffic shaping parameters are set incorrectly.
- The CIR value for traffic shaping on an interface is smaller than the sum of CIR values for traffic shaping in queues on the interface. As a result, the bandwidth of traffic shaping in queues cannot be ensured.
- Packets do not enter queues configured with traffic shaping because the configuration is incorrect. For example, priority mapping is incorrect.
- Each queue uses the combined scheduling mode and excessive packets enter Priority Queuing (PQ) queues. As a result, other queues cannot obtain sufficient bandwidth.

  NOTE

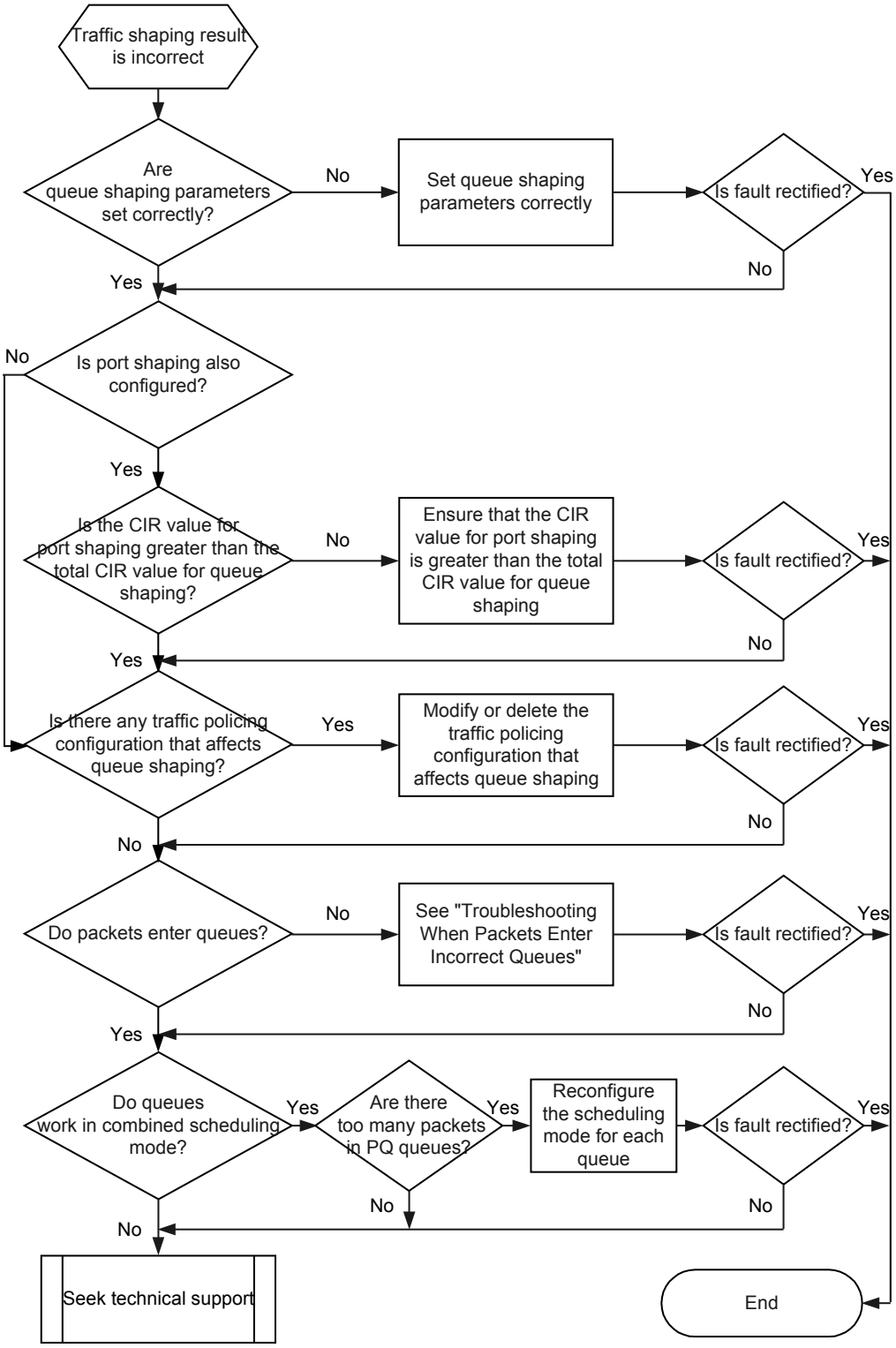
  In combined scheduling mode, if the bandwidth is insufficient, the Peak Information Rate (PIR) value of other queues cannot be reached. This is a correct traffic shaping result.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 8-15 shows the troubleshooting flowchart.

Figure 8-15 Troubleshooting flowchart for incorrect traffic shaping results



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether traffic shaping parameters of queues are set correctly.

Run the **display this** command in the interface view to check whether the **qos queue shaping** command is used.

- If traffic shaping parameters of queues are set incorrectly or not set, run the **qos queue shaping** command to set the parameters correctly.
- If traffic shaping parameters of queues are set and the CIR value for traffic shaping on an interface is set by using the **qos lr outbound** command, go to step 2.
- If traffic shaping parameters of queues are set but the CIR value for traffic shaping on an interface is not set, go to step 3.

Step 2 Check whether the CIR value for traffic shaping on an interface is greater than the sum of CIR values for traffic shaping in queues on the interface.

Compare the CIR value for traffic shaping on an interface with the sum of CIR values for traffic shaping in queues on the interface:

- If the CIR value for traffic shaping on an interface is smaller than the sum of CIR values for traffic shaping in queues on the interface, queues on the interface cannot obtain sufficient bandwidth. The traffic shaping result may be incorrect. In this case, run the **qos lr outbound** and **qos queue shaping** commands to modify related parameters accordingly so that the CIR value for traffic shaping on an interface is greater than the sum of CIR values for traffic shaping in queues on the interface.
- If the CIR value for traffic shaping on an interface is greater than the sum of CIR values for traffic shaping in queues on the interface, go to step 3.

Step 3 Check whether traffic policing affecting queue shaping is configured.

1. Check whether interface-based traffic policing is configured on the inbound interface.

   If interface-based traffic policing is configured on the inbound interface and its CIR value is smaller than the specified CIR value for queue shaping, queue shaping uses the CIR value for interface-based traffic policing.

   Run the **display this** command in the inbound interface view to check whether the **qos lr inbound** command is run on the inbound interface and whether its CIR value is smaller than the CIR value for queue shaping.

   - If the **qos lr inbound** command is run and the CIR value of the inbound interface is smaller than the CIR value for queue shaping, disable interface-based traffic policing or modify the configuration so that the CIR value for interface-based traffic policing is greater than the CIR value for queue shaping.
   - If the **qos lr inbound** command is not run or this command is run but the CIR value of the inbound interface is greater than the CIR value for queue shaping, go to step b.
2. Check whether class-based traffic policing is configured on the device.

Copyright © Huawei Technologies Co., Ltd.

If class-based traffic policing is configured on the device, its CIR value is smaller than the CIR for queue shaping, and traffic in queues matches the traffic classifier, the CIR for class-based traffic policing is used as the actual CIR value of queue shaping.

Run the **display this** command in the system view, inbound interface view, and VLAN view to check whether the **traffic-policy** command is run:

- If the **traffic-policy** command is run, run the **display traffic policy user-defined** command to check whether a CIR value is defined in the traffic policy and whether the CIR value is smaller than the CIR value for queue shaping.
  - If the CIR value is set, run the **display traffic classifier user-defined** command to check whether traffic in queues matches the traffic classifier in the configured traffic policy. If traffic in queues matches the traffic classifier, delete the CIR value defined in the traffic policy or modify the configuration so that the CIR value in the traffic policy is greater than the CIR value for queue shaping. If traffic in queues does not match the traffic classifier, go to step 4.
  - If no CIR value is set, go to step 4.
- If the **traffic-policy** command is not run, go to step 4.

NOTE

- If both interface-based traffic policing and class-based traffic policing are configured, class-based traffic policing takes effect.
- The traffic policies configured in the interface view, VLAN view, and system view take effect in descending order of priority.

Step 4 Check whether packets enter traffic shaping queues.

Run the following commands based on device models:

- On the S3700SI or S3700EI, run the **display qos port statisticsinterface** *interface-type interface-number* command to view the packet statistics on each queue on an interface.
- On the S3700HI, run the **display qos queue statistics interface** *interface-type interface-number* command to view the packet statistics on each queue on an interface.
- If packets do not enter traffic shaping queues, rectify the fault according to **8.2.1 Packets Enter Incorrect Queues**(S3700SI and S3700EI), or (S3700HI).
- If packets enter traffic shaping queues but excessive packets (for example, the traffic rate on a GigabitEthernet interface exceeds 100 Mbit/s, and the traffic rate on an Ethernet interface exceeds 10 Mbit/s) enter PQ queues, go to step 4.
- If packets enter traffic shaping queues and excessive packets do not enter PQ queues, go to step 5.

Step 5 Check whether queues on the interface use the combined scheduling mode.

Run the **display this** command in the interface view to check the scheduling mode used by each queue on the interface.

- If **qos wrr** or **qos drr** is used on an interface and **qos queue** *queue-index* **drr weight 0** or **qos queue** *queue-index* **wrr weight 0** is configured in a queue, each queue on the interface uses the combined scheduling mode.

  In combined scheduling mode, if no bandwidth limit is configured for PQ queues, some packets in WRR or DRR queues may be not processed when PQ queues contain a large number of packets. Because queue shaping is configured on WRR or DRR queues, queue shaping is also affected.. In this case, run the **qos** { **pq** | **drr** | **wrr** }, or **qos queue** *queue-index* { **drr** | **wrr** }**weight** command to replan the scheduling mode and parameters of each queue, thereby reducing packets to enter PQ queues.

Copyright © Huawei Technologies Co., Ltd.

NOTE

In combined scheduling mode, if the bandwidth is insufficient, the PIR value of other queues cannot be reached. This is a correct traffic shaping result.

- If each queue uses the scheduling mode of **qos pq** or **qos wrr/drr**, go to step 5.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

8.5.2 Troubleshooting Cases

This section provides traffic shaping troubleshooting cases.

Traffic Shaping Results of Queues Are Incorrect

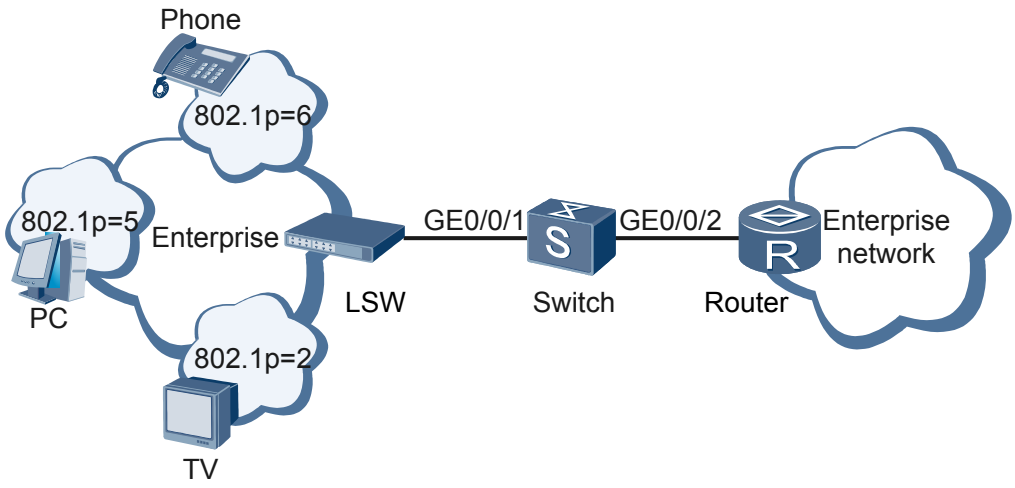
Fault Symptom

As shown in **Figure 8-16**, the transmission rate of network-side traffic is greater than the transmission rate of traffic supported by the LSW, which may lead to jitter on the downlink interface GE 0/0/1 of the Switch. To prevent jitter and ensure bandwidth of services, the Switch is configured to send traffic of voice, video, and data services to queues 6, 2, and 5 respectively. In addition, traffic shaping is configured to:

- Limit the maximum transmission rate of voice services to 128 kbit/s.
- Limit the maximum transmission rate of video services to 2000 kbit/s.
- Limit the maximum transmission rate of data services to 512 kbit/s.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-16 Network diagram



After the configuration, the bandwidth for voice services and video services is insufficient.

Fault Analysis

1. Check the traffic shaping parameters in queues on the downlink interface GE 0/0/1.

   Run the **display this** command in the view of the downlink interface GE 0/0/1 to check the traffic shaping parameters.

```
[Switch-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 200
 qos lr outbound cir 2000 cbs 250000
 qos drr
 qos queue 0 drr weight 0
 qos queue 1 drr weight 0
 qos queue 2 drr weight 20
 qos queue 3 drr weight 0
 qos queue 4 drr weight 0
 qos queue 5 drr weight 50
 qos queue 6 drr weight 80
 qos queue 7 drr weight 0
 qos queue 2 shaping cir 2000 pir 2000
 qos queue 5 shaping cir 512 pir 512
 qos queue 6 shaping cir 128 pir 128

#
return
```

   The preceding information indicates that the outbound interface is configured with traffic shaping and queue shaping. Queue 2, queue 5, and queue 6 use the DRR scheduling mode, and the traffic shaping parameters of each queue are correct. The CIR value for traffic shaping on the interface, however, is smaller than the sum of CIR values for traffic shaping in queue 2, queue 5, and queue 6 on the interface.

   On the S3700, if the CIR value for traffic shaping on an interface is smaller than the sum of CIR values for traffic shaping in queues on the interface, the bandwidth of the queues cannot be ensured.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **interface gigabitethernet0/0/1** command to enter the interface view.

Step 2 Run the **qos lr outbound cir 3000** command to change the CIR for traffic shaping on the interface to 3000 kbit/s so that this value is greater than the sum of CIR values for traffic shaping in queues on the interface.

After the configuration, the bandwidth for voice, video, and data services is sufficient.

----End

Summary

On the Switch, if the CIR value of traffic shaping on an interface is smaller than the sum of the CIR values of queue shaping, the committed rate of the queues cannot be provided.

8.6 Congestion Avoidance Troubleshooting

This chapter describes common causes of congestion avoidance faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

8.6.1 Congestion Avoidance Fails to Take Effect (S3700SI or S3700EI)

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when Congestion Avoidance fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

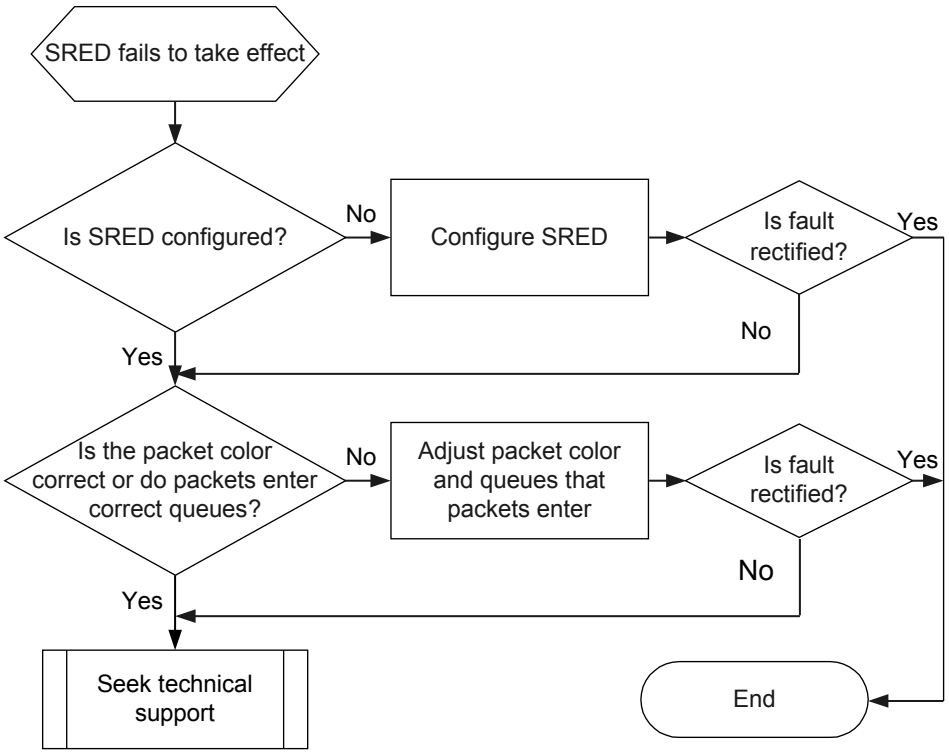
- Queues are not configured with SRED.
- Packet colors or queues that packets enter are incorrect. For example:
  - The queues that packets enter are not the queues configured with SRED.
  - All packets are colored green.

Troubleshooting Flowchart

When congestion occurs, run the **display qos port statistics** command to view the traffic statistics on an interface. If the value of the **Dropped** field is 0 or small, SRED fails to take effect. Use the troubleshooting flowchart in **Figure 8-17**.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-17 Troubleshooting flowchart for ineffective SRED



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that SRED is configured.

Run the **display qos sred** command to check whether SRED parameters are set correctly.

- If "-none-" is displayed, SRED is not configured. Run the **qos sred** command to set SRED parameters of queues.
- If "-none-" is not displayed, go to step 2.

Step 2 Check whether packet colors are correct and whether packets enter correct queues.

Run the **display this** command in the inbound interface view to check the **trust** command and determine the queues that packets enter and packet colors.

Copyright © Huawei Technologies Co., Ltd.

Trusted Priority	Queuing	Coloring
trust 8021p	1. If a traffic policy containing the **remark local-precedence** action is configured on the S3700, packets matching this traffic policy enter a queue according to the re-marked local priority. 2. If a traffic policy containing the **remark 8021p** action is configured on the S3700, packets matching this traffic policy enter a queue according to the re-marked 802.1p priority. 3. If the local priority or 802.1p priority is not configured: ● If packets carry the 802.1p priority, the S3700 sends the packets to a queue corresponding to the 802.1p priority. ● If packets do not carry any priority, the packets enter queue 0.	1. If a traffic policy containing **remark local-precedence** with *color* specified is configured on the S3700, packets matching this traffic policy are marked with the specified color. 2. If a traffic policy containing **remark 8021p** is configured on the S3700, the S3700 colors packets matching this traffic policy according to the re-marked 802.1p priority. 3. If the **dei enable** command is used on the inbound interface, the S3700 colors packets according to the CFI field. 4. If none of the preceding conditions are met: ● If packets carry the 802.1p priority, the S3700 colors packets according to the 802.1p priority. ● If packets do not carry any priority, the S3700 colors packets based on queues.

Copyright © Huawei Technologies Co., Ltd.

Trusted Priority	Queuing	Coloring
trust dscp	1. If a traffic policy containing the **remark local-precedence** action is configured on the S3700, packets matching this traffic policy enter a queue according to the re-marked local priority. 2. If a traffic policy containing **remark 8021p** is configured on the S3700, packets matching this traffic policy enter a queue according to the re-marked 802.1p priority. 3. If the local priority or 802.1p priority is not re-marked: a. If packets carry the DSCP priority or match a traffic policy containing **remark dscp** on the S3700, packets enter a queue according to the mapped 802.1p priority. If DSCP priority re-marking is configured, the priority of packets is the re-marked DSCP priority. b. If packets carry only the 802.1p priority, the S3700 sends the packets to a queue corresponding to the 802.1p priority. c. If packets do not carry any priority, the packets enter queue 0.	1. If a traffic policy containing **remark local-precedence** with *color* specified is configured on the S3700, packets matching this traffic policy are marked with the specified color. 2. If packets carry the DSCP priority or a traffic policy containing **remark dscp** is configured on the S3700, the S3700 colors packets matching this traffic policy according to the mapped drop priority. If DSCP priority re-marking is configured, the priority of packets is the re-marked DSCP priority. 3. If the **dei enable** command is used on the inbound interface, the S3700 colors packets according to the CFI field. 4. If none of the preceding conditions are met, the S3700 colors packets based on queues.

Copyright © Huawei Technologies Co., Ltd.

Trusted Priority	Queuing	Coloring
trust ip-precedence	1. If a traffic policy containing the **remark local-precedence** action is configured on the S3700, packets matching this traffic policy enter a queue according to the re-marked local priority. 2. If a traffic policy containing **remark 8021p** is configured on the S3700, packets matching this traffic policy enter a queue according to the re-marked 802.1p priority. 3. If the local priority or 802.1p priority is not re-marked: a. If packets carry the IP priority or a traffic policy containing **remark local-precedence** is configured on the S3700, packets matching this traffic policy enter a queue according to the mapped 802.1p priority. If IP priority re-marking is configured, the priority of packets is the re-marked IP priority. b. If packets carry only the 802.1p priority, the S3700 sends the packets to a queue according to the 802.1p priority. c. If packets do not carry any priority, the packets enter queue 0.	1. If a traffic policy containing **remark local-precedence** with *color* specified is configured on the S3700, packets matching this traffic policy are marked with the specified color. 2. If the **dei enable** command is used on the inbound interface, the S3700 colors packets according to the CFI field. 3. If none of the preceding conditions are met, the S3700 colors packets based on queues.

Copyright © Huawei Technologies Co., Ltd.

Trusted Priority	Queuing	Coloring
trust no priority	1. If a traffic policy containing the **remark local-precedence** action is configured on the S3700, packets matching this traffic policy enter a queue according to the re-marked local priority. 2. If a traffic policy containing **remark 8021p** is configured on the S3700, the packets matching this traffic policy enter a queue according to the re-marked 802.1p priority. 3. If the local priority or 802.1p priority is not configured: ● If packets carry the 802.1p priority, the S3700 sends the packets to a queue according to the 802.1p priority. ● If packets do not carry the 802.1p priority, the packets enter queue 0.	1. If a traffic policy containing **remark local-precedence** with *color* specified is configured on the S3700, packets matching this traffic policy are marked with the specified color. 2. If the local priority or 802.1p priority is not configured but the **dei enable** command is used on the inbound interface, the S3700 colors packets according to the CFI field. 3. If none of the preceding conditions are met, the S3700 colors packets according to the queue.

NOTE

Determine the traffic policy that takes effect according to **8.1.1 Traffic Policy Fails to Take Effect** in **Troubleshooting Procedure**.

- When the S3700 colors packets according to the drop priority, packets with drop priority 0 are colored green, packets with drop priority 1 are colored yellow, and packets with drop priority 2 are colored red.
- When the S3700 colors packets according to the CFI field, packets with CFI value 0 are colored green and packets with CFI value 1 are colored yellow.
- When the S3700 colors packets according to the 802.1p priority, packets with 802.1p priorities 0 to 4 are colored green and packets with 802.1p priorities 5 to 7 are colored yellow.
- When the S3700 colors packets according to the queue, packets entering queues 0 to 4 are colored red and packets entering queues 5 to 7 are colored yellow.

- Adjust the configuration in the following scenarios:
  - The queues packets enter are not the queues configured with SRED.

    Adjust the configuration so that packets enter the queues configured with SRED.
  - All the packets are colored green.

Copyright © Huawei Technologies Co., Ltd.

If the traffic policy is configured on the S3700 and the traffic policy re-marks the packet color with green, change the re-marked color or cancel color re-marking.

If DSCP priorities are trusted and the mapped drop priority is 0, modify the mapping between DSCP priorities and DP priorities so that the drop priority is not 0.

- Otherwise, go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

8.6.2 Congestion Avoidance Fails to Take Effect (S3700HI)

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when congestion avoidance fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

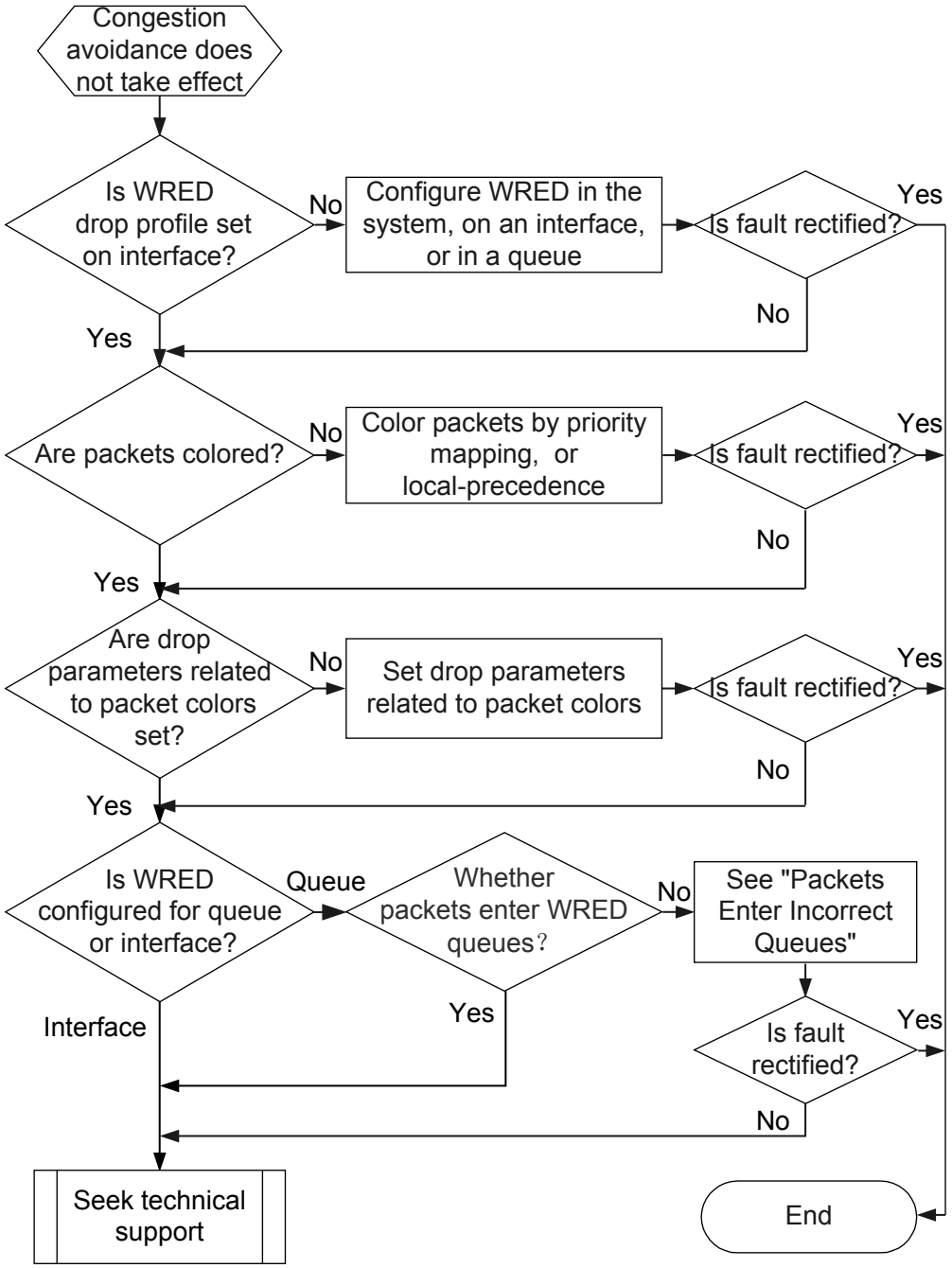
- The interface or queue is not configured with the Weighted Random Early Detection (WRED) drop profile.
- Packets are not colored by using priority mapping, or **remark local-precedence**.
- The parameters corresponding to packet colors are not configured in the WRED drop profile.
- When using queue-based congestion avoidance, packets do not enter queues configured with WRED drop profiles.

Troubleshooting Flowchart

Figure 8-18 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-18 Troubleshooting flowchart for ineffective congestion avoidance



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check whether the WRED drop profile is configured in the system, on an interface, or in a queue on the interface.

1. Run the **display this** command in the interface view to check whether the **qos wred** or **qos queue wred** command is used.
   - If yes, go to step 2.
   - If not, go to step b.
2. Run the **display this** command in the system view to check whether the **qos queue wred** command is used.
   - If the **qos queue wred** command is not used, run the **qos queue wred** or **qos wred** command to configure WRED globally or on an interface.
   - If the **qos queue wred** command is used, go to step 2.

NOTE

The WRED drop profile configured in the system takes effect on all the interfaces. If a WRED drop profile is applied to the system and an interface simultaneously, the WRED drop profile applied to the interface takes effect.

If the WRED drop profiles are configured on an interface and in a queue on the interface, the system applies the WRED drop profiles in the queue and on the interface in sequence.

Step 2 Check whether parameters are set correctly in the WRED drop profile.

Run the **display drop-profile** command to check whether the WRED drop profile contains the parameters related to packet colors configured in step 2.

- If not, run the **color** command to set the parameters.
- If parameters are set and the **qos queue wred** command is used on the interface, go to step 3.
- If parameters are set and the **qos wred** command is used on the interface, go to step 4.

Step 3 Check whether packets enter the queue configured with the WRED drop profile.

Run the **display qos queue statistics** command to check whether there are packet statistics about the queue configured with the WRED drop profile.

- If yes, go to step 5.
- If not, packets are not entering the queue. Rectify the fault according to **8.3.1 Packets Enter Incorrect Queues**.

Step 4 Check whether packets are colored by using priority mapping or traffic action.

Run the **display this** command in the interface view to check whether the following configurations are performed on the interface.

1. Check whether the **traffic-policy** command is used on the interface.
   - If yes, run the **display traffic policy** command to view the actions in the traffic policy. Check whether **remark local-precedence** is configured.
     - If **remark local-precedence** is configured but *color* is not specified, run the **remark local-precedence** command to configure *color*.
     - If **remark local-precedence** is configured and the parameter relevant to the color is configured, the system colors packets based on the configuration. Go to step 5.
     - If the action and related parameter are not configured, go to step b.
2. Check whether the **dei enable** command is used on the interface.

Copyright © Huawei Technologies Co., Ltd.

- If yes, verify that the system correctly marks packets with colors based on the CFI field (if the CFI field is 1, packets are colored yellow; if the CFI field is 0, packets are colored green). Then go to step 5.
- If not, go to step c.

3. Check whether the **trust upstream** { **default** | *ds-domain-name* } command is used on the interface.

   If the **trust upstream** { **default** | *ds-domain-name* } command is used, run the **display diffserv domain name** *diffserv-domain-name* command to check whether the mappings between packet priorities and colors are correct. If the **trust upstream** { **default** | *ds-domain-name* } command is not used, the system trusts the default DiffServ domain by default. Run the **display diffserv domainname default** command to check whether the mappings between packet priorities and colors are correct.

   - If the mappings are incorrect, run the **8021p-inbound**, command to modify the mappings between packet priorities and colors.
   - If the mappings are correct, go to step 5.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

8.7 Congestion Management Troubleshooting

This chapter describes common causes of congestion management faults, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

8.7.1 Congestion Management Fails to Take Effect

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when congestion management fails to take effect.

Common Causes

This fault is commonly caused by one of the following:

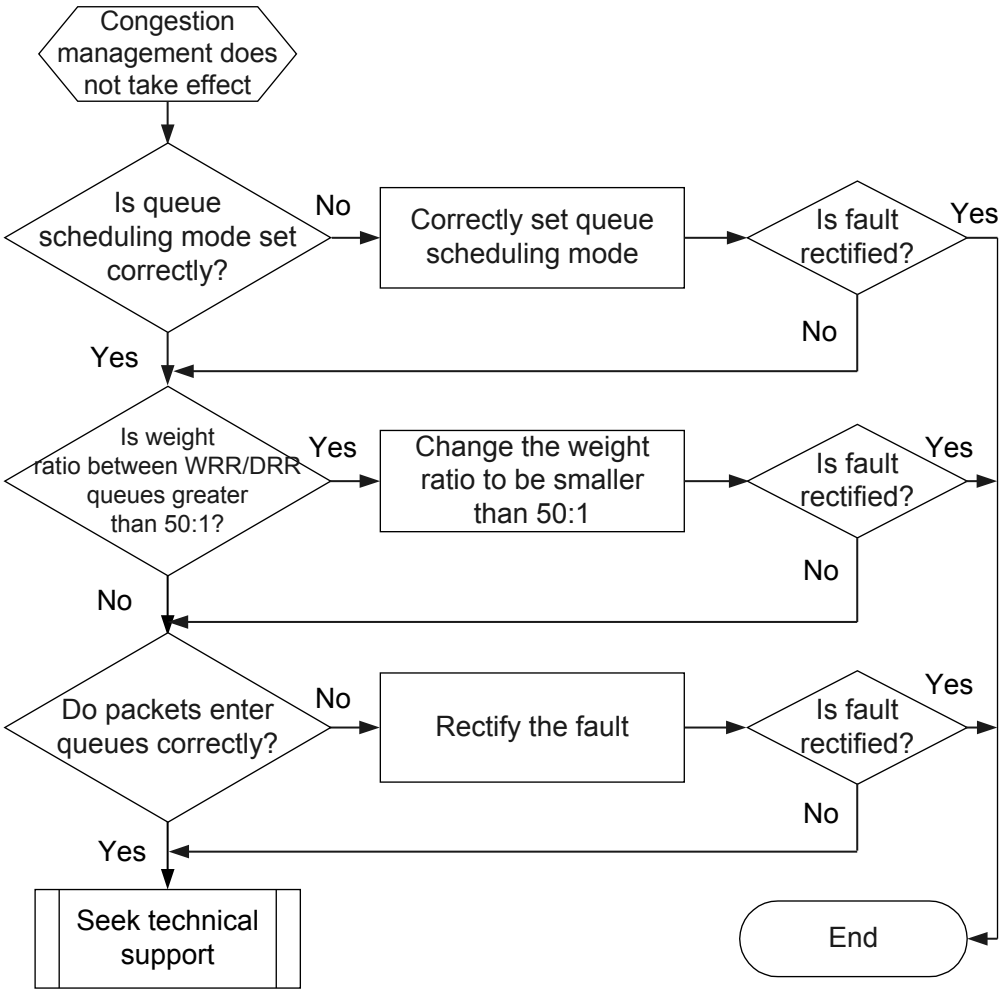
- The queue scheduling mode is configured incorrectly.
- The weight ratio between WRR or DRR queues is greater than 50:1.
- Packets enter incorrect queues.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

If packets in a queue are not scheduled or scheduling results are incorrect, congestion management fails to take effect. Use the troubleshooting flowchart in **Figure 8-19**.

Figure 8-19 Troubleshooting flowchart for ineffective congestion management



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the queue scheduling mode is configured correctly.

Run the **display this** command in the interface view to check whether the queue scheduling mode is correct.

Copyright © Huawei Technologies Co., Ltd.

NOTE

When you configure the queue scheduling mode:

- The combined scheduling mode of PQ+WRR or PQ+DRR is recommended. Specifically, the delay-sensitive key services are scheduled in PQ mode and other services are scheduled in WRR/DRR mode.
- If each queue is configured with PQ scheduling, delay-sensitive key services enter queues with a higher priority and non-key services enter queues with a lower priority.
- If each queue is configured with WRR/DRR scheduling, key services are assigned higher weights and non-key services are assigned lower weights.
- If the average length of different types of packets varies slightly, WRR scheduling is used; if such an average length differs a lot, DRR scheduling is used.

- If not, run the **qos** { **pq** | **wrr** | **drr** } command to reconfigure the queue scheduling mode.
- If yes, go to step 2.

Step 2 Check whether the weight ratio in WRR or DRR queues is overlarge.

NOTE

In WRR or DRR scheduling, if the weight ratio between queues is greater than 50:1, the WRR or DRR scheduling may be incorrect and congestion management may fail.

Run the **display this** command in the interface view to check whether the weight ratio is greater than 50:1 in WRR or DRR scheduling.

- If yes, run the **qos queue** *queue-index* **drr weight** *weight* or **qos queue** *queue-index* **wrr weight** *weight* command to change the queue weights. Ensure that the weight ratio between any two queues is smaller than 50:1.
- If yes, go to step 3.

Step 3 Check whether packets enter queues correctly.

Use a tester to send service packets to the S3700 and run the **display qos queue statistics** command to view the statistics on queues. Check whether packets enter queues corresponding to the scheduling mode.

- If not, rectify the fault according to **8.2.1 Packets Enter Incorrect Queues**(S3700SI and S3700EI) or **8.3.1 Packets Enter Incorrect Queues**(S3700HI).
- If yes, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

8.7.2 Troubleshooting Cases

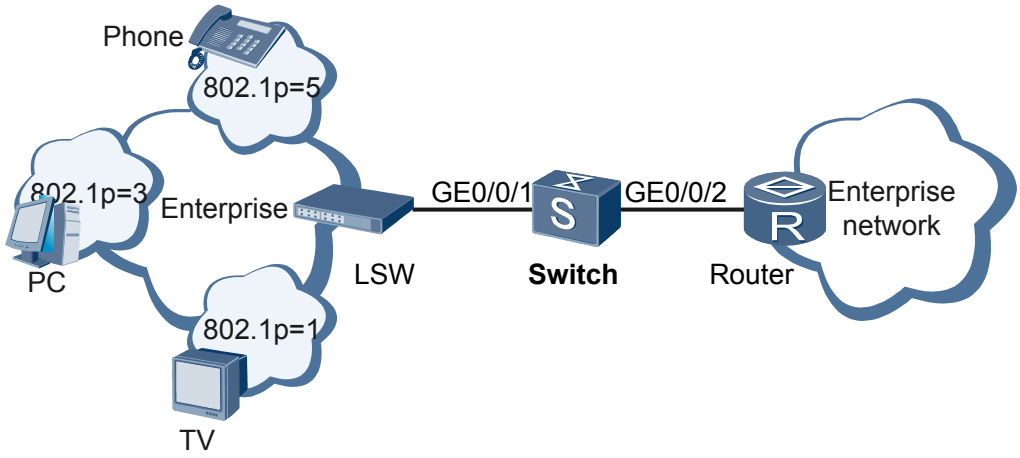
This section provides congestion management troubleshooting cases.

QoS of the Services with High Priority Cannot Be Guaranteed (S3700SI or S3700EI)

Symptom

As shown in **Figure 8-20**, the Switch is connected to the router through GE 0/0/2. The network transmits voice service, video service, and data service. The 802.1p priority of voice service is 5, of video service is 1, and of data service is 3. The services are transmitted to users through the router and the Switch.

Figure 8-20 Networking diagram of congestion management



After the configuration, you find that the voice signal is broken. The QoS of the voice service, which has the highest priority, cannot be guaranteed.

Fault Analysis

The possible causes are as follows:

1. If the fault occurs on other nodes on the link, see the troubleshooting documents of the corresponding nodes.
2. The packets cannot enter the correct queue; thus the packets with lower priority pass but the packets with higher priority are discarded.
3. The scheduling modes and weights of the queues are improper.

Procedure

- Identify the cause of the fault.
  1. Check whether the trust priority and scheduling parameters are configured on the interface.

Copyright © Huawei Technologies Co., Ltd.

Run the **display this** command in the interface view to check whether the priority of the inbound packets is mapped to other priority.

- If the packets passing through the interface is the IP packets carrying the DSCP priority, run the **trust dscp** command on the interface.
- If the packets passing through the interface are from a VLAN, run the **trust 8021p** command on the interface.

```
[Switch-GigabitEthernet0/0/2] display this
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 qos queue 1 wrr weight 10
 qos queue 2 wrr weight 20
 qos queue 3 wrr weight 30
 qos queue 4 wrr weight 0
 qos queue 5 wrr weight 0
 qos queue 6 wrr weight 0
 qos queue 7 wrr weight 0
 trust 8021p
#
return
```

The preceding information indicates that GE 0/0/2 trusts the 802.1p priority. Queue 1, Queue 2, and Queue 3 adopt WRR scheduling and their weights are 10, 20, and 30. Queue 4, Queue 5, Queue 6, and Queue 7 adopt PQ scheduling.

2. Check the traffic statistics and scheduling parameters of each queue.

   Run the **qos port statistics enable** and **display qos port statistics** command to check the queue-based traffic statistics on a specified interface.

```
[Switch] qos port statistics enable interface gigabitethernet 0/0/2
[Switch] display qos port statistics interface GigabitEthernet 0/0/2
Port: GigabitEthernet0/0/2
--------------------------------------------------------------------------------
Queue                    Passed(Packet)                 Dropped(Packet)
--------------------------------------------------------------------------------
0                        0                              0
--------------------------------------------------------------------------------
1                        42355                          0
--------------------------------------------------------------------------------
2                        76663                          0
--------------------------------------------------------------------------------
3                        24354                          0
--------------------------------------------------------------------------------
4                        0                              0
--------------------------------------------------------------------------------
5                        0                              0
--------------------------------------------------------------------------------
6                        0                              0
--------------------------------------------------------------------------------
7                        0                              0
--------------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

The preceding information indicates that the packets enter Queue 1, Queue 2, and Queue 3.

3. Check the mapping between local precedences and queues.

   Run the **display qos local-precedence-queue-map** command to check the mapping between local precedences and queues.

```
<Switch> display qos local-precedence-queue-map
Current configurations of mapping between local-precedence and queue:
  local-precedence value: be     queue index: 0
  local-precedence value: af1    queue index: 1
  local-precedence value: af2    queue index: 2
  local-precedence value: af3    queue index: 2
  local-precedence value: af4    queue index: 4
  local-precedence value: ef     queue index: 3
  local-precedence value: cs6    queue index: 6
  local-precedence value: cs7    queue index: 7
```

   The preceding information indicates that the packets with the 802.1p priority being 5 enter Queue 3, the packets with the 802.1p priority being 3 enter Queue 2, and the packets with the 802.1p priority being 1enter Queue 1. Queue 1, Queue 2 and Queue 3 adopt WRR scheduling and their weights are 10, 20, and 30. Therefore, when service traffic is not heavy, the QoS of the delay-sensitive services can be guaranteed; however, when service traffic is heavy, the QoS cannot be guaranteed. Thus, the voice signal is broken.

- Rectify the fault.
  1. Run the **system-view** command to enter the system view.
  2. Run the **qos local-precedence-queue-map af3 4** command to map packets with the 802.1p priority being 3 to queue 4.
  3. Run the **qos local-precedence-queue-map ef 5** command to map packets with the 802.1p priority being 5 to queue 5.

  After the configuration, the voice signal is not damaged.

----End

Summary

When configuring the congestion management, you need to correctly map the packet priorities to queues.

PQ, WRR, and DRR have their own advantages and disadvantages. If only PQ scheduling is used, the packets in the queues with a low priority cannot obtain bandwidth. If only WRR or DRR scheduling is used, delay-sensitive services cannot be scheduled in time. Therefore, when various services are transmitted on the network, you should use the PQ+WRR or PQ+DRR scheduling.

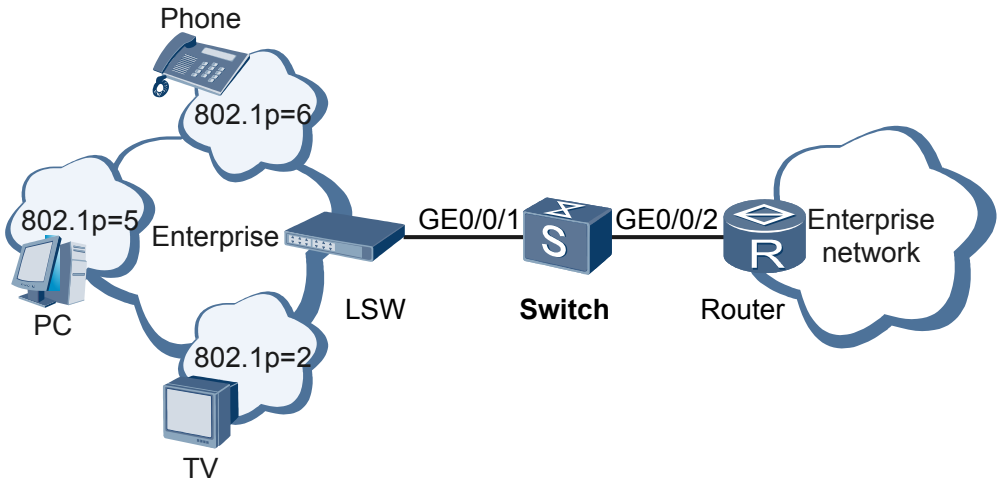
QoS of Services with a Higher Priority Cannot Be Guaranteed (S3700HI)

Fault Symptom

As shown in **Figure 8-21**, the Switch is connected to the router by using GE 0/0/2. Voice, video, and data services are transmitted on the network. The 802.1p priorities of voice, video, and data services are 6, 2, and 5 respectively. These services are transmitted to users through the router and the Switch. To ensure QoS of services, congestion management is configured.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-21 Network diagram



After the configuration, the QoS of voice and video services with a higher priority cannot be guaranteed, and voice and video signals are interrupted sometimes. That is, congestion management fails to take effect.

Fault Analysis

The possible causes are as follows:

- The packets cannot enter correct queues. As a result, the packets with a lower priority are forwarded but the packets with a higher priority are discarded.
- The scheduling modes and weights of the queues are improper.

1. Check the traffic statistics and scheduling parameters of each queue.

   Run the **display qos queue statistics** command to check the traffic statistics and scheduling parameters of the queues on a specified interface.

```
<Quidway> display qos queue statistics interface gigabitethernet 0/0/2
 Queue  CIR/PIR(kbps)         Passed(Packet/Byte)        Dropped(Packet/Byte)
  ------------------------------------------------------------------------------
    0        1000000                        0                            0
             1000000                        0                            0
  ------------------------------------------------------------------------------
    1        1000000                        0                            0
             1000000                        0                            0
  ------------------------------------------------------------------------------
    2         2000                  2457863                           0
              2000                  245786300                           0
  ------------------------------------------------------------------------------
    3       1000000                 2012324                           0
            1000000                 201232400                           0
  ------------------------------------------------------------------------------
    4       1000000                 2047189                           0
            1000000                 204718900                           0
  ------------------------------------------------------------------------------
    5            512                        0                            0
                 512                        0                            0
  ------------------------------------------------------------------------------
    6        1000000                        0                            0
             1000000                        0                            0
  ------------------------------------------------------------------------------
    7            128                        0                            0
```


Copyright © Huawei Technologies Co., Ltd.

```
                128                          0                          0
-------------------------------------------------------------------------------
```

The preceding information indicates that the packets enter queues AF2, AF3, and AF4.

2. Check the priority mapping and scheduling parameters on the interface.

   Run the **display this** command in the interface view to check whether the priority of the incoming packets is mapped to the priority specified by the DiffServ domain.

   - If the packets passing through the interface are the IP packets carrying the DSCP priority, run the **trust upstream** and **trust dscp** commands on the interface.
   - If the packets passing through the interface come from a VLAN, run the **trust upstream** and **trust 8021p** commands on the interface.

```
[Quidway-GigabitEthernet0/0/2] display this
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 qos queue 0 wrr weight 0
 qos queue 1 wrr weight 10
 qos queue 2 wrr weight 20
 qos queue 3 wrr weight 30
 qos queue 4 wrr weight 40
 qos queue 5 wrr weight 0
 qos queue 6 wrr weight 0
 qos queue 7 wrr weight 0
 trust upstream ds1
#
return
```

   The preceding information indicates that GE 0/0/2 is bound to the DiffServ domain **ds1** and trusts the 802.1p priority in the outer VLAN tag. Queues AF1 to AF4 use WRR scheduling and their weights are 10, 20, 30, and 40 respectively. Queues BE, EF, CS6, and CS7 use PQ scheduling.

3. Check the configuration of the DiffServ domain.

   Run the **display diffserv domain name ds1** command to view the mapping of 802.1p priorities in the DiffServ domain **ds1**.

```
<Quidway> display diffserv domain name ds1
diffserv domain name:ds1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 green
 8021p-inbound 2 phb AF2 green
 8021p-inbound 3 phb af3 green
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb AF3 green
 8021p-inbound 6 phb AF4 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 8021p-outbound be yellow map 0
```

   The preceding information indicates that the packets with the 802.1p priority being 6 enter the AF4 queue, the packets with the 802.1p priority being 5 enter the AF3 queue, and the packets with the 802.1p priority being 2 enter the AF2 queue. The mapping is correct. Queues AF4, AF3, and AF2 use WRR scheduling and their weights are 40, 30, and 20 respectively. Therefore, when service traffic is light, the QoS of delay-sensitive services can be guaranteed; however, when service traffic is heavy, the QoS of delay-sensitive services cannot be guaranteed and therefore voice signals are interrupted sometimes.

Procedure

Step 1 Run the **diffserv domain ds1** command to enter the view of the DiffServ domain **ds1**.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Run the **8021p-inbound 2 phb af2 green** command to map the packets with the 802.1p priority being 2 to the AF2 queue.

Step 3 Run the **8021p-inbound 5 phb ef green** command to map the packets with the 802.1p priority being 5 to the EF queue.

Step 4 Run the **8021p-inbound 6 phb cs7 green** command to map the packets with the 802.1p priority being 6 to the CS7 queue.

After the configuration, voice signals are transmitted continuously.

----End

Summary

When configuring the DiffServ domain, correctly map the packet priorities to queues.

PQ, WRR, and DRR have their own advantages and disadvantages. If only PQ scheduling is used, the packets in the queues with a low priority cannot obtain bandwidth for a long period of time. If only WRR or DRR scheduling is used, delay-sensitive services cannot be scheduled in time. Therefore, when various services are transmitted on the network, use PQ+WRR or PQ +DRR scheduling.

Copyright © Huawei Technologies Co., Ltd.

9 Reliability

About This Chapter

9.1 Smart Link Troubleshooting
This chapter describes common causes of a Smart Link fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedures, alarms, and logs.

9.2 VRRP Troubleshooting
This chapter describes common causes of Virtual Router Redundancy Protocol (VRRP) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

9.3 Ethernet OAM Troubleshooting
This chapter describes common causes of an Ethernet OAM fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

9.4 Y.1731 Troubleshooting

9.5 BFD Troubleshooting
This chapter describes common causes of a BFD fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

9.6 DLDP Troubleshooting
This chapter describes common causes of a DLDP fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

9.7 RRPP Troubleshooting

9.8 SEP Troubleshooting
This chapter describes common causes of SEP faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

9.1 Smart Link Troubleshooting

This chapter describes common causes of a Smart Link fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedures, alarms, and logs.

9.1.1 Active/Standby Switchover Failure in a Smart Link Group

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the active/standby switchover failure in a Smart Link group.

Common Causes

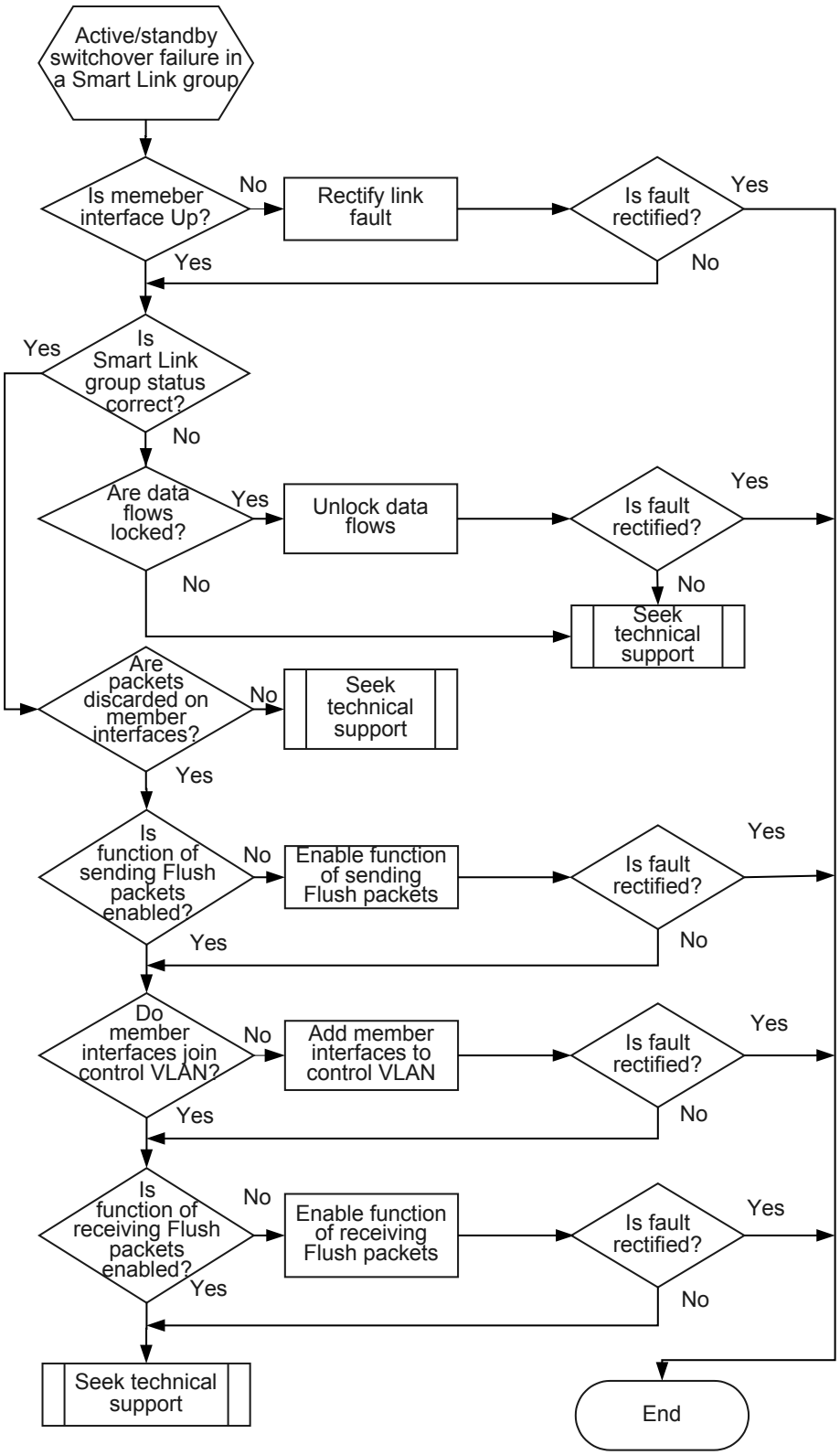
This fault is commonly caused by one of the following:

- The Smart Link group is configured incorrectly. For example, the Smart Link group function is disabled or member interfaces are not added to the service VLAN.
- The link is faulty.
- Data flows are locked on an interface in the Smart Link group.
- Flush packets are incorrectly received or sent.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 9-1 Smart Link group troubleshooting flowchart



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check the member interface status in the Smart Link group.

Run the **display interface** *interfacetype interface-number* command to view the interface status, that is, the value of the **current state** field.

- If the value of the **current state** field is **Down**, rectify the fault according to **Connected Ethernet Interfaces Down**.
- If the value of the **current state** field is **Up**, the interface is Up. Go to step 2.

Step 2 Check the Smart Link group status.

Run the **display smart-link group** { **all** | *group-id* } command to view the Smart Link group status, that is, the value of the **State** field.

- If one interface is active and the other interface is inactive, the Smart Link group is in Up state. Go to step 4.
- If the Smart Link group is in Down state, go to step 3.

Step 3 Check whether data flows are locked on an interface in the Smart Link group.

Run the **display smart-link group** *group-id* command to check whether data flows are locked on an interface in the Smart Link group, that is, view the value of the **Link status** field.

- If the value of the **Link status** field is **lock** or **force**, data flows are locked on the master or slave interface in the Smart Link group. Run the **undo smart-link** { **force** | **lock** } command to unlock data flows on an interface in the Smart Link group.
- If the **Link status** field is not displayed, data flows are not locked on an interface in the Smart Link group. Go to step 8.

Step 4 Check whether packets are discarded on member interfaces in the Smart Link group.

Use the following method to check whether packets are discarded:

Run the **ping-c** *count* **-t** *timeout* command to view packet loss information in the command output.

NOTE

If the network is unreliable, set the packet transmission count (-c) and timeout (-t) to the upper limits. This makes the test result accurate.

- If there are discarded packets, go to step 5.
- If no packet is discarded, go to step 8.

Step 5 Check whether the function of sending Flush packets is enabled.

Run the **display this** command in the Smart Link group view to check whether the function of sending Flush packets is enabled.

- If the information "flush send control-vlan vlan-id" is not displayed, run the **flush send** command to enable the function of sending Flush packets.

Copyright © Huawei Technologies Co., Ltd.

- If the information "flush send control-vlan vlan-id" is displayed, go to step 6.

Step 6 Check whether the control VLAN is created. Ensure that member interfaces of the Smart Link group join the control VLAN.

Run the **display vlan** *vlan-id* command.

- If the following information is displayed, member interfaces of the Smart Link group join the control VLAN. Go to step 7.

```
--------------------------------------------------------------------------------
--
U: Up;         D: Down;         TG: Tagged;         UT:
Untagged;
MP: Vlan-mapping;               ST: Vlan-
stacking;
#: ProtocolTransparent-vlan;    *: Management-
vlan;
--------------------------------------------------------------------------------
--

VID  Type
Ports
--------------------------------------------------------------------------------
--
10   common  TG:Eth0/0/3(U)     Eth0/0/2
(U)
```

- If the following information is not displayed, create a control VLAN and add member interfaces of the Smart Link group to the control VLAN.

Step 7 Check whether the function of receiving Flush packets is enabled on the peer device.

Run the **display this** command in the interface view.

- If the information "smart-link flush receive control-vlan vlan-id" is displayed, go to step 8.
- If the information "smart-link flush receive control-vlan vlan-id" is not displayed, run the **smart-link flush receive** command to enable the function of receiving Flush packets.

Step 8 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700
- MAC address of the device configured with the Smart Link group

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

9.1.2 Monitor Link Group Status Is Down

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when the Monitor Link group status is Down.

Copyright © Huawei Technologies Co., Ltd.

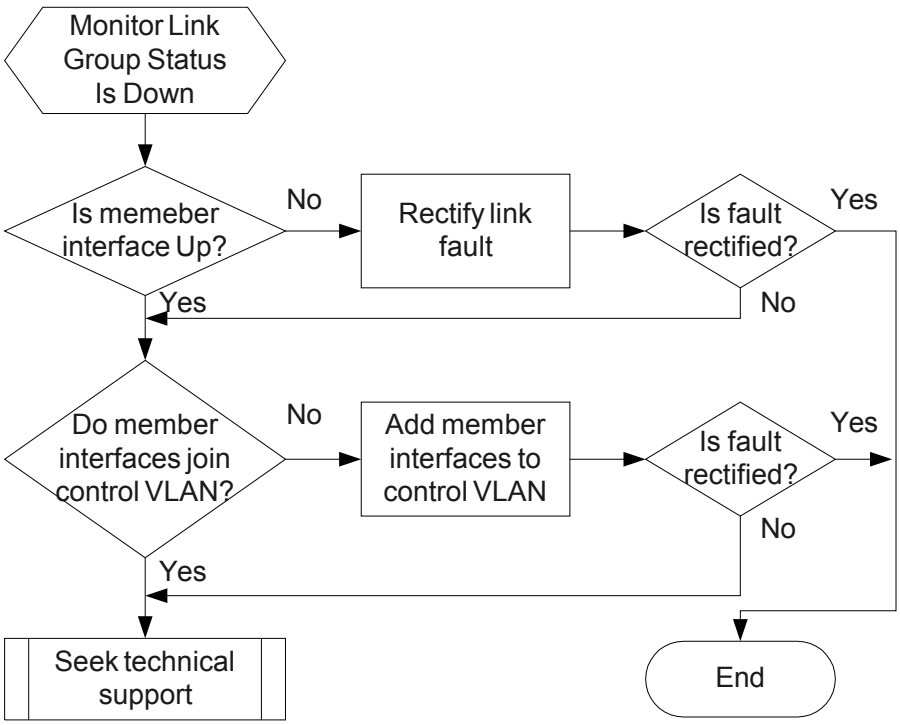
Common Causes

This fault is commonly caused by one of the following:

- The link is faulty.
- The member interface of the Monitor Link group is not added to the service VLAN.
- The downlink interface is manually shut down.

Troubleshooting Flowchart

Figure 9-2 Troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check the member interface status in the Monitor Link group.

Run the **display monitor-link group** *group-id* command to view the **State** field.

- If the value of the **State** field is **DOWN**, rectify the fault according to **Connected Ethernet Interfaces Down**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

A link fault, a unidirectional OAM connectivity fault, or a failure to establish OAM connections may occur on the uplink interface. When the uplink interface belongs to a Smart Link group, the uplink interface is considered as faulty if none of the maser and slave interfaces of the Smart Link group are in active state or the Smart Link group is not enabled.

- If the value of the **State** field is **UP**, go to step 2.

Step 2 Check whether the member interface of the Monitor Link group is added to the service VLAN.

Run the **display current-configuration interface** *interface-type interface-number* command in the member interface view to check whether the member interface of the Monitor Link group is added to the service VLAN.

- If the member interface of the Monitor Link group is not added to the service VLAN, add the member interface to the service VLAN.
- If the member interface of the Monitor Link group is added to the service VLAN, go to step 3.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None

Relevant Logs

None

9.2 VRRP Troubleshooting

This chapter describes common causes of Virtual Router Redundancy Protocol (VRRP) faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

NOTE

The S3700SI does not support VRRP.

9.2.1 VRRP Group Flaps

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when the VRRP group flaps.

Common Causes

This fault is commonly caused by one of the following:

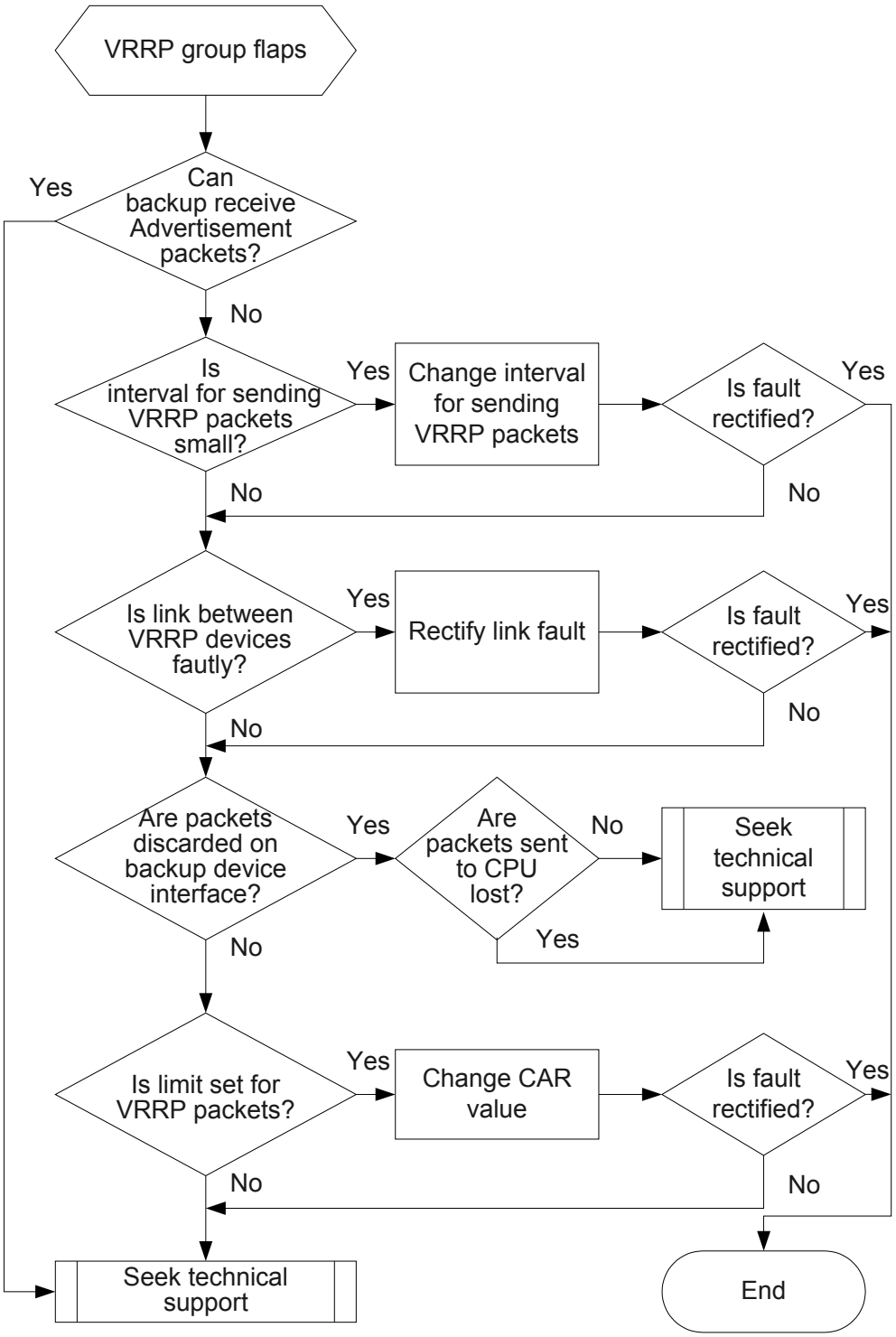
Copyright © Huawei Technologies Co., Ltd.

- The interface where VRRP Advertisement packets are transmitted changes between Up and Down frequently.
- The interval for sending VRRP Advertisement packets is small.
- Packets are discarded on the backup device interface.
- VRRP packets are discarded randomly because congestion occurs.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 9-3 VRRP group troubleshooting flowchart



Troubleshooting Procedure

Copyright © Huawei Technologies Co., Ltd.

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the backup device can receive VRRP Advertisement packets.

Run the **debugging vrrp packet** command on the backup device to check whether the following information is displayed.

```
*Aug 27 19:45:04 2009 Quidway VRRP/7/DebugPacket:
Vlanif45 | Virtual Router 45:receiving from 45.1.1.4, priority = 100,timer = 1,
auth type is no, SysUptime: (0,121496722)
```

By default, the master device sends one VRRP Advertisement packet every second.

- If the backup device cannot receive VRRP Advertisement packets, go to step 2.
- If the backup device can receive VRRP Advertisement packets, go to step 6.

Step 2 Check whether the interval for sending VRRP Advertisement packets is short.

Run the **vrrp vrid timer advertise** command to set a greater interval for sending VRRP Advertisement packets. Then run the **display vrrp** command repeatedly on the Backup device to view the **State** field. If the command output does not change, the backup device works stably.

- If the backup device works stably, the interval for sending VRRP Advertisement packets is small.
- If the backup device works unstably, restore the interval for sending VRRP Advertisement packets. Go to step 3.

Step 3 Check whether the link between devices in the VRRP group is faulty.

Run the **ping** command repeatedly to check whether IP addresses of devices in the VRRP group can be pinged.

- If all the ping operations fail, rectify the fault on the link according to A Ping Operation Fails.
- If some ping operations succeed, loops may occur. Remove the loops.
- If all the ping operations succeed, go to step 4.

Step 4 Check whether packets are discarded on the backup device interface.

Use the following method to check whether packets are discarded:

NOTE

Before running the **display interface** command, run the **reset counters interface** command to clear the statistics on the interface.

Run the **display interface** *interface-type interface-number* command to check the values of **Discard** fields under **Input** and **Output**.

- If packets are discarded, go to step 5.
- If no packet is discarded, go to step 7.

Step 5 Check whether the limit for VRRP packets is configured on the LPU.

Run the **display cpu-defend** [*packet-type*]**configuration** { **all** | **slot** *slot-id* } command to check whether the following information is displayed:

```
------------------------------------------------------------------------
Packet Name                    Status  Cir(Kbps)    Cbs(Byte)   Queue
------------------------------------------------------------------------
vrrp                          Enabled          64       10000         2
```


Copyright © Huawei Technologies Co., Ltd.

The default CIR value is 64 kbit/s. Each board supports about 100 VRRP groups.

- If there are more than 100 VRRP backup groups, run the **car** command to change the CAR value to be greater.
- If there are 100 VRRP backup groups or less, go to step 7.

Step 6 Check whether VRRP packets sent to the CPU are discarded.

Run the **display cpu-defend statistics slot** *slot-id* command to check whether VRRP packets sent to the CPU are discarded.

- If the value of the **Drop(Packets)** field is not 0, VRRP packets sent to the CPU are discarded. Record the result and go to step 7.
- If the value of the **Drop(Packets)** field is 0, VRRP packets sent to the CPU are not discarded. Go to step 7.

Step 7 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

9.2.2 Two Master Devices Exist in a VRRP Group

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure to use when two master devices exist in a VRRP group.

Common Causes

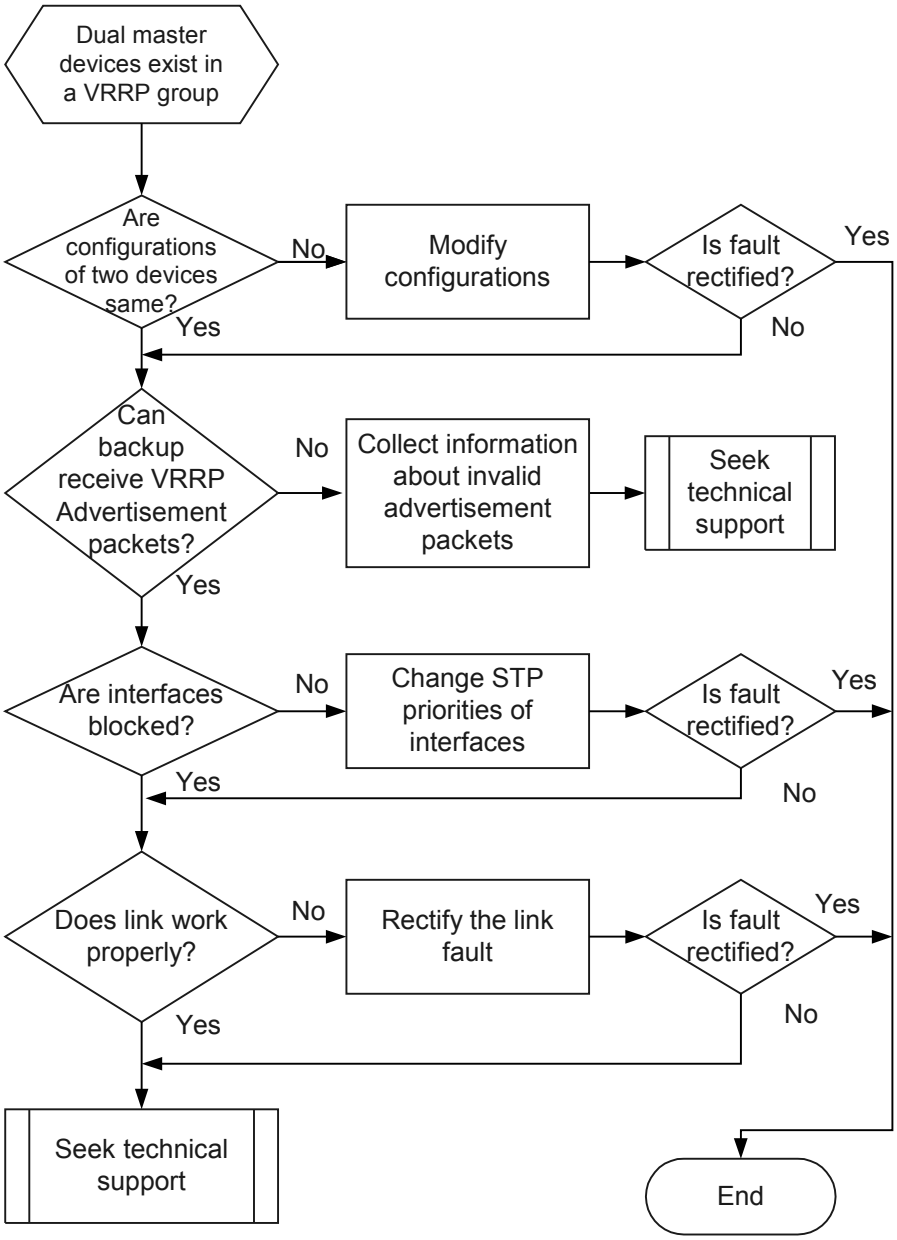
This fault is commonly caused by one of the following:

- The configurations of the devices in the VRRP group are different.
- The link where VRRP Advertisement packets are transmitted is faulty.
- A loop occurs on the link.
- The VRRP Advertisement packets received by the VRRP group with a lower priority are taken as invalid packets mistakenly and are discarded.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 9-4 Troubleshooting flowchart for dual master devices in a VRRP group



Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check that the configurations of the devices in the VRRP group are the same.

Run the **display this** command on VLANIF interfaces of the devices to check the configurations.

Field	Method
ip address	Check whether interface IP addresses are on the same network segment. If not, run the **ip address** command to change IP addresses to be on the same network segment.
vrid	Check whether the virtual router IDs on the interfaces are the same. If not, run the **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* command to change the virtual router IDs to be the same.
Virtual IP	Check whether virtual IP addresses on the interfaces are the same. If not, run the **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* command to change the virtual IP addresses to be the same.
TimerRun	Check whether the interfaces are configured with the same interval for sending Advertisement packets. If not, run the **vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval* command to change the intervals to be the same.
Auth Type	Check whether VRRP packet authentication modes on the interfaces are the same. If not, run the **vrrp vrid** *virtual-router-id* **authentication-mode** { **simple** *key* | **md5** *md5-key* } command to change the authentication modes to be the same.

If the fault persists, go to step 2.

Step 2 Check whether the backup device can receive VRRP Advertisement packets.

Enable debugging on the backup device and check whether the following information is displayed:

```
*Aug 27 19:45:04 2009 Quidway VRRP/7/DebugPacket:
Vlanif45 | Virtual Router 45:receiving from 45.1.1.4, priority = 100,timer = 1,
auth type is no, SysUptime: (0,121496722)
```

By default, the master device sends one VRRP Advertisement packet every second.

- If the backup device does not receive VRRP Advertisement packets, go to step 3.
- If the backup device receives VRRP Advertisement packets, go to step 5.

Step 3 Check whether any interface on the device in the VRRP group and devices on the transmission path of VRRP Advertisement packets is blocked.

Run the **display stp brief** command to check the **STP State** field.

- If the value of the **STP State** field is **FORWARDING**, the corresponding interface is not blocked. Go to step 4.
- If the value of the **STP State** field is **DISCARDING**, the corresponding interface is blocked. Change STP priorities of interfaces to ensure that interconnected interfaces can forward VRRP packets.

Step 4 Run the **ping** command to check whether the link between devices in the VRRP group is faulty.

Copyright © Huawei Technologies Co., Ltd.

- If the ping operation fails, rectify link faults according to A Ping Operation Fails.
- If the ping operation succeeds, go to step 6.

Step 5 Check whether the VRRP group with a lower priority receives invalid VRRP Advertisement packets.

Run the **display vrrp statistics** command to check the **Received invalid type packets** field.

- If the value of the **Received invalid type packets** field is not 0, invalid VRRP Advertisement packets are received. Go to step 6.
- If the value of the **Received invalid type packets** field is 0, invalid VRRP Advertisement packets are not received. Go to step 6.

Step 6 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

9.2.3 Trouble Cases

Data Packets Are Discarded on a Network Configured with VRRP

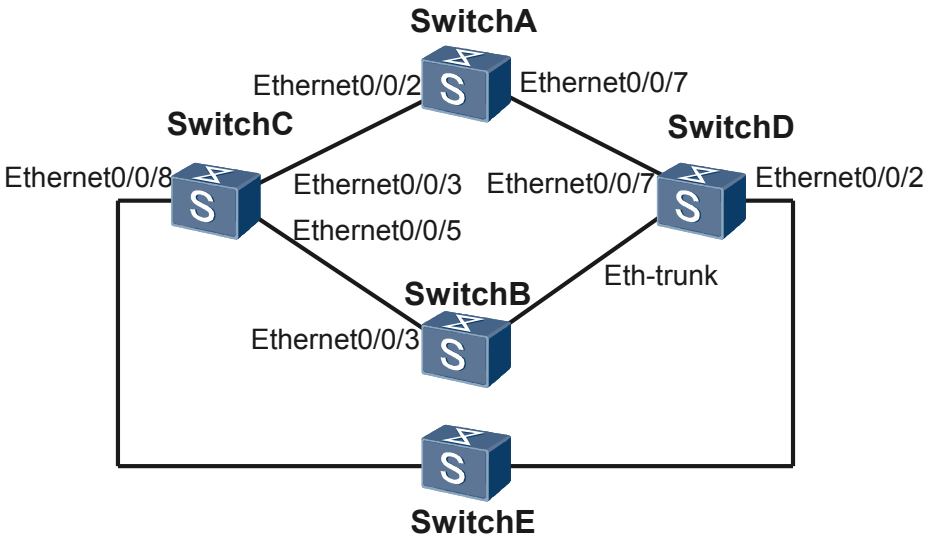
On a network configured with a VRRP backup group, a device connected to VRRP routers is incorrectly configured, causing incorrect MAC address learning and thus packet loss.

Fault Symptom

On the network shown in **Figure 9-5**, a VRRP backup group is configured on Switch A and Switch B. Switch A functions as a master device and Switch B functions as a backup device. Switch C functions as a switch connecting Switch A and Switch B.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-5 Networking diagram of a VRRP backup group



After the configurations, a large number of packets sent from Switch E to Switch D are discarded.

Fault Analysis

1. Run the **display vrrp** [**interface** *interface-type interface-number*] [*virtual-router-id*] **statistics** command on Switch A and then Switch B to check traffic on Eth0/0/2 of Switch A and Eth0/0/3 of Switch B. A small volume of traffic is transmitted on Eth0/0/2 of Switch A connected to Switch C, and no traffic is transmitted on Eth0/0/3 of Switch B connected to Switch C.

   Run the **display statistics interface** *interface-type interface-number* command on Switch C to check traffic on Eth0/0/4, Eth0/0/3, and Eth0/0/5. A small volume of traffic is transmitted on Eth0/0/3 connected to Eth0/0/2, and no traffic is transmitted on Eth0/0/5 connected to Eth0/0/3. A large amount of traffic is transmitted on Eth0/0/4. The statistics show that traffic is dropped on Switch C.

2. Run the **display mac-address dynamic** command on Switch C to check MAC addresses. The learned MAC address of Switch A is sent by Eth0/0/4, but not Eth0/0/3 connected to Switch A or Eth0/0/5 connected to Switch B, indicating that the learned MAC address is incorrect. For example:

```
MAC address table of slot
0:

-------------------------------------------------------------------------------
-
       MAC Address    VLAN/       PEVLAN CEVLAN Port            Type
LSP/
                      VSI/SI                                              MAC-
Tunnel

-------------------------------------------------------------------------------
-
       0000-0a0a-0102  1           -      -      Ethernet0/0/4       dynamic
-
       0000-5e00-0101  1           -      -      Ethernet0/0/4
dynamic     -
       0098-0113-0005  1           -      -      Ethernet0/0/4       dynamic
-
```


Copyright © Huawei Technologies Co., Ltd.

```
      0018-824f-f5d1  1           -      -      Ethernet0/0/3        dynamic
-

------------------------------------------------------------------------------
-
```

3. Run the **display current-configuration interface** *interface-type interface-number* command on Switch C to check the configuration on Eth0/0/4. For example:

```
 #
        interface Ethernet0/0/4
         undo shutdown
         loopback internal
         portswitch
         port default vlan 1
```

The loopback function has been configured on Eth0/0/4, indicating that Eth0/0/4 loops traffic back after receiving it.

4. Run the **display statistics interface** *interface-type interface-number* command on Switch C to check traffic on Eth0/0/3, Eth0/0/4, and Eth0/0/5. A great amount of traffic is transmitted on Eth0/0/4. A small volume of traffic is transmitted on Eth0/0/3. This indicates that traffic loss is caused by the loopback function on Eth0/0/4.

5. Run the **display mac-address dynamic** command multiple times on Switch C to check MAC addresses. Switch C learns different MAC addresses at different times. For example:

```
[SwitchC] display mac-address
dynamic
      MAC address table of slot
0:

------------------------------------------------------------------------------
-
      MAC Address    VLAN/       PEVLAN CEVLAN Port            Type
LSP/
                     VSI/SI                                            MAC-
Tunnel

------------------------------------------------------------------------------
-
      0000-0a0a-0102 1           -      -      Ethernet0/0/4         dynamic
-
      0000-5e00-0101 1           -      -      Ethernet0/0/4         dynamic
-
      0098-0113-0005 1           -      -      Ethernet0/0/5         dynamic
-
      0018-824f-f5d1 1           -      -      Ethernet0/0/4         dynamic
-

------------------------------------------------------------------------------
-
      Total matching items on slot 0 displayed =
4
[SwitchC] display mac-address dynamic
      MAC address table of slot
0:

------------------------------------------------------------------------------
-
      MAC Address    VLAN/       PEVLAN CEVLAN Port            Type
LSP/
                     VSI/SI                                            MAC-
Tunnel

------------------------------------------------------------------------------
-
      0000-0a0a-0102 1           -      -      Ethernet0/0/4         dynamic
-
      0000-5e00-0101 1           -      -      Ethernet0/0/3         dynamic
```


Copyright © Huawei Technologies Co., Ltd.

```
-
      0098-0113-0005 1           -      -      Ethernet0/0/5         dynamic
-
      0018-824f-f5d1 1           -      -      Ethernet0/0/4         dynamic
-

------------------------------------------------------------------------------
-
      Total matching items on slot 0 displayed=4
```

In a VRRP backup group, a device with a higher priority functions as a master device. If the IP address of a device is the same as the virtual IP, the router priority is considered highest and always functions as the master device. The master device sends a VRRP packet to the backup device every one second by default. If a backup device fails to receive three consecutive packets from the master device, the backup device preempts to be the master device and sends a VRRP packet indicating that it becomes the master. In normal situations, the backup device does not send VRRP packets.

NOTE

If a device is assigned an IP address the same as the virtual IP address, the device always functions as the master router.

On this network, a packet sent by the master device arrives at the switch. The switch learns the source MAC address (in this example, 0000-5e00-0101), VLAN ID, and interface connected to the master device, and adds them to the MAC address table. The switch searches the MAC address table for the interface connected to the master device, thus forwarding the packet to the backup device. If a VRRP switchover occurs, the backup device becomes the master device and then sends a VRRP packet. After receiving the VRRP packet, the switch learns the MAC address and maps it to another interface connected to the new master device.

On this network, after receiving a VRRP packet that is sent every one second, Switch C learns the MAC address of Switch A and forwards the VRRP packet to all interfaces belonging to VLAN 1. Eth0/0/4 of VLAN 1 receives the VRRP packet, and then loops the VRRP packet back by using the loopback function. After receiving the returned VRRP packet, Switch C adds the mapping between Eth0/0/4 and 0000-5e00-0101 to the MAC address table to overwrite the previous mapping. In this manner, the newly-learned MAC address overwrites the previous one repeatedly, causing traffic loss.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **undo loopback** command to disable the loopback function on the interface.

After the preceding operations, no traffic is discarded. The fault is cleared.

----End

Summary

Do not enable the loopback function on an interface of a Layer 2 device; otherwise, incorrect MAC addresses are learned.

Copyright © Huawei Technologies Co., Ltd.

9.3 Ethernet OAM Troubleshooting

This chapter describes common causes of an Ethernet OAM fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

9.3.1 MAC Trace Based on Ethernet OAM 802.1ag Fails

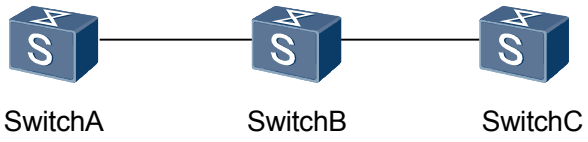
This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the Ethernet OAM 802.1ag-based MAC trace failure.

Common Causes

As shown in **Figure 9-6**, SwitchA fails to trace the MAC address of SwitchC based on 802.1ag.

```
[SwitchA-md-1-ma-1] trace mac-8021ag mac 0018-823c-c449
Tracing the route to 0018-823c-c449 over a maximum of 64 hops:
Request timed out.
```

Figure 9-6 Network diagram



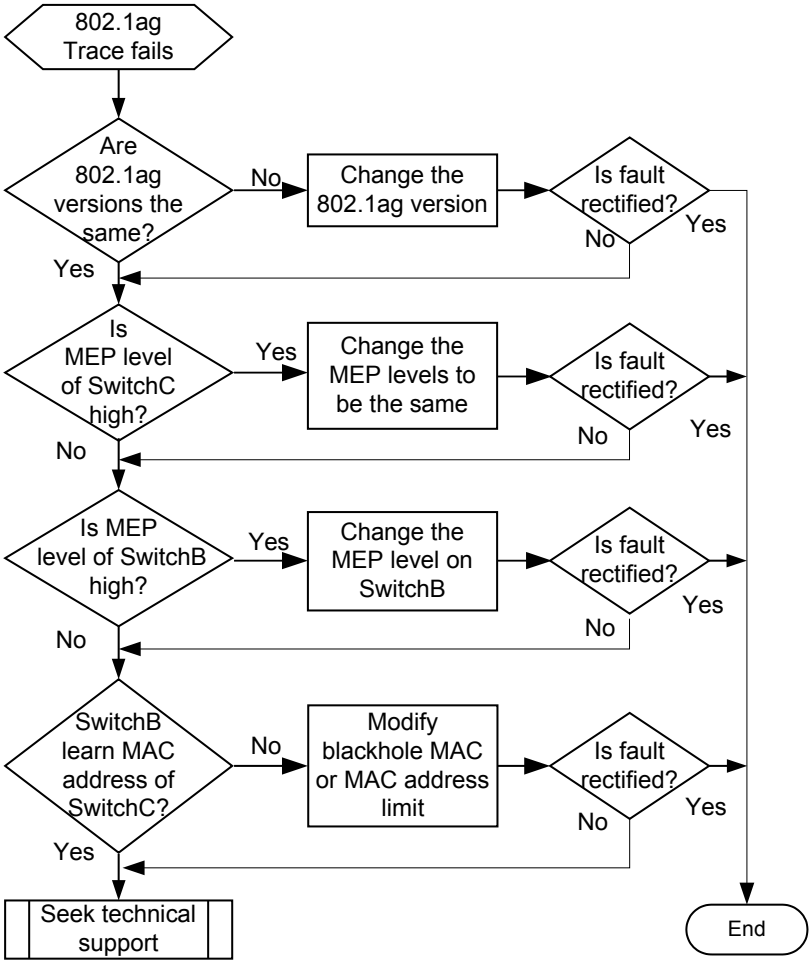
This fault is commonly caused by one of the following:

- The destination node SwitchC is not configured with the MEP of the same level as the MEP on SwitchA.
- The MEP level of the intermediate node is the same as or higher than the MEP level of SwitchA.
- The intermediate node does not have a MAC address entry with the destination being SwitchC.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 9-7 Troubleshooting flowchart for the Ethernet OAM 802.1ag-based MAC trace failure



Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Perform the following operations on the device where the fault occurs and on the downstream MEP or MIP of the device.

Procedure

Step 1 Run the **display oam global configuration** command to check whether all the devices on the trace path use the same 802.1ag version.

- If yes, go to step **Step 2**.
- If not, run the **cfm version** command to switch the Ethernet CFM 802.1ag version between draft7 and standard2007.

Copyright © Huawei Technologies Co., Ltd.

CAUTION

After the IEEE 802.1ag version is changed, the original CFM configuration will be deleted. Therefore, use this command with caution.

- If SwitchA successfully traces the MAC address of SwitchC based on 802.1ag, the fault has been rectified
- If SwitchA still fails to trace the MAC address of SwitchC, go to step **Step 2**.

Step 2 Run the **display this** command on the MD view on source node and destination node to check whether the MEP levels of the destination node and the source node are the same.

- If yes, go to step **Step 3**.
- If not, delete the MD, run the **cfm md** command to create a new one, set the MEP level of the destination node to be the same as that of the source node.
  - If SwitchA successfully traces the MAC address of SwitchC based on 802.1ag, the fault has been rectified.
  - If SwitchA still fails to trace the MAC address of SwitchC, go to step **Step 3**.

Step 3 Run the **display cfm mep** command to check whether the MEP level of the intermediate node is the same as or higher than the MEP level of SwitchA.

NOTE

The 802.1ag packets of a low-level MD are discarded in a high-level MD. The 802.1ag packets of a high-level MD can traverse a low-level MD, The 802.1ag packets of an MD cannot be transmitted through the MD of the level same as that of the MD.

- If not, go to step **Step 4**.
- If yes, delete the MD, run the **cfm md** command to create a new one, change the MEP level on the intermediate node.
  - If SwitchA successfully traces the MAC address of SwitchC based on 802.1ag, the fault has been rectified.
  - If SwitchA still fails to trace the MAC address of SwitchC, go to step **Step 4**.

Step 4 Run the **display mac-address dynamic unit** *unit-id* command to check whether the intermediate node has a MAC address entry with the destination being SwitchC.

- If yes, go to step **Step 5**.
- If not, run the **ping mac-8021ag** command to enable the intermediate node to learn the MAC address of SwitchC.
  - If SwitchA successfully traces the MAC address of SwitchC based on 802.1ag, the fault has been rectified.
  - If SwitchA still fails to trace the MAC address of SwitchC, go to step **Step 5**.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms

EOAM1AG_1.3.6.1.4.1.2011.5.25.136.1.6.1 hwCfmFaultAlarm

Relevant Logs

EOAM1AG/0/ALARM_CONFIG_ERR

EOAM1AG/3/DEL_MD_ERR

9.4 Y.1731 Troubleshooting

9.4.1 Troubleshooting of the Fault that One-way Delay Is Not Collected Though One-way Frame Delay Measurement Is Configured for a VLAN

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the fault that one-way delay is not collected though one-way frame delay measurement is configured for a VLAN.

Common Causes

This fault is commonly caused in one of the following situations:

- The service link is faulty.
- The action of displaying one-way frame delay measurement is not performed on the remote MEP.
- The receive command is not configured on the remote MEP.
- The remote MEP ID is specified for one-way frame delay measurement but the local MEP has not learned MAC address from the remote MEP.
- The remote MAC address is specified for one-way frame delay measurement but the specified MAC address is not the MAC address of the remote MEP.

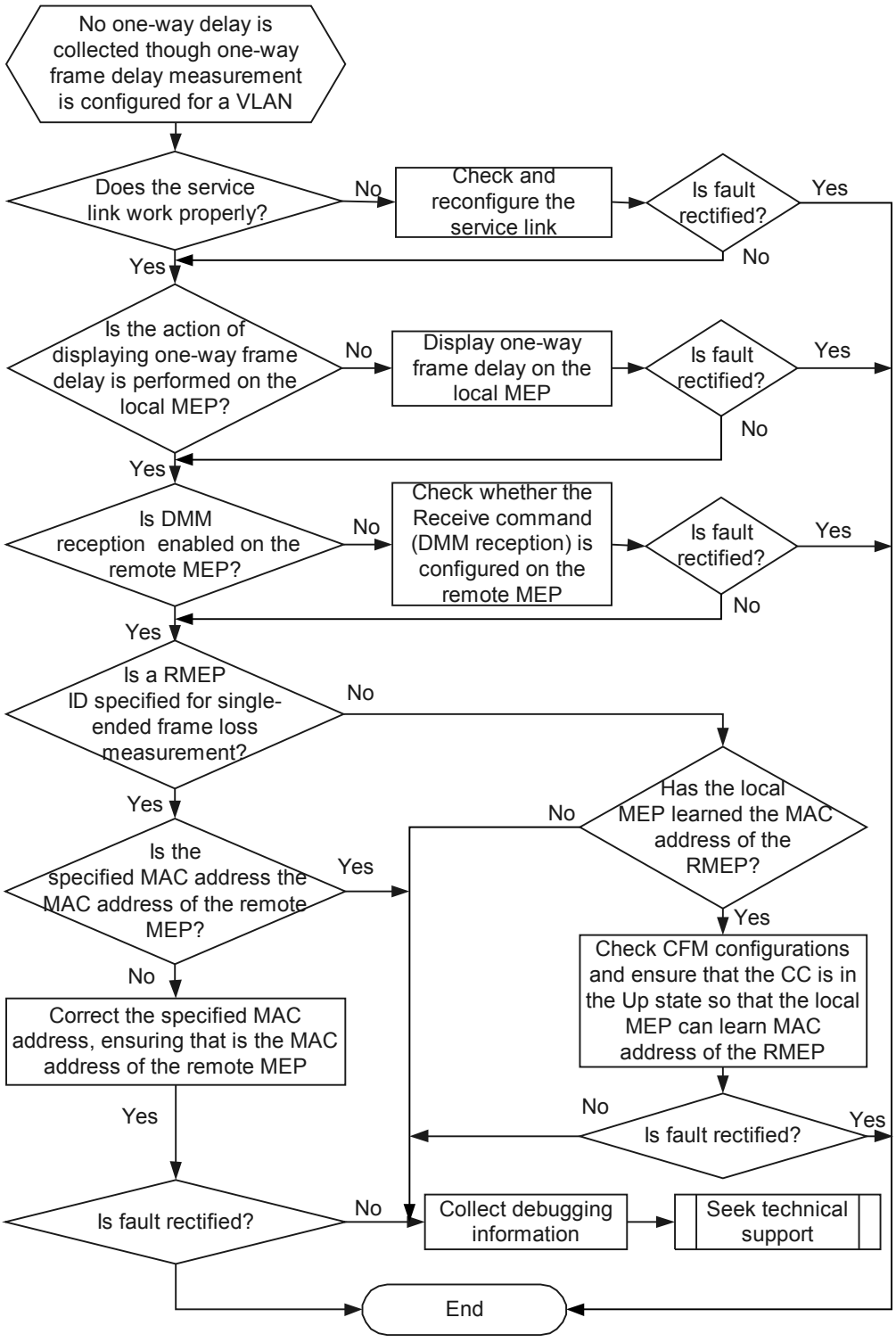
Troubleshooting Flowchart

In VLAN networking, the one-way delay is not collected though one-way frame delay measurement is configured.

Figure 9-8 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-8 Troubleshooting flowchart for the fault that the one-way delay is not collected though one-way frame delay measurement is configured for a VLAN



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the service link works properly.

Run the **display vlan** *vlan-id* **verbose** command to view the **VLAN state** field.

- If the **VLAN state** field in the command output displays **Up**, go to Step**Step 2**.
- If the **VLAN state** field in the command output does not display **Up**, check VLAN configurations. For the correct VLAN configuration, see "VLAN Configuration in the *Quidway S3700 Series Ethernet Switches Configuration Guide - Ethernet*.

Step 2 Check that the action of displaying one-way delay is performed on the remote MEP.

The one-way delay is collected only by the remote MEP that receives DMM frames but not by the initiator of one-way frame delay measurement (local MEP). If the action of displaying one-way delay is performed on the remote MEP, go to Step**Step 3**.

Step 3 Check whether the **delay-measure one-way receive** command is configured on the remote MEP.

Run the **display this** command in the MD view of the remote MEP to view configuration information.

- If the **delay-measure one-way receive** command is not configured, configure this command.
- If the **delay-measure one-way receive** command is configured, go to Step**Step 4**.

Step 4 Check the parameter specified for one-way frame delay measurement.

If **remote-mep mep-id** *mep-id* is specified, run the **display cfm remote-mep md** *md-name* **ma** *ma-name* **mep-id** *mep-id* command to view the value of the **MAC** field and check whether the local MEP has learned the MAC address of the remote MEP.

- If the **MAC** field is displayed as **-**, check CFM configurations and ensure that the CC is Up so that the local MEP can learn the MAC address of the remote MEP.
- If the **MAC** field is not displayed as **-**, go to Step**Step 5**.

If **mac** *mac-address* is specified, check whether the value of *mac-address* is the MAC address of the remote MEP.

- If the value of *mac-address* is the MAC address of the remote MEP, go to Step**Step 5**.
- If the value of *mac-address* is not the MAC address of the remote MEP, correct the specified MAC address, ensuring that it is the MAC address of the remote MEP.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures.
- Configuration files, log files, and alarm files of the device.

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

None.

9.4.2 Troubleshooting of the Fault that Two-way Delay Is Not Collected Though Two-way Frame Delay Measurement Is Configured for a VLAN

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the fault that two-way delay is not collected though two-way frame delay measurement is configured for a VLAN.

Common Causes

This fault is commonly caused in one of the following situations:

- The service link is faulty.
- The action of displaying two-way frame delay is not performed on the local MEP.
- Displaying two-way delay is not performed on the local MEP.
- The Receive command (DMM reception) is not configured on the remote MEP.
- The remote MEP ID is specified for two-way frame delay measurement but the local MEP has not learned MAC address from the remote MEP.
- The remote MAC address is specified for two-way frame delay measurement but the specified MAC address is not the MAC address of the remote MEP.

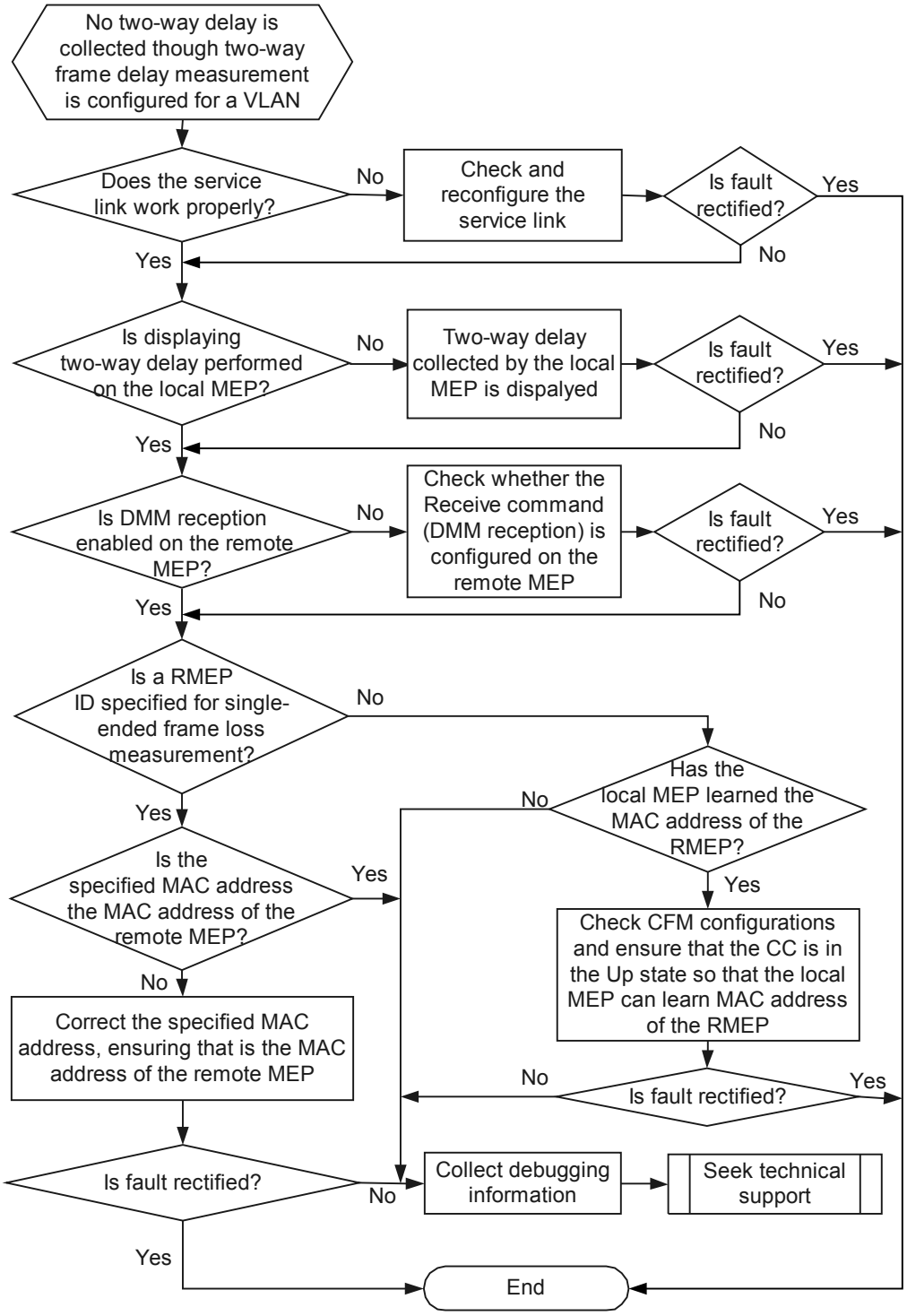
Troubleshooting Flowchart

In VLAN networking, the two-way delay is not collected though two-way frame delay measurement is configured.

Figure 9-9 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-9 Troubleshooting flowchart for the fault that the two-way delay is not collected though two-way frame delay measurement is configured for a VLAN



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that the service link works properly.

Run the **display vlan** *vlan-id* **verbose** command to view the **VLAN state** field.

- If the **VLAN state** field in the command output displays **Up**, go to Step**Step 2**.
- If the **VLAN state** field in the command output does not display **Up**, check VLAN configurations. For the correct VLAN configuration, see "VLAN Configuration in the *Quidway S3700 Series Ethernet Switches Configuration Guide - Ethernet*.

Step 2 Check that displaying two-way delay is performed on the local MEP.

The two-way delay is collected by the local MEP. If the action of displaying two-way frame delay is performed on the local MEP, go to Step**Step 3**.

Step 3 Check whether the **delay-measure two-way receive** command is configured on the remote MEP.

Run the **display this** command in the MD view of the remote MEP to view configuration information.

- If the **delay-measure two-way receive** command is not configured, configure this command.
- If the **delay-measure two-way receive** command is configured, go to Step**Step 4**.

Step 4 Check the parameter specified for two-way frame delay measurement.

If **remote-mep mep-id** *mep-id* is specified, run the **display cfm remote-mep md** *md-name* **ma** *ma-name* **mep-id** *mep-id* command to view the value of the **MAC** field and check whether the local MEP has learned the MAC address of the remote MEP.

- If the **MAC** field is displayed as **-**, check CFM configurations and ensure that the CC is Up so that the local MEP can learn the MAC address of the remote MEP.
- If the **MAC** field is not displayed as **-**, go to Step**Step 5**.

If **mac** *mac-address* is specified, check whether the value of *mac-address* is the MAC address of the remote MEP.

- If the value of *mac-address* is the MAC address of the remote MEP, go to Step**6**.
- If the value of *mac-address* is not the MAC address of the remote MEP, correct the specified MAC address, ensuring that it is the MAC address of the remote MEP.

Step 5 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedures.
- Configuration files, log files, and alarm files of the device.

----End

Copyright © Huawei Technologies Co., Ltd.

Relevant Alarms and Logs

None.

9.5 BFD Troubleshooting

This chapter describes common causes of a BFD fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

NOTE

The S3700SI does not support BFD.

9.5.1 BFD Session Cannot Go Up

Common Causes

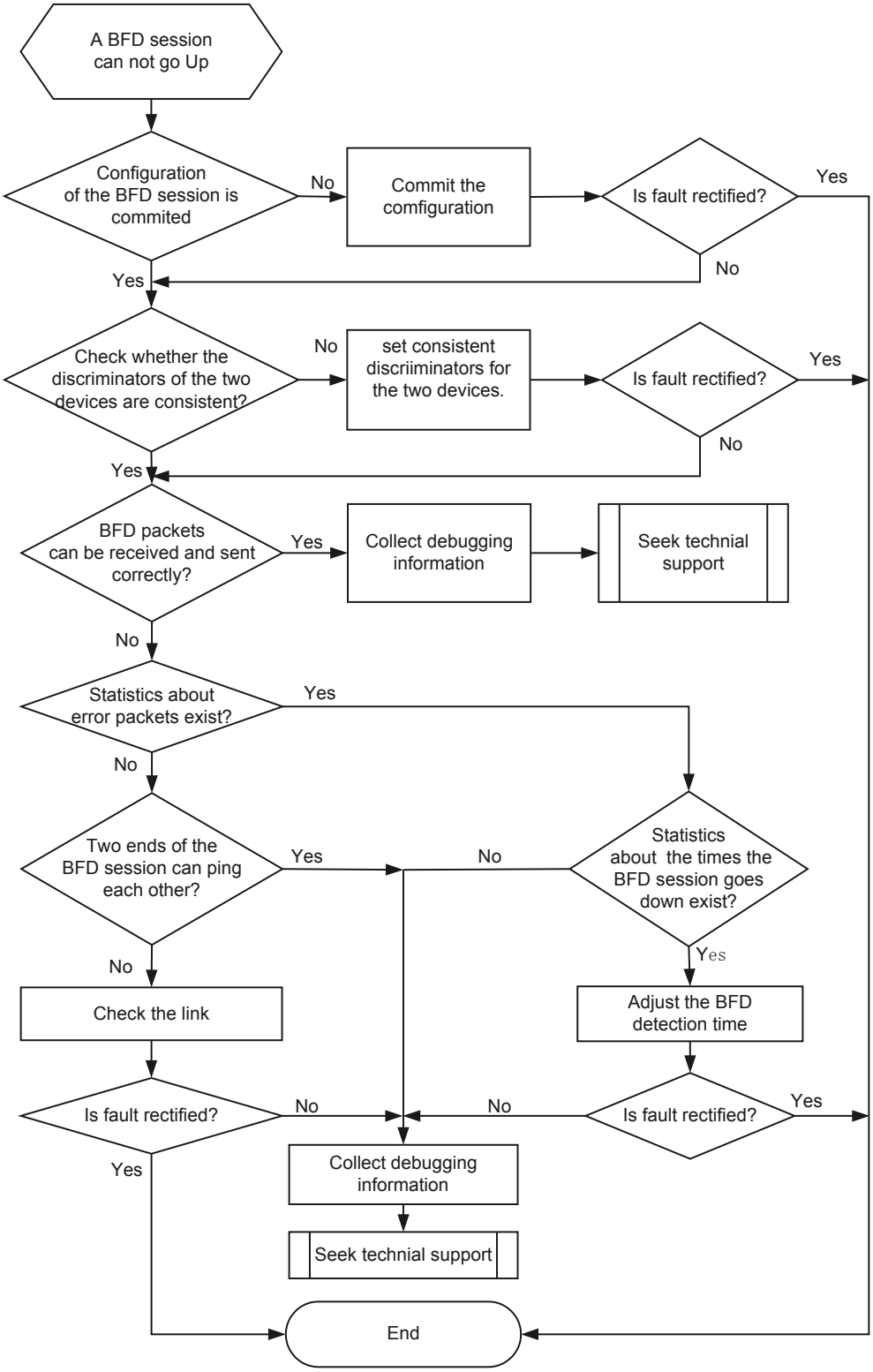
This fault is commonly caused by one of the following:

- Check whether the discriminators of the two devices are consistent.
- The link detected by the BFD session fails. As a result, BFD packets cannot be exchanged between the two ends of the BFD session.
- The BFD session status flaps.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 9-10 Troubleshooting flowchart for the fault that a BFD session cannot go Up



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display current-configuration** command to check that the configurations of the BFD session are committed.

- If the **commit** command is displayed, it indicates that the configurations of the BFD session have been committed. Then, go to **Step 2**.
- If the **commit** command is not displayed, it indicates that the configurations of the BFD session have not been committed. In this case, run the **commit** command to make the configurations take effect. After doing so, run the **display bfd session all** command to check the **State** field.
  - If **Up** is displayed, it indicates that the BFD session is successfully established.
  - If **Up** is not displayed, go to **Step 2**.

Step 2 Run the **display current-configuration** command to check whether the discriminators of the two devices are consistent.

- If they are inconsistent, run the **undo bfd** command to delete the existing bfd session, and then run the **bfd bind peer-ip** command to create a new bfd session. At last run the **discriminator** { **local** *discr-value* | **remote** *discr-value* } command to configure the local and remote discriminators. Ensure that the local discriminator on the local end is the same as the remote discriminator on the remote end and the remote discriminator on the local end is the same as the local discriminator on the remote end. Then, go to**Step 3**.
- If they are consistent, go to **Step 4**.

Step 3 Run the **display bfd session all** command to check the **State** field.

- If **Up** is displayed, it indicates that the BFD session is successfully established.
- If **Up** is not displayed, go to **Step 4**.

Step 4 Run the **display bfd statistics session all** command several times to check statistics about the BFD packets of the BFD session.

- If the value of the **Received Packets** field does not increase, go to **Step 5**.
- If the value of the **Send Packets** field does not increase, go to **Step 6**.
- If the values of **Received Packets** and **Send Packets** fields increase, go to **Step 9**.
- If none of the values of the **Received Packets**, **Send Packets**, **Received Bad Packets**, and **Send Bad Packets** fields increase, go to **Step 7**.
- If the value of the **Down Count** field increases, it indicates that the BFD session flaps. Then, go to **Step 7**.

Step 5 Run the **display bfd statistics session all** command several times to check the **Received Bad Packets** field.

Copyright © Huawei Technologies Co., Ltd.

- If the value of this field increases, it indicates that the BFD packets have been received and discarded. Then, go to **Step 9**.
- If the value of this field does not increase, it indicates that the BFD packets have not been received. Then, go to **Step 7**.

Step 6 Run the **display bfd statistics session all** command several times to check the **Send Bad Packets** field.

- If the value of this field increases, it indicates that the BFD packets sent by the BFD session have been discarded. Then, go to **Step 9**.
- If the value of this field does not increase, it indicates that the BFD packets failed to be sent. Then, go to **Step 7**.

Step 7 Run the **display bfd statistics session all** command several times. If the BFD session still does not go Up, run the **ping** command on one end to ping the other end of the BFD session.

- If the ping fails, it indicates that the link fails. See the section The Ping Operation Fails to rectify the fault on the link.
- If the ping is successful, view the configurations on the related interfaces.

  NOTE

  BFD packets are transmitted in the default VLAN. Before a BFD session is established on an interface, configure the interface to allow packets of the default VLAN to pass through.

  - If the configurations on the interface are incorrect, correct the configurations.
  - If the configurations on the interface are correct, go to **Step 8**.

Step 8 Run the **display current-configuration** command to view the **min-tx-interval** and **min-rx-interval** fields to check that the BFD detection period is longer than the delay on the link.

- If the BFD detection period is shorter than the delay on the link, run the **detect-multiplier**, **min-rx-interval**, and **min-tx-interval** commands to adjust the values to make the BFD detection timer longer than the delay on the link.
- If the BFD detection time is longer than the delay time on the link, go to **Step 9**.

Step 9 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure.
- Configuration files, log files, and alarm files of the devices.

----End

Relevant Alarms and Logs

Relevant Alarms

- BFD_1.3.6.1.4.1.2011.5.25.38.3.1 hwBfdSessDown
- BFD_1.3.6.1.4.1.2011.5.25.38.3.2 hwBfdSessUp

Relevant Logs

- BFD/4/STACHG_TODWN
- BFD/4/STACHG_TOUP

Copyright © Huawei Technologies Co., Ltd.

9.5.2 Interface Forwarding Is Interrupted After a BFD Session Detects a Fault and Goes Down

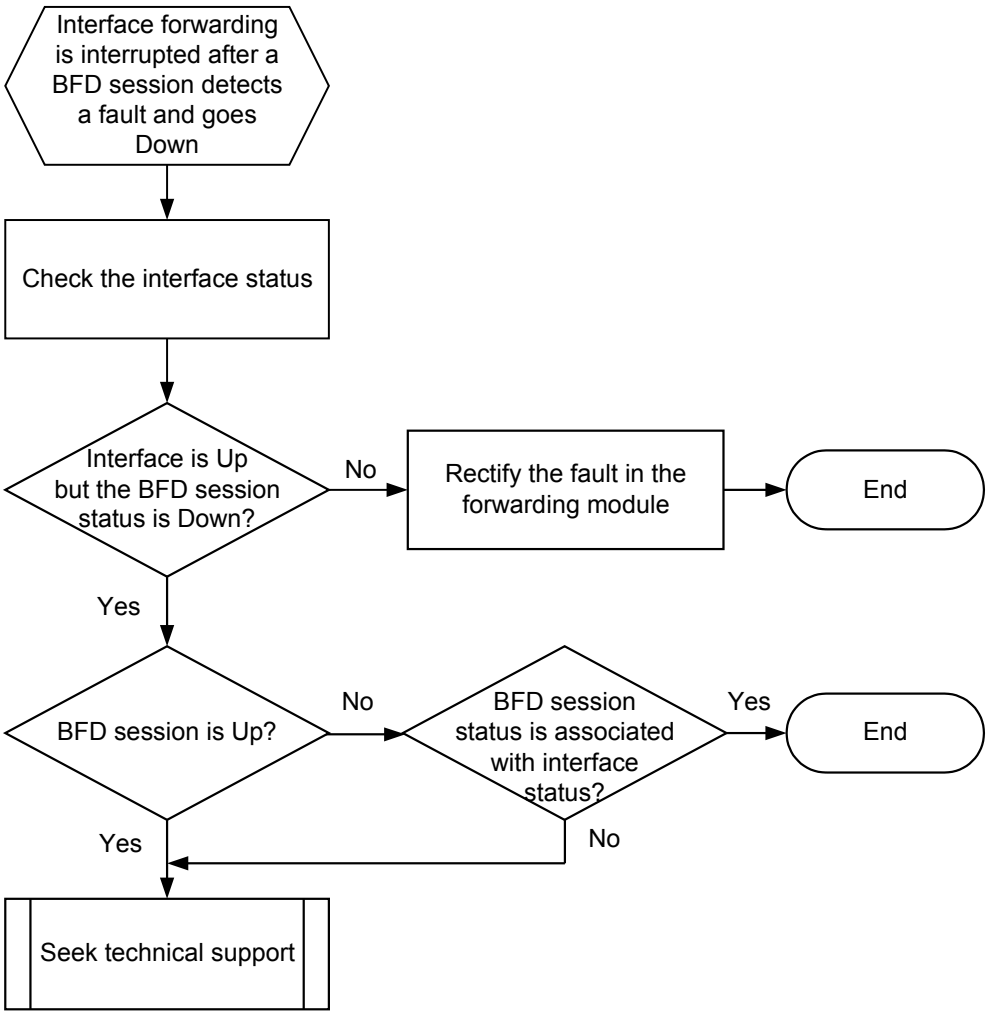
Common Causes

This fault is commonly caused by the following:

- The BFD session status is associated with the interface status.

Troubleshooting Flowchart

Figure 9-11 Troubleshooting flowchart for the fault that the interface forwarding is interrupted after a BFD session detects a fault and goes Down



Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display interface** *interface-type interface-number* command to check the status of the interface to which the BFD session is bound.

- If the **Line protocol current state** field displays **DOWN(BFD status down)**, it indicates that the interface status is set to **BFD status down** after the BFD session detects a link fault. Then, go to **Step 2**.
- If the **Line protocol current state** field displays **UP** but the interface cannot forward packets, it indicates that the forwarding module is faulty. See the section The Ping Operation Fails to rectify the forwarding fault.

Step 2 Run the **display bfd session all** command to check the status of the BFD session.

- If the BFD session is **Down**, go to **Step 3**.
- If the BFD session is **Up**, go to **Step 4**.

Step 3 Run the **display current-configuration configuration bfd-session** command to check that the **process-interface-status** command is configured.

- If the **process-interface-status** command is configured, it indicates that the interface is set to **DOWN(BFD status down)** because the BFD session detects a fault and goes Down.
- If the **process-interface-status** command is not configured, go to **Step 4**.

Step 4 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure.
- Configuration files, log files, and alarm files of the devices.

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

9.5.3 Changed BFD Session Parameters Do Not Take Effect

Copyright © Huawei Technologies Co., Ltd.

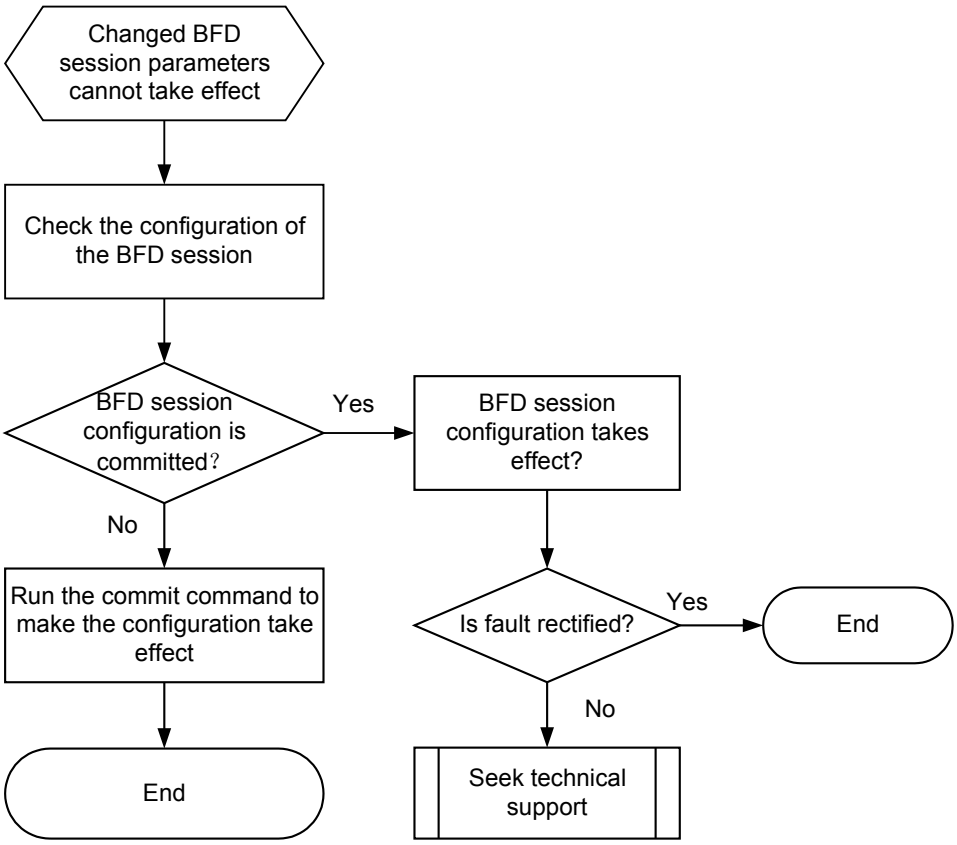
Common Causes

This fault is commonly caused by the following:

- After parameters of a BFD session have been changed, changed configurations are not committed.

TroubleshootingFlowchart

Figure 9-12 Troubleshooting flowchart for the fault that the changed BFD session parameters do not take effect



Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display current-configuration configuration bfd** command to check that the **commit** command is configured.

Copyright © Huawei Technologies Co., Ltd.

- If the **commit** command is configured, the changed BFD session parameters have been committed. Then, go to **Step 3**.
- If the **commit** command is not configured, the changed BFD session parameters have not been committed. Then, run the **commit** command, and then go to **Step 2**.

Step 2 Run the **display bfd session all** command check whether the BFD session parameters are specified values.

- If yes, the modified parameters take effect.
- If no, go to **Step 3**.

Step 3 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure.
- Configuration files, log files, and alarm files of the devices.

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

9.5.4 Dynamic BFD Session Fails to Be Created

Common Causes

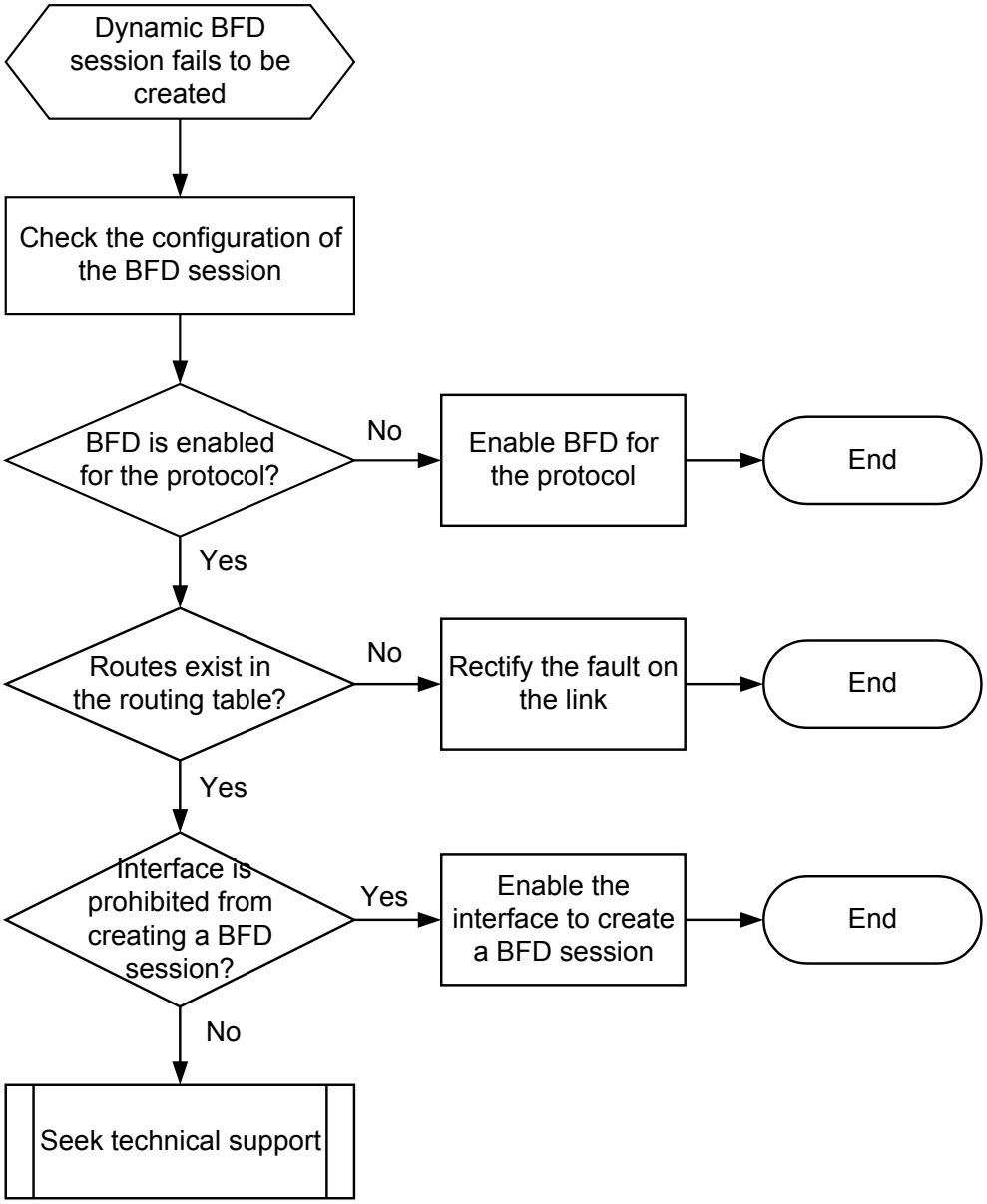
This fault is commonly caused by one of the following:

- BFD is not enabled for the protocol.
- The route to the peer of the BFD session does not exist in the routing table.
- The dynamic BFD session is not supported on the interface.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting Flowchart

Figure 9-13 Troubleshooting flowchart for the fault that a dynamic BFD session fails to be created



Troubleshooting Procedure

Context

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **display current-configuration configuration bfd** command to check that BFD is enabled for a specified protocol.

- If BFD is not enabled for the specified protocol, enable BFD. Then, go to **Step 2**.
- If BFD is enabled, go to **Step 3**.

Step 2 Run the **display bfd session all** command to view the **state** field.

- If the **state** field in the command output displays **Up**, it indicates that the BFD section to be created.
- If the **state** field in the command output displays not **Up**, go to **step 3**.

Step 3 Run the **display ip routing-table** command to check whether the route of the link detected by the BFD session exists.

- If the route exists, go to **step 4**.
- If the route does not exist, it indicates that the BFD session associated with the protocol fails to be created. see the section The Ping Operation Fails.

Step 4 Run the **interface***interface-typeinterface-number* command to enter the view of the existing interface,then run the **display this** command to check that a command is configured to disable an interface to dynamically create a BFD session.

- If there is, Run the **undo ospf bfd block**command to enable the interface to dynamically create a BFD session. Then, run the **display bfd session all** command to check whether the BFD session is Up. If not, go to **step 5**.
- If there is not, go to **step 5**.

Step 5 If the fault persists, collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure.
- Configuration files, log files, and alarm files of the devices.

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.

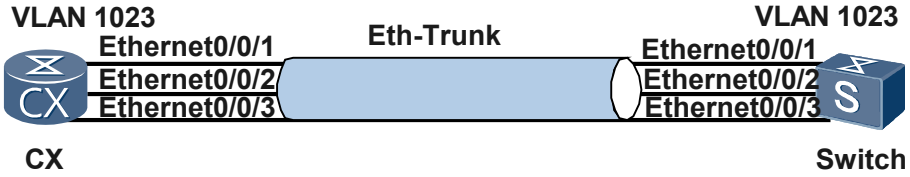
9.5.5 Trouble Cases

BFD Session Is Down Because the Interface Does Not Allow Packets from the Default VLAN to Pass Through

Fault Symptom

As shown in **Figure 9-14**, the Eth-Trunk between the CX600 and the Switch is bound to static BFD. After the configuration, the BFD session becomes Down.

Figure 9-14 Network diagram



Fault Analysis

1. Run the **display current-configuration configuration bfd-session** command on the Switch to check whether the BFD session configuration is committed. If the **commit** field is displayed, the BFD session configuration is committed.
2. Run the **ping** command on the Switch to check whether the network is reachable. The ping operation succeeds, indicating that the network is reachable.
3. Run the **display current-configuration interface** *interface-type interface-number* command on the Switch to check the interface configuration.

```
#
interface Eth-Trunk1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 1023
#
```

The preceding information indicates that the interface allows only packets from VLAN 1023 to pass through. On the Switch, BFD packets are transmitted in the default VLAN (that is, VLAN 1), so the BFD session cannot be established.

Procedure

Step 1 Modify the configuration or the PVID of the interface to allow BFD packets from VLAN 1 to pass through.

1. Modify the configuration of the interface so that BFD packets from VLAN 1 can pass through.
   a. Run the **system-view** command on the Switch to enter the system view.
   b. Run the **interface** *interface-type interface-number* command to enter the Eth-Trunk interface view.

Copyright © Huawei Technologies Co., Ltd.

c. Run the **port trunk allow-pass vlan 1** command to configure the interface to allow packets from VLAN 1 to pass through.

2. Change the PVID of the interface.

a. Run the **system-view** command on the Switch to enter the system view.

b. Run the **interface** *interface-type interface-number* command to enter the Eth-Trunk interface view.

c. Run the **port trunk pvid vlan** *vlan-id* command to configure the default VLAN of the interface.

d. Run the **port trunk allow-pass vlan** *vlan-id* command to configure the interface to allow packets from the default VLAN to pass through.

After the preceding operations are complete, the BFD session status on the Switch is checked. The BFD session is established successfully. The fault is rectified.

----End

Summary

BFD packets are transmitted in the default VLAN. Before a BFD session is established on an interface, configure the interface to allow packets of the default VLAN to pass through.

If the BFD session configuration is not committed or the configurations at two ends of the session are different, the BFD session may be Down. Check the configuration to locate faults.

9.6 DLDP Troubleshooting

This chapter describes common causes of a DLDP fault, and provides the corresponding troubleshooting flowchart, troubleshooting procedure, alarms, and logs.

9.6.1 DLDP Fails to Detect a Directly Connected Neighbor

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for a failure to detect a directly connected neighbor.

Common Causes

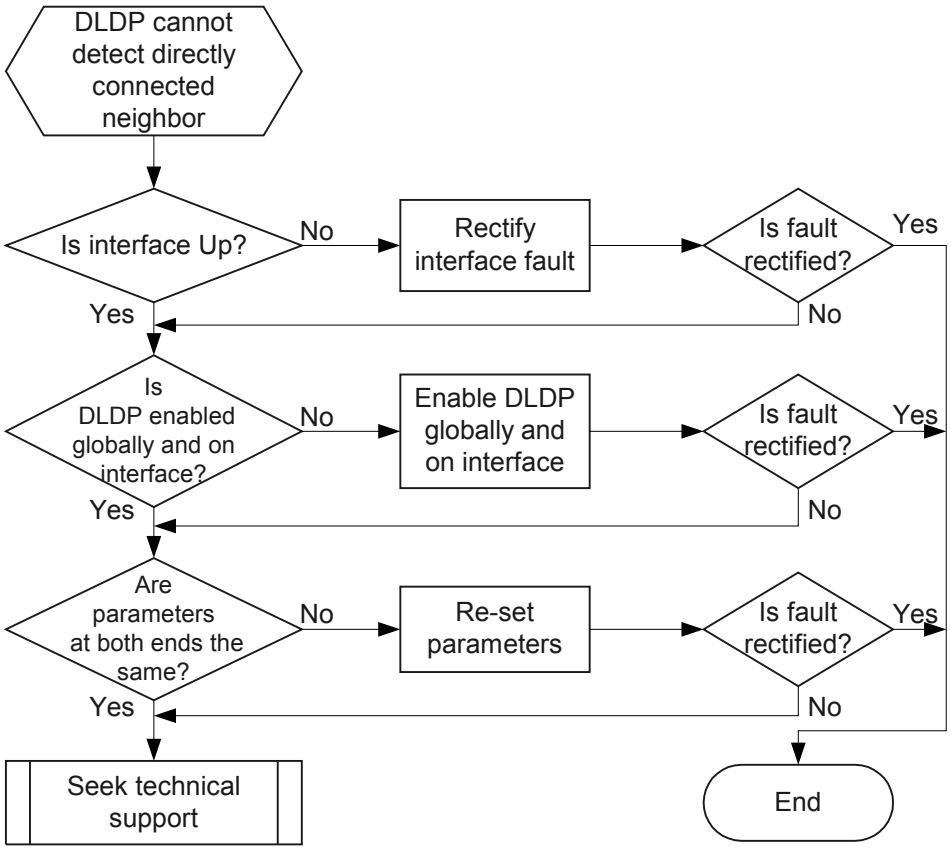
This fault is commonly caused by one of the following:

- The link is faulty.
- The DLDP function is disabled on the remote end.
- DLDP parameters on the local device and the neighbor are different.

Troubleshooting Flowchart

Copyright © Huawei Technologies Co., Ltd.

Figure 9-15 DLDP troubleshooting flowchart



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check whether the interface that cannot detect a neighbor is Up.

Run the **display interface** *interface-type interface-name* command to view the **current state** field.

- If the interface is Down, rectify the fault according to **Connected Ethernet Interfaces Down**.
- If the interface is Up, go to step 2.

Step 2 Check that DLDP is enabled.

Run the **display dldp** command to check whether DLDP is enabled globally, that is, view the **DLDP global status** field. Run the **display this** command in the interface view. If the output information contains the **dldp enable** field, DLDP is enabled on the interface. If the output information does not contain the **dldp enable** field, the interface works in auto-negotiation mode.

Copyright © Huawei Technologies Co., Ltd.

- If DLDP is not enabled globally or on an interface, run the **dldp enable** command in the corresponding view to enable DLDP.
- If DLDP is enabled, go to step 3.

Step 3 Check whether DLDP parameters at both ends are the same.

Run the **display dldp** command to view the information in the following table.

Field	Method
DLDP interval	Check whether the intervals for sending DLDP packets at both ends are the same. If the intervals for sending DLDP packets at both ends are different, run the **dldp interval** *interval-value* command in the system view on both devices to set the same interval on both devices.
DLDP authentication-mode	Check whether authentication modes and passwords at both ends are the same. If the two devices use different authentication modes or passwords, run the **dldp authentication-mode** { **md5** *cipher-value* | **none** | **simple** *cipher-value* } command in the system view to set the same authentication mode and password on both devices.

If the fault persists, go to step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, log file, and alarm file of the S3700

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

9.7 RRPP Troubleshooting

9.7.1 RRPP Loop Occurs Temporarily

Common Causes

After RRPP is configured on a device, a loop occurs temporarily.

This fault is commonly caused by one of the following:

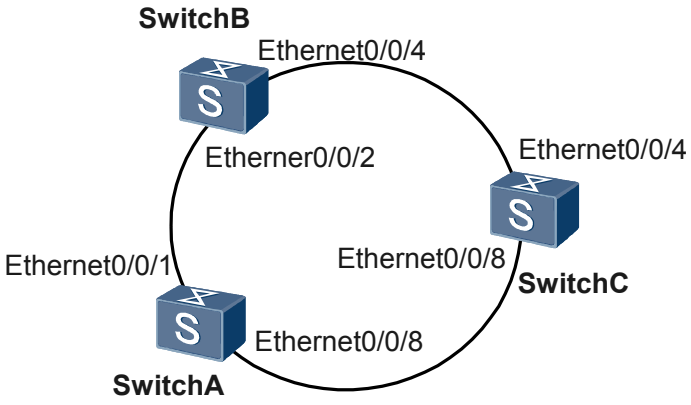
Copyright © Huawei Technologies Co., Ltd.

- The configuration is incorrect.
- Values of the Failtime timers configured for nodes along the RRPP ring are different.

Troubleshooting Flowchart

Temporary RRPP loop troubleshooting is based on the network shown in **Figure 9-16**.

Figure 9-16 Networking diagram of RRPP



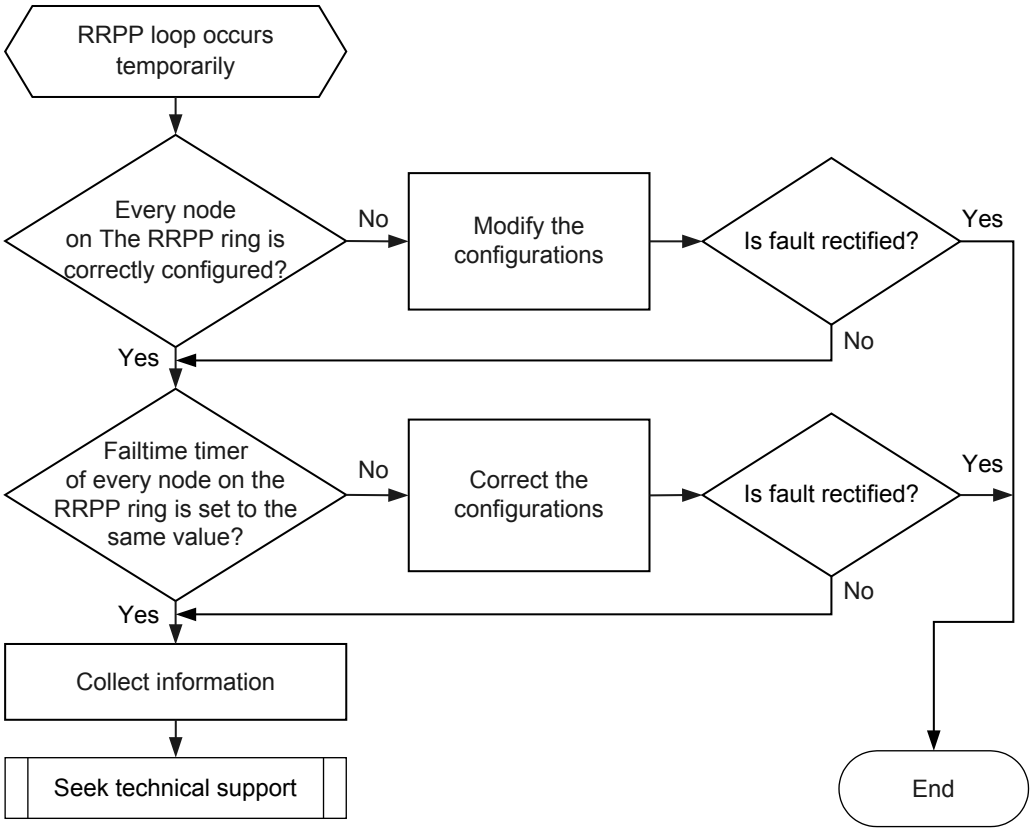
The troubleshooting roadmap is as follows:

- Check that every node on the RRPP ring is correctly configured.
- Check that the Failtime timer of every node on the RRPP ring is set to the same value.

Figure 9-17 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-17 Troubleshooting flowchart for the fault that an RRPP loop occurs temporarily



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Check that every node on the RRPP ring is correctly configured.

Run the **display this** command in the RRPP view of each node on the RRPP ring to view RRPP configurations.

```
[RouterA-rrpp-domain-region1] display this
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 0
 timer hello-timer 1 fail-timer 3
 ring 1 node-mode master primary-port Ethernet0/0/2 secondary-port Ethernet0/0/4
level 0
 ring 1 enable
#
return
```

Check whether all nodes on the RRPP ring belong to the same domain, whether the nodes are configured with the same control VLAN ID and instance number, and whether the RRPP ring has only one master node.

Copyright © Huawei Technologies Co., Ltd.

- If all configurations are correct, go to **Step 2**.
- If any of the preceding configurations is incorrect, RRPP configurations may be incorrect. For correct configurations, see the chapter "RRPP Configuration" in the *S3700 Configuration Guide - LAN Access and MAN Access*.

Step 2 Check that the Failtime timer of every node on the RRPP ring is set to the same value.

Run the **display rrpp verbose domain** *domain-id* command in any view to check detailed RRPP configurations.

```
[RouterA-rrpp-domain-region1] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 20    sub 21
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)
RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                        Is Active : Yes
Primary port  : Ethernet0/0/1         Port status: UP
Secondary port: Ethernet0/0/2         Port status: BLOCKED
```

- If the Failtime timers of the nodes on the RRPP ring are set to different values, correct the configurations according to the chapter "RRPP Configuration" in the *S3700 Configuration Guide - Reliability*.
- If the Failtime timer of every node on the RRPP ring is set to the same value, go to **Step 3**.

Step 3 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration files, log files, and alarm files of the device

----End

Relevant Alarms and Logs

Relevant Alarms

RRPP_1.3.6.1.4.1.2011.5.25.113.4.2 hwRrppRingFail

Relevant Logs

RRPP/3/FAIL

RRPP/5/PBLK

RRPP/5/RESTORE

9.8 SEP Troubleshooting

This chapter describes common causes of SEP faults, and provides the corresponding troubleshooting flowcharts, troubleshooting procedures, alarms, and logs.

Copyright © Huawei Technologies Co., Ltd.

9.8.1 Traffic Forwarding Fails on a SEP Link

This section describes the troubleshooting flowchart and provides a step-by-step troubleshooting procedure for the fault that traffic forwarding fails on a SEP link.

Possible Causes

After SEP is configured on a ring network, traffic cannot be forwarded normally.

The possible causes are:

- The SEP configuration is incorrect.
- The corresponding port is not added to the data VLANs.
- The physical port fails.

Troubleshooting Flowchart

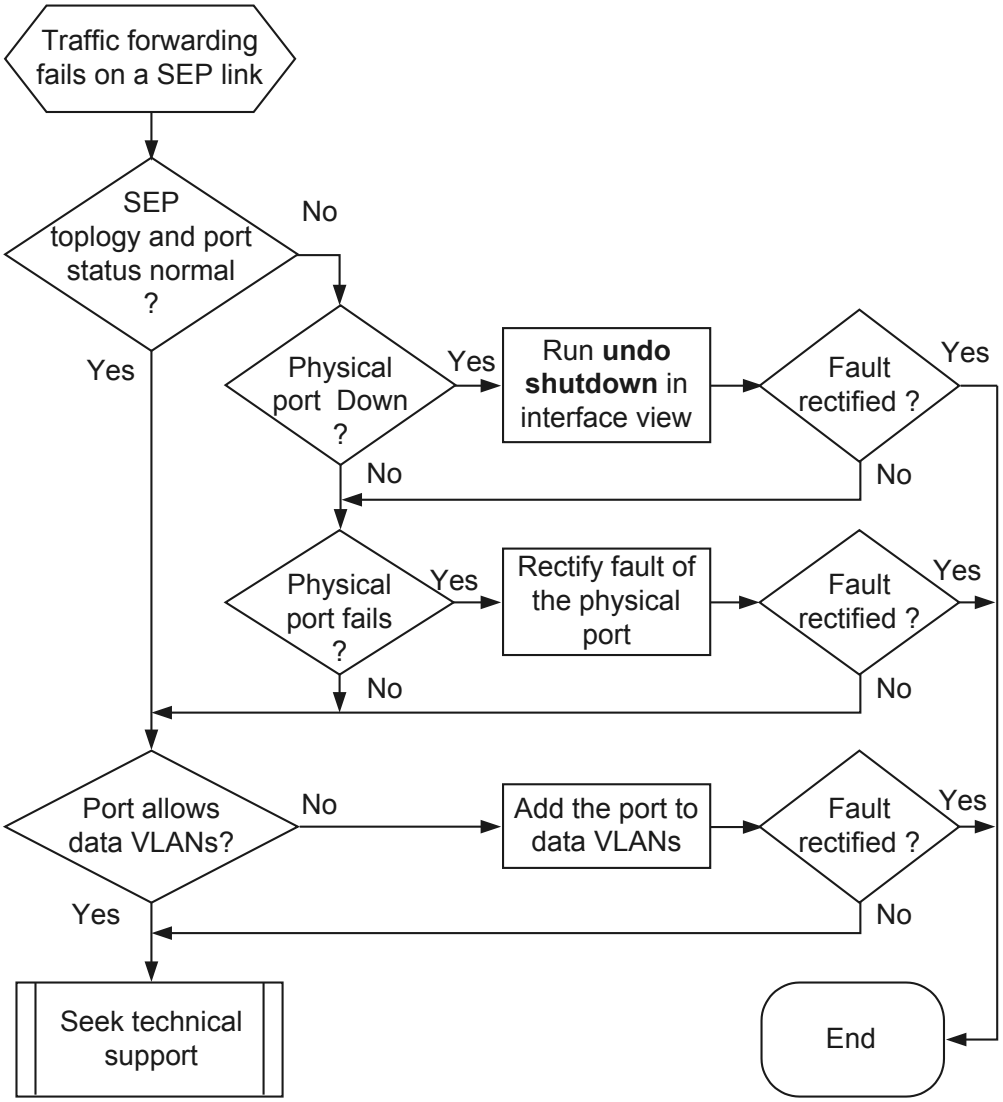
The troubleshooting roadmap is as follows:

- Check whether the SEP topology and SEP port status are normal.
- Check whether the ports on the ring network are added to the data VLANs.
- Check whether any physical port on the ring network is in Down state.
- Check whether any fault occurs on the physical ports.

Figure 9-18 shows the troubleshooting flowchart.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-18 Flowchart for troubleshooting forwarding failure on a SEP link



Troubleshooting Procedure

NOTE

Save the result of every step and report the information to Huawei technical personnel if the fault cannot be rectified.

Procedure

Step 1 Check whether the SEP topology and SEP port status are normal.

Normally, a SEP segment contains a primary edge port, a secondary edge port, and some common ports.

Run the **display sep topology** [**segment** *segment-id*] [**verbose**] command to check the topology information of a SEP segment.

```
<Quidway> display sep topology
SEP segment 1
```


Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------
System Name      Port Name           Port Role       Port Status
--------------------------------------------------------------
LSW1             Ethernet0/0/1       primary         forwarding
LSW2             Ethernet0/0/1       common          forwarding
LSW2             Ethernet0/0/2       common          forwarding
LSW3             Ethernet0/0/0       common          forwarding
LSW3             Ethernet0/0/2       common          discarding
LSW4             Ethernet0/0/1       common          forwarding
LSW4             Ethernet0/0/2       common          forwarding
LSW5             Ethernet0/0/1       common          forwarding
LSW5             Ethernet0/0/3       common          forwarding
LSW1             Ethernet0/0/3       secondary       forwarding
```

- If the SEP topology or the port status is abnormal:
  - Check whether the SEP configuration is correct. For the correct SEP configuration, see "SEP Configuration" in the *Quidway S3700 Series Ethernet Switches Configuration Guide - Ethernet*. If the SEP configuration is incorrect, modify the configuration.
  - If the SEP configuration is correct, go to **Step 2**.
- If the STP topology and port status are normal, go to **Step 4**.

Step 2 Check the status of interfaces on the SEP segment.

Run the **display interface** command in any view to check the interface status.

```
<Quidway> display interface Ethernet 0/0/1
Ethernet0/0/1 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, Quidway Series, Ethernet0/0/1 Interface
Switch Port, PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 1600
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 000b-0918-8bc1
Port Mode: COMMON COPPER
Speed :   10,  Loopback: NONE
Duplex: HALF,  Negotiation: ENABLE
Mdi   : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: -
Output peak rate 0 bits/sec, Record time: -
Input:  0 packets, 0 bytes
Unicast        :                  0, Multicast          :                  0
Broadcast      :                  0, Jumbo              :                  0
CRC            :                  0, Giants             :                  0
Jabbers        :                  0, Fragments          :                  0
Runts          :                  0, DropEvents         :                  0
Alignments     :                  0, Symbols            :                  0
Ignoreds       :                  0, Frames             :                  0
Discard        :                  0, Total Error        :                  0
Output:  0 packets, 0 bytes
Unicast        :                  0, Multicast          :                  0
Broadcast      :                  0, Jumbo              :                  0
Collisions     :                  0, Deferreds          :                  0
Late Collisions:                  0, ExcessiveCollisions:                  0
Buffers Purged :                  0
Discard        :                  0, Total Error        :                  0
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

- If an interface is in Down state, run the **display this** command in the corresponding interface view to check whether the interface is shut down.
  - If the interface is shut down, run the **undo shutdown** command in the interface view.
  - If not, go to **Step 3**.

Copyright © Huawei Technologies Co., Ltd.

- If the interface status is Up, go to **Step 4**.

Step 3 Check whether any fault occurs on the physical port.

- If a fault occurs on the physical port, see the section**4.1.1 Connected Ethernet Interfaces Down** to rectify the fault.
- If the physical port is normal, go to **Step 4**.

Step 4 Check whether the ports on the SEP segment are added to the data VLANs.

Run the **display this** command in the interface view to check whether an interface allows specified data VLANs.

```
[Quidway] interface ethernet 0/0/1
[Quidway-Ethernet0/0/1] display this
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1 edge primary
#
return
```

- If the interface does not allow the specified data VLANs, add the interface to the VLANs.
- If the interface allows the specified data VLANs, go to **Step 5**.

Step 5 Collect the following information and contact Huawei technical personnel.

- The results of the preceding steps.
- Configuration files, logs, and alarms of the devices.

----End

Relevant Alarms and Logs

Relevant Alarms

None.

Relevant Logs

None.

Copyright © Huawei Technologies Co., Ltd.