

**Quidway S9300 Terabit Routing Switch  
V100R003C01**

**Troubleshooting - IP Routing**

**Issue      01**  
**Date        2010-12-15**



**Copyright © Huawei Technologies Co., Ltd. 2010. 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**



HUAWEI 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](mailto:support@huawei.com)



# About This Document

## Intended Audience

This document describes how to troubleshoot the services of the S9300 in terms of common faults and causes, troubleshooting cases, and FAQs.






This document describes the procedure and method for troubleshooting for the S9300.

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

## Command Conventions

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

Convention	Description
<b>Boldface</b>	The keywords of a command line are in <b>boldface</b> .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[ ]	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 (2010-12-15)

Initial commercial release.

---

# Contents

---

<b>About This Document.....</b>	<b>iii</b>
<b>1 RIP Troubleshooting.....</b>	<b>1-1</b>
1.1 RIP Overview.....	1-2
1.2 RIP Route Receiving Troubleshooting.....	1-2
1.2.1 Typical Networking.....	1-2
1.2.2 Configuration Notes.....	1-3
1.2.3 Troubleshooting Flowchart.....	1-4
1.2.4 Troubleshooting Procedure.....	1-5
1.3 RIP Route Sending Troubleshooting.....	1-7
1.3.1 Typical Networking.....	1-7
1.3.2 Configuration Notes.....	1-7
1.3.3 Troubleshooting Flowchart.....	1-7
1.3.4 Troubleshooting Procedure.....	1-8
1.4 Troubleshooting Cases.....	1-10
1.4.1 Discontinuous Subnet Fault.....	1-10
1.5 FAQs.....	1-12
1.6 Diagnostic Tools.....	1-14
1.6.1 display Commands.....	1-14
1.6.2 debugging Commands.....	1-14
<b>2 OSPF Troubleshooting.....</b>	<b>2-1</b>
2.1 OSPF Overview.....	2-2
2.1.1 Introduction to OSPF.....	2-2
2.1.2 Basic Concepts.....	2-2
2.2 OSPF Neighbor Troubleshooting.....	2-4
2.2.1 Typical Networking.....	2-4
2.2.2 Configuration Notes.....	2-4
2.2.3 Troubleshooting Flowchart.....	2-6
2.2.4 Troubleshooting Procedure.....	2-8
2.3 OSPF VPN Troubleshooting.....	2-9
2.3.1 Typical Networking.....	2-9
2.3.2 Configuration Notes.....	2-10
2.3.3 Troubleshooting Flowchart.....	2-11

2.3.4 Troubleshooting Procedure.....	2-12
2.4 Troubleshooting Cases.....	2-13
2.4.1 Routers Cannot Learn the Internal Route After the Vlink is Configured.....	2-14
2.4.2 Routing Loops Occur When a CE Is Dual-homed to Two PEs, and the OSPF Multi-instance Is Configured on the PEs.....	2-15
2.4.3 In Inter-AS VPN Option A, ASBRs Fail to Exchange Routes.....	2-17
2.5 FAQs.....	2-19
2.6 Diagnostic Tools.....	2-26
2.6.1 display Commands.....	2-26
2.6.2 debugging Commands.....	2-27
<b>3 IS-IS Troubleshooting.....</b>	<b>3-1</b>
3.1 IS-IS Overview.....	3-2
3.1.1 Basic Concepts of IS-IS.....	3-2
3.1.2 IS-IS Features Supported by the S9300.....	3-2
3.2 IS-IS Neighbor Troubleshooting.....	3-5
3.2.1 Typical Networking.....	3-5
3.2.2 Configuration Notes.....	3-6
3.2.3 Troubleshooting Flowchart.....	3-7
3.2.4 Troubleshooting Procedure.....	3-8
3.3 IS-IS Routing Table Troubleshooting.....	3-10
3.3.1 Typical Networking.....	3-10
3.3.2 Configuration Notes.....	3-10
3.3.3 Troubleshooting Flowchart.....	3-11
3.3.4 Troubleshooting Procedure.....	3-13
3.4 IS-IS Interface Troubleshooting.....	3-14
3.4.1 Typical Networking.....	3-14
3.4.2 Configuration Notes.....	3-14
3.4.3 Troubleshooting Flowchart.....	3-15
3.4.4 Troubleshooting Procedure.....	3-16
3.5 IS-IS MT Troubleshooting.....	3-16
3.5.1 Typical Networking.....	3-16
3.5.2 Configuration Notes.....	3-17
3.5.3 Troubleshooting Flowchart.....	3-18
3.5.4 Troubleshooting Procedure.....	3-19
3.6 FAQs.....	3-20
3.7 Diagnostic Tools.....	3-26
3.7.1 display Commands.....	3-26
3.7.2 debugging Commands.....	3-27
<b>4 BGP Troubleshooting.....</b>	<b>4-1</b>
4.1 BGP Overview.....	4-2
4.1.1 Introduction to BGP.....	4-2
4.1.2 BGP Routing Attributes.....	4-2



4.1.3 BGP Policy.....	4-3
4.2 BGP Connection Troubleshooting.....	4-4
4.2.1 Typical Networking.....	4-5
4.2.2 Configuration Notes.....	4-5
4.2.3 Troubleshooting Flowchart.....	4-8
4.2.4 Troubleshooting Procedure.....	4-9
4.3 Accidental Interruption of BGP Connection Troubleshooting.....	4-11
4.3.1 Typical Networking.....	4-12
4.3.2 Configuration Notes.....	4-12
4.3.3 Troubleshooting Flowchart.....	4-12
4.3.4 Troubleshooting Procedure.....	4-12
4.4 Route Loss Troubleshooting When BGP Exchange Update Messages.....	4-15
4.4.1 Typical Networking.....	4-15
4.4.2 Configuration Notes.....	4-15
4.4.3 Troubleshooting Flowchart.....	4-15
4.4.4 Troubleshooting Procedure.....	4-16
4.5 Troubleshooting Cases.....	4-18
4.5.1 Routing Loop and Route Flapping.....	4-18
4.5.2 Peer Connection Is Closed but the Number of Routes Does not Exceeds the Limit.....	4-20
4.6 FAQs.....	4-23
4.7 Diagnostic Tools.....	4-27
4.7.1 display Commands.....	4-27
4.7.2 debugging Commands.....	4-28
<b>5 Routing Policy Troubleshooting.....</b>	<b>5-1</b>
5.1 Routing Policy and Filter Overview.....	5-2
5.1.1 Routing Policy.....	5-2
5.1.2 IP-Prefix List.....	5-2
5.1.3 AS-Path-Filter.....	5-3
5.1.4 Community-Filter.....	5-3
5.1.5 Extcommunity-Filter.....	5-3
5.1.6 Route-Policy.....	5-3
5.2 Troubleshooting the Routing Policy.....	5-3
5.2.1 Typical Networking.....	5-4
5.2.2 Configuration Notes.....	5-5
5.2.3 Troubleshooting Flowchart.....	5-11
5.2.4 Troubleshooting Procedure.....	5-13
5.3 Troubleshooting Cases.....	5-14
5.3.1 Routes Are Lost After IP-Prefix Is Used.....	5-14
5.3.2 Routes Are Lost After AS-Path Is Used.....	5-15
5.3.3 Routes Are Not Filtered Correctly After Community-Filter Is Used.....	5-18
5.3.4 Routes Are Not Filtered Correctly After Extcommunity-Filter Is Used.....	5-18
5.3.5 Routes Are Not Correctly Filtered After Route-Policy Is Used.....	5-20

5.4 FAQs.....	5-22
5.5 Diagnostic Tools.....	5-23
5.5.1 display Commands.....	5-23
5.5.2 debugging Commands.....	5-24

---

# Figures

---

<b>Figure 1-1</b> Typical networking of RIP.....	1-2
<b>Figure 1-2</b> RIP route receiving troubleshooting flowchart.....	1-5
<b>Figure 1-3</b> RIP route sending troubleshooting flowchart.....	1-8
<b>Figure 1-4</b> Networking diagram of RIP.....	1-10
<b>Figure 2-1</b> OSPF typical networking.....	2-4
<b>Figure 2-2</b> Troubleshooting flowchart of the establishment failure of the OSPF adjacency.....	2-7
<b>Figure 2-3</b> OSPF VPN typical networking.....	2-10
<b>Figure 2-4</b> Troubleshooting flowchart of the OSPF VPN fault.....	2-12
<b>Figure 2-5</b> OSPF Vlink networking.....	2-14
<b>Figure 2-6</b> Networking diagram of a dual-homed CE.....	2-15
<b>Figure 2-7</b> Networking diagram of the inter-AS VPN Option A.....	2-17
<b>Figure 3-1</b> IS-IS typical networking.....	3-5
<b>Figure 3-2</b> IS-IS neighbor troubleshooting flowchart.....	3-8
<b>Figure 3-3</b> IS-IS routing table troubleshooting flowchart.....	3-12
<b>Figure 3-4</b> IS-IS interface troubleshooting flowchart.....	3-15
<b>Figure 3-5</b> IS-IS MT networking.....	3-17
<b>Figure 3-6</b> IS-IS MT neighbor troubleshooting flowchart.....	3-19
<b>Figure 4-1</b> BGP typical networking.....	4-5
<b>Figure 4-2</b> BGP connection troubleshooting flowchart.....	4-9
<b>Figure 4-3</b> BGP connection troubleshooting flowchart.....	4-12
<b>Figure 4-4</b> BGP route loss troubleshooting flowchart.....	4-16
<b>Figure 4-5</b> BGP typical networking.....	4-18
<b>Figure 4-6</b> BGP typical networking.....	4-21
<b>Figure 5-1</b> Typical networking of the Route-Policy troubleshooting in the public networking.....	5-4
<b>Figure 5-2</b> Typical networking of the Route-Policy troubleshooting in a VPN.....	5-5
<b>Figure 5-3</b> Troubleshooting flowchart of the routing policy.....	5-12
<b>Figure 5-4</b> Scenario of the AS-Path-Filter troubleshooting.....	5-16



---

# Tables

---

<b>Table 3-1</b> Relationship between the interface cost and the bandwidth.....	3-22
<b>Table 4-1</b> Category of BGP route attribute.....	4-2
<b>Table 4-2</b> Several types of BGP route attributes.....	4-3
<b>Table 4-3</b> Precedence of policies modifying MED.....	4-24



# 1 RIP Troubleshooting

---

## About This Chapter

This chapter describes the knowledge related to RIP troubleshooting, including RIP overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases, fault information collection, and FAQs.

### [1.1 RIP Overview](#)

This section describes the knowledge you need to know before troubleshooting the Routing Information Protocol (RIP).

### [1.2 RIP Route Receiving Troubleshooting](#)

This section describes the notes about configuring RIP, and provides the RIP troubleshooting flowchart and the troubleshooting procedure in a typical RIP networking environment.

### [1.3 RIP Route Sending Troubleshooting](#)

This section describes the notes about configuring RIP, and provides the RIP troubleshooting flowchart and the troubleshooting procedure in a typical RIP networking environment.

### [1.4 Troubleshooting Cases](#)

This section presents several troubleshooting cases.

### [1.5 FAQs](#)

This section lists frequently asked questions and their answers.

### [1.6 Diagnostic Tools](#)

This section describes common diagnostic tools: display commands and debugging commands.

## 1.1 RIP Overview

This section describes the knowledge you need to know before troubleshooting the Routing Information Protocol (RIP).

The Routing Information Protocol (RIP) is a simple interior gateway protocol and is used mainly in small-scale networks. In general, RIP is not applied to the complex environment and the network of large scale.

The core features of RIP are:

- Based on the Distance-Vector algorithm.
- Exchanges the routing information through UDP packet.
- Uses port number 520.
- Uses the hop count to measure the distance to the destination. The hop count is called the metric.

In RIP, the hop count of the network that is directly connected to the router is 0. The hop count of the network that is connected through one router is 1. The remaining may be deduced by analogy.

The metric is an integer ranging from 0 to 15. If the hop count is more than 15, then it is infinity. That is, the destination network or host is unreachable. Therefore, RIP is not applicable to the network of large scale.

### NOTE

The S9300 defines that the default cost of the incoming interface is 0 and that of the outgoing interface is 1 for RIP.

## 1.2 RIP Route Receiving Troubleshooting

This section describes the notes about configuring RIP, and provides the RIP troubleshooting flowchart and the troubleshooting procedure in a typical RIP networking environment.

[1.2.1 Typical Networking](#)

[1.2.2 Configuration Notes](#)

[1.2.3 Troubleshooting Flowchart](#)

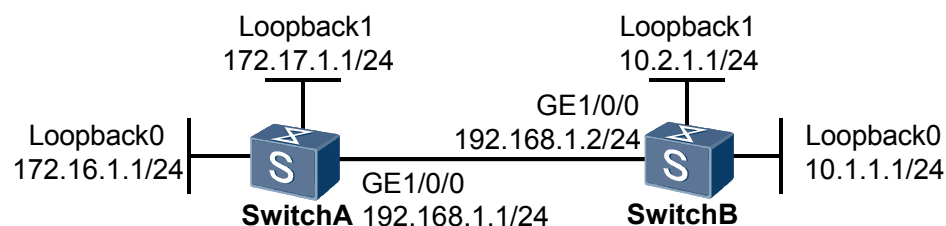
[1.2.4 Troubleshooting Procedure](#)

### 1.2.1 Typical Networking

**Figure 1-1** shows the typical RIP networking.

Take the networking as an example to explain the troubleshooting of the RIP protocol.

**Figure 1-1** Typical networking of RIP





In **Figure 1-1**:

- RIP is enabled on Switch A and Switch B.
- Loopback interfaces are used to simulate the related network segment.

Through the RIP protocol, Switch A and Switch B can communicate with each other on the IP layer.

## 1.2.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configure RIP	Configuring a process	<p>Enable RIP and enter the RIP view. RIP supports multi-instance. Thus, RIP can be associated with the VPN instance.</p> <p>To configure a process, run the <b>rip</b> [ <i>process-id</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] command in the system view.</p>
	Configuring a network	<p>Enable RIP in the specified network segment. The network address that is enabled by the <b>network</b> command must be a natural network segment.</p> <p>For example, 172.16.0.0 and 172.17.0.0 must be configured respectively because 172 belongs to Class B. The two interfaces cannot be enabled if 172.0.0.0 is configured.</p> <p>To configure a network, run the <b>network</b><i>network-address</i> command in the RIP view.</p>
	Configuring RIP to import routes	<p>Import the route from other routing protocols. By configuring the routing policy, you can specify the imported route and the attribute of the route.</p> <p>To configure RIP to import routes, run the <b>import-route</b> <i>protocol</i> [ <i>process-id</i> ] [ <b>cost</b> <i>cost</i> ] [ <b>route-policy</b> <i>route-policy-name</i> ] command in the RIP view.</p>
	Configuring the RIP version	<p>Specify the global RIP version. By default, it is RIP-1. RIP-1 is a type of classful routing protocol. It supports only the broadcast mode. The protocol packet of RIP-1 does not carry the information about mask. The packet does not support route aggregation and discontinuous subnet. And the RIP-1 can only identify the natural network segment to which Class A, Class B, and Class C routes belongs to.</p> <p>RIP-2 is a type of classless routing protocol. The route that is advertised by RIP-2 may carry the detailed information about the subnet mask.</p> <p>To configure the RIP version, run the <b>version</b> { <b>1</b>   <b>2</b> } command in the RIP view.</p>

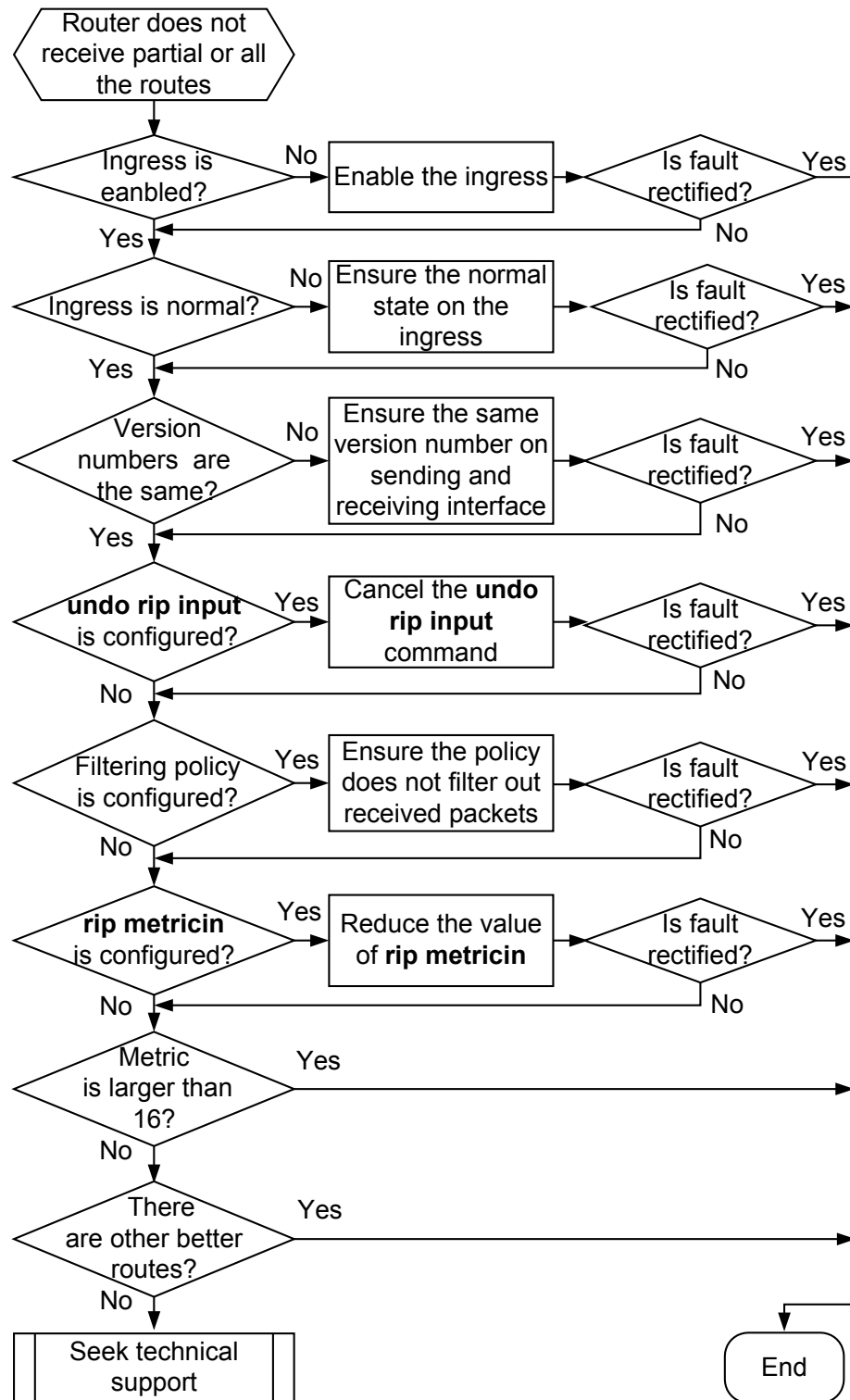
## 1.2.3 Troubleshooting Flowchart

In the networking process shown in [Typical Networking](#), you can note the following when all switches are configured:

- Some switches do not learn partial or all the routes.
- The output of the **display ip routing-table** command shows no routing information learned by RIP.

[Figure 1-2](#) shows the troubleshooting flowchart of RIP Route receiving.

Figure 1-2 RIP route receiving troubleshooting flowchart



## 1.2.4 Troubleshooting Procedure

## Procedure

**Step 1** Check that the incoming interface is enabled with RIP.

The **network** command is used to specify the interface network segment. Only the interface enabled with RIP can receive and send the RIP routing information.

Run the **display current-configuration configuration rip** command to check information about the network segment where RIP is enabled. Check whether the incoming interface is enabled.

The network address enabled by the **network** command must be that of the natural network segment.

**Step 2** Check that the incoming interface works normally.

Run the **display interface** command to check the operating status of the incoming interface:

- If the current physical status of the interface is Down or Administratively Down, RIP cannot receive any route from the interface.
- If the current protocol status of the interface is Down, the cost of routes learnt by RIP from the interface changes to 16, and then is deleted.

Therefore, ensure the normal status of the interface.

**Step 3** Check that the version number sent by the peer matches with that received on the Local Interface.

By default, the interface sends only RIP-1 packets, but can receive packets of RIP-1 and RIP-2. If the version number of the incoming interface and that of the RIP packet are different, the RIP routing information may not be received correctly.

**Step 4** Check whether the **undo rip input** command is configured on the incoming interface.

The **rip input** command enables the specified interface to receive the RIP packet.

The **undo rip input** command disables the specified interface from receiving the RIP packet.

If the **undo rip input** command is configured on the incoming interface, all the RIP packets from the interface cannot be processed. Therefore, the routing information cannot be received.

**Step 5** Check whether the policy that is used to filter the received RIP routes is configured.

The **filter-policy import** command is used to filter the received RIP routes.

If the ACL is used, run the **display current-configuration configuration acl-basic** command to view whether the RIP routes learned from the neighbor are filtered.

The IP-Prefix list is used to filter routes. The **display ip ip-prefix** command is used to check the configured policy.

If routes are filtered by the routing policy, the correct routing policy must be configured.

**Step 6** Check whether the incoming interface is configured with the **rip metricin** command and the metric is larger than 16.

The **rip metricin** command is used to set the metric that is added to the route when the interface receives the RIP packet.

If the metric exceeds 16, the route is regarded as unreachable and is not added to the routing table.

**Step 7** Check whether the metric of the received routes is larger than 16.

Similarly, if the metric of the received route exceeds 16, the route is regarded as unreachable and is not added to the routing table.

**Step 8** Check whether other protocols learning the same routes in the routing table.

Run the **display rip 1 route** command to check whether there are routes received from the neighbor.

The possible cause is that the RIP route is received correctly and the local device learns the same route from other protocols such as OSPF and IS-IS.

In general, the weights of OSPF or IS-IS are larger than that of RIP. The route learned through OSPF or IS-IS is preferred by the routing management.

Run the **display ip routing-table protocol rip verbose** command to view the route whose status is Inactive.

If the fault persists, contact the Huawei technical personnel.

---End

## 1.3 RIP Route Sending Troubleshooting

This section describes the notes about configuring RIP, and provides the RIP troubleshooting flowchart and the troubleshooting procedure in a typical RIP networking environment.

[1.3.1 Typical Networking](#)

[1.3.2 Configuration Notes](#)

[1.3.3 Troubleshooting Flowchart](#)

[1.3.4 Troubleshooting Procedure](#)

### 1.3.1 Typical Networking

See section [Typical Networking](#).

### 1.3.2 Configuration Notes

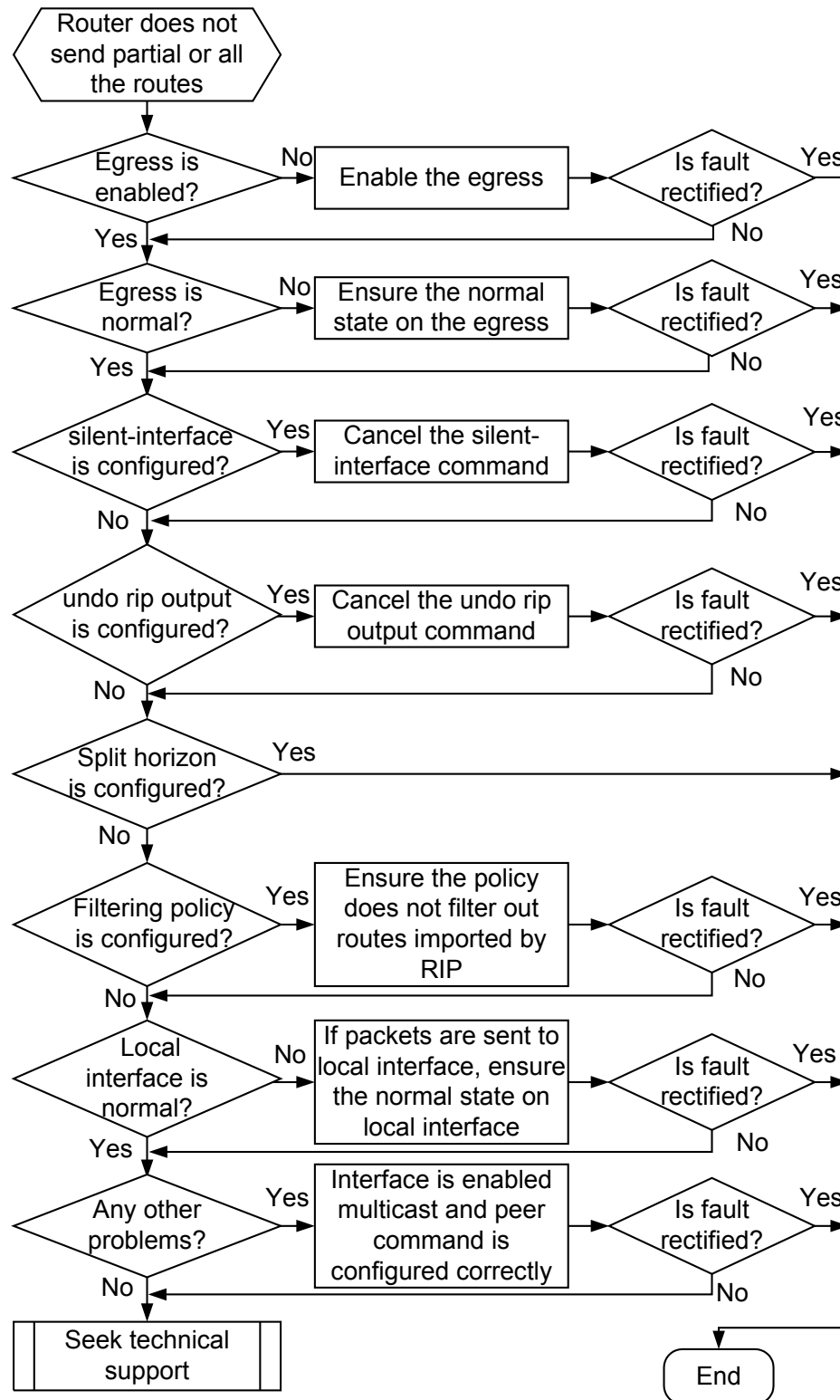
See section [Configuration Notes](#).

### 1.3.3 Troubleshooting Flowchart

In the networking process shown in [Typical Networking](#), the switch cannot send partial or all of the routes even after the configuration on each switch.

[Figure 1-3](#) shows the troubleshooting flowchart of RIP route sending.

Figure 1-3 RIP route sending troubleshooting flowchart



### 1.3.4 Troubleshooting Procedure

## Procedure

### Step 1 Check whether the outgoing interface is enabled with RIP.

The **network** command is used to specify the interface network segment. Only the interface enabled with RIP can receive and send RIP routes.

Run the **display current-configuration configuration rip** command to check information about the network segment where RIP is enabled. Check whether the outgoing interface is enabled.

The network address enabled by using the **network** command must be that of the natural network segment.

### Step 2 Check whether the outgoing interface works normally.

Run the **display interface** command to check the operating status of the outgoing interface.

If the physical status of the interface is Down or Administratively Down, or the status of the current protocol is Down, RIP cannot work normally on the interface.

Ensure the normal status of the interface.

### Step 3 Check whether the **silent-interface** command is configured on the outgoing interface.

The **silent-interface** command is used to suppress the interface from sending the RIP packet.

The **display current-configuration configuration rip** command is used to check whether the interface is suppressed from sending the RIP packet.

If the **silent-interface** command is configured, disable suppression on the interface.

### Step 4 Check whether the **undo rip output** command is configured on the outgoing interface.

Run the **display current-configuration** command on the outgoing interface to view if the **rip output** command is configured.

The **rip output** command enables the interface to send the RIP packet.

The **undo rip output** command disables the interface from sending the RIP packet.

If the outgoing interface is configured with the **undo rip output** command, the RIP packet cannot be sent on the interface.

### Step 5 Check whether the **rip split-horizon** command is configured on the outgoing interface.

Run the **display current-configuration** command on the outgoing interface to view whether the **rip split-horizon** command is configured.

By default, the split-horizon is enabled on all outgoing interfaces, and the display of the command does not contain configuration items about the split-horizon.

For the outgoing interface (such as X.25, FR) of the NonBroadcast Multiple Access (NBMA) network, if the display contains no configuration item about the split-horizon, it indicates that split-horizon is not enabled on the outgoing interface.

The split-horizon means that the route learned from an interface cannot be advertised on the interface.

The split-horizon is used to prevent the loop between adjacent neighbors. Do not remove the split-horizon on the interface hastily.

**Step 6** Check whether the policy filtering the imported RIP route is configured in RIP.

Run the **filter-policy export** command to configure the filtering policy on the global interface.

Only the route that passes the filtering policy can be added to the advertised routing table of RIP. It is advertised through the updated packet.

**Step 7** Check the status of the interface when the route is sent to the local interface address.

Run the **display interface** command to check the operating status of the interface.

If the physical status of the interface is Down or Administratively Down, or the current status of the protocol on the outgoing interface is Down, the IP address of the interface cannot be added to the advertised routing table of RIP. Therefore, the routing information is not sent to the neighbor.

**Step 8** Check whether there are other problems.

If the outgoing interface does not support the multicast or broadcast mode and a packet needs to be sent to the multicast or broadcast address, the fault occurs.

You can rule out that fault occurs on the interface, and configure the **peer** command in the RIP mode to make switches send packets with unicast address. Thus, the fault is removed.

If the fault persists, contact the Huawei technical personnel.

----End

## 1.4 Troubleshooting Cases

This section presents several troubleshooting cases.

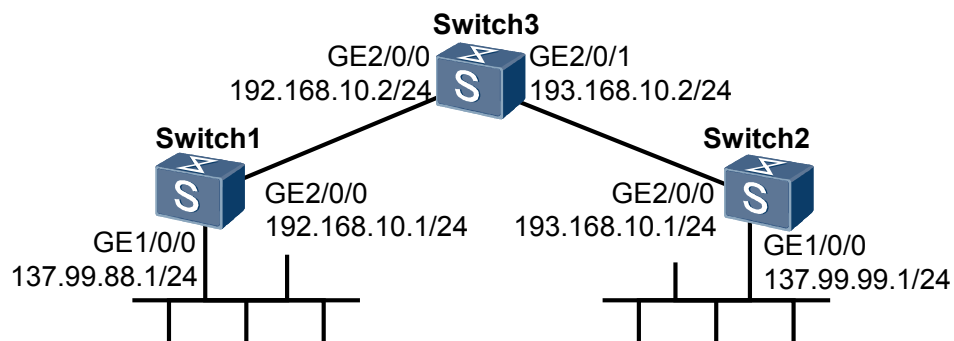
### 1.4.1 Discontinuous Subnet Fault

#### 1.4.1 Discontinuous Subnet Fault

##### Fault Symptom

As shown in [Figure 1-4](#), the RIP routing protocol is configured.

**Figure 1-4** Networking diagram of RIP





After the configuration, run the **display ip routing-table** command to check the routing table.

The display shows:

- Only one route to 137.99.0.0 exists in the routing table of Switch 3.
- The next hop of the route is 192.168.10.1 or 193.168.10.1.

```
<Switch3> display ip routing-table
Routing Tables: Public
Destinations : 9          Routes : 10
Destination/Mask  Proto  Pre  Cost    NextHop          Interface
127.0.0.0/8       Direct 0    0       127.0.0.1         InLoopBack0
127.0.0.1/32      Direct 0    0       127.0.0.1         InLoopBack0
137.99.0.0/16     RIP     100  1       D 192.168.10.1    Vlanif10
                  RIP     100  1       D 193.168.10.1    Vlanif20
192.168.10.0/24   Direct 0    0       D 192.168.10.2    Vlanif10
192.168.10.1/32   Direct 0    0       D 192.168.10.1    Vlanif10
192.168.10.2/32   Direct 0    0       D 127.0.0.1        InLoopBack0
193.168.10.0/24   Direct 0    0       D 193.168.10.2    Vlanif20
193.168.10.1/32   Direct 0    0       D 193.168.10.1    Vlanif20
193.168.10.2/32   Direct 0    0       127.0.0.1        InLoopBack0
```

In **Figure 1-4**, Switch 3 should have two routes:

- 137.99.88.0/24 that is forwarded to Switch 1
- 137.99.99.0/24 that is forwarded to Switch 2

## Fault Analysis

1. Run the **debugging rip send** command on Switch 1 and Switch 2 respectively. Then, by observing the RIP packet that is sent from VLANIF20, you can find:
  - Switch 1 sends classful 137.99.0.0 to Switch 3.
  - Switch 2 sends classful 137.99.0.0 to Switch 3.
2. View the routing table of Switch 3, and you can find that Switch 3 accepts only the route 137.99.0.0.

The cause may be that RIP-1 does not support discontinuous subnets.

The discontinuous subnets refer to several subnets belonging to the same network that are segmented by different networks. As shown in the preceding networking diagram, the network 137.99.0.0 is divided by the network 192.168.10.0 and the network 193.168.10.0.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **rip process-id** command to enable an RIP process and enter the RIP view.
- Step 3** Run the **version 2** command to specify the RIPv2 version.
- Step 4** Run the **undo summary** command to cancel the classful aggregation.

----End

## Summary

RIP-1 does not support the discontinuous subnets. To solve this problem, you can adopt the following methods:

- It is recommended to configure RIP-2 in the network and cancel the automatic aggregation of RIP-2 on Switch 1 and Switch 2.
- It is not recommended to configure the subnets of 137.99.0.0/24 (subnet addresses with the same mask and belonging to the same network) on network segments 192.168.10.0/24 and 193.168.10.0/24 by running the `ip address sub` command.

For example, you can configure the network segment 137.99.66.0/24 between Switch 1 and Switch 3 and configure the network segment 137.99.77.0/24 between Switch 3 and Switch 2.

This solution requires more bandwidth and causes unnecessary configuration errors. For example, when you configure a subnet, the primary address is replaced incorrectly if you forget to add the keyword **sub**. Therefore, it is not recommended to use this method.

## 1.5 FAQs

This section lists frequently asked questions and their answers.

### Q: After the Configuration of RIP, Why Cannot RIP Set up the Adjacency with the Neighbor or the Peer?

A: To locate the fault, follow the steps described below:

- Check whether the RIP process is enabled on the main network.
- Check whether the IP address of at least one interface is configured on the main network.
- Run the **display ip interface** command to check whether the interface is in the Up status. The physical status and protocol status should be Up on the interface.
- Check that the RIP process and the IP address on the interface belong to the same instance. They must also belong to the same interface.

### Q: After the Route is Imported, Why Does the RIP Database not Show any Imported Route?

A: To locate the fault, follow the steps described below:

- Check that there are routes, including static routes and routes imported from other protocols.
- Check that the outgoing interface of the static route or other protocols is configured with an IP address.
- Check that the outgoing interface of the static route or other protocols is Up.

### Q: After the Configuration of RIP, Why Cannot Partial RIP Routing Information Be Received?

A: To locate the fault, follow the steps described below:

- Check whether the **default-route originate cost** command is configured on the switch. If the command is configured, the default routing information sourced from other routes cannot be received.
- Check whether the RIP receives other routes with better metrics.
- Check whether the RIP receives the equal-cost route of the maximum number.
- Check whether the sum of the routing metric and additional metric is larger than 15.

- Check whether the **verify-source** is enabled in the RIP process when the packet comes from the peers that belong to different networks. By default, it is enabled.
- Check whether the RIP version is RIP-2 and whether the host route is enabled on the interface, if the routing information is received from the host. By default, it is enabled.

**Q: Configure the Interface to Send RIP-2 Routes. Debugging shows that the routes sent by RIP-2 are the routes with the classful mask, that is, Class A, Class B, or Class C mask. How does RIP-2 send the routes with the classless mask?**

A: By default, RIP-2 sends the aggregated route to reduce the RIP packets.

Run the **undo summary** command in the RIP view to remove the aggregation. Thus, the route with the classless mask is produced.

**Q: After the silent-interface all Command Is Configured in the RIP View, Why is the RIP Route Received yet?**

A: The **silent-interface** command disables only the sending of the RIP packet. The RIP packet can still be received to update the routing table.

**Q: In RIP, When other Routing Protocols Are Imported by Using the import-route Command, Why Is the Tag Value Incorrect?**

A: The length of tag field ruled by RIP is 16 bits, while the length of tag field ruled by other routing protocols is 32 bits. When other routing protocols are imported, you should ensure that the tag value cannot exceed 65535 if the routing policy uses tag. Otherwise, the routing policy is invalid or the incorrect match is produced.

**Q: Why Is the Summary Command Invalid, When Route Aggregation Is Performed Using the Summary Command in RIP?**

A: For RIP-2, the **summary** command takes effect on the condition that the split-horizon and poison reverse are not enabled on the interface. RIP-1 does not support route aggregation. Hence, the **summary** command does not take effect on RIP-1.

**Q: How to Solve the Problem of RIP Flapping?**

A: RIP route flapping may occur in the following cases:

- If the value of the four timers is not configured reasonably, route flapping occurs. To solve this problem, configure the value of timers correctly. The relationship of the value is that: update < age, suppress < garbage - collect.
- When routes of other protocols are imported, the flapping of the imported routes causes the flapping of the RIP route. The solution is to solve the problem of the route flapping that occurs in the imported protocol.
- If the physical status of the interface on which RIP is enabled changes repeatedly, route flapping occurs. To address this problem, find out why the status of the interface changes repeatedly.

## Q: What Are the Requirements for Configuring RIP Authentication Words?

A: RIP authentication words are expressed by plain text and cipher text words by complying with the following rules:

- Plain text word is a string of 1 to 16 bytes.
- Cipher text word can be either a plain text word of 1 to 16 bytes or a cipher text word of 24 bytes.
- Space is not allowed in all authentication words.

## 1.6 Diagnostic Tools

This section describes common diagnostic tools: display commands and debugging commands.

### 1.6.1 display Commands

#### 1.6.2 debugging Commands

### 1.6.1 display Commands

Command	Description
<b>display rip</b> [ <i>process-id</i>   <b>vpn-instance</b> <i>vpn-instance-name</i> ]	Displays the current running status and configuration of RIP.
<b>display rip</b> <i>process-id</i> <b>database</b> [ <b>verbose</b> ]	Displays all the active routes in the RIP advertising database.
<b>display rip</b> <i>process-id</i> <b>interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [ <b>verbose</b> ]	Displays information about RIP interfaces.
<b>display rip</b> <i>process-id</i> <b>neighbor</b> [ <b>verbose</b> ]	Displays information about RIP neighbors.
<b>display rip</b> <i>process-id</i> <b>route</b>	Displays the route received from the neighbor.
<b>display ip routing-table</b> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] <b>protocol rip</b>	Displays all the active and inactive RIP routes.

### 1.6.2 debugging Commands

Command	Description
<b>debugging rip</b> <i>process-id</i> <b>brief</b>	Enables the debugging of the brief of RIP packets.
<b>debugging rip</b> <i>process-id</i> <b>error</b>	Enables the debugging of incorrect brief of RIP.
<b>debugging rip</b> <i>process-id</i> <b>event</b>	Enables the debugging of RIP events.

Command	Description
<b>debugging rip <i>process-id</i> job</b>	Enables the debugging of RIP job.
<b>debugging rip miscellaneous</b>	Enables the debugging of RIP packets that are not related to the process.
<b>debugging rip <i>process-id</i> packet</b>	Enables the debugging of RIP packets. You can then know the process of transmitting RIP packets.
<b>debugging rip <i>process-id</i> receive</b>	Enables the debugging of the process of receiving RIP packets.
<b>debugging rip <i>process-id</i> replay-protect</b> [ <i>interface-type interface-number</i> ]	Enables the debugging of RIP sequence number recovery.
<b>debugging rip <i>process-id</i> route-processing</b>	Enables the debugging of the RIP route calculation.
<b>debugging rip <i>process-id</i> send</b>	Enables the debugging of the process of sending RIP packets.
<b>debugging rip <i>process-id</i> timer</b>	Enables the debugging of RIP timers.



# 2 OSPF Troubleshooting

---

## About This Chapter

This chapter describes the knowledge related to OSPF troubleshooting, including OSPF overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases and diagnostic tools and FAQs.

### [2.1 OSPF Overview](#)

This section describes the knowledge you need to know before troubleshooting the Open Shortest Path First (OSPF).

### [2.2 OSPF Neighbor Troubleshooting](#)

This section describes the notes about configuring OSPF, and provides the troubleshooting flowchart and the troubleshooting procedure in a typical OSPF networking environment.

### [2.3 OSPF VPN Troubleshooting](#)

This section describes the notes about configuring OSPF VPN, and provides the troubleshooting flowchart and the troubleshooting procedure in a typical OSPF VPN networking environment.

### [2.4 Troubleshooting Cases](#)

This section presents several troubleshooting cases.

### [2.5 FAQs](#)

This section lists frequently asked questions and their answers.

### [2.6 Diagnostic Tools](#)

This section describes common diagnostic tools: display commands and debugging commands.

## 2.1 OSPF Overview

This section describes the knowledge you need to know before troubleshooting the Open Shortest Path First (OSPF).

### 2.1.1 Introduction to OSPF

#### 2.1.2 Basic Concepts

## 2.1.1 Introduction to OSPF

The Open Shortest Path First (OSPF) protocol is a dynamic routing protocol used within an autonomous system (AS).

OSPF functions can be configured for a process only after OSPF is enabled and the address of the network segment and area number are specified. On the contrary, OSPF functions can be configured on an interface regardless of whether the OSPF process is enabled.

## 2.1.2 Basic Concepts

### Router ID

Router ID indicates the ID of the switch.

To run the OSPF protocol, a switch must have the router ID. If the ID is not configured, the system chooses an ID for the switch from the IP addresses of the current interfaces.

### Designated Router (DR)

The DR is not specified by the user, but elected by the switches on the network segment. All the switches send messages to the DR. The DR advertises the status of the network link.

The switch other than the DR/Backup Designated Router (BDR) is called DR Other.

DR Others do not set up adjacencies between each other. In addition, no routing information is exchanged between them.

### Backup Designated Router (BDR)

The BDR is the backup router of the DR.

The BDR is elected together with the DR. The BDR sets up the adjacency and exchanges the routing information among the switches on the network segment. When the DR fails, the BDR becomes the DR instantly.

### Area

In OSPF, an AS is often divided into different areas.

Logically, the area divides the switches in the AS into different groups. The switch resides on the border of the area. Thus, some switches belong to different areas.



The switch that connects the backbone area and non-backbone area is called the Area Border Router (ABR).

The connection between the ABR and the backbone area can be either a physical or logical one.

## Backbone Area

In OSPF, not all the areas are of the same level. The area with ID as 0 is called the backbone area.

## Virtual link

All the areas must connect with the backbone area logically. The virtual link ensures the logical connection between the physically-divided areas.

## Summary

Summary indicates route aggregation.

The AS is divided into different areas. Areas are connected with each other through the OSPF ABR.

The route aggregation can reduce the routing information between areas, diminish the size of the routing table, and quicken the calculating speed of the router.

## Graceful Restart (GR)

After being enabled with the OSPF Graceful Restart (GR) function, if a switch performs GR due to abnormalities, the switch can ensure that traffic forwarding is not affected and route flapping can be avoided, which prevent key services from being interrupted.

## Traffic Engineering (TE)

The OSPF protocol sets up and maintains the Label Switch Path (LSP) of TE.

When the Constraint-based Routed LSP (CR-LSP) is constructed by MPLS, the information about the traffic attributes of all the links in the local area is needed. The TE is obtained through OSPF.

## Virtual Private Network (VPN)

In general, the customers of a VPN are connected through the BGP peer. The local network of the customers often uses the OSPF protocol as the interior routing protocol.

In a common OSPF topology, even though two VPNs belong to the same client, they are considered to be of different ASs. The route, thus learned on one node is considered as the external route when the route is advertised to another node.

## Sham Link

The sham link refers to the point-to-point link between two PEs on the MPLS VPN backbone network.

The sham link uses the unnumbered address.

BGP peers exchange the routing information through the BGP extended community attribute on the MPLS VPN backbone network. OSPF that runs on the PE can use the information to generate Type 3 Summary LSAs from the remote PE to CE. These routes are known as inter-area routes.

## 2.2 OSPF Neighbor Troubleshooting

This section describes the notes about configuring OSPF, and provides the troubleshooting flowchart and the troubleshooting procedure in a typical OSPF networking environment.

### 2.2.1 Typical Networking

#### 2.2.2 Configuration Notes

#### 2.2.3 Troubleshooting Flowchart

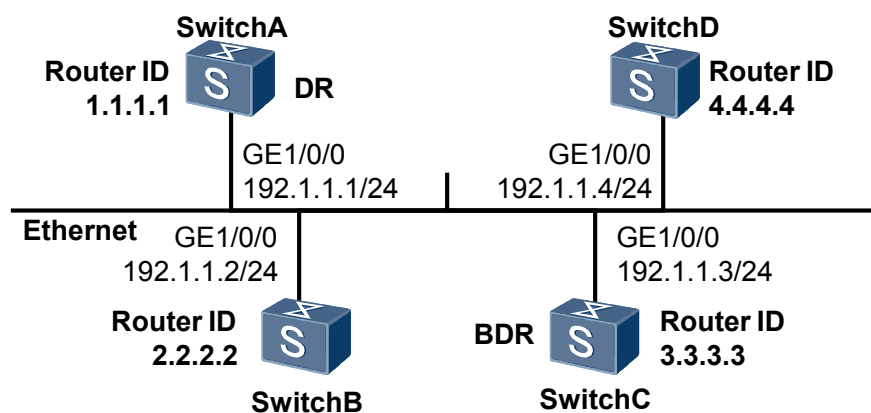
#### 2.2.4 Troubleshooting Procedure

### 2.2.1 Typical Networking

**Figure 2-1** shows the typical OSPF networking.

Take the networking process in **Figure 2-1** as an example to explain the OSPF troubleshooting.

**Figure 2-1** OSPF typical networking



In **Figure 2-1**:

- Switch A has the highest priority of 100. It is elected as the DR.
- Priority of Switch C is second to that of Switch A. It is elected as the BDR.
- Priority of Switch B is 0.
- Switch D uses the default priority of 1.

Switch A, Switch B, Switch C, and Switch D set up OSPF neighbor with each other.

### 2.2.2 Configuration Notes

Item	Sub-item	Notes and Configuration Commands
Enabling OSPF	Configuring a router ID	Router IDs in the same AS must be different from each other.  To configure a router ID, run the <b>ospf</b> [ <i>process-id</i>   <b>router-id</b> <i>router-id</i>   <b>vpn-instance</b> <i>vpn-instance-name</i> ] * command in the system view.
	Configuring a peer	On an X.25 or frame relay network, you can configure mappings to implement full connection in the entire network. That is, any two routes in the network can be reachable to each other through a virtual circuit. In this manner, OSPF can process the operations such as DR and BDR election as like as in a broadcast network. But a switch cannot detect neighboring routers by broadcasting hello packets, you must manually configure the IP addresses of its adjacent routers for this interface and their election rights.  To configure a peer, run the <b>peer</b> <i>ip-address</i> [ <b>dr-priority</b> <i>priority</i> ] command in the OSPF view.
	Configuring OSPF to import routes	Routes learned by other protocols are imported.  To configure OSPF to import routes, run the <b>import-route</b> { <b>limit</b> <i>limit-number</i>   <i>protocol</i> [ <i>process-id</i> ] [ <b>cost</b> <i>cost</i>   <b>route-policy</b> <i>route-policy-name</i>   <b>tag</b> <i>tag</i>   <b>type</b> <i>type</i> ] *} command in the OSPF view.
	Configuring an area	The OSPF network must contain a backbone area. When multiple areas exist, the backbone area must be configured as area 0. In addition, area 0 must be reachable to the other areas logically or physically.  To configure an area, run the <b>area</b> <i>area-id</i> command in the OSPF view.
	Configuring a network	The <b>network</b> command is used to specify the interface enabled with OSPF and the area to which the interface belongs. An interface can only belong to a specified area.  To configure a network, run the <b>network</b> <i>address wildcard-mask</i> [ <b>description</b> <i>text</i> ] command in the OSPF area view.
	Configuring the authentication mode	It is used to set the authentication mode and check word in the area. To configure the authentication mode, run the following commands in the OSPF area view: <ul style="list-style-type: none"> <li>● <b>authentication-mode simple</b> [ [ <b>plain</b> ] <i>plain-text</i>   <b>cipher</b> <i>cipher-text</i> ]</li> <li>● <b>authentication-mode</b> { <b>md5</b>   <b>hmac-md5</b> } [ <i>key-id</i> { <b>plain</b> <i>plain-text</i>   [ <b>cipher</b> ] <i>cipher-text</i> } ]</li> </ul>

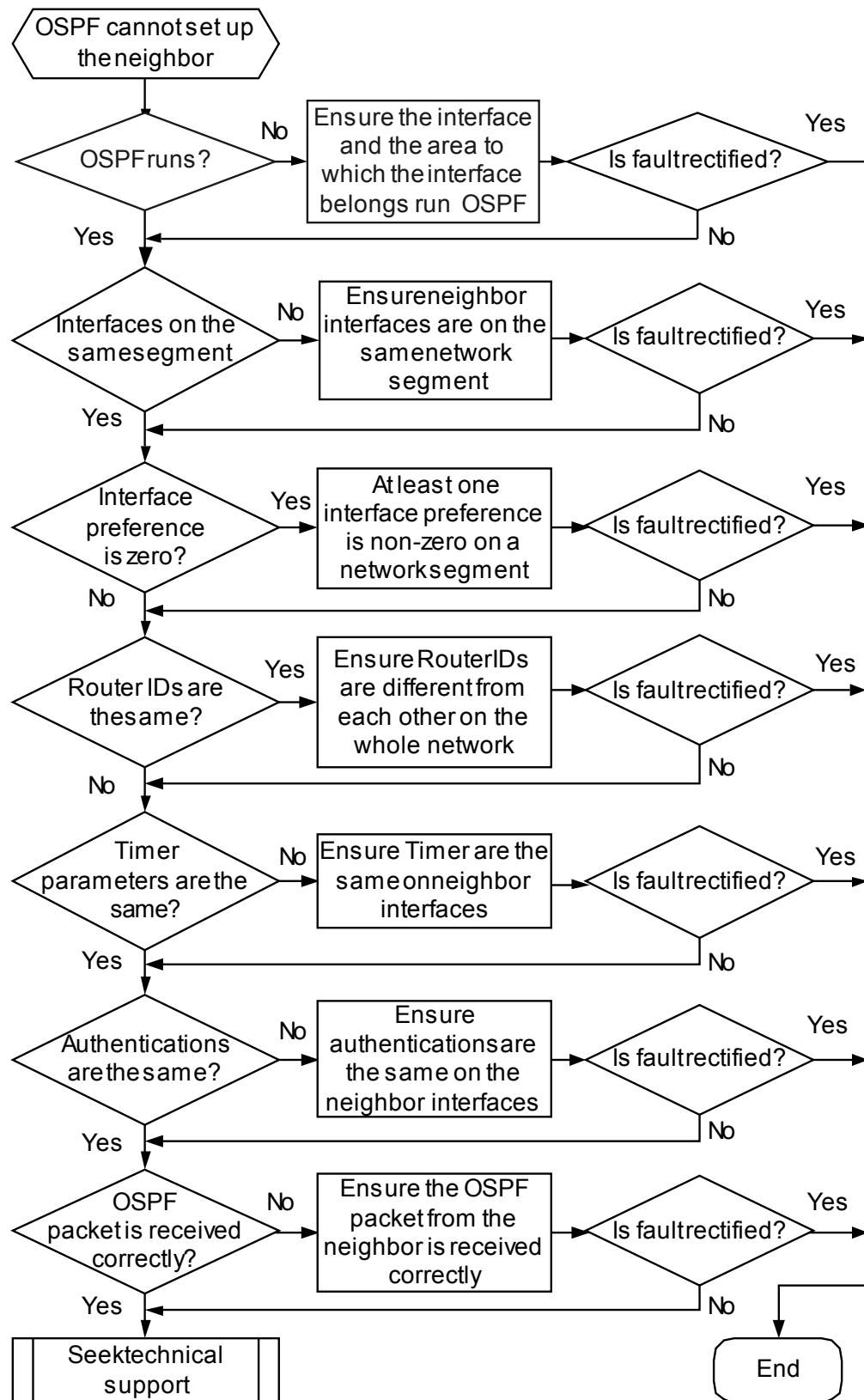
Item	Sub-item	Notes and Configuration Commands
	Configuring an Not-So-Stubby Area (NSSA)	Configure an NSSA area. To configure an NSSA area, run the <b>nssa [ default-route-advertise   flush-waiting-timer <i>interval-value</i>   no-import-route   no-summary   set-n-bit   suppress-forwarding-address   translator-always   translator-interval <i>interval-value</i>   zero-address-forwarding ] *</b> command in the OSPF area view.
	Configuring a stub area	Configure a Stub area. To configure a stub area, run the <b>stub [ no-summary ]</b> command in the OSPF area view.
	Configuring the cost of an OSPF interface	Configure the cost of the OSPF protocol on the interface. To configure the cost of an OSPF interface, run the <b>ospf cost <i>cost</i></b> command in the interface view.
	Configuring the DR priority	The DR priority of an interface determines the qualification of the interface in DR election. The interface with a higher priority has a more preferential qualification when two switches on one network segment announce to be the DR. To configure the DR priority, run the <b>ospf dr-priority <i>priority</i></b> command in the interface view.
	Configuring a network type	It is used to set the network type of the OSPF interface. To configure a network type, run the <b>ospf network-type { broadcast   nbma   p2mp   p2p }</b> command in the interface view.
	Configuring a timer	It is used to set the interval for sending such packets as the Hello packet and the Dead packet on the interface. To configure a timer, run the following commands in the interface view: <ul style="list-style-type: none"> <li>● <b>ospf timer dead <i>interval</i></b></li> <li>● <b>ospf timer hello <i>interval</i></b></li> <li>● <b>ospf timer poll <i>interval</i></b></li> <li>● <b>ospf timer retransmit <i>interval</i></b></li> </ul>

## 2.2.3 Troubleshooting Flowchart

In the network process shown in [Typical Networking](#), the OSPF adjacency cannot be set up after the configuration.

[Figure 2-2](#) shows the troubleshooting flowchart of the establishment failure of the OSPF adjacency.

Figure 2-2 Troubleshooting flowchart of the establishment failure of the OSPF adjacency



## 2.2.4 Troubleshooting Procedure

### Procedure

**Step 1** Check whether the neighbor interfaces of both ends are on the same network segment.

When the OSPF neighbor relationship is configured, the broadcast interface and the NBMA interface should be in the same network segment. The two interfaces at the both ends of the link on which the OSPF neighbor relationship is set up can thus ping through each other. The area IDs and area types (such as NSSA, stub, and normal area) of the interfaces must be consistent.

**Step 2** Check whether there is at least one interface whose priority is non-zero.

As for the broadcast and NBMA network segments, there should be at least one interface with non-zero priority. This ensures that the DR can be elected. Otherwise, each neighbor can only reach the 2-Way state.

You can run the **display ospf interface** command to check the priority of the interface.

**Step 3** Check the Router ID is unique in the whole network.

Router IDs in the whole network should be different from each other. Otherwise, the route flapping occurs.

You can run the **display ospf brief** command to check the Router ID.

**Step 4** Check that the timer parameters on the two interfaces are consistent.

The **ospf timer hello** command sets the interval for sending the Hello packet on the interface.

By default, the Point-to-Point (P2P) and broadcast interfaces send the Hello packet at the interval of 10 seconds, while the Point-to-Multipoint (P2MP) and NBMA interfaces send the Hello packet every 30 seconds.

The **ospf timer dead** command sets the expiry time of the OSPF neighbor.

By default, the expiration time of OSPF neighbor on the P2P and broadcast interfaces is 40 seconds, while that on the P2MP and NBMA interfaces is 120 seconds.

The neighbor relationship can be established between two interfaces only when the timer parameters of the interfaces are the same.

You can run the **display ospf interface verbose** command to check the parameter.

**Step 5** Check that the authentication information is the same on the neighboring interfaces at both ends.

In OSPF, the authentication information is configured on the Area and interface, respectively.

The principle of OSPF authentication is as follows:

- If the interface is configured with the authentication, the authentication is adopted.
- If the authentication on the interface is configured as Null, the interface adopts no authentication.
- If no authentication is configured on the interface (Null does not mean no authentication), the authentication configured on the area is adopted.
- If the authentication is configured on neither the interface nor area, no authentication is performed.

The neighbor can reach the Full state only when the two ends are configured with the same authentication.

**Step 6** Check that the OSPF packets can be received correctly.

Check the connectivity of the data link layer firstly.

You can check the receiving and sending of the packet by using the **debugging ospf packet** command and the **debugging ospf event** command.

You can run the **display ospf error** command to check the OSPF error count.

If OSPF packets are normal, check whether GTSM is correctly configured on the interface. If only the private policy or the public policy is configured, and the default action of the packets that do not match the GTMS policy is set to pass, OSPF packets of other instances may be discarded incorrectly.

Enable the IP packet debugging to check if the packet is forwarded normally on the IP layer. Run the **debugging ip packet** command to enable IP packet debugging. The ACL can be specified in the command to filter the debugging information. Debugging information includes the following:

- If debugging information "OSPF 1: SEND Packet." is displayed, it indicates that OSPF packets can be sent correctly.
- If the following debugging information is displayed, it indicates that packets are forwarded successfully (the debugging information of Gigabit Ethernet 6/0/0 is taken as an example).
  - prompt: Sending the packet from local at Gigabitethernet6/0/0
  - prompt: Receiving IP packet from Gigabitethernet6/0/0
  - prompt: IP packet is delivering up!
- If the following debugging information is displayed, it indicates that packets fail to be forwarded.
  - prompt: Destination is unreachable!
  - prompt: Not forwarding local multicast packets!

If the fault persists, contact the Huawei technical personnel.

---End

## 2.3 OSPF VPN Troubleshooting

This section describes the notes about configuring OSPF VPN, and provides the troubleshooting flowchart and the troubleshooting procedure in a typical OSPF VPN networking environment.

### [2.3.1 Typical Networking](#)

### [2.3.2 Configuration Notes](#)

### [2.3.3 Troubleshooting Flowchart](#)

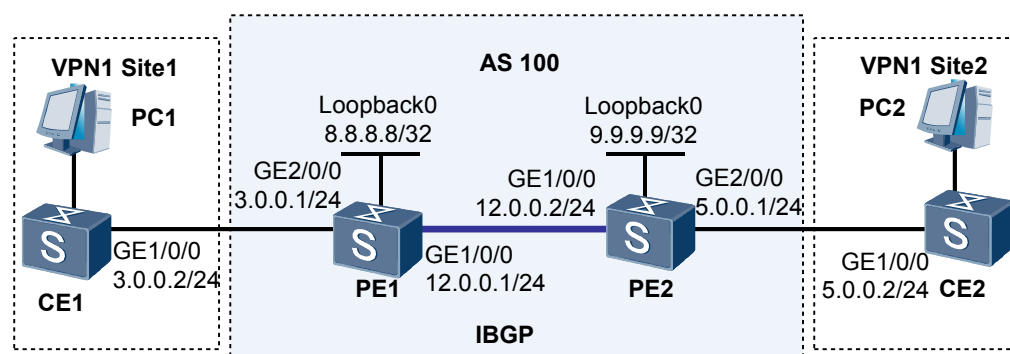
### [2.3.4 Troubleshooting Procedure](#)

## 2.3.1 Typical Networking

**Figure 2-3** shows the typical OSPF VPN networking.

Take the following networking as an example to explain the OSPF VPN troubleshooting.

Figure 2-3 OSPF VPN typical networking



In Figure 2-3:

- CE1 and PC1 belong to Site1 of VPN1; CE2 and PC2 belong to Site2 of VPN1.
- OSPF runs on PE1 and CE1, and PE2 and CE2.
- MP-IBGP (Multiprotocol Extensions for IBGP) runs on PE1 and PE2.
- The neighbor relationship between PE1 and PE2 is set up through the OSPF protocol.
- OSPF and BGP import routes from each other on PE1 and PE2 respectively.

## 2.3.2 Configuration Notes

Item	Sub-item	Notes
Configuring the OSPF instance	Configuring a VPN instance	OSPF supports multiple instances. It is configured between PE and CE in the VPN. VPN instances are configured a VPN instance, run the <b>ospf [ process-id   router-id router-id   vpn-instance vpn-instance-name ] *</b> command in the system view.
	Configuring a domain ID	Different VPNs must be configured with different domain IDs on PEs. To configure a domain ID, run the <b>domain-id { null   domain-id [ type type value value   secondary ] }</b> command in the OSPF view.
	Configuring VPN-Instance-Capability Simple	Loop detection is restricted, and route calculation is performed directly. By default, loop detection is enabled. When the MCE supports VPN multi-instance, loop detection needs to be cancelled. To configure VPN-Instance-Capability Simple, run the <b>vpn-instance-capability simple</b> command in the OSPF view.

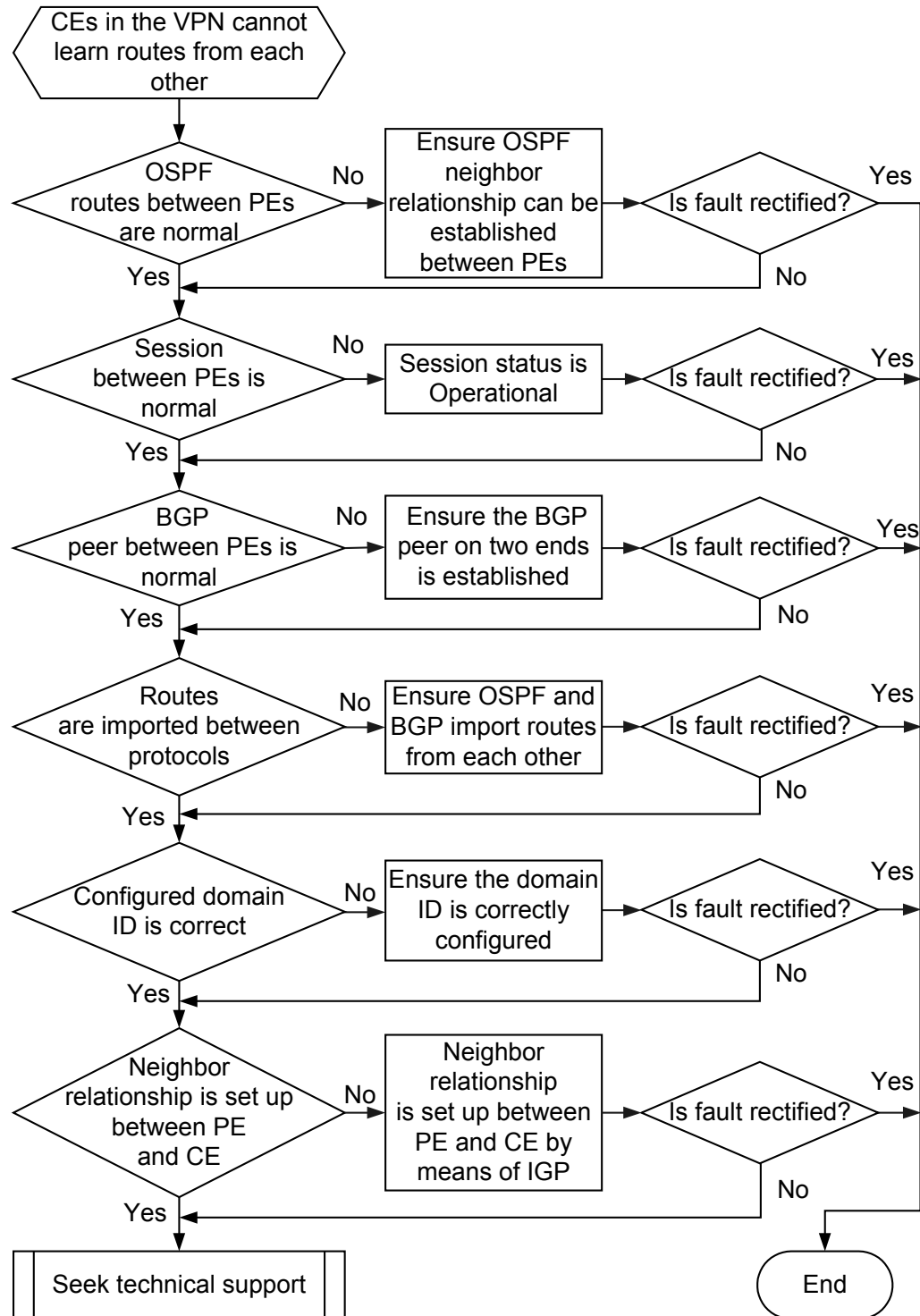


## 2.3.3 Troubleshooting Flowchart

In the networking shown in [Typical Networking](#), CEs cannot learn routes from each other in the VPN after the configuration.

You can diagnose the fault according to the flowchart shown in [Figure 2-4](#).

**Figure 2-4** Troubleshooting flowchart of the OSPF VPN fault



### 2.3.4 Troubleshooting Procedure

## Procedure

**Step 1** Check that the IGP connection between two PEs is normal.

In general, the connection between two PEs is set up through the IGP protocol. Here, the OSPF protocol is adopted to set up the connection between the two PEs.

Using the **display ospf peer** command, you can view the establishment of the OSPF neighbor through OSPF.

**Step 2** Check whether the session between two PEs is normal.

Check the **mpls ldp session** command. Using the **display mpls ldp session** command, you can check whether the session between PEs is in Operational status.

**Step 3** Check that the BGP neighbor relationship between two PEs is normal.

Using the **display bgp vpnv4 all peer** command, you can view information about the BGP neighbor. "Establish" indicates that the BGP neighbor has been set up.

If the BGP neighbor is in the Active or Idle state all the time, run the **display current-configuration** command to check whether the BGP configuration is correct.

**Step 4** Check that OSPF and BGP protocols import routes from each other.

OSPF and BGP should import routes from each other to produce corresponding routes.

Run the **display current-configuration** command to check the current protocol configuration.

**Step 5** Check that the domain ID is configured correctly.

The domain ID affects the LSA in the following ways:

- When the domain ID of the remote PE is the same as that of the local PE, for Type-1, Type-2, and Type-3 LSAs on the remote PE, Type-3 LSAs are generated on the local PE; for Type-5 and Type-7 LSAs on the remote PE, Type-5 and Type-7 LSAs are generated on the local PE. (The LSA type is relevant to the domain type.)
- When the domain ID of the remote PE is different from that of the local PE, for Type-1, Type-2, and Type-3 LSAs on the remote PE, Type-5 or Type-7 LSAs are generated on the local PE; for Type-5 and Type-7 LSAs on the remote PE, Type-5 and Type-7 LSAs are generated on the local PE. (The LSA type is relevant to the domain type.)

Therefore, the correct domain ID must be configured to generate the required LSA.

**Step 6** Check that the neighbor relationship between the PE and CE is correct.

The neighbor between the PE and CE should be set up through the IGP protocol.

You can run the **display ospf peer** command to check if the neighbor relationship is correct.

If the fault persists, contact the Huawei technical personnel.

---End

## 2.4 Troubleshooting Cases

This section presents several troubleshooting cases.

### 2.4.1 Routers Cannot Learn the Internal Route After the Vlink is Configured

2.4.2 Routing Loops Occur When a CE Is Dual-homed to Two PEs, and the OSPF Multi-instance Is Configured on the PEs

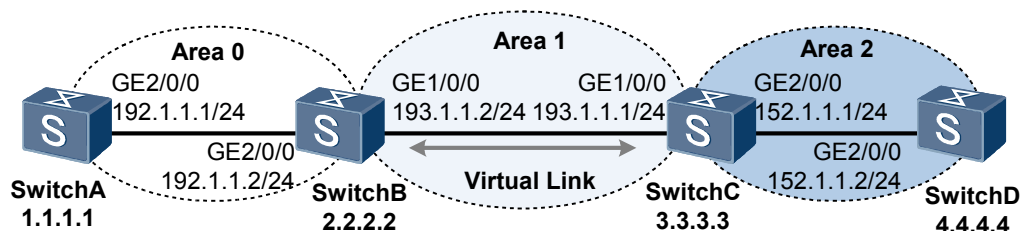
2.4.3 In Inter-AS VPN Option A, ASBRs Fail to Exchange Routes

## 2.4.1 Routers Cannot Learn the Internal Route After the Vlink is Configured

### Fault symptom

Figure 2-5 shows the OSPF virtual link (Vlink) networking.

Figure 2-5 OSPF Vlink networking



After the configurations are complete, the switches in area 2 cannot learn the internal routes in area 0.

### Fault Analysis

To locate the fault, follow the procedures described below:

1. Run the **display ospf lsdb** command to check the generation of Summary LSA of the route on ABR Switch C. The Summary LSA is normal.
2. Run the **display ospf peer** to check the neighbor relation. The neighbor relationship between Switch A, Switch B, and Switch C is normal.
3. Run the **ospf** command to enter the OSPF view to check the Vlink configuration.

OSPF prescribes that all the areas must be connected with the backbone area, namely the Area 0. Run the **vlink-peer** command to set the logical connectivity.

Check the Vlink configuration to verify if the configuration is incorrect. When specifying the peer of the Vlink, you should specify the router ID of the peer rather than the IP address of the peer interface. Thus, the Vlink neighbor can be set up. Run the **display ospf vlink** command to check the neighbor state.

### Procedure

- Step 1** Do as follows on the ABR SwitchC to configure the switch ID for the peer of the Vlink. Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf [ process-id | router-id router-id | vpn-instance vpn-instance-name ] \*** command to enable an OSPF process and enter the OSPF view.

- Step 3** Run the **area area-id** command to enter the OSPF area view.
- Step 4** Run the **vlink-peer router-id** command to create and configure a Vlink.
- Step 5** Run the **return** command to return to the user view, and then run the **save** command to save the modification.
- End

## Summary

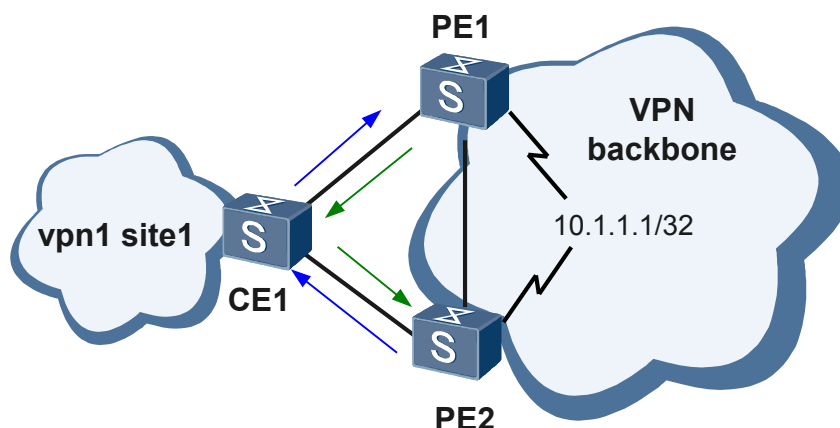
When configuring an OSPF Vlink, the Vlink neighbor relationship can be correctly set up only after the router ID for the peer of the Vlink is correctly specified.

## 2.4.2 Routing Loops Occur When a CE Is Dual-homed to Two PEs, and the OSPF Multi-instance Is Configured on the PEs

### Fault symptom

As shown in [Figure 2-6](#), CE1 is dual-homed to PE1 and PE2, and the OSPF multi-instance is configured on PE1 and PE2. CE1 and PE1 exchange routes by means of OSPF; CE1 and PE2 exchange routes by means of OSPF; PE1 and PE2 exchange routes by means of IBGP. PE1 and PE2 import a BGP route with the destination address being 10.1.1.1/32 from the VPN backbone network, and then advertise the route to CE1 through OSPF.

**Figure 2-6** Networking diagram of a dual-homed CE



After the preceding configurations, it is detected that routing loops and route flapping occur.

### Fault Analysis

To locate the fault, follow the procedures described below:

- Run the following commands on PE1 and PE2:
  - **display ospf [ process-id ] lsdb summary [ link-state-id ]**
  - **display ospf [ process-id ] lsdb ase [ link-state-id ]**

- **display ospf [ process-id ] lsdb nssa [ link-state-id ]**

Check the Options field in the command output. Here, take the **display ospf [ process-id ] lsdb summary [ link-state-id ]** command as an example.

```
<Quidway> display ospf 1 lsdb summary

          OSPF Process 1 with Router ID 100.1.1.200
                Area: 0.0.0.0
                Link State Database

Type       : Sum-Net
Ls id      : 192.168.13.0
Adv rtr    : 1.1.1.3
Ls age     : 1308
Len        : 28
Options    : E
```

The command output shows that the DN bit of the Options field is not set.

According to RFC 4576, the DN bit in the Type 3, Type 5, or Type 7 LSA, which is generated when a PE running OSPF imports a BGP VPNv4 route from the backbone network, is set to avoid routing loops. The receiving router ignores the LSA with the set DN bit when performing OSPF route calculation.

In this case, PE1 and PE2 import a BGP VPNv4 route from the backbone network, and the DN bit in the generated Type 3, Type 5, or Type 7 LSA should be set to 1. The command output, however, does not contain the DN bit information. This indicates that PE1 and PE2 do not support RFC 4576. As a result, routing loops cannot be avoided by setting the DN bit.

2. Run the **display ospf [ process-id ] brief** command on PE1 and PE2 to check the route-tag value:

```
<Quidway> display ospf 1 brief

          OSPF Process 1 with Router ID 100.1.1.200
                OSPF Protocol Information
RouterID: 100.1.1.200      Border Router:
Route Tag: 0
```

The command output shows that PE1 and PE2 have different route-tag values.

By default, the PEs in the same AS have the same route-tag value. Therefore, it is concluded that the two PEs are configured with different route-tag values.

According to OSPF, to avoid routing loops, PEs with the same route-tag value do not learn routes from each other. PE1 and PE2, however, are configured with different route-tag values. This makes them learn routes from each other. As a result, the following network faults occur.

- Routing loops

- On PE1, OSPF imports a BGP route with the destination address being 10.1.1.1/32, and then a Type 5 or Type 7 LSA is generated and advertised to CE1. Then, CE1 learns an OSPF route with the destination address and next hop being 10.1.1.1/32 and PE1 respectively, and advertises it to PE2. PE2 then learns an OSPF route with the destination address and next hop being 10.1.1.1/32 and CE1 respectively. Similarly, CE1 also learns an OSPF route with the destination address and next hop being 10.1.1.1/32 and PE2 respectively. PE1 learns an OSPF route with the destination address and next hop being 10.1.1.1/32 and CE1 respectively.

As a result, CE1 has two equal-cost routes with the next hops being PE1 and PE2 respectively, whereas the next hop of the routes to 10.1.1.1/32 on PE1 and PE2 is CE1. Thus, routing loops occur.

- Route flapping
  - The priority of an OSPF route is higher than that of a BGP route. Therefore, on PE1 and PE2, the BGP route to 10.1.1.1/32 is replaced by the OSPF route. That is, in the routing tables of PE1 and PE2, the OSPF route to 10.1.1.1/32 with the next hop being CE1 is active.  
The BGP route becomes inactive, and thus the LSA generated when this route is imported by OSPF is deleted. The OSPF route, therefore, is withdrawn.  
After that, there is no OSPF route in the routing table, and the BGP route becomes active. The same process occurs repeatedly, which causes route flapping.

## Procedure

- Step 1** Do as follows on PE1 and PE2. 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 **route-tag tag** command to set the same route-tag for PE1 and PE2.
- Step 4** Run the **return** command to return to the user view, and then run the **save** command to save the modification.
- End

## Result

After the preceding operations, routing loops and route flapping are eliminated.

## Summary

In OSPF multi-instance, the DN bit and route-tag are used to avoid routing loops. PEs do not calculate the LSA with the set DN bit, and the PEs with the same route-tag value do not learn routes from each other. According to RFC 4576, setting the DN bit and identifying the route-tag value can be used to avoid routing loops. On those devices that do not support RFC 4576, generally, the route-tag value is identified to avoid routing loops. Alternatively, you can upgrade the devices to set the DN bit to avoid routing loops.

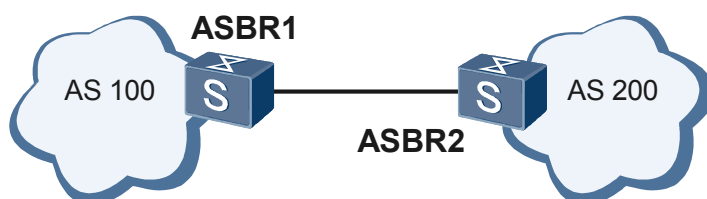
By default, the PEs in the same AS do not learn routes from each other. If these PEs are configured with different route-tag values, routing loops or route flapping may occur.

## 2.4.3 In Inter-AS VPN Option A, ASBRs Fail to Exchange Routes

### Fault symptom

As shown in [Figure 2-7](#), the inter-AS VPN Option A is configured, and AS 100 and AS 200 are connected through ASBR 1 and ASBR 2. ASBR 1 and ASBR 2 function as the PEs and exchange routes through OSPF.

**Figure 2-7** Networking diagram of the inter-AS VPN Option A



After the preceding configurations, it is detected that ASBR 1 and ASBR 2 cannot learn VPN routes from each other, and the inter-AS VPN functions improperly.

## Fault Analysis

To locate the fault, follow the procedures described below:

1. Run the **display ospf [ process-id ] brief** command on PE1 and PE2 to check the route-tag value:

```
<Quidway> display ospf 1 brief

          OSPF Process 1 with Router ID 100.1.1.200
                OSPF Protocol Information
RouterID: 100.1.1.200      Border Router:
Route Tag: 0
```

The command output shows that ASBR 1 and ASBR 2 have different route-tag values. This excludes the possibility that the same route-tag value causes PEs to fail to learn routes from each other.

2. Run the following commands on PE1 and PE2:
  - **display ospf [ process-id ] lsdb summary [ link-state-id ]**
  - **display ospf [ process-id ] lsdb ase [ link-state-id ]**
  - **display ospf [ process-id ] lsdb nssa [ link-state-id ]**

Check the Options field in the command output. Here, take the **display ospf [ process-id ] lsdb summary [ link-state-id ]** command as an example.

```
<Quidway> display ospf 1 lsdb summary

          OSPF Process 1 with Router ID 100.1.1.200
                Area: 0.0.0.0
                Link State Database

Type       : Sum-Net
Ls id      : 192.168.13.0
Adv rtr    : 1.1.1.3
Ls age     : 1308
Len        : 28
Options    : E
```

The command output shows that the DN bit in the Options field is set.

According to RFC 4576, the DN bit in the Type 3, Type 5, or Type 7 LSA, which is generated when a PE running OSPF imports a BGP VPNv4 route from the backbone network, is set to avoid routing loops. The receiving router ignores the LSA with the set DN bit when performing OSPF route calculation.

In the inter-AS VPN, PEs need to learn routes from each other. However, the DN bits in the Type 3, Type 5, or Type 7 LSAs generated on ASBR 1 and ASBR 2 are set. In this case, ASBR 1 and ASBR 2 do not process the LSA advertised by each other, and thus they cannot learn routes from each other. As a result, the inter-AS VPN functions improperly.

In the inter-AS VPN Option A, ASBRs can exchange routes through EBGP.

## Procedure

- Step 1** Do as follows on ASBR 1 and ASBR 2. Run the **system-view** command to enter the system view.



- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **ipv4-family vpn-instance vpn-name** command to enter the IPv4 VPN instance view.
- Step 4** Run the **peer ipv4-address as-number as-number** command to specify the IP address and AS number of the peer to establish the EBGP neighbor relationship. The EBGP neighbor relationship can be established only when the specified AS number of the peer is different from the local AS number.
- Step 5** Run the **return** command to return to the user view, and then run the **save** command to save the modification.
- End

## Result

After the preceding operations, ASBR 1 and ASBR 2 can learn VPN routes from each other.

## Summary

In OSPF multi-instance, to avoid routing loops, PEs are required not to calculate the LSAs with the set DN bits. The DN bits in the Type 3, Type 5, or Type 7 LSAs, which are generated when PEs running OSPF import BGP VPNv4 routes from the backbone network, are set. In this case, if the PEs in the inter-AS VPN use OSPF to exchange routes, they cannot exchange VPN routes normally.

Therefore, the PEs in the inter-AS VPN cannot exchange routes through OSPF. In the inter-AS VPN Option A, it is recommended that ASBRs exchange routes through EBGP.

## 2.5 FAQs

This section lists frequently asked questions and their answers.

### Q: Why Does OSPF Fail to Locate the Address in the VLSM Mode?

A: To locate the fault, follow the steps described below:

- Ensure that the network address is not allocated to other networks.
- Ensure that the host portion of the address is not all 1s.

For example, in a certain area:

- Two network segments are connected with the serial port
- On another network segment, there are six routers that are connected in Ethernet mode.

The following Variable Length Subnet Mask (VLSM) mode can be used in allocating addresses:

- The addresses of the two network segments connected through the serial port are 21.1.1.0/30 and 21.1.1.4/30.
- The address of the Ethernet network segment is 21.1.1.8/29.

### Q: How Can I Locate the Fault that Occurs in the Process of Configuring the Network Address/Mask and Host Address/Mask?

A: To locate the fault, follow the steps described below:

- Ensure that the host addresses belong to the same network segment and the mask is correct.
- Ensure that the host address and mask together can form a network address.
- Ensure that there is no repeated host address on the network.
- Ensure that there is no repeated network address on the network.

### Q: Why Are Import External Routes Not Displayed in the LSDB?

A: To locate the fault, perform the following the steps:

- Run the **display ospf interface** command to check that the interface that runs OSPF is not Down.
- Run the **display ospf brief** command to check that the switch importing the external route does not belong to the Stub area.
- If the external route is learned from the neighbor, run the **display ospf peer** command to check if the neighbor status is Full.
- Check whether the **lsdb-overflow-limit** command is configured and whether the number of external routes exceeds the upper limit.
- Run the **display ospf asbr-summary** command to check whether the **asbr-summary** command is used to aggregate the external route.

### Q: Why Cannot ABR Aggregate the Area Network Addresses?

A: To locate the fault, follow the steps described below:

- Run the **display current-configuration** command to check whether the network segment addresses in the area are continuous.  
If the addresses are discontinuous, divide them into several groups of continuous network segment addresses.  
Run the **abr-summary** command to configure ABR summary on the ABR for each group of continuous network segment addresses.
- Check the **filter { acl | ip-prefix *prefix* | route-policy *route-policy-name* } { import | export }** command in area view to ensure the aggregated LSA of the ABR is not filtered out.

### Q: LSA related to the OSPF Route Is Contained in the LSDB. Why Cannot the LSA related to the OSPF Route Be Found in the Routing Table?

A: To locate the fault, follow the steps described below:

- Check that the IP address is correctly configured.
- Check whether the forwarding address is known.
- Check that the route is aggregated and imported correctly.
- Check whether the list of routes that need to be advertised is configured.
- Check whether the backbone area is disconnected.

### Q: Why Cannot the Sham Link Be Set up?

A: To locate the fault, follow the steps described below:

- Using the **display ospf sham-link** command, you can check the establishment of sham-link. The status of the sham-link should not be Down.
- Using the **display mpls ldp session** command, you can check whether the session is set up. If the status of the session is not Operational, run the **display ip routing-table** command to check whether the node obtains the routes that contain the peer LSR ID.
- Check whether the VPN instance is enabled on the loopback interface on the switch.
- Ensure that the destination address of the sham link contains the loopback address of the neighboring router configured with the sham link.
- Ensure that there is only one sham link between two addresses.
- Run the **display ospf lsdb router self-originate** command to check if the Router-LSA advertised by the switch contain an link related to the configuration of the sham link.

### Q: Why Cannot the Vlink Be Set up?

A: To locate the fault, follow the steps described below:

- Ensure that the router ID of the peer is configured correctly on the local router.
- Run the **display ospf vlink** command to check whether the status of the Vlink is Full.

### Q: Why Cannot the Management Information Base (MIB) of OSPF Work Normally?

A: To locate the fault, follow the steps described below:

- Check if the network connection is normal.
- Check if there are repeated IP addresses in the network.
- If the network is busy, lessen the resending interval and the resending interval of the MIB browser.
- Check if the OSPF instance is enabled with MIB-Binding.
- The Trap address specified by the **snmp-agent target-host** command must be the same with the interface address of the MIB browser.

### Q: Why Cannot the GR Run Normally after the Standby Board Replaces the Active One?

A: The possible causes are as follows:

- GR is not correctly configured on the main board.
- GR is not correctly configured on the Helper end.
- The topology on the Helper end changes.
- The ACL filtering configuration on the Helper end is incorrect.
- The state of the interface on the Restarter end changes.

### Q: Why Cannot the LSDB Import External Routes?

A: To locate the fault, follow the steps described below:

- Check whether the Lsdb-Overflow-Limit is configured on the switch.
- Check the configuration of the PAF/License parameter.

### Q: Why Is the VPN Routes Learned from the Peer Incorrect?

A: Locate the fault according to the following procedures:

- Ensure that the **vpn-instance-capability simple** command is not executed on PE routers of two ends.
- Run the **display ospf brief** command to ensure the PEs at both ends are configured with the domain ID. Ensure that at least one ID (first-level or second-level) matches that of the other router.
- Run the **display bgp vpnv4 all peer** command to check if the BGP neighbor relation reaches the Establish state.
- Run the **display bgp vpnv4 all routing-table** command to check if the BGP route is correct.

### Q: Why Cannot IGP-Shortcut and Forwarding-Adjacency Be Forwarded?

A: To locate the faults, follow the steps described below:

- Ensure that the **enable traffic-adjustment** command or the **enable traffic-adjustment** command is configured by using the **display ospf brief** command.
- Ensure that OSPF supports the tunnel traffic modulation by using the **display interface tunnel** command.
- Ensure that the metric and the metric type are configured on the tunnel.
- Ensure that the MPLS TE is correctly configured on the tunnel interface.

### Q: How Does OSPF Calculate the Metric or Cost?

A: OSPF uses 100 Mbit/s as the reference bandwidth to calculate the cost. The formula is the reference bandwidth divided by the interface bandwidth.

For example, the cost of the Ethernet is that  $100 \text{ Mbit}/100 \text{ Mbit} = 1$ .

### Q: What Is the Resending Interval of the Link Status and the Configuration Command?

A: OSPF sends the acknowledgement packet after receiving the LSA of the updated LSA packet. If no acknowledge packet is received, the switch resends the updated packet to the peer.

The interval between the sending and resending of the updated packet is called Link-State Retransmit Interval, which can be set by using the **ospf timer retransmit interval** command.

By default, the interval is 5 seconds.

### Q: What Are the DR, BDR, and DR Other?

A: The DR refers to the designated router. The DR can advertise the link status of the network to all the switches on the network.

The BDR refers to the backup designated router.

The DR Other refers to the switch that is neither the DR nor BDR.

### Q: Why Cannot the DR and BDR in the Full State Be Seen on the Serial Link?

A: It is the normal condition. There is no DR and BDR on the P2P and P2MP networks.

## Q: Can OSPF Set up the Neighbor Relationship with the switch on the Other Subnet?

A: Neighbor relationship can be set up between two switches that are at different subnets and are connected through P2P. The situation usually occurs when the **ip unnumbered** command is configured. In other cases, two switches must be on the same subnet.

## Q: What Is the Interval for OSPF to Advertise LSAs?

A: The interval for updating OSPF LSAs is 5 seconds. In a stable network where routes need to be fast converged, you can run the **lsa-originate-interval 0** command to set the interval for updating LSAs to 0 seconds. In this case, the change of the topology or the route can be advertised to the network through the LSA. The route convergence is thus speed up.

## Q: How Can the switch on an Interface Be Disabled from Setting up the Neighbor Relation with other Routers?

A: Configuring the **silent-interface** command in the OSPF view can prohibit switches from setting up neighbor relationship through the interface. The command takes effect only on the interface on which OSPF is enabled.

If many interfaces need to be enabled with OSPF and most interfaces need to be disabled from setting up the OSPF neighbor, run the **silent-interface all** command firstly. Then run the **undo silent-interface** command to enable the specified interface.

## Q: What Is the Function of the Domain ID?

A: In general, routes that are imported from a PE are advertised as External-LSA. Routes that belong to different nodes of the same OSPF domain are advertised as Type 3 LSA (intra domain area), and the domain ID of the same OSPF should be consistent.

The function of the domain ID depends on the following two cases:

- When the domain ID of the remote PE is the same as that of the local PE, for Type 1, Type 2, and Type 3 LSAs on the remote PE, Type 3 LSAs are generated on the local PE; for Type 5 and Type 7 LSAs on the remote PE, Type 5 and Type 7 LSAs are generated on the local PE.
- When the domain ID of the remote PE is different from that of the local PE, for Type 1, Type 2, and Type 3 LSAs on the remote PE, Type 5 or Type 7 LSAs are generated on the local PE; for Type 5 and Type 7 LSAs on the remote PE, Type 5 and Type 7 LSAs are generated on the local PE.

## Q: What Is the Difference Between the Route Tag and the Default Tag?

A: The route tag is used only when the OSPF multiple-instance imports BGP. It is valid only for imported external routes from BGP.

The default tag is set for the external route imported by the public network.

## Q: What Is the Function of the Route Tag?

A: The route tag is used only in the private network.

If the tag of a Type 5 LSA is the same with the route tag of OSPF on the PE, then the route is ignored.

When the CE belongs to two private networks, the route tag is used to prevent the routing loop that occurs in the Type 5 LSA.

When a CE accesses two PEs, the PE1 sends the Type 5 LSA based on the BGP route to the CE. Then the CE sends the LSA to the PE2. Because the priority of the OSPF route is higher than that of the BGP route, the OSPF route replaces the BGP route on the PE2. Thus, the routing loop occurs.

When the route tag is configured, the LSA is ignored if the route tag of the LSA is the same with that of the PE. Thus, the routing loop is prevented.

## Q: How Is the Forwarding Address (FA) Filled out?

A: The contents of the FA vary with different situations:

- For Autonomous System External (ASE) LSAs:
  - If OSPF is not enabled on the next hop interface of the imported route, the FA that is related with the imported route is filled with 0.
  - If OSPF is enabled on the next hop interface of the imported route and one of the two conditions, that is, the next hop of ASBR is set to silent-interface for OSPF and the next hop of ASBR is defined as P2P type or P2MP type, is satisfied, the FA is still filled with 0.
  - If OSPF is enabled on the next hop interface of the imported route and the next hop of ASBR is defined as Broadcast type or NBMA type, the FA is filled with the next hop address.
  - If the imported route is the static route that is configured by specifying the egress, the imported route is processed as direct route, and the FA is filled with 0.
- For NSSA LSA:
  - If OSPF is enabled on the next hop interface of the imported route and the interface is in NSSA area X, the FA is filled with the next hop when the interface is of NBMA type or Broadcast type; the FA is filled with the local address when the interface is of P2MP type or P2P type.
  - If OSPF is not enabled on the next hop interface of the imported route, or the OSPF is enabled but the area is not X, the FA is filled with the IP address of the interface that is the first one to run OSPF in X area.

## Q: What Is the DN Bit?

On a VPN network, when a PE imports BGP routes and sends Type 3, 5, or 7 LSAs that are triggered by the BGP routes to a CE, the highest optional bit of the LSAs must be set, which is called the DN bit. The DN bit is used to prevent loops. A PE does not process the received LSA that contains a DN bit. This prevents the peer PE from learning the same LSA from the CE. In this manner, loops are avoided.

## Q: What Are the Principles of OSPF Authentication?

A: In an area, the authentication modes consist of:

- Simple
- MD5
- HMAC-MD5

On the interface, the authentication modes consist of:

- Null
- Simple
- MD5
- HMAC-MD5

The OSPF authentication is adopted according to the following rules:

- If the interface is configured with the authentication, the authentication mode on the interface is adopted.
- If the mode on the interface is Null, the interface performs no authentication.
- If no authentication is configured on the interface, the authentication mode in the area is adopted.
- If no authentication is configured in the area, no authentication is performed.

The rules of configuring OSPF authentication words are as follows:

- Plain text authentication word: In simple mode, it is a string of 1 to 8 bytes; in MD5 and HMAC-MD5 modes, it is a string of 1 to 255 bytes.
- Cipher text authentication word: In simple mode, it can be a plain text string of 1 to 8 bytes or a cipher string of 24 bytes; in MD5 and HMAC-MD5 modes, it can be a plain text string of 1 to 255 bytes or a cipher string of 20 to 392 bytes.
- Space is not allowed in the two types of authentication words.

## Q: Why Cannot the OSPF Neighbor Be Set up?

A: If the physical connection and protocols of lower layers work normally, check the OSPF parameters configured on the interface. These parameters must be consistent with that of the neighboring router. That is, area number, network segment, and mask must be consistent. (For P2P connection and virtual connection, the network, and mask can be inconsistent.)

Network type of interfaces of two neighboring routers must be consistent. If the network is broadcast network or NBMA, there should be more than one interface which has a DR priority greater than zero.

Do as follows to solve the problem:

- Run the **display ospf peer** command to check the status of the OSPF neighbor.
- Run the **display ospf interface** command to check the OSPF interface.
- Check whether the physical connection and protocols of lower layers work normally. You can test using the **ping** command. If you cannot ping the other router from the local router, it means the physical connection and protocols of lower layers are abnormal.
- Run the **display ospf brief** command to check the OSPF timer. The Dead interval should be at least 4 times of the Hello interval on the same interface.
- If the network type is NBMA, specify a neighbor manually by using the **peer ip-address** command.
- If the network type is broadcast or NBMA, there should be more than one interface whose DR priority is greater than 0.

## Q: Why Cannot OSPF Discover Routes of Other Areas?

A: Ensure that the backbone area is connected with all other areas. If a switch is configured with more than two areas, at least one area must be configured as the backbone area. The backbone area cannot be configured as Stub area. Routers in the Stub area cannot receive routes from external ASs. If an area is configured as Stub area, all switches which connect with the area should configure the area as Stub.

Do as follows to solve the problem:

- Check the status of OSPF neighbor relationship by using the **display ospf peer** command.
- Check the OSPF interface by using the **display ospf interface** command.
- Check whether the LSDB information is integrated by using the **display ospf lsdb** command.
- Check whether the area is correctly configured by using the **display current-configuration configuration ospf** command. If more than two areas are configured, one area is the backbone area and the stub command cannot be configured in the backbone area.
- If an area is Stub area, all switches in the area need to be configured with the **stub** command.
- If the virtual connection is configured, check whether the neighbor is in the normal state by using the **display ospf vlink** command.

## Q: Why Do Multiple Processes That Set Up 4000 Neighbors Consume Less CPU Than a Single Process That Sets Up 2000 Neighbors?

A: During the setup of neighbors, LSAs are flooded independently between multiple processes. In a single process, each LSA needs to be flooded to all neighbors at the same time. This consumes a large number of CPU resources.

## 2.6 Diagnostic Tools

This section describes common diagnostic tools: display commands and debugging commands.

### [2.6.1 display Commands](#)

### [2.6.2 debugging Commands](#)

### 2.6.1 display Commands

Command	Description
<b>display ospf asbr-summary</b>	Displays the summary information about the aggregated route imported by OSPF. If the IP address and mask are not specified, the summary information about all the aggregated routes imported by OSPF is displayed.
<b>display ospf abr-asbr</b>	Displays the information about ABRs and ASBRs of OSPF.
<b>display ospf brief</b>	Displays the OSPF summary information.
<b>display ospf cumulative</b>	Displays the OSPF statistics.



Command	Description
<b>display ospf error</b>	Displays the OSPF errors.
<b>display ospf graceful-restart</b>	Displays the restart status of OSPF GR.
<b>display ospf interface</b>	Displays the OSPF interface information.
<b>display ospf lsdb</b>	Displays the database information about the OSPF connection state. You can use different parameters to display one piece of the following data: <ul style="list-style-type: none"> <li>● Summary information</li> <li>● The LSA information of specified type</li> <li>● The LSA information originated by routers rather than the local router</li> <li>● The LSA information sent by the local router</li> </ul>
<b>display ospf migp-routing</b>	Displays the OSPF MIGP routing information.
<b>display ospf nexthop</b>	Displays information about the next hop.
<b>display ospf [process-id ] bfd session</b>	Displays the BFD session.
<b>display ospf peer</b>	Displays the OSPF neighbor information. The output of the command can help you to diagnose the OSPF fault and check the effect of the configuration.
<b>display ospf request-queue</b>	Displays information about the OSPF request queue. The output of the command can help you to diagnose and remove the OSPF fault.
<b>display ospf retrans-queue</b>	Displays information about the OSPF retransmission queue. The output can help to diagnose and remove OSPF faults.
<b>display ospf routing</b>	Displays information about the OSPF routing table. By choosing different parameters, you can check the route to the specified interface or the next hop.
<b>display ospf vlink</b>	Displays information about the OSPF Vlink.
<b>display ospf sham-link</b>	Displays information about all the sham links belonging to the specified OSPF process or area and all the attributes related to those sham links.

## 2.6.2 debugging Commands

Command	Description
<b>debugging ospf bfd</b>	Enables the OSPF BFD debugging. By default, the debugging is disabled.

Command	Description
<b>debugging ospf event</b>	Debugs the OSPF event.
<b>debugging ospf hot-standby</b>	Enables the debugging of the OSPF hot standby. Hot standby is also called incremental backup.
<b>debugging ospf graceful-restart</b>	Enables GR debugging of the specified OSPF process to debug the process of setting up GR.
<b>debugging ospf lsa-originate</b>	Displays the original information about the LSA.
<b>debugging ospf packet</b>	Displays the sent and received OSPF packet. The packet types include: ACK, DD, Hello, Request, Update, brief, Grace, rcv-dump, snd-dump, and all. If the packet type is not specified, information about all the packets is displayed.
<b>debugging ospf spf</b>	Displays detailed information about the SPF processing, including: spf asbr-summary, ase, brief, intra, net-summary, and nssa.

# 3 IS-IS Troubleshooting

---

## About This Chapter

This chapter describes the knowledge related to IS-IS troubleshooting, including IS-IS overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases and diagnostic tools and FAQs.

### [3.1 IS-IS Overview](#)

This section provides the information you need to know before troubleshooting IS-IS.

### [3.2 IS-IS Neighbor Troubleshooting](#)

This section describes the notes about configuring IS-IS neighbor, and provides the IS-IS neighbor troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

### [3.3 IS-IS Routing Table Troubleshooting](#)

This section describes the notes about configuring IS-IS, and provides the IS-IS routing table troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

### [3.4 IS-IS Interface Troubleshooting](#)

This section describes the notes about configuring IS-IS interface, and provides the IS-IS interface troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

### [3.5 IS-IS MT Troubleshooting](#)

This section describes the notes about configuring IS-IS MT, provides the troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

### [3.6 FAQs](#)

This section lists frequently asked questions and their answers.

### [3.7 Diagnostic Tools](#)

This section describes common diagnostic tools: display commands and debugging commands.

## 3.1 IS-IS Overview

This section provides the information you need to know before troubleshooting IS-IS.

### 3.1.1 Basic Concepts of IS-IS

#### 3.1.2 IS-IS Features Supported by the S9300

### 3.1.1 Basic Concepts of IS-IS

The Intermediate System-to-Intermediate System (IS-IS) protocol is a link state protocol, which is used inside an AS and uses the Shortest Path First (SPF) algorithm to calculate routes. There are many similarities between IS-IS and the Open Shortest Path First (OSPF).

### 3.1.2 IS-IS Features Supported by the S9300

#### Multi-instance and Multi-process

Multi-process associate a specified IS-IS process to a group of interfaces. Thus, all the process operations related to the protocol take effect only on the group of interfaces.

For the switch that supports the Virtual Private Network (VPN), each IS-IS process is associated with a specified VPN instance. Thus, all the interfaces of the process are associated with the VPN instance.

#### IS-IS Hot Standby

A switch with the distributed structure can support the IS-IS Hot Standby (HSB). In the IS-IS HSB process, IS-IS configurations on the Active Main Board (AMB) and the Slave Main Board (SMB) are kept consistent. In addition, IS-IS adopts Graceful restart (GR) to minimize the impact of HSB on traffic forwarding.

#### IS-IS Multi-Topology

IS-IS Multi-Topology (MT) indicates multiple independent IP topologies running in an IS-IS domain. Through MT, the routes are calculated respectively according to IPv4 or IPv6 networks. Thus, network shielding is implemented.

#### Local Multicast-Topology

When multicast and a Multiprotocol Label Switching Traffic Engineering (MPLS TE) tunnel are deployed in a network, the multicast function may be affected by the TE tunnel, and multicast services may become unavailable. After local MT is enabled, a separate MIGP routing table can be created for multicast to guide the forwarding of multicast packets.

#### NOTE

For details of the local MT, refer to the chapter "IS-IS" in the *Quidway S9300 Terabit Routing Switch Feature Description - IP Routing*.

## IS-IS GR

GR refers to the smooth restart of the router, which can minimize the impact of router restart on traffic forwarding. Router restart in the GR period does not lead to route flapping.

### NOTE

The S9300 supports IS-IS GR. For details of IS-IS GR, refer to the chapter "IS-IS" in the *Quidway S9300 Terabit Routing Switch Feature Description - IP Routing*.

## IS-IS TE

IS-IS TE provides MPLS the synchronized TE DataBase (TEDB) of the entire IS-IS network. When MPLS constructs the Constraint-based Routing LSP (CR-LSP), information about the traffic attribute of all the links in the local area is needed. TE is obtained through IS-IS.

### NOTE

For details of IS-IS TE, refer to the *Quidway S9300 Terabit Routing Switch Configuration Guide - MPLS*.

## Administrative Tag

The administrative tag value is associated with some attributes. It simplifies the management of routing information. By sticking to the IP address prefix, the tag is flooded throughout the IS-IS routing domain. The administrative tag carries administrative information about an IP address prefix. It is used to control the route import between different levels and areas, and control the different routing protocols and multiple IS-IS instances running on the same router.

## LSP Fragment Extension

The IS-IS LSP fragment extension enables an IS-IS router to generate more LSP fragments. By configuring the additional system ID on the switch, you can enable the fragment extension. Each system ID represents a virtual system.

Each virtual system can produce 256 LSP fragments. Through up to 50 additional system IDs, an IS-IS router can produce a maximum of 13056 LSP fragments.

## Exchange of Dynamic HostNames

The exchange mechanism of dynamic hostnames simplifies the management and maintenance of the IS-IS network. The mechanism provides the IS-IS router with the mapping from the hostname to the system ID. After the function is enabled, the system ID is replaced by the hostname of the switch in the output of the **display** command related to IS-IS.

## IS-IS Fast Convergence

- Incremental SPF (I-SPF)
- When the network topology changes, I-SPF calculates only the affected router node and maintains the Shortest Path Tree (SPT).
- Partial Route Calculation (PRC)
- After I-SPF calculation is complete, if the SPT changes, PRC updates all the leaf routes on the changed nodes. If the SPT does not change, PRC only processes the changed leaf messages.

 **NOTE**

In the S9300, only the I-SPF and PRC are adopted in the IS-IS routing calculation.

- LSP quick flooding
- When the switch receives one or more than one relatively new LSP, the LSPs less than the specified ones are flooded even before the route calculation. The LSDB synchronization is thus accelerated.
- Intelligent timer

If the network topology is stable, the first triggering time of the timer can be set extremely short in milliseconds. Thus, the timer can respond quickly to the emergency such as the interface Up and Down. Then the convergence speed can be accelerated.

If the network topology changes frequently, the interval of the intelligent timer extends automatically with the increasing in calculations. Thus, the excessive occupation of the CPU resources can be prevented.

 **NOTE**

The intelligent timer should be configured cautiously and should comply with the actual network environment and router performance.

## BFD for IS-IS

In the S9300, bidirectional forwarding detection (BFD) is used to detect the IS-IS neighbor relationship. BFD can fast detect the faults on links between IS-IS neighbors and report them to IS-IS. The fast convergence of IS-IS is thus implemented.

- Static BFD
- Static BFD means configuring BFD session parameters manually, including local and remote identifiers, and delivering BFD session setup requests manually.
- Dynamic BFD
- Dynamic BFD refers to that routing protocols dynamically trigger the establishment of BFD sessions.
- When setting up new neighbor relationship, routing protocols send parameters of neighbors and detection parameters (including source and destination IP addresses) to the BFD module. BFD then sets up sessions according to the received parameters between neighbors. Dynamic BFD is more flexible than static BFD.

 **NOTE**

BFD detects only the one-hop link between IS-IS neighbors. This is because IS-IS establishes only one-hop neighbors.

For details of BFD for IS-IS, refer to the chapter "IS-IS" in the *Quidway S9300 Terabit Routing Switch Feature Description - IP Routing*.

## 3-Way Handshake

A 3-way adjacency state is exchanged, which allows a switch to declare an adjacency to be in the UP state only when it knows that the adjacent router also receives its packets. The 32-bit extended circuit ID used in the 3-way handshake eliminates the limitation of 255 P2P links imposed currently by the local 8-bit circuit ID field.

## 3.2 IS-IS Neighbor Troubleshooting

This section describes the notes about configuring IS-IS neighbor, and provides the IS-IS neighbor troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

### 3.2.1 Typical Networking

#### 3.2.2 Configuration Notes

#### 3.2.3 Troubleshooting Flowchart

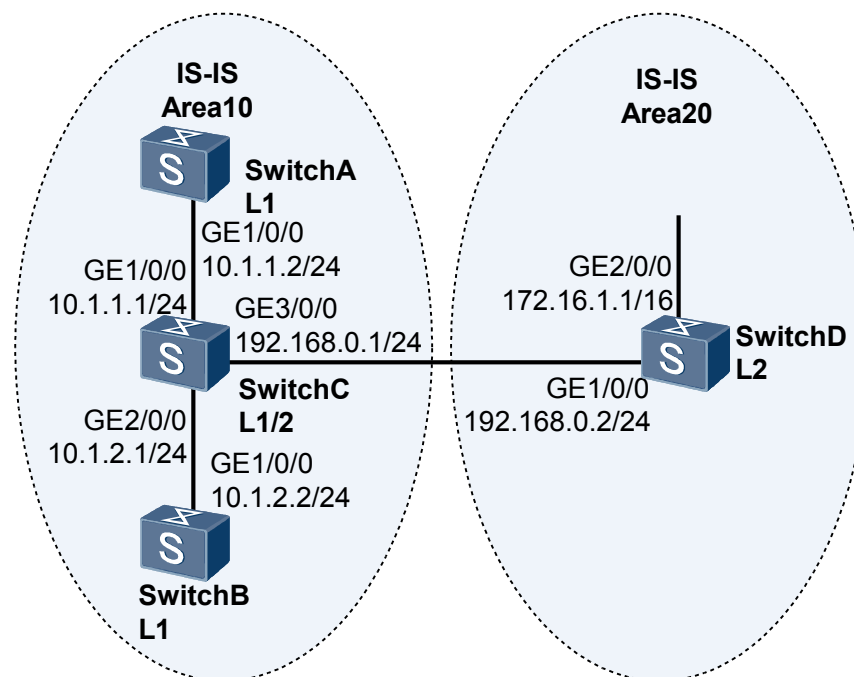
#### 3.2.4 Troubleshooting Procedure

### 3.2.1 Typical Networking

**Figure 3-1** shows the typical networking of the IS-IS neighbor.

Take this networking as an example to explain the IS-IS neighbor troubleshooting.

**Figure 3-1** IS-IS typical networking



In **Figure 3-1**:

- Switch A, Switch B, Switch C, and Switch D belong to the same AS.
- Switch A and Switch B are Level-1 routers. Switch D is a Level-2 router. As a Level-1-2 router, Switch C connects the two areas.
- The area number of Switch A, Switch B, and Switch C is 10, while that of Switch D is 20.

Through the IS-IS protocol, IP connectivity can be established among the switches.

## 3.2.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring IS-IS	Setting levels	<ul style="list-style-type: none"> <li>● The Level-1 router establishes the neighbor relationship only with the Level-1 or Level-1-2 router.</li> <li>● The Level-2 router establishes the neighbor relationship only with the Level-2 or Level-1-2 router.</li> <li>● The Level-1-2 router can establish the neighbor relationship with the Level-1, Level-2, or Level-1-2 router.</li> <li>● The Level-1 router can form the neighbor relationship only with the switch in the same area. However, the Level-2 router can construct the neighbor relationship with the cross-area router.</li> </ul> <p>To set levels, run the <b>is-level { level-1   level-2   level-1-2 }</b> command in the IS-IS view.</p>
	Configuring a network entity	<p>Different switches contain different network entities.</p> <p>To configure a network entity, run the <b>network-entity net</b> command in the IS-IS view.</p>
	Configuring an IP address	<p>Each interface on all switches must use a unique IP address.</p> <p>To configure an IPv4 address, run the <b>ip address ip-address { mask   mask-length }</b> command in the interface view.</p> <p>To configure an IPv6 address, run the <b>ipv6 address { ipv6-address prefix-length   ipv6-address/prefix-length }</b> command in the interface view.</p>



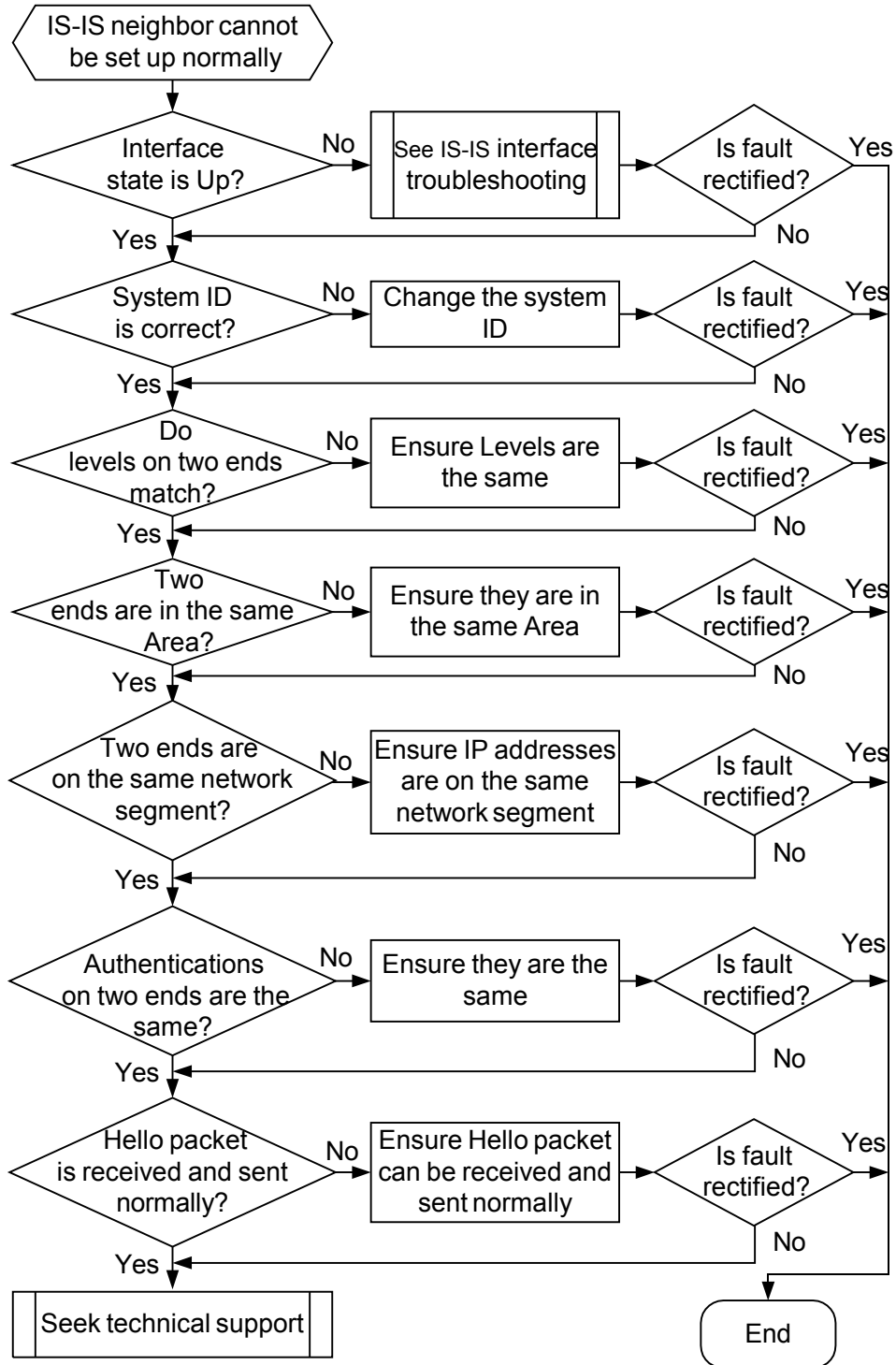
Item	Sub-item	Configuration Notes and Commands
	Configuring a routing protocol	<p>The two ends must have the same type of the routing protocol. If one end is configured with IPv4 while the other IPv6 end, the neighbor relationship cannot be set up. Before configuring IPv6, you need to enable IPv6 on the switch.</p> <p>To enable IPv4 for the IS-IS interface, run the <b>isis enable</b> command in the interface view.</p> <p>To enable IPv6 on the switch, run the <b>ipv6</b> command in the system view.</p> <p>To enable IPv6 in the IS-IS process, run the <b>ipv6 enable</b> command in the IS-IS view.</p> <p>To enable IPv6 on the interface, run the <b>ipv6 enable</b> command in the interface view.</p> <p>To configure an IPv6 address, run the <b>ipv6 address</b> command in the interface view.</p> <p>To enable IPv6 for the IS-IS interface, run the <b>isis ipv6 enable</b> command in the interface view.</p>

### 3.2.3 Troubleshooting Flowchart

After IS-IS (IPv4 or IPv6) is enabled on all the switches, a switch cannot set up the IS-IS neighbor relationship with the peer.

**Figure 3-2** shows the flowchart of IS-IS neighbor troubleshooting.

Figure 3-2 IS-IS neighbor troubleshooting flowchart



### 3.2.4 Troubleshooting Procedure

## Procedure

**Step 1** Check that the interface is Up.

Run the **display isis interface** command to check whether the interface status is Up.

If the interface status is Down or no interface information is displayed, see [3.4 IS-IS Interface Troubleshooting](#).

**Step 2** Check that the system ID is configured correctly.

Run the **display this** command in the interface view to check whether the system ID of the local switch is the same as that of the peer.

If so, run the **undo network-entity** command on the local switch to delete the system ID, and then run the **network-entity** command to configure a new system ID that is different from that of the peer.



### NOTE

The **undo network-entity** command must be used with caution.

**Step 3** Check that the levels on two ends are matched.

Run the **display current-configuration** command. Check the level on the switch and interface.

The common cause is that the levels on the two ends of the neighbor are not matching:

- Levels of the IS-IS on the two ends are different: one end is Level-1, and the other end is Level-2.  
By running the **is-level** command, you can change the levels of the IS-IS processes to be the same.
- Levels of the interface on the two ends are different: one end is Level-1, and the other end is Level-2.  
By running the **isis circuit-level** command on the interfaces, you can change the link types to be the same.

**Step 4** Check that two ends are in the same area.

Run the **display current-configuration** command to check the area configuration of the IS-IS process.

The common cause is that the two Level-1 neighbors are located in different areas.

If the two Level-1 neighbors are located in different areas, run the **network-entity** command to change the areas to be the same.

**Step 5** Check that two ends are on the same network segment.

Run the **display current-configuration** command to check whether the IP address configured on the local switch and the opposite IP address belong to the same network segment.

If the IP addresses of the two ends are not on the same segment, run the **ip address** command to change the IP address on one end to make the IP addresses of the two ends are on the same segment.

**Step 6** Check that the switches are configured with the same interface authentication mode and password.

Run the **display isis peer** command to check whether the neighbor status is displayed as Up on one end but cannot be displayed on the other end, or the neighbor status cannot be displayed on both ends.

If so, the common cause is that the Hello packet authentication failed on the interface. Then on one end, run the **isis authentication-mode** command in the interface view to modify the Hello packet authentication, and ensure that the interface authentication mode and password of this end are consistent with those on the other end.

**Step 7** Check that the Hello packet is sent and received normally.

The common fault is that the local switch receives the Hello packet sent by the peer, however, the peer cannot receive the Hello packet sent by the local switch.

If the fault occurs, run the **debugging isis adjacency** command to check whether the Hello PDU is sent and received normally.

----End

## 3.3 IS-IS Routing Table Troubleshooting

This section describes the notes about configuring IS-IS, and provides the IS-IS routing table troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

[3.3.1 Typical Networking](#)

[3.3.2 Configuration Notes](#)

[3.3.3 Troubleshooting Flowchart](#)

[3.3.4 Troubleshooting Procedure](#)

### 3.3.1 Typical Networking

See the section [Typical Networking](#).

### 3.3.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring IS-IS routing table	Setting levels	By default, IS-IS imports the route to the Level-2 database. That is, if you run the <b>import route</b> command specifying no level, IS-IS imports the route to the Level-2 routing table.  To set levels, run the <b>import route protocol [ level-1   level-2   level-1-2 ]</b> command in the IS-IS view.
	Configuring the cost type	Configure all the switches to adopt the same cost type.  To configure the cost type, run the <b>cost-style</b> command in the IS-IS view.

Item	Sub-item	Configuration Notes and Commands
	Configuring the LSP fragment extension and virtual ID	If too many routes are imported, the LSP fragment extension and adequate virtual IDs must be configured. To configure the LSP fragment extension and virtual ID, run the following commands: <ul style="list-style-type: none"> <li>● <b>lsp-fragments-extend</b> (IS-IS view)</li> <li>● <b>virtual-system</b> (IS-IS view)</li> </ul>
	Clearing the overload flag bit	After the overload flag bit is set on an IS, other ISs do not send the packets destined for other ISs to this switch. Packets with the destination address of the direct switch are still forwarded to the switch. To clear the overload flag bit, run the <b>undo set-overload</b> command in the IS-IS view.
	Configuring the size of the LSP	If the size of an LSP sent by the peer is larger than that originated by the local, the LSP will be dropped. To configure the size of the LSP, run the <b>lsp-length { originate   receive } max-size</b> command in the IS-IS view.

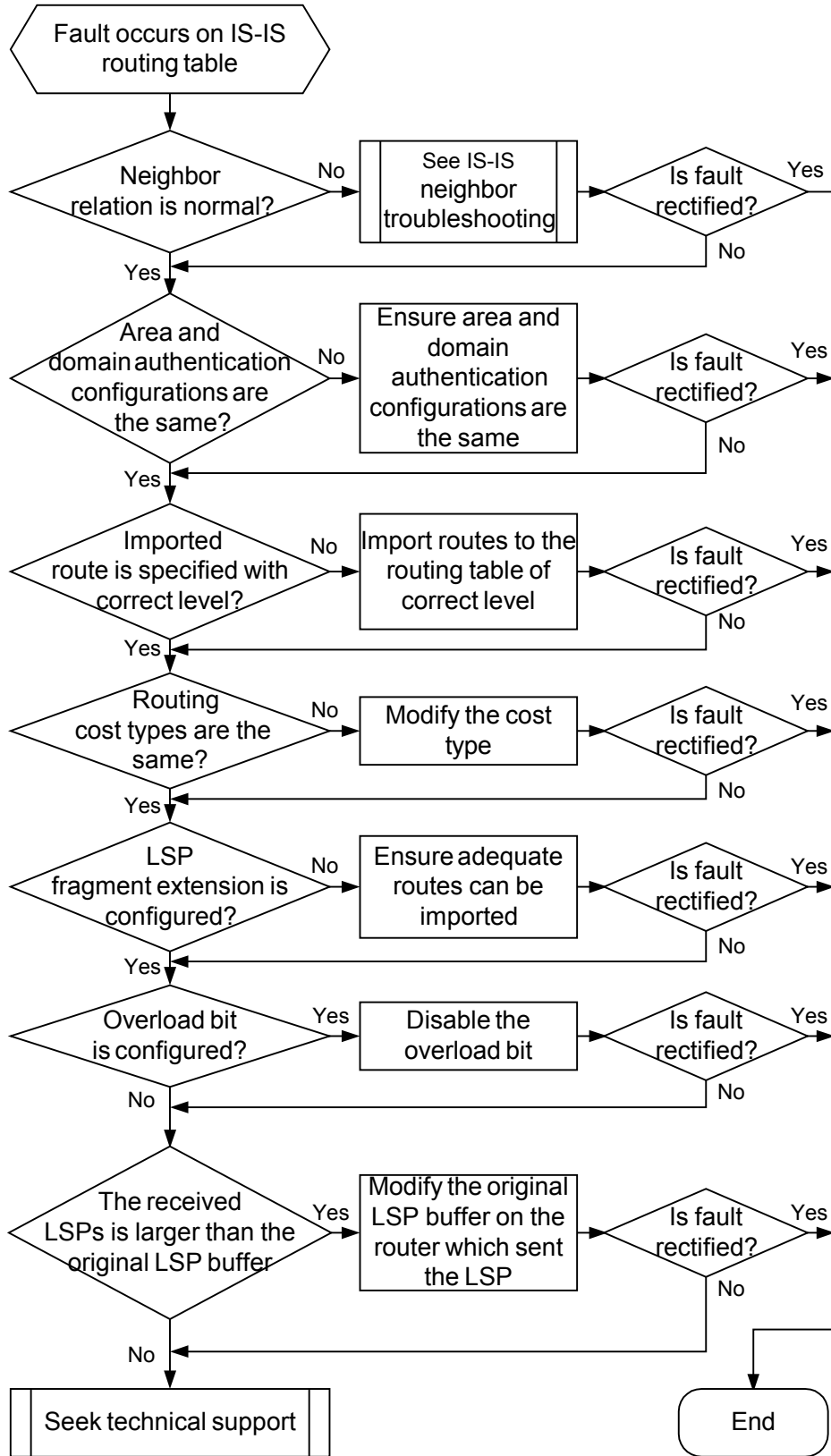
### 3.3.3 Troubleshooting Flowchart

After the IS-IS (IPv4 or IPv6) protocol is configured, the following situation may arise:

- The IS-IS Level-1 routing table does not show the imported route.
- The IS-IS Level-1/Level-2 routing table shows only 255 fragments.
- The IS-IS routing table can show only three equivalent routes.

**Figure 3-3** shows the flowchart of IS-IS routing table troubleshooting.

Figure 3-3 IS-IS routing table troubleshooting flowchart



## 3.3.4 Troubleshooting Procedure

### Procedure

**Step 1** Check that the neighbor relationship is Up.

Run the **display isis peer** command to check whether the neighbor relationship is Up.

If the neighbor status is Down, see [3.2 IS-IS Neighbor Troubleshooting](#).

**Step 2** Check that the area authentication and domain authentication of each switch are the same.

Run the **display isis lsdb** command to check whether the LSDBs on both ends of the neighbor are consistent.

If the LSDBs on both ends are different, check whether the area authentication and domain authentication on both ends are the same.

**Step 3** Check that the level is specified for the route to be imported into the routing table.

If the route is imported into the Level-1 or Level-1-2 routing table, run the **display this** command in the IS-IS view to check whether the level is specified.

**Step 4** Check that all the switches use the same cost type.

Ensure all the switches on the same network adopt the same routing cost type.

**Step 5** Check that the LSP fragment and adequate virtual system IDs are configured.

Run the **display isis statistics** command to check the number of LSP fragments used in the originating system. If the number of used LSP fragments reaches 256, you need to configure the LSP fragment extension and adequate virtual system IDs.

**Step 6** Check whether the overload flag bit is set.

If the overload flag bit is configured on a switch, the LSPs generated by the switch notify other switches that the database in the current system is overloaded and cannot forward packets. Other switches then do not send packets to this switch for forwarding unless the destination address of these packets is the directly connected address of this switch.

Run the **undo set-overload** command to clear the overload bit.

**Step 7** Check whether the size of the received LSPs is larger than the size of the original LSP buffer on the local end.

If the size of the original LSP buffer on the remote end is larger than the original LSP buffer on the local end, IS-IS on the local end discards the received LSPs.

In such a situation, run the **lsp-length** command to modify the size of the original LSP buffer on the remote end or the local end. This can ensure that the size of the LSPs sent by the peer is smaller than the size of the LSPs generated on the local end.

If the fault persists, contact the Huawei technical personnel.

----End

## 3.4 IS-IS Interface Troubleshooting

This section describes the notes about configuring IS-IS interface, and provides the IS-IS interface troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

### 3.4.1 Typical Networking

#### 3.4.2 Configuration Notes

#### 3.4.3 Troubleshooting Flowchart

#### 3.4.4 Troubleshooting Procedure

### 3.4.1 Typical Networking

In [Figure 3-1](#), all the switches are configured with the IS-IS protocol. Then run the **display isis interface** command, and you can find that an IS-IS interface is Down or has no interface information.

### 3.4.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring an IS-IS interface	Setting the MTU	<p>The MTU value on the physical interface must be greater than the LSP-Length value configured in the IS-IS process. The MTU values of interfaces on both ends of a link must be the same.</p> <p>To set the MTU, run the <b>mtu mtu</b> command in the interface view.</p> <p>To set the LSP-Length value, choose one of the following commands as required:</p> <ul style="list-style-type: none"> <li>● <b>lsp-length originate max-size</b> (IS-IS view)</li> <li>● <b>lsp-length receive max-size</b> (IS-IS view)</li> </ul>
	Configuring a link	<p>If the IS-IS link state is Down, the cause may be that the IS-IS process is not configured with the correct Network-Entity.</p> <p>To ensure that the link is Up, run the <b>network-entity net</b> command in the IS-IS view.</p>
	Configuring an IP address	<p>If the MTU status of the IS-IS interface is Up whereas the link status and IP address status of the IS-IS interface are Down, the cause may be that the interface is enabled with IS-IS but not configured with the IP address.</p> <p>To configure an IP address, run the <b>ip address ip-address { mask   mask-length }</b> command in the interface view.</p>



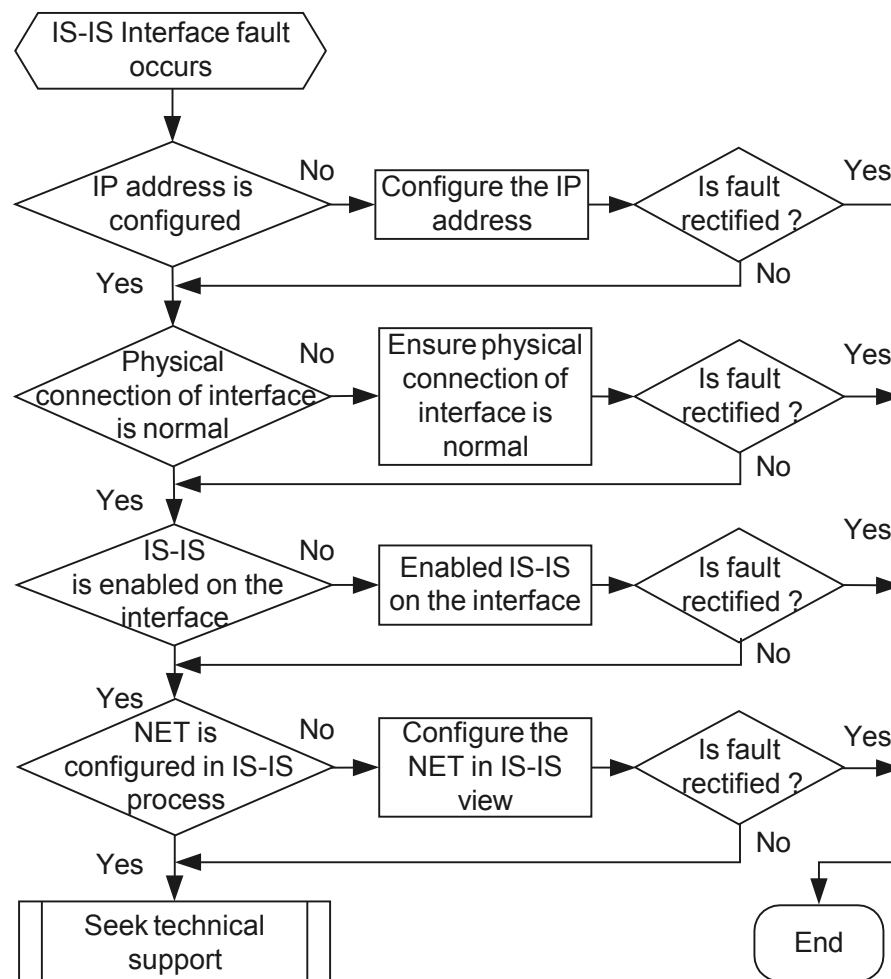
Item	Sub-item	Configuration Notes and Commands
	Configuring a P2P interface	The interface status is Up only when the following conditions are satisfied: <ul style="list-style-type: none"> <li>● The interfaces of switches on both ends are enabled with IS-IS.</li> <li>● The interfaces are configured with valid IP addresses.</li> <li>● The MTU values of the interfaces are the same.</li> </ul> To configure a P2P interface, run the <b>isis enable</b> command in the interface view.

### 3.4.3 Troubleshooting Flowchart

After the configuration of the IS-IS protocol on all the switches, the IS-IS interface state is Down.

Figure 3-4 shows the flowchart of the IS-IS interface troubleshooting.

Figure 3-4 IS-IS interface troubleshooting flowchart



## 3.4.4 Troubleshooting Procedure

### Procedure

**Step 1** Check that the IP address is configured.

Run the **display ip interface brief** *ip-configured* command to check whether the interface is configured with an IP address.

If not, configure an IP address for the interface.

**Step 2** Check that the physical status and protocol status of the interface are Up.

Run the **display ip interface brief** command to check the interface status.

If the physical status and protocol status of the interface are Down, you need to check the physical connection of the interface.

**Step 3** Check that the interface is enabled with IS-IS.

Run the **display this** command in the interface view to check whether the **isis enable** command is configured on the interface. If the command is not configured, run the **isis enable** command to enable IS-IS in the interface view.

For a P2P interface, check whether the interface status of neighbor router is Up according to the preceding steps.

If the fault persists, contact the Huawei technical personnel.

**Step 4** Check that the Network Entity Title (NET) is configured in the IS-IS process.

Run the **display isis brief** command in any view to check whether NET is configured. If not, run the **network-entity** command in the IS-IS view to configure NET for the IS-IS process.

----End

## 3.5 IS-IS MT Troubleshooting

This section describes the notes about configuring IS-IS MT, provides the troubleshooting flowchart and the troubleshooting procedure in a typical IS-IS networking environment.

[3.5.1 Typical Networking](#)

[3.5.2 Configuration Notes](#)

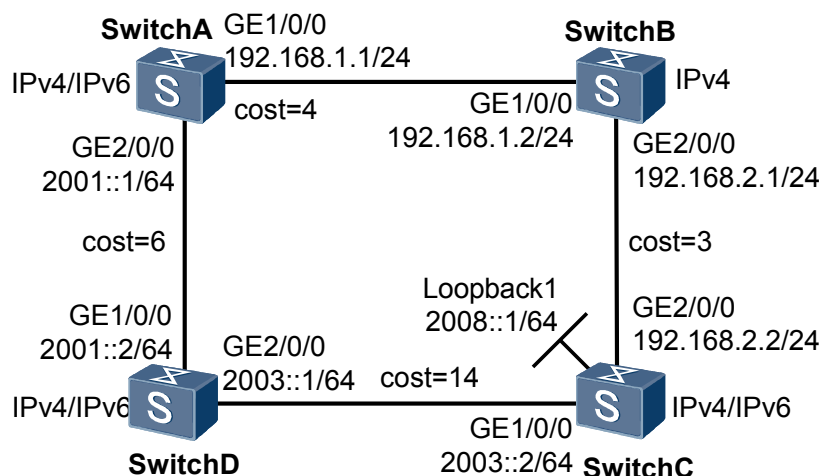
[3.5.3 Troubleshooting Flowchart](#)

[3.5.4 Troubleshooting Procedure](#)

### 3.5.1 Typical Networking

[Figure 3-5](#) shows the typical networking of the IS-IS MT.

Figure 3-5 IS-IS MT networking



In Figure 3-5:

- Switch A, Switch B, Switch C, and Switch D belong to the same AS.
- Switch A, Switch B, Switch C, and Switch D are the Level-2 routers. The area number of the switches is 10.
- Switch B supports IPv4 topology, Switch A, Switch B and Switch C all supports IPv4 and IPv6 topologies.

Through the IS-IS protocol, IP connectivity can be established among the switches.

### 3.5.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring IS-IS	Performing basic IS-IS configurations	The IS-IS process is created and NET is configured. To perform basic configurations, run the following commands in the related views: <ul style="list-style-type: none"> <li>● <b>isis</b> (system view)</li> <li>● <b>network-entity net</b> (IS-IS view)</li> </ul>

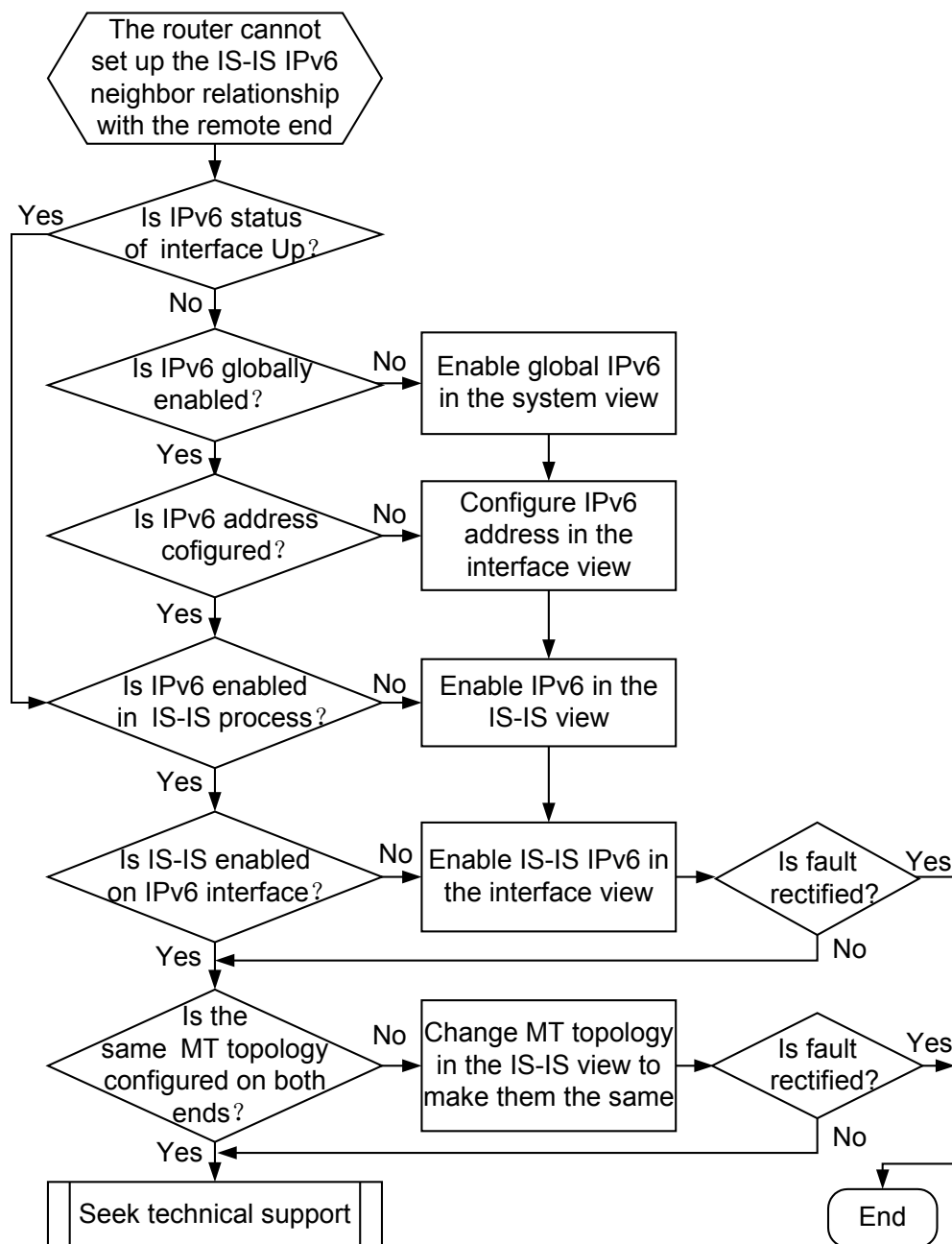
Item	Sub-item	Configuration Notes and Commands
	Configuring IS-IS IPv6	<p>To enable IPv6 on a switch, run the <b>ipv6</b> command in the system view.</p> <p>To enable IPv6 on an interface, run the <b>ipv6 enable</b> command in the interface view.</p> <p>To configure an IPv6 address for an interface, run the <b>ipv6 address { ipv6-address prefix-length   ipv6-address / prefix-length }</b> command in the interface view. Each interface must use the unique IPv6 address.</p> <p>To enable IPv6 on an IS-IS process, run the <b>ipv6 enable</b> command in the IS-IS view.</p> <p>To enable IPv6 on an IS-IS interface, run the <b>isis ipv6 enable</b> command in the interface view.</p>
	Configuring IS-IS MT	<p>The topology should be correctly configured so that switches enabled with IS-IS on both ends have the same MT.</p> <p>To configure IS-IS MT, run the <b>ipv6 enable [ topology { compatible [ enable-mt-spf ]   ipv6   standard } ]</b> command in the IS-IS view.</p>

### 3.5.3 Troubleshooting Flowchart

After the configuration of the IS-IS (IPv4 or IPv6) protocol on all the switches, the switch cannot set up the IS-IS IPv6 neighbor relationship with the peer.

[Figure 3-6](#) shows the flowchart of IS-IS neighbor troubleshooting.

Figure 3-6 IS-IS MT neighbor troubleshooting flowchart



### 3.5.4 Troubleshooting Procedure

#### Procedure

- Step 1** Run the **display ipv6 interface brief** command to check that the IPv6 status of the interface is Up.  
 If yes, go Step 4.

If not, perform the operations according to the flowchart.

**Step 2** Check that global IPv6 is enabled.

If not, run the **ipv6** command in the system view to enable global IPv6.

**Step 3** Check that an IPv6 address is assigned to the interface.

If not, run the **isis ipv6 enable** command in the interface view to enable IPv6 on the interface, run the **ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }** command to assign an IPv6 address.

**Step 4** Check that IPv6 is enabled in an IS-IS process.

If not, run the **ipv6 enable** command in the IS-IS view to enable IPv6 in the IS-IS process.

**Step 5** Check that the interface is enabled with an IS-IS process.

If not, run the **isis ipv6 enable** command on the interface to enable an IS-IS process.

**Step 6** Check that switches enabled with IS-IS have the same MT topology.

In the IS-IS process, run the **display this** command to check whether switches enabled with IS-IS have the same MT topology through MT attributes. The MT attributes are as follows:

- **standard**: includes only the topology with the MT ID as 0.
- **compatible**: includes the topologies with the MT IDs as 0 and 2.
- **compatible enable-mt-spf**: includes the topologies with the MT IDs as 0 and 2.
- **ipv6**: includes only the topology with the MT ID as 2.

In order that switches on both ends include the topologies with the same MT ID, run the **ipv6 enable [ topology { compatible [ enable-mt-spf ] | ipv6 | standard } ]** command.

If the fault persists, contact the Huawei technical personnel.

---End

## 3.6 FAQs

This section lists frequently asked questions and their answers.

### Q: Why Cannot the Feature of the IS-IS Protocol Be Configured?

A: The cause may be that the user is not allowed to configure the feature.

Check the License to confirm whether users obtain the license for configuring various features.

### Q: Why Is the LSDB Not Refreshed After the IS-IS Protocol Is Disabled on the Interface or the Interface Is Shut Down?

A: After the IS-IS protocol is disabled on the interface or the interface is shut down, IS-IS responds to this change and performs the internal processing. As a result, there is a certain delay for refreshing the LSDB.

### **Q: After the Physical Links of a Router and Those of Another Router Are Interconnected, Information About the Peer Neighbor Is Not Displayed When the display isis peer Command Is Used? That Is, Why Cannot the Neighbor Relationship Be Set Up?**

A: The possible causes are:

- The levels, area numbers, and interface authentication types and passwords of the two switches are different.
- The system IDs of the two switches are configured to be the same.

To rectify the fault, see [3.2 IS-IS Neighbor Troubleshooting](#).

### **Q: The IS-IS LSDB Does Not Show the Tag Value. How to Rectify the Fault?**

A: To locate the fault, do as follows:

- If the tag value is configured but cannot be found in the IS-IS LSDB, check whether the cost type is configured.
- If the cost style is not specified, run the **cost-style** command to set the cost style to wide, wide-compatible, or compatible, and ensure the cost styles of the switches are consistent. Only the cost styles wide, wide-compatible, and compatible support tags.

### **Q: The IS-IS TE Database Does Not Show the TE Link and Network Information. How to Rectify the Fault?**

A: To locate the fault, do as follows:

- If the database does not show the link or network information after the IS-IS TE is configured, check whether the MPLS TE is configured globally and on the interface.
- If not, enable the MPLS TE globally and on the interface.

### **Q: How Does IS-IS Calculate the Metric or Cost ?**

A: IS-IS has three modes to calculate the link cost. They are listed in the descending order of the priority:

- Interface cost: The link cost is set for a single interface.
- Global cost: The link cost is set for all the interfaces in the specified IS-IS process.
- Automatic calculation: The link cost is calculated automatically according to the interface bandwidth.

If the IS-IS link cost is not calculated according to the preceding three modes, the link cost is 10 by default.

The configuration of the bandwidth reference takes effect only when the cost type is Wide or wide-compatible.

Here, the cost of each interface is calculated by the formula:  $\text{cost} = (\text{bandwidth} - \text{reference} / \text{bandwidth}) \times 10$ .

When the cost type is narrow, narrow-compatible, or compatible, the cost of each interface is calculated as shown in [Table 3-1](#).

**Table 3-1** Relationship between the interface cost and the bandwidth

Cost	Interface Bandwidth Range
60	interface bandwidth $\leq$ 10 Mbit/s
50	10 Mbit/s < interface bandwidth $\leq$ 100 Mbit/s
40	100 Mbit/s < interface bandwidth $\leq$ 155 Mbit/s
30	155 Mbit/s < interface bandwidth $\leq$ 622 Mbit/s
20	622 Mbit/s < interface bandwidth $\leq$ 2.5 Gbit/s
10	2.5 Gbit/s < interface bandwidth

 **NOTE**

Run the **isis cost** command in the interface view to change the cost of loopback interface.

**Q: In the Interface View, Which IS-IS Packet Timers Can Be Configured?**

A: In the interface view, the configurable IS-IS packet timers are as follows:

Item	Configuration Command	Default
Interval for sending the Hello packet	<b>isis timer hello</b> <i>hello-interval1</i> [ <b>level-1</b>   <b>level-2</b> ]	10s
Number of Hello packets that are not continuously received before IS-IS advertises the neighbor as Down	<b>isis timer holding-multiplier</b> <i>number</i> [ <b>level-1</b>   <b>level-2</b> ]	3
Interval for sending the LSP packet	<b>isis timer lsp-throttle</b> <i>throttle-interval</i> [ <b>count</b> <i>count</i> ]	50ms
Interval for retransmitting LSPs on a P2P link	<b>isis timer retransmit</b> <i>retransmit-interval</i>	5s
Interval for sending CSNPs on the broadcast network (is valid only for the DIS)	<b>isis timer csnp</b> <i>csnp-interval</i> [ <b>level-1</b>   <b>level-2</b> ]	10s

**Q: In the IS-IS View, Which IS-IS Timers Can Be Configured?**

A: In the IS-IS view, the configurable IS-IS timers are as follows:

Item	Configuration Command	Default
LSP refreshing period	<b>timer lsp-refresh</b> <i>refresh-time</i>	900s



Item	Configuration Command	Default
LSP expiration interval	<b>timer lsp-max-age</b> <i>age-time</i>	1200s
the maximum duration for SPF calculation	<b>spf-slice-size</b> <i>duration-time</i>	4ms
Delay for generating an LSP	<b>timer lsp-generation</b> <i>max-interval</i> [ <i>init-interval</i> [ <i>incr-interval</i> ] ] [ <b>level-1</b>   <b>level-2</b> ]	2s
Interval for the SPF calculation	<b>timer spf</b> <i>max-interval</i> [ <i>init-interval</i> [ <i>incr-interval</i> ] ]	5s

### Q: What Is the DIS? How Is the DIS Elected?

A: DIS is abbreviated from Designated Intermediate System.

The system with the highest priority is elected as the DIS. When more than one system has the same precedence, the one with the largest MAC address is the DIS.

The DIS can broadcast the CSNP packets to other routers on the network, and these routers can synchronize its LSDBs according to the CSNP packets.

### Q: How to Prevent a Router Interface from Establishing the IS-IS Neighbor Relationship with the Peer Interface?

A: Run the **isis silent** command on the interface of a switch to disable the interface from setting up the neighbor relationship with the peer interface. The network segment to which the interface belongs is advertised.

### Q: Why Cannot the IS-IS Process Be Set Up?

A: If too much CPU or too many memory resources are occupied, the IS-IS process cannot be set up.

Check the usage of the CPU and memory. Release some resources if necessary.

### Q: Why Cannot the Level-1 Router Generate the Default Route to Other Areas?

A: The Level-1 router can generate the default route to other areas only after it sets up the Level-1 neighbor relationship with the Level-1-2 router in the local area. If the Level-1-2 router at the area border has Level-2 neighbors in different areas, the Level-1-2 router sets the Attachment (ATT) flag bit in the generated LSPs. This indicates that the Level-1-2 router is connected to other areas and has routes to other areas. In this case, after all the Level-1 routers in the same area receive this LSP, the default route with the destination address as 0.0.0.0 is generated.

### Q: Why IS-IS Cannot Learn the Route Correctly?

A: The possible causes for the fault are as follows:

- The neighbor cannot be set up normally.
- The cost styles are different on the two ends.

- Different IPv4 and IPv6 topologies lead to the non-existence of the next hop.
- The route is filtered out by the routing policy. The route cannot be added into the URT.
- LSP fragments are filled up. As a result, the Neighbor TLV is lost. If excessive routes are imported and the number of used LSP fragments reaches 255, you must configure the LSP fragment extension.
- The area or domain authentication configured on the switch fails. As a result, LSDBs are not synchronized.

### **Q: Run the circuit-cost Command in the IS-IS View to Set the Global Cost on the IS-IS Interface to 16777215. Why Cannot the Neighbor Figure Out the Route?**

A: If the cost is 16777215, the Neighbor TLV with the cost 16777215 produced on the link cannot be used to calculate the route. It is only used in transmitting information about TE.

### **Q: Why Cannot the IS-IS Neighbor Be Set up even After IS-IS Is Enabled on the ATM Interface?**

A: IS-IS supports only broadcast links and P2P links. ATM belongs to an NBMA network. IS-IS cannot run on the Point to Multi Point (P2MP) link, therefore, the ATM interface should be configured as an IS-IS sub-interface. Note that the type of the sub-interface cannot be P2MP.

### **Q: Is There Any Requirement for the Configuration of IS-IS Authentication Password?**

A: The IS-IS authentication type can be classified into the plain text mode, the encrypted text mode and the keychain mode. The rules are shown as below:

- The authentication password in plain text mode (the simple mode) is a string of 1 to 16 characters. The string can be composed of letters, numbers, or combination of letters and numbers.
- The authentication password in encrypted text mode (the Message Digest 5 mode) is also a string. The string can be composed of letters, numbers, or combination of letters and numbers. The string with 1 to 255 characters corresponds to the plain text password, whereas the string with 20 to 392 characters corresponds to the encrypted text password.
- The authentication password in keychain mode is a string of 1 to 47 characters. The string can be composed of letters, numbers, or combination of letters and numbers. The meaning of the authentication password is the keychain that changes with time and is transmitted after being encrypted by MD5.
- None of the authentication password can contain spaces.

### **Q: Which Types of Packets Carry the MT TLV and What Is the Function of the MT TLV?**

A: The MT TLV indicates that the switch supports MT. This TLV carried in Hello packets is used to set up the neighbor relationship on MT. The TLV is carried in the LSP with the fragment number as 0. Thus, the advertising router can participate in the calculation of routes related to MT.

### Q: What Is the Difference Between Standard IPv6 and IPv4 When the Neighbor Relationship Is Set up on MT?

A: There is no difference. When IPv4 and IPv6 are configured, and IPv4 and standard IPv6 share the topology with the MT ID as 0, that is, the standard topology, they advertise the same neighbor TLV on the LSP.

### Q: What Is the Difference Between the P2P Interface and Broadcast Interface When the Neighbor Relationship Is Set up on MT?

A: On the P2P interface, the neighbor relationship can be set up only when switches on both ends include the topologies with the same MT ID. On the broadcast interface, the neighbor relationship can be set up regardless of whether switches have the same topology type (the same MT ID); however, the interfaces of these two switches must be from the same IP address family, that is, they are either IPv4 or IPv6.

### Q: How to Differentiate the Overload and ATT Bits in the LSDB in IPv4 Topology and Different Modes of MT?

A: You can learn the status of Attachment and Overload of the system through the ATT and OL bits in the LSP packet header.

- In **standard** and **compatible** modes of IPv4 and IPv6, the topology with the MT ID as 0 is used and ATT and OL bits in the LSP packet header are shared.
- In the modes of **compatible enable-mt-spf** and **ipv6**, the system that advertises the MT TLV of the LSP supports the topology with the MT ID as 2, which indicates the status of Attachment and Overload of IPv6.

### Q: Why the Costs of the ipv6 reachability TLV and MT ipv6 reachability TLV Do Not Change After isis ipv6 cost 25 Is Configured?

A: IPv4 and standard IPv6 share the topology with the MT ID as 0.

- When the **ipv6 enable topology standard** command is used in the IS-IS view, the default costs of the ipv6 reachability TLV and the MT ipv6 reachability TLV change with the cost set by the **isis cost** command.
- When the **ipv6 enable topology compatible** command or the **ipv6 enable topology compatible enable-mt-spf** command or the **ipv6 enable topology ipv6** command is used in the IS-IS view, the default cost of the ipv6 reachability TLV and the MT ipv6 reachability TLV changes with the cost set by the **isis ipv6 cost** command.

### Q: What Are the Functions of the Commands of ipv6 enable topology compatible and ipv6 enable topology compatible enable-mt-spf?

A: On the network where IS-IS is run, if the **ipv6 enable topology standard** command used on all the switches changes to the **ipv6 enable topology ipv6** command, routing information changes suddenly.

This is because the switch uses the topology with the MT ID as 0 in **standard** mode and uses the topology with the MT ID as 2 in **ipv6** mode. They do not have the same MT topology. As a result, IPv6 routes are lost and restored in a period. Importing the two modes of **compatible** and **compatible enable-mt-spf** can effectively avoid the loss of IPv6 routing information in the period.

- From **standard** to **compatible**, the topology with the MT ID as 0 is shared.
- From **compatible** to **compatible enable-mt-spf**, the topology with the MT ID as 0 and the topology with the MT ID as 2 are shared.
- From **compatible enable-mt-spf** to **ipv6**, the topology with the MT ID as 2 is shared.

This ensures that all switches have the same MT topology type and IPv6 routes are not lost when the MT mode switches at any time.

### Q: Why Level-1 and Level-2 Do Not Exist When the isis authentication-mode Command Is Used to Set IS-IS Authentication on the Interface?

A: The parameters of **level-1** and **level-2** are displayed on the Ethernet interface only and you must first use the **isis enable** command to enable the Ethernet interface.

## 3.7 Diagnostic Tools

This section describes common diagnostic tools: display commands and debugging commands.

[3.7.1 display Commands](#)

[3.7.2 debugging Commands](#)

### 3.7.1 display Commands

Command	Description
<b>display isis interface</b>	Displays information about the IS-IS interface.
<b>display isis lsdb</b>	Displays the LSDB information about IS-IS.
<b>display isis mesh-group</b>	Displays the configuration of the Mesh Group on the interface of the current switch.
<b>display isis name-table</b>	Displays the mapping from the local router name to the system ID.
<b>display isis peer</b>	Displays information about the IS-IS peer.
<b>display isis graceful-restart status</b>	Displays the status of IS-IS graceful restart (IS-IS GR).
<b>display isis route</b>	Displays the IS-IS routing information. If neither IPv4 nor IPv6 is specified, all IPv4 and IPv6 IS-IS routing information is displayed. By default, the level is Level-1 and Level-2. If the parameter <b>verbose</b> is used, the IS-IS routing information with the preference and administrative tag is displayed.
<b>display isis spf-log</b>	Displays the IS-IS SPF calculation log.
<b>display isis statistics</b>	Displays the statistics of the IS-IS process.

Command	Description
<b>display isis traffic-eng statistics</b>	Displays IS-IS TE information, including advertisement information, link information, network information, statistics, and extended sub-TLV information.

## 3.7.2 debugging Commands

Command	Description
<b>debugging isis adjacency</b>	Debugs the IS-IS adjacency relationship.
<b>debugging isis all</b>	Enables all the debugging of IS-IS.
<b>debugging isis authentication-error</b>	Debugs the IS-IS authentication error.
<b>debugging isis bfd</b>	Debugs IS-IS BFD.
<b>debugging isis checksum-error</b>	Debugs the LSP checksum error of IS-IS.
<b>debugging isis circuit-information</b>	Debugs the IS-IS interface (circuit).
<b>debugging isis configuration-error</b>	Debugs the IS-IS configuration error.
<b>debugging isis datalink-receiving-packet</b>	Debugs the receiving of the packet on the data link layer.
<b>debugging isis datalink-sending-packet</b>	Debugs the sending of the packet on the data link layer.
<b>debugging isis event</b>	Debugs the IS-IS event.
<b>debugging isis general-error</b>	Debugs the IS-IS protocol error.
<b>debugging isis graceful-restart</b>	Debugs the IS-IS GR event.
<b>debugging isis ha-events</b>	Debugs the IS-IS hot standby event.
<b>debugging isis interface-information</b>	Debugs the IS-IS data link layer.
<b>debugging isis ldp-sync</b>	Debugs the synchronization status change of LDP and IS-IS.
<b>debugging isis memory-allocating</b>	Debugs the IS-IS memory allocation.
<b>debugging isis miscellaneous-errors</b>	Debugs various IS-IS errors.
<b>debugging isis receiving-packet-regular-content</b>	Debugs the details of received IS-IS packets.

Command	Description
<b>debugging isis sending-packet-regular-content</b>	Debugs the details of sent IS-IS packets.
<b>debugging isis self-originate-update</b>	Debugs the IS-IS local update of the packet.
<b>debugging isis snp-packet</b>	Debugs the CSNP/PSNP packet of IS-IS.
<b>debugging isis spf-event</b>	Debugs the SPF event of IS-IS.
<b>debugging isis spf-prc</b>	Debugs the IS-IS SPF calculation process.
<b>debugging isis spf-summary</b>	Debugs the timing and statistics of the IS-IS SPF calculation.
<b>debugging isis spf-timer</b>	Debugs the SPF timer of IS-IS.
<b>debugging isis task-error</b>	Debugs the IS-IS service status.
<b>debugging isis timer</b>	Debugs the IS-IS timer.
<b>debugging isis traffic-eng</b>	Debugs the IS-IS TE advertisement or event.
<b>debugging isis update-packet</b>	Debugs IS-IS update packets.
<b>debugging isis update-process</b>	Debugs an IS-IS update process.

---

# 4 BGP Troubleshooting

---

## About This Chapter

This chapter describes the knowledge related to BGP troubleshooting, including BGP overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases and diagnostic tools and FAQs.

### [4.1 BGP Overview](#)

This section describes the knowledge you need to know before troubleshooting the Border Gateway Protocol (BGP).

### [4.2 BGP Connection Troubleshooting](#)

This section describes the notes about configuring BGP, and provides the BGP peer troubleshooting flowchart and the troubleshooting procedure in a typical BGP networking environment.

### [4.3 Accidental Interruption of BGP Connection Troubleshooting](#)

This section describes the notes about configuring BGP, and provides the accidental interruption of BGP connection troubleshooting flowchart and the troubleshooting procedure in a typical BGP networking environment.

### [4.4 Route Loss Troubleshooting When BGP Exchange Update Messages](#)

This section describes the notes about configuring BGP, and provides the route loss troubleshooting flowchart and the troubleshooting procedure in a typical BGP networking environment.

### [4.5 Troubleshooting Cases](#)

This section presents several troubleshooting cases.

### [4.6 FAQs](#)

This section lists frequently asked questions and their answers.

### [4.7 Diagnostic Tools](#)

This section describes common diagnostic tools: display commands and debugging commands.

## 4.1 BGP Overview

This section describes the knowledge you need to know before troubleshooting the Border Gateway Protocol (BGP).

### 4.1.1 Introduction to BGP

### 4.1.2 BGP Routing Attributes

### 4.1.3 BGP Policy

## 4.1.1 Introduction to BGP

The Border Gateway Protocol (BGP) is a dynamic routing protocol used between ASs. The current BGP version is BGP-4 (RFC 4271).

## 4.1.2 BGP Routing Attributes

The BGP routing attribute consists of a set of parameters. It describes certain routes in detail, and thus enables BGP to filter and choose the route.

The BGP routing attribute falls into the following four categories.

**Table 4-1** Category of BGP route attribute

Category	Description
Well-Known mandatory	All the BGP routers can recognize the attribute. The attribute is mandatory in the Update message. Without the attribute, the routing information is in the faulty state.
Well-Known discretionary	All the BGP routers can recognize the attribute. It is optional in the Update message.
Optional transitive	It is a transitive attribute between the ASs. The BGP router may not support the attribute. However, the router still receives the route with the attribute and advertises to the other peers.
Optional non-transitive	If the BGP router does not support the attribute, the corresponding Update message is ignored and not advertised to the other peers.

The major attributes and their corresponding categories of the BGP route are as follows:



**Table 4-2** Several types of BGP route attributes

Attribute	Description	Category
Origin	It defines the source of the path information, including: <ul style="list-style-type: none"> <li>● IGP: It has the highest precedence.</li> <li>● EGP: It has precedence next to that of IGP.</li> <li>● Incomplete: It is of the lowest precedence. It indicates that the source of the route cannot be figured out.</li> </ul>	Well-known mandatory
AS_Path	It records all the numbers of the AS that the route passes by from the local device to the destination address in the reverse order.	Well-known mandatory
Next_Hop	When the route is advertised to the EBGp peer, Next_Hop is the local interface address that is connected with the peer. When the route is advertised to the IBGP peer, Next_Hop of the routing information is not changed.	Well-known mandatory
Local_Pref	It is only exchanged between the IBGP peers. It is used to decide on the optimal route when the traffic leaves the AS. The bigger the Local-Pref, the higher the precedence.	Well-known discretionary
Community	It is a set of destination addresses with the same features. It has no physical boundary and no relation with the AS on which it resides.	Optional transitive
MED	It is only exchanged between the two adjacent ASs. It decides the optimal route when the traffic enters the AS. The smaller the MED, the higher the precedence.	Optional non-transitive

### 4.1.3 BGP Policy

#### BGP Load Balancing

In BGP, the next hop of the route may not be the directly-connected neighbor of the current router. The common cause is that the next hop is not changed when the routing information is advertised between IBGPs. In this situation, BGP adopts the iterative route to find the dependent route according to the next hop address.

The S9300 supports the BGP load balancing based on the iterative route. That is, if the dependent routes are carried out through the load balancing, for example, there are three next hop addresses, BGP automatically produces three next hop addresses to guide the forwarding of the packet.

The process of the BGP load balancing is added into the BGP routing policy. That is, the BGP load balancing is carried out according to the maximum lists of routes when all the attributes with the higher precedence are the same.

 **NOTE**

For details about BGP route selection, refer to the *Quidway S9300 Terabit Routing Switch Feature Description - IP Routing*.

## Faults in the BGP Network of Large Scale and the Solution

Fault	Solution
The BGP routing table is excessively large.	Aggregate multiple routes. Thus, BGP can only advertise the aggregated route to the peer. The scale of the routing table decreases drastically.
The route flapping occurs frequently.	Use the routing damping to add up the penalty value for the flapping route. When the penalty value exceeds the suppressing threshold, the route is not added into the routing table. After multiple half lives, the penalty value decreases to the reusing threshold and then the route is added into the routing table again. At the same time, the updated packet is sent to the BGP peer.
The same attribute are configured too many times on the peers.	Adopt the peer group. Configure the same attribute to members in the group at the same time. When a peer joins a peer group, it obtains the same configuration as the other members. When the configuration of the peer group changes, the configuration of each member is changed correspondingly.
The same policy is configured on the BGP routers distributing in multiple ASs.	Adopt the community. Configure the BGP route with the community attribute. Thus, all the members in the same community share the same policy. The community attribute takes effects on the BGP peers of the same community. It is not limited by the AS.
An AS has too many IBGP peers.	<ul style="list-style-type: none"> <li>● Adopt the route reflection. Configure the router reflector (RR). The RR sets up the IBGP connection with multiple BGP routers, constituting a cluster within which the routing information is exchanged. The BGP router outside the cluster and the RR are full-meshed.</li> <li>● Adopt the confederation. Divide the confederation into sub-ASs. The IBGP peers within the AS are full-meshed. The sub-ASs keep the EBGP connection with each other.</li> </ul> <p>In the BGP network of a large scale, RR and the confederation can be adopted at the same time.</p>

The preceding solutions can be used in combination.

## 4.2 BGP Connection Troubleshooting

This section describes the notes about configuring BGP, and provides the BGP peer troubleshooting flowchart and the troubleshooting procedure in a typical BGP networking environment.

### [4.2.1 Typical Networking](#)

### [4.2.2 Configuration Notes](#)

### [4.2.3 Troubleshooting Flowchart](#)

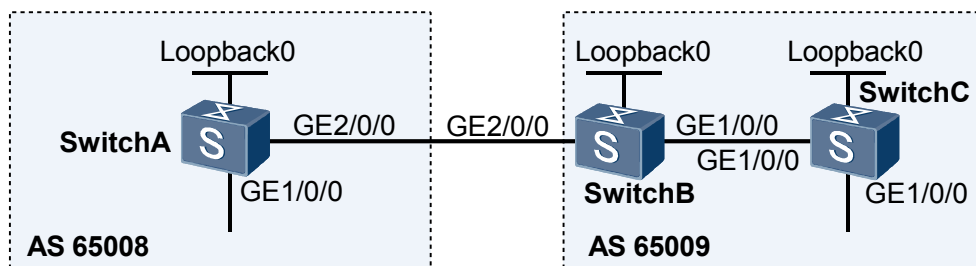
#### 4.2.4 Troubleshooting Procedure

### 4.2.1 Typical Networking

**Figure 4-1** shows the typical BGP networking.

Take the following networking as an example to explain the BGP troubleshooting.

**Figure 4-1** BGP typical networking



Device	Interface	IP Address
Switch A	GE1/0/0	8.1.1.1/24
	GE2/0/0	3.1.1.2/24
	Loopback0	10.1.1.1/32
Switch B	GE1/0/0	9.1.1.1/24
	GE2/0/0	3.1.1.1/24
	Loopback0	10.1.1.2/32
Switch C	GE1/0/0	9.1.2.1/24
	GE1/0/0	9.1.1.2/24
	Loopback0	10.1.1.3/32

In **Figure 4-1**:

- Switch A belongs to AS 65008. Switch B and Switch C belong to AS 65009. The physical interface address and Loopback0 address are shown in **Figure 4-1**.
- An EBGP connection is set up between Switch A and Switch B. On both Switch A and Switch B, the peer addresses are configured as the Loopback0 address.
- An IBGP connection is set up between Switch B and Switch C. On both Switch B and Switch C, the peer addresses are configured as the directly-connected VLANIF interface address.

### 4.2.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring BGP	Configuring an AS	The locally configured AS number must be the same as that specified on the peer. To configure an AS, run the <b>bgp as-number</b> command in the system view.
	Configuring a router ID	If router ID is not configured, the global router ID is adopted by default. The ID of the local router must be different from that of its peer. Otherwise, the connection cannot be set up. To configure a router ID, run the <b>router-id ipv4-address</b> command in the BGP view.
Configuring BGP peers	Configuring an AS	The AS number of the specified peer must be the same as that of the peer. To configure an AS, run the <b>peer ipv4-address as-number as-number</b> command in the BGP view.
	Configuring the connect-interface	If it is not configured, the physical interface directly-connected with the peer is used as the local interface of the TCP connection. The specified local interface must be the same as the address of the local router specified on the peer. To configure the connect-interface, run the <b>peer ipv4-address connect-interface interface-type interface-number</b> command in the BGP view.
	Configuring the maximum EBGP hops	By default, the directly-connected physical link should exist between the EBGP peers. If not, run the <b>peer ebgp-max-hop</b> command to permit the EBGP peers to set up the TCP connection through multiple hops. To configure maximum EBGP hops, run the <b>peer ipv4-address ebgp-max-hop [ hop-count ]</b> command in the BGP view.
Configuring the advertisement of BGP local routes	Configuring the network	The local routes to be advertised must exist in the local IP routing table. Using the routing policy, you can control the advertised route more flexibly. To configure the network, run the <b>network ipv4-address [ mask   mask-length ]</b> command in the BGP-IPv4 unicast address family view.

Item	Sub-item	Configuration Notes and Commands
	Configuring BGP to import routes	Configure BGP to import routes of other protocols, including IGP, Static, and Direct. To configure the import policy, run the <b>import-route protocol</b> command in the BGP-IPv4 unicast address family view.
Configuring route aggregation	Configuring automatic summary	Aggregates only the route imported by the <b>import-route</b> command into the route of the natural segment. To configure automatic summary, run the <b>summary automatic</b> command in the BGP-IPv4 unicast address family view.
	Configuring manual aggregation	You can manually aggregate the route imported by the <b>network</b> command and the <b>import</b> command, and the route learned from other peers. The aggregated route does not take part in the further aggregation. The precedence of the manual aggregation is higher than that of the automatic aggregation. To configure manual aggregation, run the <b>aggregate ipv4-address { mask   mask-length }</b> command in the BGP-IPv4 unicast address family view.
Configuring the BGP routing-advertisement policy	Configuring the policy for filtering routes to be exported	It takes effect when the route is advertised to all the BGP peers. To configure the policy for filtering routes to be exported, run the <b>filter-policy { acl-number   acl-name acl-name   ip-prefix ip-prefix-name } export</b> command in the BGP-IPv4 unicast address family view.
	Configuring the policy for filtering routes to be exported to a specified peer	It takes effect only when the route is advertised to the specified BGP peer. To configure the policy for filtering routes to be exported to a specified peer, run the <b>peer ipv4-address route-policy route-policy-name export</b> command in BGP-IPv4 unicast address family view.
Configuring the BGP receiving policy of the routing information	Configuring the policy for filtering routes to be imported	It takes effect when the route is received from all the BGP peers. To configure the policy for filtering routes to be imported, run the <b>filter-policy { acl-number   acl-name acl-name   ip-prefix ip-prefix-name } import</b> command in the BGP-IPv4 unicast address family view.

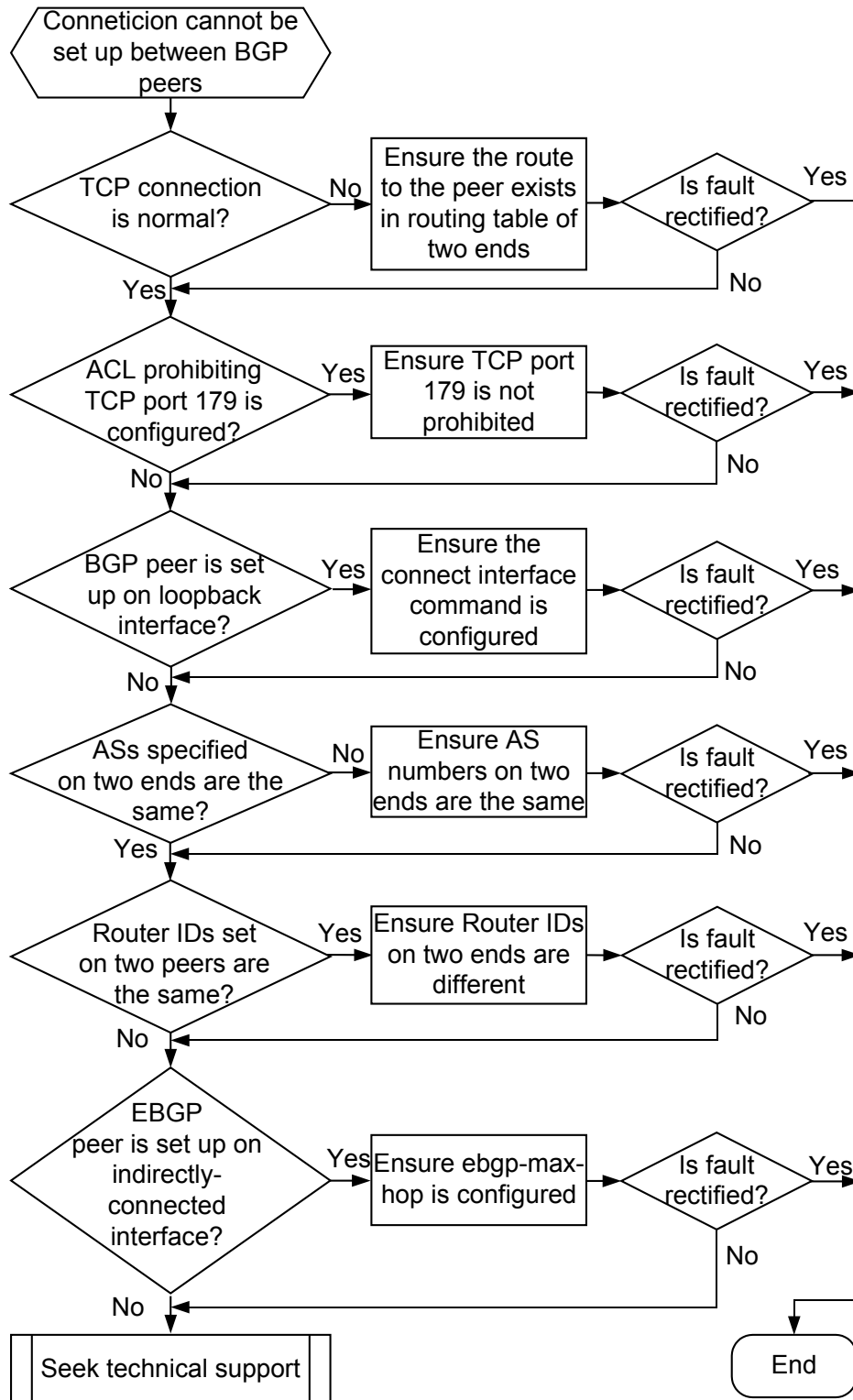
Item	Sub-item	Configuration Notes and Commands
	Configuring the policy for filtering routes to be imported from a specified peer	It takes effect only when the route is received from the specified BGP peer.  To policy for filtering routes to be imported from a specified peer, run the <b>peer ipv4-address route-policy route-policy-name import</b> command in the BGP-IPv4 unicast address family view.

## 4.2.3 Troubleshooting Flowchart

In the network shown in [Typical Networking](#), after the BGP peer is configured for each switch, the neighbor relation cannot be set up between the BGP peers.

[Figure 4-2](#) shows the troubleshooting flowchart that is used when the neighbor relation cannot be set up between the BGP peers.

Figure 4-2 BGP connection troubleshooting flowchart



## 4.2.4 Troubleshooting Procedure

## Context

The following are the prerequisites to set up the BGP neighbor.

Objective	Requirements
Establishing the TCP session.	Port 179 is usable.
	The connection of the IP layer is valid. The route learned from IGP or the static route is configured.
Exchanging the Open packet.	The configured neighbor address must be the same as the address used by the TCP session.
	The locally-configured AS parameters must be the same as that on the peer.

If the prerequisites are met, then the errors in setting up the neighbor can be removed.

## Procedure

**Step 1** Run the **ping** command with the source address parameter to check that the route is normal.

Run the **ping -a source-ip-address host** command to check that the route is normal.

For example, run the following command on Switch B to check whether the route between loopback interfaces of Switch A and Switch B is correct.

**ping -a 10.1.1.2 10.1.1.1**

**Step 2** Check whether the ACL disabling the TCP Port 179 is configured.

Run the **display current-configuration** command or the **display acl all** command to check whether the ACL of TCP port 179 is disabled.

The 179 port works as the interception port of the TCP connection for the BGP peers. If it is disabled, the TCP connection cannot be set up.

**Step 3** Check that the connect-interface is configured if the Loopback Interface is used to set Up the peer.

Run the **display current-configuration configuration bgp** command to check the BGP configuration.

If the configuration is incorrect, the TCP connection cannot be set up.

**Step 4** Check that the BGP configuration is correct by using the debugging Information.

Run the **debugging bgp ipv4-address all** command to debug a certain peer.

For example, if Switch B and Switch A cannot set up the connection, run the **debugging bgp 10.1.1.1 all** command on Switch B to enable the BGP debugging. This allows to view why the connection cannot be set up.

- If "Send/Receive NOTIFICATION Err/SubErr: 2/2 (OPEN Message Error/Bad Peer AS)" appears, it indicates the AS configuration is incorrect.



Check if the ASs on Switch A and Switch B are the same as that specified on the peer.

- If "Send/Receive NOTIFICATION Err/SubErr: 2/3 (OPEN Message Error/Bad BGP Identifier)", it indicates the router ID is configured incorrectly.

Check if the router ID on Switch A and Switch B are the same. They must be configured with different values.

If the error code appears in Send Notification, it indicates that the above errors occur on the BGP router.

If the error code appears in Receive Notification, it indicates that the above errors occur on the peer.

- Step 5** Check whether ebgp-max-hop is configured if the indirectly-connected interface is used to set up the EBGP peer.

If the prompt "Might miss configuring ebgp-max-hop or GTSM for ebgp multi-hop peer" appears, it indicates that the indirectly-connected interface is used in setting up the EBGP peer. Ebgp-Max-Hop, however, is not configured.

The error code of Open message is as follows:

Error Code	Description
2/1	Unsupported version number
2/2	Wrong AS number
2/3	Wrong BGP ID, namely router ID
2/4	Unsupported option parameter
2/5	Authentication failure
2/6	Unsupported Hold time

If the fault persists, contact the Huawei technical personnel.

----End

## 4.3 Accidental Interruption of BGP Connection Troubleshooting

This section describes the notes about configuring BGP, and provides the accidental interruption of BGP connection troubleshooting flowchart and the troubleshooting procedure in a typical BGP networking environment.

[4.3.1 Typical Networking](#)

[4.3.2 Configuration Notes](#)

[4.3.3 Troubleshooting Flowchart](#)

[4.3.4 Troubleshooting Procedure](#)

## 4.3.1 Typical Networking

See [Typical Networking](#).

## 4.3.2 Configuration Notes

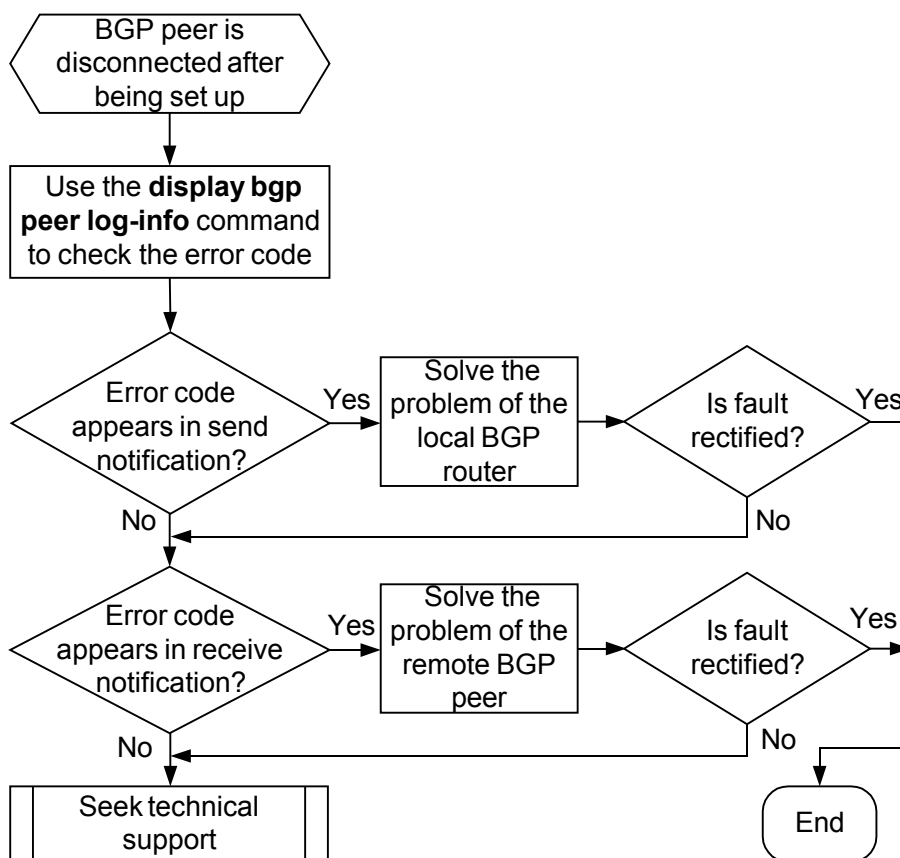
See [Configuration Notes](#).

## 4.3.3 Troubleshooting Flowchart

In the network shown in [Typical Networking](#), the BGP peer connection is closed after the BGP peer is configured for each switch.

[Figure 4-3](#) shows the flowchart of BGP connection troubleshooting.

**Figure 4-3** BGP connection troubleshooting flowchart



## 4.3.4 Troubleshooting Procedure

### Fault Analysis

The prerequisites for setting up the BGP peer are as follows:

Objective	Requirements
Keep the TCP connection.	The link layer is stable.
	The reachable route is stable.
Exchange the Keepalive packet correctly.	The network is not congested.
	The data packet is reachable.
Exchange the Update packet correctly.	The network is not congested.
	The big data packet is reachable.
	BGP is configured correctly. The wrong BGP configuration may lead to the wrong attribute in the Update packet.

If the preceding requirements are met, the fault in keeping the BGP connection can be removed.

Check the error code when the BGP connection is closed.

Run the **display bgp peer peer-address log-info** command to check the error code when the BGP connection is closed.

Error Code	Action
6/1	Check whether the number of prefixes reach the upper limit.
6/2	Check whether the administrative is shutdown.
6/3	Check whether the neighbor is deleted.
6/4	Check whether the administrative reset.
6/5	Check whether the connection fails.
6/6	Check whether the setting that leads to the disconnection of the BGP neighbor is configured, including: <ul style="list-style-type: none"> <li>● Configuration of the <b>peer ignore</b> command</li> <li>● Change of the router ID</li> <li>● Configuration of the confederation</li> </ul>
6/7	Check whether the connections conflict.
6/8	Check whether the resource is insufficient.
6/9	Check whether the BFD session is down.
5/0	Check whether the route and TCP connection is normal.
4/0	Check whether the route is reachable.
	Check whether the network is congested.
	Check whether the data packet is reachable.

Error Code	Action
3/0	Check whether the confederations are configured on both sides and the configurations are the same.
1/1	Check whether the message header error occurs in the packet format: the connection not synchronized.
1/2	Check whether the message header error occurs in the packet format: the wrong message length.
1/3	Check whether the message header error occurs in the packet format: the wrong message type.
3/1	Check whether the update error occurs in the packet format: the wrong attribute list.
3/2	Check whether the update error occurs in the packet format: the unsupported well-known attribute.
3/3	Check whether the update error occurs in the packet format: no well-known attribute.
3/4	Check whether the update error occurs in the packet format: the wrong attribute flag.
3/5	Check whether the update error occurs in the packet format: the wrong attribute length.
3/6	Check whether the update error occurs in the packet format: the invalid Original attribute.
3/7	Check whether the update error occurs in the packet format: the AS routing loop.
3/8	Check whether the update error occurs in the packet format: the invalid Next_Hop attribute.
3/9	Check whether the update error occurs in the packet format: the wrong optional attribute.
3/10	Check whether the update error occurs in the packet format: the invalid network field.
3/11	Check whether the update error occurs in the packet format: the wrong AS-Path.

If the error code appears in Send Notification, it indicates the preceding error occurs on the local BGP router.

If the error code appears in Receive Notification, it indicates the preceding error occurs on the peer.

If the fault persists, contact the Huawei technical personnel.

## 4.4 Route Loss Troubleshooting When BGP Exchange Update Messages

This section describes the notes about configuring BGP, and provides the route loss troubleshooting flowchart and the troubleshooting procedure in a typical BGP networking environment.

[4.4.1 Typical Networking](#)

[4.4.2 Configuration Notes](#)

[4.4.3 Troubleshooting Flowchart](#)

[4.4.4 Troubleshooting Procedure](#)

### 4.4.1 Typical Networking

See [Typical Networking](#).

### 4.4.2 Configuration Notes

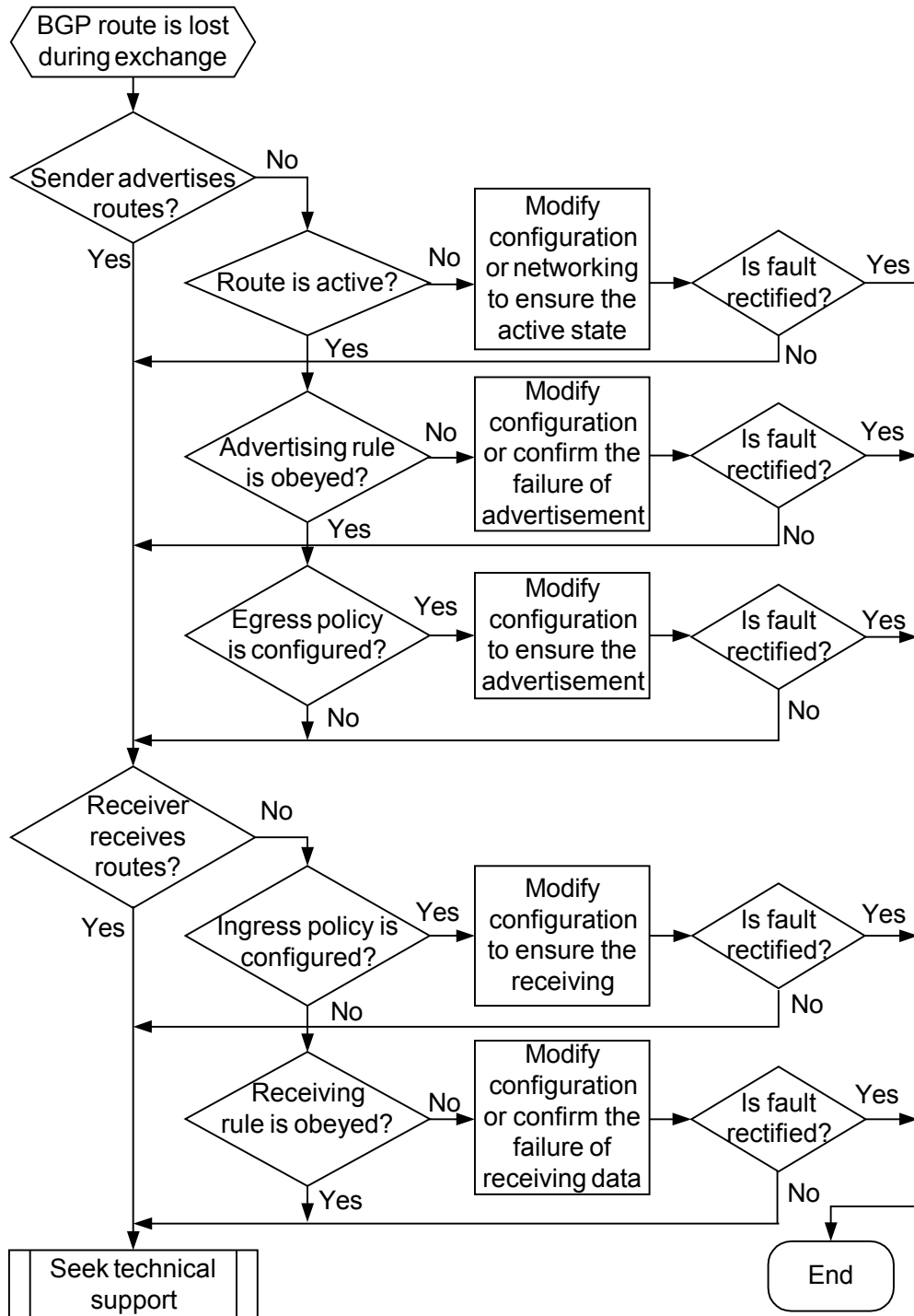
See [Configuration Notes](#).

### 4.4.3 Troubleshooting Flowchart

In the network shown in [Typical Networking](#), after the BGP peer is configured for each switch, the route is lost in the BGP exchange of the Update message.

Follow the flowchart shown in [Figure 4-4](#) to diagnose the fault.

Figure 4-4 BGP route loss troubleshooting flowchart



### 4.4.4 Troubleshooting Procedure

## Procedure

### Step 1 Check that the sender advertises the route.

Run the **display bgp routing-table peer *peer-address* advertised-routes** command on the sender to check whether the route is sent.

If the sender does not send the route, troubleshoot according to the following procedure:

- Check whether the local route is Active.

Run the **display bgp routing-table** command to check whether the route is Active.

That is, check whether the route is marked with \*>. If the route is Inactive, the next hop may be unreachable or the other route with higher precedence exists locally.

- Check whether the advertisement rule is obeyed.

- The route suppressed by aggregation cannot be advertised.

Run the **display bgp routing-table** command to check which routes are suppressed by aggregation. The route marked with "s" is the suppressed route.

- The route suppressed by Damping cannot be advertised.

Run the **display bgp routing-table** command to check which routes are suppressed routes. The route marked with "d" is the dampened route.

- The route learned from the IBGP peer cannot be forwarded to the IBGP peer.

- Check whether the egress policy is configured to filter the advertised route.

The BGP filters include the following:

- IP prefix list
- AS\_Path filter
- Community filter
- Route-Policy

The preceding filters can be applied to the routing information both learned from the peer and advertised to the peer.

Run the **display current-configuration configuration bgp** command to check the configuration.

### Step 2 Check that the receiver receives the route.

Run the **display bgp routing-table peer *peer-address* received-routes** command on the receiver to check whether the route is received.

If the receiver does not receive the route, troubleshoot according to the following procedure:

- Check whether the ingress policy is used to filter the received route.

Run the **display current-configuration configuration bgp** command to check the configuration.

- Check whether the rule used to receive routes is obeyed.

The route is rejected if the following situation occurs:

- The route is not configured with the **peer allow-as-loop** command and the local AS number appears in the AS\_Path attribute in the received route.

- The route is configured with the **peer allow-as-loop** [ *number* ] command and the number of times the AS number appears in the AS\_Path of the received route is larger than the value specified in *number*. (The default is 1.)
- The first AS number in the AS\_Path attribute of the route learned from the EBGP peer is not the AS number of the peer.
- The Originator\_ID is the same as the local Router ID or is the invalid 0.0.0.0.
- The Cluster-List in the route received by the reflector contains the local Cluster-ID.
- Aggregator is the invalid 0.0.0.0.
- Next\_Hop is the local interface address.
- The next hop of the route received from the directly-connected EBGP peer is unreachable.
- If the **peer route-limit alert-only** command is configured, after the limit is reached, all the reached routes are rejected.

If the fault persists, contact the Huawei technical personnel.

----End

## 4.5 Troubleshooting Cases

This section presents several troubleshooting cases.

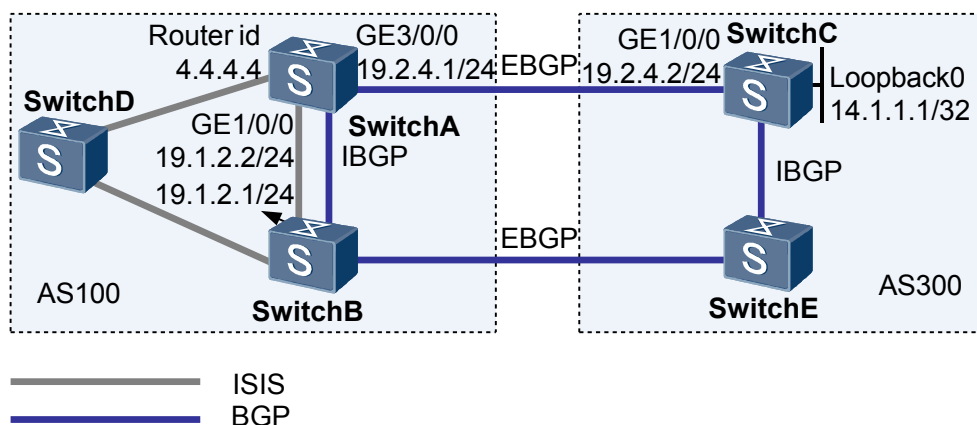
### 4.5.1 Routing Loop and Route Flapping

#### 4.5.2 Peer Connection Is Closed but the Number of Routes Does not Exceeds the Limit

### 4.5.1 Routing Loop and Route Flapping

#### Fault Symptom

Figure 4-5 BGP typical networking



In [Figure 4-5](#):



- Inside AS100, IS-IS and double egress are used.
- Through Switch A and Switch B, AS100 advertises the interior domain route (the **import-route isis** command in BGP view) and receives the exterior route (the **import-route bgp** command in IS-IS view).
- After the configuration on the network, the ping to 14.1.1.1 on Switch A is disconnected intermittently.

Run the **tracert 14.1.1.1** command to check all the gateways that the ping packet passes from Switch A to Switch C.

```
<SwitchA> tracert 14.1.1.1
traceroute to 14.1.1.1(14.1.1.1), max hops: 30 ,packet length: 40
 1 19.1.2.1 47 ms 31 ms 16 ms [SwitchB]
 2 19.1.2.2 46 ms 16 ms 31 ms [SwitchA]
 3 19.1.2.1 63 ms 47 ms 47 ms [SwitchB]
 4 19.1.2.2 62 ms 47 ms 47 ms [SwitchA]
 5 19.1.2.1 78 ms 78 ms 63 ms
 6 19.1.2.2 93 ms 63 ms 78 ms
 7 19.1.2.1 109 ms 94 ms 94 ms
 8 19.1.2.2 78 ms 94 ms 93 ms
 9 19.1.2.1 141 ms 109 ms 125 ms
```

## Fault Analysis

1. The ping disconnects intermittently. The output of the **tracert** command shows that the routing loop occurs between Switch A and Switch B. Check the route first. Run the **display ip routing-table** command repeatedly on Switch A.

```
<SwitchA> display ip routing-table 14.1.1.1
Route Flags: R - relay, D - download to fib
-----
Routing Table : Public
Summary Count : 1
Destination/Mask Proto Pre Cost Flags NextHop Interface
 14.1.1.1/32 BGP 255 74 D 19.1.2.1 Vlanif10
<SwitchA> display ip routing-table 14.1.1.1
Route Flags: R - relay, D - download to fib
-----
Routing Table : Public
Summary Count : 1
Destination/Mask Proto Pre Cost Flags NextHop Interface
 14.1.1.1/32 BGP 255 0 D 19.2.4.2 Vlanif30
<SwitchA> display ip routing-table 14.1.1.1
Route Flags: R - relay, D - download to fib
-----
Routing Table : Public
Summary Count : 1
Destination/Mask Proto Pre Cost Flags NextHop Interface
 14.1.1.1/32 ISIS 15 74 D 19.1.2.1 Vlanif10
```

The display shows that the route changes continuously. The BGP route comes from Switch C, while the IS-IS route comes from Switch B.

In the S9300, by default, the IS-IS route is of higher precedence than that of the BGP route. If the IS-IS route is stable, the flapping cannot occur.

2. Run the **display ip routing-table** command on Switch B to check the source of the IS-IS route on Switch B. Run the **display ip routing-table 14.1.1.1** command and find the flapping also occurs between the BGP and IS-IS protocol.

Check the configuration on the two switches.

```
<SwitchA> display current-configuration configuration bgp
<SwitchA> display current-configuration configuration isis
<SwitchB> display bgp current-configuration configuration bgp
<SwitchB> display current-configuration configuration isis
```

The preceding information shows that between Switch A and Switch B, BGP and IS-IS import routes from each other.

Based on the topology, the following points can be inferred:

- The original route is transmitted to Switch A and Switch B through EBGP.
- Switch A and Switch B retransmit the routing information to IS-IS. Through IS-IS, the routing information is transmitted between Switch A and Switch B.
- By default, the precedence of the IS-IS route is higher than that of the BGP protocol. Thus, the IS-IS route replaces the BGP route.
- The BGP route is no more the optimal. Thus, the BGP route is cancelled after that information is passed to the peer.
- After the BGP route is cancelled, because the IS-IS route originates from BGP, the IS-IS route is also cancelled.
- After the IS-IS route is cancelled, the BGP route becomes optimal again. Then the BGP route is re-advertised to IS-IS. Thus, the continuous loop and flapping occur.

In addition, the IS-IS route is re-advertised to BGP, and thus the route coming from AS300 is retransmitted to AS300 through Switch A and Switch B. The repeated routing of the exterior route gives rise to the flapping.

## Procedure

- Step 1** Configure the export policy of Switch A and Switch B. Only the route in its area can be advertised.
- Step 2** Run the **preference** command to change the precedence on Switch A and Switch B. Ensure the precedence of the route learned from EBGP is higher than that of the IS-IS route inside the area.

---End

## Summary

The loop or flapping is often caused by the incorrect configuration.

In the case that BGP and IGP import each other, the real source must be made out clearly. Ensure the source route has higher precedence to keep the route stable.

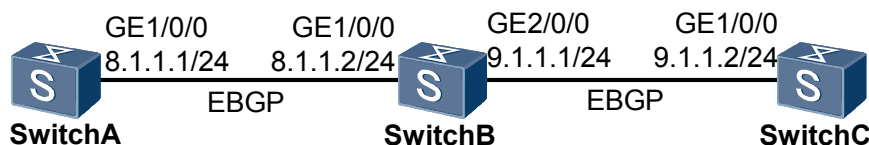
AS for multi-exit AS, if IGP and BGP import each other, the filtering policy for the exported route is needed to ensure that the route learned from the AS cannot be retransmitted to the same AS. This may affect the stability of the route outside the area.

## 4.5.2 Peer Connection Is Closed but the Number of Routes Does not Exceeds the Limit

### Fault Symptom

Run the **peer route-limit** command on Switch C to limit the number of routes received from Switch B. Switch C closes the peer connection with Switch B, even if the number of routes sent by Switch B to Switch C does not exceed the limit.

Figure 4-6 BGP typical networking



As shown in [Figure 4-6](#), the detailed configuration procedure is as follows:

1. Set up EBGP connection between the Switch A, Switch B, and Switch C.
2. Configure five static routes on Switch A and advertise them to other switches through BGP.

# Configure Switch A.

```
[SwitchA] ip route-static 200.1.1.1 24 NULL 0
[SwitchA] ip route-static 200.1.2.1 24 NULL 0
[SwitchA] ip route-static 200.1.3.1 24 NULL 0
[SwitchA] ip route-static 200.1.4.1 24 NULL 0
[SwitchA] ip route-static 200.1.5.1 24 NULL 0
[SwitchA] bgp 100
[SwitchA-bgp] import-route static
```

# View the BGP routing table on Switch C. You can find that Switch C learns the five static routes of Switch A.

```
[SwitchC-bgp] display bgp routing-table
Total Number of Routes: 5
BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
   Network          NextHop          MED           LocPrf        PrefVal Path/Ogn
*> 200.1.1.0        9.1.1.1          0              0             200 100?
*> 200.1.2.0        9.1.1.1          0              0             200 100?
*> 200.1.3.0        9.1.1.1          0              0             200 100?
*> 200.1.4.0        9.1.1.1          0              0             200 100?
*> 200.1.5.0        9.1.1.1          0              0             200 100?
```

3. Configure the routing policy on Switch B to filter the two routes to Switch C.

# Configure the routing policy named out on Switch B and apply the routing policy to the routes sent to Switch C.

```
[SwitchB] acl 2001
[SwitchB-acl-basic-2001] rule permit source 200.1.1.0 0.0.0.255
[SwitchB-acl-basic-2001] rule permit source 200.1.2.0 0.0.0.255
[SwitchB-acl-basic-2001] quit
[SwitchB] route-policy out deny node 20
[SwitchB-route-policy] if-match acl 2001
[SwitchB-route-policy] quit
[SwitchB] route-policy out permit node 30
[SwitchB-route-policy] quit
[SwitchB] bgp 200
[SwitchB-bgp] peer 9.1.1.2 route-policy out export
```

# View the BGP routing table on Switch C. You can find that the routes 200.1.1.1/24 and 200.1.2.1/24 are filtered out.

```
<SwitchC> display bgp routing-table
Total Number of Routes: 3
BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
   Network          NextHop          MED           LocPrf        PrefVal Path/Ogn
*> 200.1.3.0        9.1.1.1          0              0             200 100?
*> 200.1.4.0        9.1.1.1          0              0             200 100?
```

```
*> 200.1.5.0          9.1.1.1          0          200 100?
```

4. Run the **peer route-limit** command on Switch C to set the maximum number of routes to 4 sent by Switch B. When the number of the routes sent by Switch B exceeds the limit, the peer connection is closed.

# Configure Switch C.

```
[SwitchC] bgp 300
[SwitchC-bgp] peer 9.1.1.1 route-limit 4
```

The neighbor relation between Switch A and Switch B is normal because Switch B sends only three routes to Switch C.

5. Change the policy on Switch B to out policy. The matching mode of out is "permit" and the index number of out is 10. After only two routes that match ACL 2001 can be sent to Switch C, the peer connection is closed.

```
[SwitchB] route-policy out permit node 10
Info: New Sequence of this List !
%Aug  9 19:22:24 2006 SwitchB RM/4/RMLOG:
  BGP.Public: 9.1.1.2 State is changed from ESTABLISHED to IDLE.
%Aug  9 19:22:55 2006 SwitchB RM/4/RMLOG:
  BGP.Public: 9.1.1.2 State is changed from OPENCONFIRM to ESTABLISHED.
%Aug  9 19:22:55 2006 SwitchB RM/4/RMLOG:
  BGP.Public: 9.1.1.2 State is changed from ESTABLISHED to IDLE.
```

## Fault Analysis

1. After the **peer route-limit** is used, the peer connection between Switch B and Switch C is closed and re-established. This is because the number of routes sent by Switch B exceeds 4.

When you check Switch C, the log indicates the number of routes exceeds the limit.

```
[SwitchC-bgp]
*0.151289355 SwitchC RM/6/RMDEBUG:
  BGP.Public: 14.1.1.1 Recv NOTIFICATION
  Err/SubErr: 6/1 (CEASE/Maximum Number of Prefixes Reached)
  Error data: 000101000000004.

*0.151289356 SwitchC RM/6/RMDEBUG:
  BGP.Public: 14.1.1.1 State is changed from ESTABLISHED to IDLE.
```

The routing policy of node 10 only is expected to be changed, and two routes are sent Switch C, which does not exceed the limit.

```
[SwitchB] route-policy out permit node 10
[SwitchB-route-policy] if-match acl 2001
```

After the **route-policy out permit node 10** is used, the peer connection is closed. This is because the command immediately takes effect. After the routing policy is applied, the route matches the node with the smallest index number. Once the matching succeeds, the route stops to match other nodes. In this example, the index number of the permit node is 10, which indicates that all routes can pass the routing policy. Therefore, the number of the routes sent to Switch C is five, which exceeds the limit.

Why is an incomplete routing policy applied?

2. Run the **display current-configuration** command to check the configuration on Switch B.

As shown in the display, the delay for applying the routing policy is not configured. That is, when the routing policy changes, RM notifies each protocol to apply new policies immediately. This is why BGP applies the incomplete routing policy even if the configuration is not complete.

## Procedure

- Step 1** Run the **route-policy-change notify-delay** command to adjust the delay when the routing policy changes.
- Step 2** The delay ranges from 1 to 180, which can be specified as required.
- Step 3** Configure the new routing policy.

When the configuration of the routing policy is complete, you need to run the **refresh bgp all export** command on Switch B immediately to view the configuration result.

This step is optional.

---End

## Summary

If the delay in updating a routing policy is too short, running the **peer route-limit** command to change the routing policy may cause the number of routes to exceed the limit. The BGP peer relationship is thus interrupted.

During network planning, take the capacity of routes into consideration to avoid route flapping. Alternatively, configure a device to generate alarms without interrupting the BGP peer relationship after the upper limit of routes is exceeded. The network stability is thus improved.

## 4.6 FAQs

This section lists frequently asked questions and their answers.

### Q: What Is the Function of Hold Timer and Keepalive Timer of BGP?

A: The value of Hold Timer and Keepalive Timer can be configured through the command. The command specifies the expiry time of the BGP connection and the interval of sending the Keepalive message. Long period can reduce the effect of the flapping, while short period can recognize the link change more sensitively. Specify the appropriate period according to the actual need.

After the connection is set up between peers, the value of the two timers is negotiated by both the peers.

- The smaller value of hold timers in Open packets of both peers is set as the value of the hold timer.
- The smaller value of the locally configured *keepalive-time* and one third of the negotiated *hold-time* is used as the actual value of the *keepalive-time*.

### Q: When Running the display bgp peer Command to Check the BGP Peer, Find That the Connection Cannot Enter the Established State. How to Remove the Fault?

A: The prerequisites for setting up a BGP neighbor are:

- TCP session is set up by using port 179.
- BGP routers can properly exchange Open messages.

To remove the fault, do as follows:

- Check whether the AS number and IP address among peers are correct by using the **display bgp peer** command.
- Check whether the router IDs configured on both BGP peers are conflicting by using the **display bgp peer** command.
- If the loopback interface is used, check whether the **peer connect-interface** command is configured to specify the loopback interface as the source interface for sending BGP packets.
- If EBGP neighbors are not directly connected to the physical layer, check whether the **peer ebgp-max-hop** command is configured.
- Check whether there are available routes to the peer in the routing table.
- Check whether there are reachable routes to the specified connect-interface by using the **ping -a source-ip-address host** command.
- Check whether the ACL that is used to disable TCP port 179 is configured.

### Q: What Is the Application Range of the peer allow-as-loop Command?

A: Check whether there is the local AS number in the route received from EBGP and the EBGP neighbor in the confederation. The command cannot be used to check the IBGP and IBGP routes in the confederation.

### Q: What Is the Application Range of the peer public-as-only Command?

A: The **peer public-as-only** command is used to delete the private AS number included in the AS-Path of the BGP routing information. The command takes effect only after the following three requirements are met:

- The peer is the neighbor of EBGP or EBGP in confederation.
- The AS-Path attribute contains the AS number of the private network.
- The AS number of the private network is different from that of the peer. If AS number of the private network is the same as that of the peer, the deletion of the AS number may result in the routing loop.

### Q: What Is the Precedence of Policies Modifying MED?

A: There are two conditions. The policy whose number is not mentioned does not take effect.

- The priority sequence used by the route sent to the EBGP neighbor is: 1 > 2 > 3 > 4 > 5 > 6.
- The priority sequence used by the route sent to the IBGP neighbor is: 1 > 4 > 5 > 6.

**Table 4-3** Precedence of policies modifying MED

No.	Policy
1	Configure the <b>apply cost</b> clause in the export policy on the peer. It is applicable to all the BGP routes.
2	Configure the <b>apply cost-type internal</b> clause in the export policy on the peer.
3	The <b>default med</b> command. It is applicable to the route (the static, direct and IGP route) that imports the BGP route and the aggregated route.

No.	Policy
4	The <b>apply cost</b> clause of the import policy.
5	The imported IGP route uses IGP Metric. The BGP route learned by the neighbor carries MED with itself.
6	Metric is not set.

### Q: What the Effective Range of the Apply Preference Clause in the Route-Policy of BGP?

A: The Apply Preference clause in the Route-Policy only takes effect when it is used in the **preference { external internal local | route-policy route-policy-name }** command.

In BGP, only the **preference** command in BGP view can modify the preference of the route.

### Q: After the Configuration of the BGP Neighbor Capability Is changed, Why Is the BGP Connection Closed?

A: The BGP connection closes automatically when the configuration of the BGP capability is changed. This is because the BGP does not support dynamic capability negotiation. The neighbor capability negotiation is performed again.

The BGP connection disconnects automatically when:

- Label-Route-Capability is enabled or disabled.
- The BGP peer in the address family is enabled or disabled. For example, the **peer enable/undo peer enable** command is executed in the VPNv4 address family, the BGP connection of the peer in other address family disconnects automatically.
- GR capability is enabled.

### Q: Why Does the BGP Neighbor not Close Instantly After the Interface Is Shutdown?

A: The EBGP neighbor is disconnected instantly after the interface is shutdown only when the EBGP is directly-connected and BGP is configured with the **ebgp-interface-sensitive** command. (By default, the command is configured.)

Otherwise, the BGP neighbor is not disconnected until the Hold Timer times out.

### Q: Why the Direct Route of the Interface Enabled with IGP Is also Imported When BGP Imports the IGP Route?

A: When the **import-route protocol** command is configured in BGP, the following two routes are imported if the *protocol* is IGP:

- The active IGP route in the IP routing table that can be viewed by using the **display ip routing-table protocol protocol** command.
- The direct route corresponding to the interface enabled with the IGP protocol.

In OSPF, you can run the **display ip routing-table protocol ospf** command to check the route. The route is displayed as inactive because there is a direct route.

In RIP, you can run the **display rip process-id database** command to check the route.

### Q: How Is the Attribute Handled When the Route Is Reflected?

A: The attribute of the route reflected by the reflector has already passed the import policy. It is not affected by the export policy and the **peer next-hop-local** command.

### Q: When the Statistics of Route Flapping Is Cleared by Running the **reset bgp flap-info** Command, Why Does not the Command Line to Which no Mask Is Added Take Effect?

A: If the mask is not specified, the address is processed as a classful address. For example, the mask of 192.168.1.2/16 is 16 bits. It is a Class C address. If the mask is not specified, the address is processed as the address with the mask of 24 bits. Therefore, the command does not take effect.

The **reset bgp dampening** command is used to clear the information of route flap dampening and suppress routes. If the mask is not specified, it is processed as a classful address.

### Q: Why Do the Routes Disconnect even After the **aggregate** Command Is Configured to Aggregate Routes?

A: Check whether the mask length of aggregated routes is correct. The local egress of aggregated routes is NULL0. If the mask length of aggregated routes is equal to that of the routes to be aggregated, aggregated routes towards NULL0 covers routes to be aggregated. Then routes disconnect.

### Q: When the **filter-policy import/export** Command Is Applied to the Default Routes, Why Does the Routing Policy not Take Effect?

A: The default routes are applied to the routing policies in the following cases:

- BGP default routes that are not in the VPNv4 address family can be applied to the routing policy that is specified by the **peer default-route-advertise** command, the **default med** command and **default local-preference** command.
- Default routes in the BGP VPNv4 address family can be applied to the routing policy that is specified by the **default med** command and the **default local-preference** command.
- The **filter-policy import** command and **filter-policy export** command do not take effect on default routes.

### Q: Is There Any Requirement for the Configuration of BGP Authenticators?

A: A BGP authenticator can be either in the plain text or the encrypted text. The rules to form a BGP authenticator are shown as below:

- In plain text mode (the simple mode), the authenticator is a string with 1 to 255 characters. The string can be composed of all letters, all numbers, or combination of letters and numbers.
- In encrypted text mode, the authenticator is also a string. The string can be composed of all letters, all numbers, or combination of letters and numbers. The string with 1 to 255



characters corresponds to the plain text while the string with 20 to 392 characters corresponds to the encrypted text.

- All authenticators cannot include any blank space.

## 4.7 Diagnostic Tools

This section describes common diagnostic tools: display commands and debugging commands.

### 4.7.1 display Commands

#### 4.7.2 debugging Commands

### 4.7.1 display Commands

Command	Description
<b>display bgp peer</b>	Displays the brief of the IPv4 neighbor of the public network.
<b>display bgp peer <i>ipv4-address</i> verbose</b>	Displays the detailed information about the specified neighbor.
<b>display bgp peer <i>ipv4-address</i> log-info</b>	Displays logs of the specified neighbor. It is very useful for locating the disconnection fault of the neighbor
<b>display bgp group <i>group-name</i></b>	Displays information about the IPv4 neighbor group of the public network.
<b>display bgp routing-table statistics</b>	Displays statistics about the IPv4 unicast route of the BGP public network.
<b>display bgp routing-table</b>	Displays the brief of the IPv4 unicast route of the BGP public network.
<b>display bgp routing-table peer <i>ipv4-address</i> advertised-routes</b>	Displays the route advertised to the specified neighbor.
<b>display bgp routing-table peer <i>ipv4-address</i> received-routes</b>	Displays the route received from the specified neighbor.
<b>display bgp network</b>	Displays the BGP route imported by the <b>network</b> command.
<b>display bgp paths</b>	Displays the path attribute of the IPv4 unicast route of the BGP public network.
<b>display bgp ipv6</b>	Displays information about IPv6 of the BGP public network. The usage of the command is the same as that of the corresponding command used for IPv4.
<b>display bgp multicast</b>	Displays information about the IPv4 multicast route of the BGP public network. The usage of the command is the same as that of the corresponding command used for the IPv4 unicast.

Command	Description
<b>display ip routing-table statistics</b>	Displays statistics of the IPv4 route of the system public network.
<b>display ip routing-table protocol bgp</b>	Displays the brief information of the BGP active and inactive routes in the IPv4 routing table of the system public network.
<b>display ip routing-table protocol bgp verbose</b>	Displays the detailed information of the BGP active and inactive routes in the IPv4 routing table of the system public network.
<b>display ip routing-table protocol bgp inactive</b>	Displays the brief of the BGP inactive route in the IPv4 routing table of the system public network.

## 4.7.2 debugging Commands

Command	Description
<b>debugging bgp all</b>	Enables all the BGP debugging. The command is helpful when a few routes are configured and a few routes change.
<b>debugging bgp <i>ipv4-address</i> all</b>	Debugs all the specified peers. The command is helpful when only a few routes change.
<b>debugging bgp <i>ipv4-address</i> event</b>	Debugs the event of the specified peer. The command can help to locate the fault in setting up the neighbor.
<b>debugging bgp <i>ipv4-address</i> raw-packet receive verbose</b>	Debugs the receiving of original packets of the specified peer. The command can help to check the original packet.
<b>debugging bgp update ip-prefix <i>ip-prefix-name</i> receive verbose</b>	Debugs the Update message that satisfies the <b>ip-prefix</b> . The command can help to locate the fault of the lost route.
<b>debugging bgp graceful-restart</b>	Debugs the BGP GR.

# 5 Routing Policy Troubleshooting

---

## About This Chapter

This chapter describes the knowledge related to routing policy troubleshooting, including routing policy overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases and diagnostic tools and FAQs.

### [5.1 Routing Policy and Filter Overview](#)

This section describes the knowledge you need to know before troubleshooting routing policy.

### [5.2 Troubleshooting the Routing Policy](#)

This section describes the notes about configuring routing policy, and provides the routing policy troubleshooting flowchart and the troubleshooting procedure in a typical networking environment.

### [5.3 Troubleshooting Cases](#)

This section presents several troubleshooting cases.

### [5.4 FAQs](#)

This section lists frequently asked questions and their answers.

### [5.5 Diagnostic Tools](#)

This section describes common diagnostic tools: display commands and debugging commands.

## 5.1 Routing Policy and Filter Overview

This section describes the knowledge you need to know before troubleshooting routing policy.

[5.1.1 Routing Policy](#)

[5.1.2 IP-Prefix List](#)

[5.1.3 AS-Path-Filter](#)

[5.1.4 Community-Filter](#)

[5.1.5 Extcommunity-Filter](#)

[5.1.6 Route-Policy](#)

### 5.1.1 Routing Policy

The routing policy is deployed on the routing information to change the path of the network traffic. The path is changed with the change of the route attribute, including reachability.

Policy-Based-Route is used to guide the forwarding of packets.

This section describes only routing policy.

To apply the routing policy, features of the routing information must be defined. That is, a set of matching rules must be defined.

Different attributes such as the destination address, which is the address of the router that advertises the route, can be used as the matching condition.

The matching rules can be pre-configured and can be applied to the routing policy adopted in advertising, receiving and importing the route.

Sometimes, it is necessary for a certain policy to filter the route. Thus, only the routes satisfying certain conditions are received or advertised.

A routing protocol such as RIPng may need to import routes of other protocols. A protocol only needs information that satisfies its own requirements. While importing routes of other protocols, the protocol may need to set some attributes on such information to meet its requirement.

### 5.1.2 IP-Prefix List

IP-Prefix list includes the IPv4 and the IPv6 prefix filter.

The function of the IP-Prefix list is similar to that of the ACL. Moreover, the IP-Prefix list is more flexible and easier to understand. When the prefix filter is used to filter the route, the destination field of the information is matched.

The IP-Prefix list is identified by the prefix filter name.

Each prefix filter may contain multiple entries. Each entry can specify a matching range in network prefix format independently.

The matching range is identified by an index number. The index number indicates the matching order.

During the matching process, the router checks each entry identified by the index number in the ascending order.

As long as one entry is matched, the route passes the filtration and the matching process ends up.

### 5.1.3 AS-Path-Filter

The AS\_Path contained in the BGP routing information lists the ASs that the prefix passes by in the reverse order.

The AS-Path-Filter filters routes based on the AS\_Path.

### 5.1.4 Community-Filter

A set of prefixes with the same features share the community of the BGP route. The Community-Filter specifies the matching condition based on the community field.

### 5.1.5 Extcommunity-Filter

The BGP extended community list defines a set of prefixes with the same features.

Currently, the S9300 Extcommunity-Filter filters the route based on a common extended community, that is, VPN-Target.

The VPN-Target defines the VPN member relation of the route of the private network.

### 5.1.6 Route-Policy

The Route-Policy is a complex filter. The Route-Policy not only matches the route based on specified conditions, but also changes the attribute of the information if certain conditions are satisfied. The Route-Policy can use the above-mentioned filters to define its own matching rules.

Each Route-Policy may consist of multiple nodes. The relation among different nodes is OR.

The system checks each node according to the node number. As long as one node is matched, the route passes filtration and the matching process ends.

Each node consists of a set of **if-match** and **apply** clauses.

- The **if-match** clause defines the matching rules aiming at certain attributes. Within the same node, the relation among different **if-match** clauses is AND. The routing information can pass the filtration of the node only when all the **if-match** clauses in a node are satisfied.
- The **apply** clause specifies the actions. If the node matches, the **apply** clause sets certain attributes of the routing information.

## 5.2 Troubleshooting the Routing Policy

This section describes the notes about configuring routing policy, and provides the routing policy troubleshooting flowchart and the troubleshooting procedure in a typical networking environment.

### 5.2.1 Typical Networking

[5.2.2 Configuration Notes](#)

[5.2.3 Troubleshooting Flowchart](#)

[5.2.4 Troubleshooting Procedure](#)

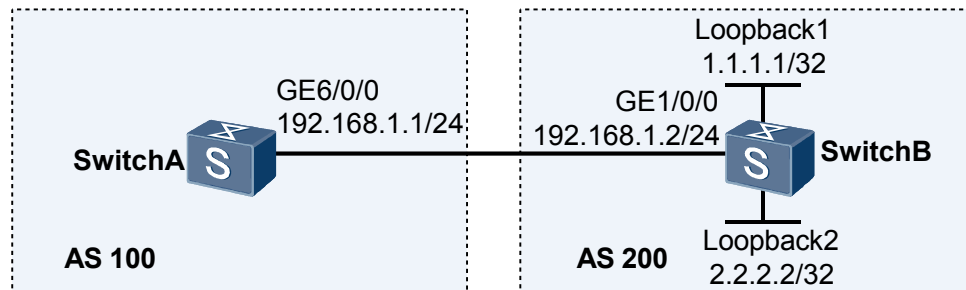
## 5.2.1 Typical Networking

**Figure 5-1** and **Figure 5-2** show the typical networking of the routing policy.

The troubleshooting of the routing policy is based on the networking.

### Typical Networking of the Public Network

**Figure 5-1** Typical networking of the Route-Policy troubleshooting in the public networking



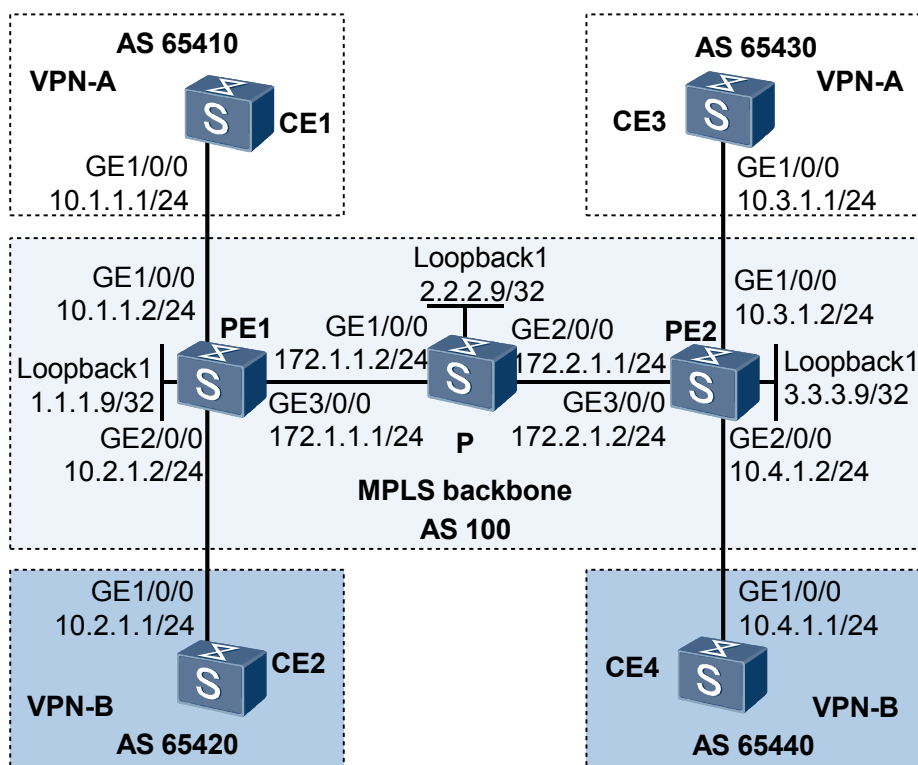
In the preceding networking:

- Switch A belongs to AS 100, Switch B belongs to AS 200, and OSPF is configured on the two switches to implement internetworking.
- An EBGP connection is set up between Switch A and Switch B.
- Routes sent by Switch B to Switch A are configured with route attributes.
- Switch A configured with Route-Policy receives specified routes.

Switch A and Switch B can thus exchange routes.

## Typical Networking of a VPN

Figure 5-2 Typical networking of the Route-Policy troubleshooting in a VPN



In the preceding networking:

- P, PE1, and PE2 belong to the same AS. CE1, CE2, CE3, and CE4 belong to different ASs.
- PE1 and PE2 set up an OSPF connection with P respectively. MPLS and MPLS LDP are configured on P, PE1, and PE2. The three set up an MPLS LSP.
- CE1 and CE2 set up an EBGP connection with PE1 respectively. CE3 and CE4 set up an EBGP connection with PE2 respectively.
- CE1 and CE3 belong to VPN-A. CE2 and CE4 belong to VPN-B.

PEs and CEs can thus exchange VPN routes.

## 5.2.2 Configuration Notes

## Common Filters in the Routing Policy

Item	Sub-item	Configuration Notes and Commands
Configuring IP-Prefix	Configuring IP-Prefix	<ul style="list-style-type: none"> <li>● It is used to configure the IPv4 prefix address filter. <i>ip-prefix-name</i> specifies the list name. Multiple matching entries can be set under each name.  Each entry may have an index number. If the number is not specified, the system dynamically assigns a number that equals the existing maximum number in the prefix list plus 10.</li> <li>● If the specified prefix length is between <i>greater-equal</i> and <i>less-equal</i>, the matching range is between the two values. The values of <i>greater-equal</i> and <i>less-equal</i> must meet the requirement: <i>mask-length</i> &lt;= <i>greater-equal</i> &lt;= <i>less-equal</i> &lt;= 32.</li> <li>● In the matching process, the system checks each entry in the ascending order of the index number. As long as the address/mask of one entry is the same as that of the route to be checked, the filter mode, <b>Permit</b> or <b>Deny</b>, of this entry is returned, and the matching process finishes.</li> <li>● If the filter modes of all entries are <b>Deny</b>, no routes can pass the filtering list.  It is suggested to set an entry of "<b>permit 0.0.0.0 greater-equal 0 less-equal 32</b>" after multiple denied entries. The entry allows the other IPv4 routes to pass the filtering list.</li> <li>● Do not confuse the configuration of IP-Prefix with that of the ACL. Actually, when only IP-Address/Mask-Length is specified, only one route is matched rather than the routes within a mask range.  To match the routes within a mask range, you must specify <i>greater-equal</i> and <i>less-equal</i>.  To configure-IP Prefix, run the <b>ip ip-prefix</b><i>ip-prefix-name</i> [ <b>index</b><i>index-number</i> ] { <b>permit</b>   <b>deny</b> } <i>ip-address mask-length</i> [ <b>greater-equal</b><i>greater-equal-</i></li> </ul>



Item	Sub-item	Configuration Notes and Commands
		<p><i>value</i>   <b>less-equal</b>/<i>less-equal-value</i> ]                      command in the system view.</p>
<p>Configuring IPv6-Prefix</p>	<p>Configuring IPv6-Prefix</p>	<ul style="list-style-type: none"> <li>● The command is used to configure the IPv6 prefix address filter.  <i>ipv6-prefix-name</i> specifies the filter name. Multiple matching entries can be set under each name.                      Each entry can specify an index number. If the number is not specified, the system dynamically assigns a number that equals the existing maximum number in the prefix list plus 10.</li> <li>● If the specified prefix length is between <i>greater-equal</i> and <i>less-equal</i>, the matching range is between the two values. The values of <i>greater-equal</i> and <i>less-equal</i> must meet the requirement: <i>mask-length</i> &lt;= <i>greater-equal</i> &lt;= <i>less-equal</i> &lt;= 128.</li> <li>● In the matching process, the system checks each node according to the index number in the ascending order. As long as one node is matched, the route passes the filtering list and the matching process finishes.</li> <li>● If the filter modes of all entries are <b>Deny</b>, no routes can pass the filtering list.                      It is suggested to set an entry of "<b>permit ::0 0 greater-equal 0 less-equal 128</b>" after multiple denied entries. The entry allows the other IPv6 routes to pass the filtering list.</li> </ul> <p>To configure IPv6-Prefix, run the <b>ip ipv6-prefix</b><i>ipv6-prefix-name</i> [ <b>index</b><i>index-number</i> ] { <b>permit</b>   <b>deny</b> } <i>ipv6-address mask-length</i> [ <b>greater-equal</b><i>greater-equal-value</i>   <b>less-equal</b>/<i>less-equal-value</i> ] command in the system view.</p>

Item	Sub-item	Configuration Notes and Commands
Configuring AS-Path	Configuring AS-Path	<ul style="list-style-type: none"> <li>● The command uses the regular expression to define the AS-Path filtering rules. BGP adopts the rule to match the AS-Path attribute of the BGP route, and thus determines whether to advertise or receive the route according to the matching result.</li> <li>● If the filter modes of all entries are <b>Deny</b>, no routes can pass the filtering list. It is recommended to set an entry of "permit .*" after multiple denied entries. The entry allows all the other routes to pass the filtering list.</li> </ul> <p>To configure AS-Path, run the <b>ip as-path-filter</b><i>as-path-filter-number</i> { <b>deny</b>   <b>permit</b> } <i>regular-expression</i> command in the system view.</p>

Item	Sub-item	Configuration Notes and Commands
Configuring Community-Filter	Configuring Community-Filter	<ul style="list-style-type: none"> <li>● The command defines a community filter. There are two modes of configuration.                      Specifying <i>basic-comm-filter-num</i> ranging from 1 to 99, you can define the filtering rule by the definite community. The command is called the basic community filter.                      Specifying <i>adv-comm-filter-num</i> ranging from 100 to 199, you can define the filtering rule by the regular expression. The command is called the advanced community filter.</li> <li>● As for the basic community filter, the Internet option indicates all communities are matched.</li> <li>● As for the advanced one, the regular expression ".*" indicates the community is matched.</li> </ul> <p>For the basic community filter, there are two matching modes: one is the whole match and the other is the common match.</p> <p>In the whole-match mode, the routing information passes the filtration only when all the community attributes given by BGP match the attributes defined in the filtering rules.</p> <p>In the common-match mode, the routing information passes the filtration only when all the communities given by BGP include the attributes defined in the filtering rules.</p> <ul style="list-style-type: none"> <li>● If <b>Deny</b> is returned for all the entries, all the routes fail to pass the filtering list. It is suggested to set an entry of "permit .*" after multiple denied entries in the advanced community filter or a permit internet entry in the basic community filter.</li> </ul> <p>To configure Community-Filter, run the following commands in the system view:</p> <ul style="list-style-type: none"> <li>● <b>ip community-filter</b> { <i>basiccomm-filter-name</i> } { <b>permit</b>   <b>deny</b> } [ <i>community-number</i>   <i>aa:nn</i> ] * &amp;&lt;1-9&gt;   <i>basic-comm-filter-num</i> { <b>permit</b>   <b>deny</b> } [ <i>community-number</i>   <i>aa:nn</i> ] *</li> </ul>

Item	Sub-item	Configuration Notes and Commands
		<p>&amp;&lt;1-16&gt; [ <b>internet</b>   <b>no-export-subconfed</b>   <b>no-advertise</b>   <b>no-export</b> ] *</p> <ul style="list-style-type: none"> <li>● <b>ip community-filter</b> { <b>advancedcomm-filter-name</b>   <i>adv-comm-filter-num</i> { <b>deny</b>   <b>permit</b> } <i>regular-expression</i></li> </ul>
Configuring Extcommunity-Filter	Configuring Extcommunity-Filter	<p>The command defines the rules of the extended community filter. To configure Extcommunity-Filter, run the <b>ip extcommunity-filter</b><i>ext-comm-list-number</i> { <b>deny</b>   <b>permit</b> } <b>rt</b> { <i>as-number : nn</i>   <i>ipv4-address : as-number</i> } command in the system view.</p>
Configuring Route-Policy	Configuring Route-Policy	<ul style="list-style-type: none"> <li>● The parameter <b>permit</b> indicates that the filter mode is the permit mode. If the routing entry matches the node, the matching process ends and the <b>apply</b> clause under the node is performed. If the routing entry does not match the node, it enters the next node for further matching. If there is no <b>if-match</b> clause, all the routes are permitted.</li> <li>● The parameter <b>deny</b> indicates that the filter mode is the deny mode. Thus, the <b>apply</b> clause is not performed. If the routing entry satisfies all the <b>if-match</b> clauses in the node, the entry fails to match the node, and does not enter the next node. If the entry does not satisfy the <b>if-match</b> clause in the node, the entry enters the next node. If there is no <b>if-match</b> clause, all the routes are denied.</li> <li>● If <b>if-match</b> clauses in all the nodes are not matched, the matching result of the whole policy is <b>deny</b> by default.</li> <li>● If all the nodes are configured with <b>deny</b>, all the routes are denied. Therefore, you need to configure at least one <b>permit</b> node to allow routes except those matching the deny nodes to pass through.</li> </ul> <p>To configure Route-Policy, run the <b>route-policy</b> <i>route-policy-name</i> { <b>permit</b>   <b>deny</b> } <b>node</b> { <i>node-number</i> } command in the system view.</p>

## Noteworthy Points

- Suppose at least one **permit** or **deny** node is configured in the current filter. If no node matches the address/mask range of the route that needs to be filtered, the route is denied.
- If a non-existent filter is used in the policy, all the routes are permitted.

## Rules of the Regular Expression

The regular expression is a formula that matches the character string with certain templates.

Character	Description
^	Matches the first value of the character string. For example, ^300 indicates if the first value of AS-Path of a route is 300, this route is matched.
\$	Matches the last value of the character string. For example, 300\$ indicates if the last value of AS-Path of a route is 300, this route is matched.
.	Matches any single character, including the space.
+	Matches the previous character or sequence that appears once or more.
_	Matches a symbol. For example, the comma, bracket, and space.
*	Matches the previous character or sequence that does not appear or appears for multiple times.
?	Matches the previous character that does not appear or appears for multiple times.
()	Matches the changing AS or an independent match, often accompanied by " ".
	Indicates the logical OR.
[ ]	Matches ASs within a certain range, often accompanied by "-".
-	Indicates the hyphen.

The following are a few examples:

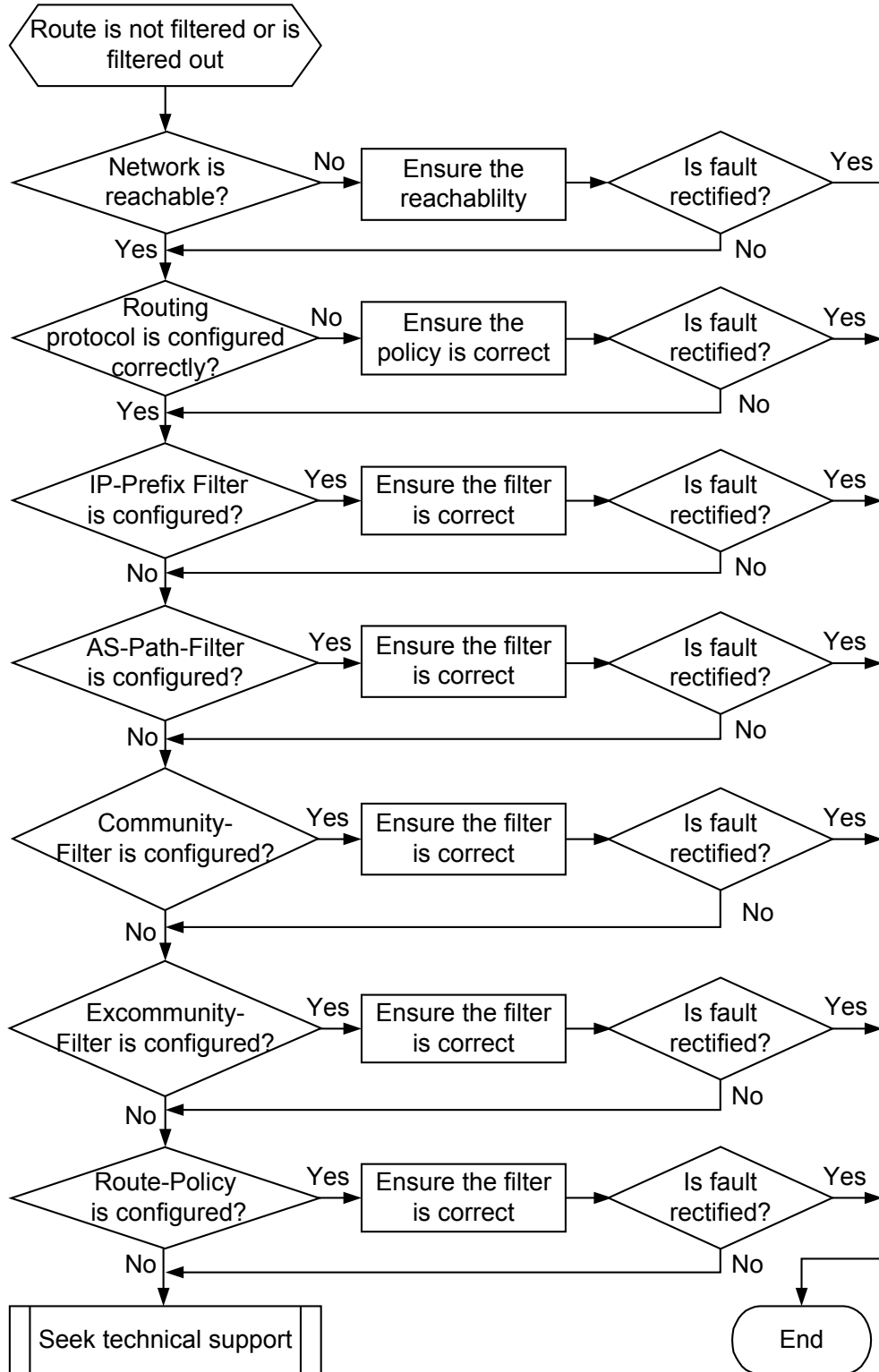
- ip as-path-filter 10 deny ^\$: denies advertising the local originated routes.
- ip as-path-filter 10 permit .\*: permits advertising and receiving the route of the other ASs.
- ip as-path-filter 2 deny (6[0-9]|7[0-9]|8[0-9]|9[0-9]|1[0-3][0-9]|130)\$: denies the route that originates from the AS with the AS number ranging from 60 to 139.
- ip community-filter 100 permit 1000:10[0-9]\$: permits the route whose community is between 1000:100 to 1000:109.

## 5.2.3 Troubleshooting Flowchart

In the networking shown in [Typical Networking](#), the specified route is not filtered or is filtered out after the switches are configured.

To locate the fault, follow the steps described in **Figure 5-3**.

**Figure 5-3** Troubleshooting flowchart of the routing policy



## 5.2.4 Troubleshooting Procedure

### Procedure

**Step 1** Checking the network connectivity.

Run the **display ip interface brief** command to check the status on each interface.

Up indicates the availability of the interface while Down indicates unavailability.

If the status is Down, check if the line is connected correctly and if the **shutdown** command is used on the interface.

**Step 2** Check whether the routing protocol is configured correctly.

Run the **display current-configuration configuration** command to check if the routing protocol is configured correctly.

If the routing protocol is not configured correctly, refer to the *Quidway S9300 Terabit Routing Switch Troubleshooting* of the corresponding protocol.

**Step 3** Checking whether the IP-Prefix list is configured.

Run the **display ip ip-prefix** command to check whether the current switch is configured with the IP-Prefix list. Check whether the IP-Prefix List takes effect by checking the matching counts.

If the current switch is not configured with the IP-Prefix list, see the section about IP-Prefix List in [Configuration Notes](#).

**Step 4** Check whether the AS-Path-Filter is configured.

Run the **display ip as-path-filter** command to check if the current switch is configured with the AS-Path-Filter.

If it is configured, see the related description in [Configuration Notes](#).

**Step 5** Check whether the community filter is configured.

Run the **display ip community-filter** command to check whether the current switch is configured with the community-filter.

If it is configured, see the Community-Filter in [Configuration Notes](#).

**Step 6** Check whether the extended community filter is configured.

Run the **display ip community-filter** command to check if the current switch is configured with the extended community-filter.

If it is configured, see the Excommunity-Filter in [Configuration Notes](#).

**Step 7** Check whether the Route-Policy filter is configured.

Run the **display route-policy** command to check whether the current switch is configured with Route-Policy filter.

If it is configured, see the Route-Policy in [Configuration Notes](#).

If the fault persists, contact the Huawei technical personnel.

----End

## 5.3 Troubleshooting Cases

This section presents several troubleshooting cases.

### 5.3.1 Routes Are Lost After IP-Prefix Is Used

### 5.3.2 Routes Are Lost After AS-Path Is Used

### 5.3.3 Routes Are Not Filtered Correctly After Community-Filter Is Used

### 5.3.4 Routes Are Not Filtered Correctly After Extcommunity-Filter Is Used

### 5.3.5 Routes Are Not Correctly Filtered After Route-Policy Is Used

## 5.3.1 Routes Are Lost After IP-Prefix Is Used

### Fault Symptom

**Figure 5-1** shows the networking.

In the network, Switch A adopts the IP-Prefix list to filter the route received from Switch B.

The configuration on Switch A:

```
#
bgp 100
 peer 192.168.1.2 as-number 200
#
 ipv4-family unicast
  undo synchronization
  peer 192.168.1.2 enable
  peer 192.168.1.2 ip-prefix rta import
#
 ip ip-prefix rta index 20 deny 2.2.2.2 32
#
```

The configuration on Switch B:

```
#
bgp 200
 peer 192.168.1.1 as-number 100
#
 ipv4-family unicast
  undo synchronization
  network 1.1.1.1 255.255.255.255
  network 2.2.2.2 255.255.255.255
  peer 192.168.1.1 enable
#
```

Run the **display ip routing-table** command to view the route received on Switch A.

The route 1.1.1.1/32 should be received. The route does not appear in the routing table.

### Fault Analysis

To locate the fault, follow the steps described below:

1. Check the routing table on Switch B to confirm whether all the routes are advertised to Switch A.

On Switch B, run the **display bgp routing-table** command and **display bgp routing-table peer 192.168.1.1 advertised-routes** command to display information of the routing table.



If the routes 1.1.1.1/32 and 2.2.2.2/32 have been advertised to Switch A, the fault occurs on Switch A.

2. Check the BGP configuration on Switch A to confirm if the filter is enabled when the route is received.

On Switch A, run the **display current-configuration configuration bgp** command to check the BGP configuration. If the IP-Prefix filter is adopted when Switch A receives the route from Switch B, there is a possibility that all the routes are filtered out.

3. Check the configuration of the IP-Prefix list and confirming if the route is filtered out by the IP-Prefix list.

On Switch A, run the **display ip ip-prefix rta** command to view the filter configuration. If only the route 2.2.2.2/32 is configured with **deny** but the route 1.1.1.1/32 is not configured with **permit**.

Thus, the fault is located.

When Switch A adopts the IP-Prefix list to filter the route received from Switch B and for the non-matched route, the system returns **deny** by default. The route 1.1.1.1/32 is, therefore, filtered out.

## Procedure

**Step 1** Delete the original filtering rule.

**Step 2** Run the **ip ip-prefix rta index 10 permit 1.1.1.1 32** command to create the new filtering rule.

----End

## Summary

When only the **deny** node is configured in the IP-Prefix list, all routes outside the matching address/mask range are denied by default.

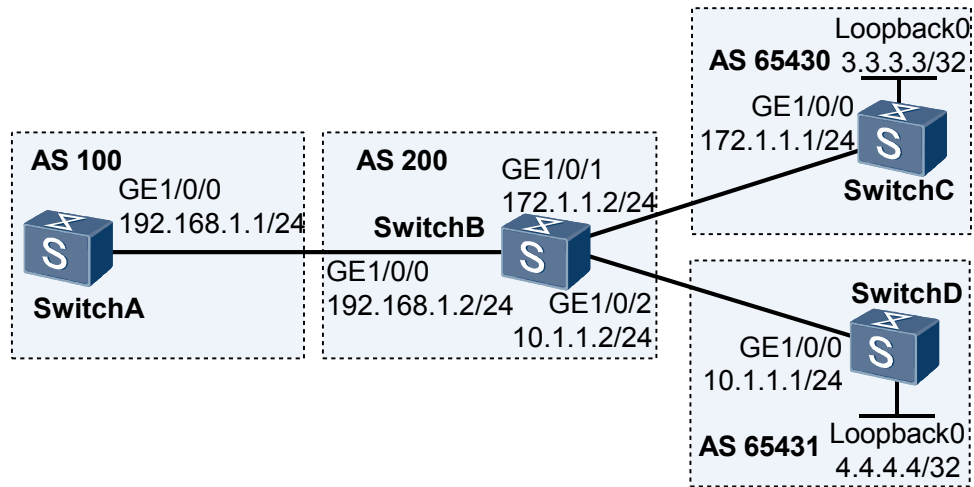
Configure the **permit** node to allow the specified route to pass through, or after the **deny** node is configured, define an entry of **permit 0.0.0.0 greater-equal 0 less-equal 32** to permit all routes to pass through.

For the details, see IP-Prefix in [Configuration Notes](#).

## 5.3.2 Routes Are Lost After AS-Path Is Used

## Fault Symptom

Figure 5-4 Scenario of the AS-Path-Filter troubleshooting



In the networking layout shown in [Figure 5-4](#), Switch A adopts the AS-Path-Filter to filter the route received from Switch B.

Configuration on Switch A:

```
#
bgp 100
 peer 192.168.1.2 as-number 200
#
ipv4-family unicast
 undo synchronization
 peer 192.168.1.2 enable
 peer 192.168.1.2 as-path-filter 10 import
#
ip as-path-filter 10 deny 65430
#
```

Configuration on Switch B:

```
#
bgp 200
 peer 192.168.1.1 as-number 100
 peer 10.1.1.1 as-number 65431
 peer 172.11.10.1 as-number 65430
#
ipv4-family unicast
 undo synchronization
 peer 192.168.1.1 enable
 peer 10.1.1.1 enable
 peer 172.11.10.1 enable
#
```

Configuration on Switch C:

```
#
bgp 65430
 peer 172.11.10.2 as-number 200
#
ipv4-family unicast
 undo synchronization
 network 3.3.3.3 255.255.255.255
```

```
peer 172.11.10.2 enable
#
```

Configuration on Switch D:

```
#
bgp 65431
peer 10.1.1.2 as-number 200
#
ipv4-family unicast
undo synchronization
network 4.4.4.4 255.255.255.255
peer 10.1.1.2 enable
#
```

Run the **display ip routing-table** command to check the route received on Switch A. Then you should find that Switch A filters out the route advertised by Switch C and receives the route advertised by Switch D.

In the routing table, all the routes from Switch C and Switch D are filtered out by Switch A.

## Fault Analysis

The fault indication is that the route advertised by Switch D does not exist in the routing table on Switch A.

To locate the fault, follow the steps described below:

1. Check whether Switch B advertises all the routes to Switch A.  
 On Switch B, run the **display ip routing-table** command to check if Switch B receives the route from Switch C and Switch D. If the route has been received, it can be inferred that the fault occurs on Switch A.
2. Check the BGP configuration on Switch A, to confirm if the filter is enabled when the route is received.  
 On Switch A, run the **display current-configuration configuration bgp** command to check the BGP configuration. Then find BGP uses the AS-Path-Filter named 10. It is possible that all the routes are filtered out.
3. Check the AS-Path regular expression and the filter configuration on Switch A.  
 On Switch A, run the **display ip as-path-filter 10** command to check the configuration of the filter. If only the route with the AS number 65430 is configured with **deny**, and the route with the AS number 65431 is not configured with **permit**, then the fault is located.

## Procedure

**Step 1** Delete the original filtering rule.

**Step 2** Run the **ip as-path-filter 10 permit 65431** command to create the new filter and to check the route received on Switch A. If the route 4.4.4.4/32 appears in the routing table, the fault is removed.

----End

## Summary

When configuring the AS-Path-Filter, note the rule of defining the regular expression. If only the **deny** node is configured, the route outside the matching AS-Path range is denied by default.

Configure the **permit** node to allow the specified route to pass through. See AS-Path-Filter in [Configuration Notes](#).

### 5.3.3 Routes Are Not Filtered Correctly After Community-Filter Is Used

#### Fault Analysis

In general, community filter serves as the matching condition of the **if-match** clause of the Route-Policy.

When **if-match community-filter** < *basic or advanced community-list* > is satisfied, the operation of the **apply** clause is performed on the route.

Pay attention to the rule defining the regular expression in *advanced community-list*. See the rules of the regular expression in the annotations of [Configuration Notes](#).

### 5.3.4 Routes Are Not Filtered Correctly After Extcommunity-Filter Is Used

#### Fault Symptom

For the scenario, see [Figure 5-2](#).

In [Figure 5-2](#):

- CE1, CE3 belong to VPN-A; CE2, CE4 belong to VPN-B.
- VPN-Target of VPN-A is 100:1 while that of VPN-B is 200:1. Users of different VPNs cannot access each other.
- CE and PE exchange the VPN routing information through EBGP.
- Among PEs, the communication is established through OSPF and the VPN routing information is exchanged through MP-IBGP.
- The user adds a VNP-C, Export VPN Targets: 300:1, Import VPN Targets: 100:1 200:1 on PE2. VNP-C can receive the routes from VPN-A and VPN-B.
- The user wants VPN-C to receive the route from VPN-A exclusively. Use the Extcommunity-Filter to filter the route.

Run the following commands:

```
[Quidway] ip vpn-instance vpnc
[Quidway-vpn-instance-vpnc] route-distinguisher 300:1
[Quidway-vpn-instance-vpnc] import route-policy excomm-filter
[Quidway-vpn-instance-vpnc] vpn-target 300:1 export-extcommunity
[Quidway-vpn-instance-vpnc] vpn-target 100:1 200:1 import-extcommunity
```

Run the **display ip routing-table vpn-instance vpnc** command to check the routing table of VPN-C.

The preceding display shows that no expected results are obtained. That is, all the routes are filtered out.

## Fault Analysis

The VPN-C routing table shows that all the routes are filtered out.

To locate the faults, follow the steps described below:

1. Similar to the preceding examples, the faulty source may be the filter.
2. Check the current route-policy and extcommunity-filter.

Run the **display current-configuration configuration route-policy** command to check the Extcommunity-Filter used when VPN-C imports the route.

```
<Quidway> display current-configuration configuration route-policy
#
route-policy excomm-filter permit node 10
  if-match extcommunity-filter 1
#
```

Run the **display ip extcommunity-filter** command to check the filtering rules used in the Extcommunity-Filter of VPN-C.

```
<Quidway> display ip extcommunity-filter
#
Extended Community filter Number 1
    permit rt : 0:0
#
```

3. Locate the cause.

The Extcommunity-Filter applies only to BGP.

BGP has two kinds of extended communities. One is the route target extended community used in VPN. The Extcommunity-Filter is the matching rule of the extended community attribute.

- If the Extcommunity-Filter contains only the VPN-Target, as long as one VPN-Target matches the VPN-Target given by BGP, the filter takes effect. The result **permit** or **deny** is returned.

For example, run the **ip extcommunity-filter permit rt 100:1 rt 200:1** command:

- **rt** configured in BGP: 100:1 300:1 400:1
- Result: **permit**
- **rt** given by BGP: 300:1 400:1
- Result: **deny**

- In the Extcommunity-Filter, if VPN-Target 0:0 is specified, all the VPN-Targets are denied.

For example, run the **ip extcommunity-filter permit rt 0:0** command:

BGP specifies any RT, no matching is performed.

- If the VPN-Target is not specified in the Extcommunity-Filter, regardless of which RT is given by BGP, the result is **permit**.
- As for the deny node, the same rule is adopted.

Check the rule of the Extcommunity-Filter in VPN-C:

**permit rt : 0:0**

RT : 0:0 is applied.

The fault is caused by the Extcommunity-Filter in VPN-C.

RT : 0:0 is used in the **permit rt : 0:0** command. The routes from VPN-A and VPN-B are all filtered out.

## Procedure

**Step 1** Delete the **ip extcommunity-filter 1** command.

**Step 2** Replace the **ip extcommunity-filter 1** command with the following configuration:

```
<Quidway> display ip extcommunity-filter 1
#
Extended Community filter Number 1
    permit rt : 100:1
#
```

----End

## Summary

This is a typical example of Extcommunity-Filter.

Before using the Extcommunity-Filter, learn its application requirements. Pay special attention to the configuration of RT 0:0.

In the Extcommunity-Filter, if VPN-Target 0:0 is specified, all the VPN-Targets are denied.

## 5.3.5 Routes Are Not Correctly Filtered After Route-Policy Is Used

### Fault Symptom

The networking diagram is shown in [Figure 5-2](#).

- CE1 and CE3 belong to VPN-A; CE2 and CE4 belong to VPN-B.
- VPN-Target of VPN-A is 100:1 while that of VPN-B is 200:1. Users of different VPNs cannot access each other.
- CE and PE exchange the VPN routing information through EBGP.
- Among PEs, the communication is achieved through OSPF and the VPN routing information is exchanged through MP-IBGP.
- The user adds a VNP-C, Export VPN Targets: 300:1, Import VPN Targets: 100:1 200:1 on PE2. VNP-C can receive the routes from VPN-A and VPN-B.
- The user wants VPN-C to receive the routes from VPN-A and VPN-B. In addition, the route cost from VPN-A increases by 100 and that from VPN-B increases by 200. Use the Route-Policy filter to achieve the object.

Configure as follows:

```
[Quidway] route-policy Filter-policy permit node 10
[Quidway-route-policy] if-match extcommunity-filter 1
[Quidway-route-policy] apply cost + 100
[Quidway-route-policy] if-match extcommunity-filter 2
[Quidway-route-policy] apply cost + 200
```

Check the VPN-C routing table.

```
<Quidway> display ip routing-table vpn-instance vpnc
#
```

Route Flags: R - relied, D - download to fib

```
-----
Routing Tables: vpnc
      Destinations : 6          Routes : 6
Destination/Mask    Proto  Pre  Cost   Flags  NextHop    Interface
10.1.1.0/24         BGP    255  200    D      1.1.1.9    Vlanif30
```

```

10.2.1.0/24      BGP    255  200      D    1.1.1.9      Vlanif30
10.3.1.0/24      BGP    255  200      D    10.3.1.2     Vlanif10
10.3.1.2/32      BGP    255  200      D    127.0.0.1    InLoopBack0
10.4.1.0/24      BGP    255  200      D    10.4.1.2     Vlanif20
10.4.1.2/32      BGP    255  200      D    127.0.0.1    InLoopBack0
#
    
```

The preceding display shows that in the VPN-C routing table, the cost of both VPN-A routes and VPN-B routes increases by 200.

## Fault Analysis

The cost of the VPN-A route should increase by 100 rather than 200.

Locate the fault according to the following procedures:

1. Similar to the preceding examples, the faulty source may be the filter.
2. Check the current Route-Policy and IP Extcommunity-Filter.

Run the **display current-configuration configuration route-policy** command to check the Route-Policy used when VPN-C imports routes.

```

<Quidway> display current-configuration configuration route-policy
#
route-policy Filter-policy permit node 10
  if-match extcommunity-filter 1 2
  apply cost + 200
#
    
```

Then run the **display ip extcommunity-filter** command to check the Extcommunity-Filter.

```

<Quidway> display ip extcommunity-filter
Extended Community filter Number 1
  permit rt : 100:1
Extended Community filter Number 2
  permit rt : 200:1
    
```

3. Locate the cause.

The application requirements of Route-Policy are as follows:

- Each Route-Policy may consist of multiple nodes.
- The relation among different nodes is OR.
- The system checks each node according to the node number.

As long as one node is matched, the routing information passes the filtration and the matching process ends.

Check the rule of the Filter-Policy in VPN-C:

```

if-match extcommunity-filter 1 2
apply cost + 200
    
```

The relation among the **if-match** clauses is AND.

If the user wants VPN-C to receive both the VPN-A route and the VPN-B route, and wants the cost of VPN-A route to increase by 100 while that of VPN-B route increases by 200, the relation among multiple nodes should be OR.

The fault is caused by the configuration of the policy filter in VPN-C.

## Procedure

- Step 1** Delete the original filtering rule.

**Step 2** Replace the **route-policy filter-policy permit** command with the following configuration.

```
<Quidway> display current-configuration configuration route-policy
route-policy Filter-policy permit node 10
if-match extcommunity-filter 1
apply cost + 100
route-policy Filter-policy permit node 20
if-match extcommunity-filter 2
    apply cost + 200
```

Run the **display ip routing-table vpn-instance vpnc** command to check the VPN-C routing table. The cost of the VPN-A route increases by 100. This indicates that fault is thus removed.

---End

## Summary

The example is the typical example of Route-Policy.

Before using the Route-Policy, learn its application requirements. Note that the relation among different nodes of the Route-Policy is OR, while that among the **if-match** clauses is AND.

## 5.4 FAQs

This section lists frequently asked questions and their answers.

### Q: Configure the IPv4 Prefix List to Filter a Route . Why Does the Filtration not Conform to the Expected Effect?

A: To locate the fault, follow the steps described below:

- Run the **display ip ip-prefix *prefix-list-name*** command to check whether the specified prefix list exists or is applied.
- If the specified prefix list does not exist, the routing policy imports all the routes.
- If the specified prefix list is not matched, the routing policy denies importing all routes.
- Ensure the entry that permits all the routes to pass through is placed after all the filtering rules.

### Q: Configure the IPv6 Prefix List to Filter a Route. Why Does the Filtration not Conform to the Expected Effect?

A: To locate the fault, follow the steps described below:

- Run the **display ip ipv6-prefix *prefix-list-name*** command to check whether the specified prefix list exists or is applied.
- If the specified prefix list does not exist, the routing policy imports all the routes.
- If the specified prefix list is not matched, the routing policy denies importing all routes.
- Ensure the entry that permits all the routes to pass through is placed after all the filtering rules.

### Q: When BGP Uses the AS-Path Filter to Filter a Route, Why Is the Route to Be Filtered out Is not Removed?

A: To locate the fault, follow the steps described below:



- Run the **display bgp routing-table**, **display current-configuration configuration bgp**, or the **display bgp vpnv4 all routing-table** command to check the BGP configuration and confirm the used AS-Path.
- Run the **display ip as-path-filter as-path-list-number** command to check the AS-Path-Filter. Ensure that the regular expression is correct and that at least one permit node is configured after all the **deny** nodes are configured.

### Q: When BGP Uses the Route-Policy to Filter the Specified Route, Why Are all the Routes Filtered out?

A: To locate the fault, follow the steps described below:

- Run the **display current-configuration configuration bgp** command to check the BGP configuration and confirm the used Route-Policy.
- Run the **display route-policy [ route-policy-name ]** command to check the configured routing policy. Configure at least one **permit** node after all the **deny** nodes are configured.

### Q: Why Cannot the BGP Accounting Be Applied When the Routing Protocol Runs Normally?

A: The possible causes include:

- The BGP route cannot be received.
- The adopted routing policy is incorrect.
- The BGP accounting policy is not enabled on the interface.

To locate the fault, follow the steps described below:

- Run the **display ip routing-table** command to check if the route is received. If not, the fault is caused by the incorrect BGP routing policy.
- Run the **display fib** command to check if the MPU delivers the traffic index parameter to the LPU. If not, the fault may be caused by the incorrect configuration of the routing policy.
- Run the **display current-configuration interface** command to check if the BGP accounting is configured on the interface correctly.

BGP accounting is valid only when the router needs to search the forwarding table. For example, if the outbound accounting is configured on the sending interface, BGP accounting is invalid.

## 5.5 Diagnostic Tools

This section describes common diagnostic tools: display commands and debugging commands.

[5.5.1 display Commands](#)

[5.5.2 debugging Commands](#)

### 5.5.1 display Commands

Command	Description
<b>display ip ip-prefix</b> [ <i>ip-prefix-name</i> ]	Displays the current configuration of the IP-Prefix list. For the application of the IP-Prefix in different protocols, refer to corresponding protocols.
<b>display ip ipv6-prefix</b> [ <i>ipv6-prefix-name</i> ]	Displays the current configuration of the IPv6-Prefix filter. For the application of the IPv6-Prefix in different protocols, refer to corresponding protocols.
<b>display ip as-path-filter</b> [ <i>as-path-filter number</i> ]	Displays the current configuration of the AS-Path-Filter. For the application of the AS-Path-Filter in different protocols, refer to corresponding protocols.
<b>display ip community-filter</b> [ <i>basic-comm-filter-num</i>   <i>adv-comm-filter-num</i>   <i>comm-filter-name</i> ]	Displays the current configuration of the Community-Filter. The filter with the number ranging from the 1 to 99 is the basic community filter, while that with the number ranging from 100 to 199 is the advanced community filter.
<b>display ip extcommunity-filter</b> [ <i>extcomm-filter number</i> ]	Displays the current configuration of the Extcommunity-Filter.
<b>display route-policy</b> [ <i>route-policy-name</i> ]	Displays the current configuration of the Route-Policy filter. For the application of the Route-Policy in different protocols, refer to corresponding protocols.

## 5.5.2 debugging Commands

Command	Description
<b>debugging rm policy</b> [ <b>ip-prefix</b> <i>ip-prefix-name</i> ]	Enables the route debugging of the routing policy. Displays information about the routing policy. If <b>ip-prefix</b> is used, check the policy of the route with specified IPv4 prefix.