



Quidway S9300 Terabit Routing Switch
V100R001C03

Troubleshooting - IP Routing

Issue 01
Date 2009-07-28

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

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

Copyright © Huawei Technologies Co., Ltd. 2009. 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 the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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 the statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

About This Document.....	1
1 RIP Troubleshooting.....	1-1
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
2 OSPF Troubleshooting.....	2-1
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.....	2-3
2.2.1 Typical Networking.....	2-3
2.2.2 Configuration Notes.....	2-4
2.2.3 Troubleshooting Flowchart.....	2-7
2.2.4 Troubleshooting Procedure.....	2-8
2.3 Troubleshooting Cases.....	2-10
2.3.1 S9300s Cannot Learn the Internal Route After the Vlink is Configured.....	2-10
2.4 FAQs.....	2-11
2.5 Diagnostic Tools.....	2-16

2.5.1 display Commands.....	2-16
2.5.2 debugging Commands.....	2-17
3 IS-IS Troubleshooting.....	3-1
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 Troubleshooting the IS-IS Neighbor Relationship.....	3-4
3.2.1 Typical Networking.....	3-4
3.2.2 Configuration Notes.....	3-5
3.2.3 Troubleshooting Flowchart.....	3-6
3.2.4 Troubleshooting Procedure.....	3-8
3.3 Troubleshooting the IS-IS Routing Table.....	3-9
3.3.1 Typical Networking.....	3-9
3.3.2 Configuration Notes.....	3-10
3.3.3 Troubleshooting Flowchart.....	3-10
3.3.4 Troubleshooting Procedure.....	3-11
3.4 Troubleshooting an IS-IS Interface.....	3-12
3.4.1 Typical Networking.....	3-12
3.4.2 Configuration Notes.....	3-12
3.4.3 Troubleshooting Flowchart.....	3-13
3.4.4 Troubleshooting Procedure.....	3-13
3.5 Troubleshooting Link Status Advertisement.....	3-14
3.5.1 Typical Networking.....	3-14
3.5.2 Configuration Notes.....	3-15
3.5.3 Troubleshooting Flowchart.....	3-15
3.5.4 Troubleshooting Procedure.....	3-16
3.6 FAQs.....	3-16
3.7 Diagnostic Tools.....	3-21
3.7.1 display Commands.....	3-21
3.7.2 debugging Commands.....	3-22
4 BGP Troubleshooting.....	4-1
4.1 BGP Overview.....	4-2
4.1.1 Introduction to BGP.....	4-2
4.1.2 BGP Route Attributes.....	4-2
4.1.3 Faults and Solutions on Large-Scale BGP Networks.....	4-3
4.2 BGP Peer Relationship Troubleshooting.....	4-4
4.2.1 Typical Networking.....	4-4
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 Peer Relationship Troubleshooting.....	4-10
4.3.1 Typical Networking.....	4-10

4.3.2 Configuration Notes.....	4-10
4.3.3 Troubleshooting Flowchart.....	4-10
4.3.4 Troubleshooting Procedure.....	4-11
4.4 Route Loss Troubleshooting When BGP Peers Exchange Update Messages.....	4-13
4.4.1 Typical Networking.....	4-14
4.4.2 Configuration Notes.....	4-14
4.4.3 Troubleshooting Procedure.....	4-14
4.4.4 Troubleshooting Procedure.....	4-15
4.5 Troubleshooting Cases.....	4-17
4.5.1 Routing Loop and Route Flapping.....	4-17
4.5.2 Peer Relationship Is Torn Down When the Number of Routes Does not Exceed the Threshold.....	4-19
4.6 FAQs.....	4-22
4.7 Diagnostic Tools.....	4-25
4.7.1 display Commands.....	4-25
4.7.2 debugging Commands.....	4-27
5 Routing Policy Troubleshooting.....	5-1
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 Routing Policy.....	5-2
5.2 Routing Policy Troubleshooting.....	5-3
5.2.1 Typical Networking.....	5-3
5.2.2 Configuration Notes.....	5-4
5.2.3 Troubleshooting Flowchart.....	5-5
5.2.4 Troubleshooting Procedure.....	5-6
5.3 Troubleshooting Cases.....	5-7
5.3.1 Routes Are Lost After the IP Prefix List Is Used.....	5-7
5.4 FAQs.....	5-8
5.5 Diagnostic Tools.....	5-9
5.5.1 display Commands.....	5-10
5.5.2 debugging Commands.....	5-10

Figures

Figure 1-1 Typical networking of RIP.....	1-2
Figure 1-2 RIP route receiving troubleshooting flowchart.....	1-5
Figure 1-3 RIP route sending troubleshooting flowchart.....	1-8
Figure 1-4 Networking diagram of RIP.....	1-10
Figure 2-1 OSPF typical networking.....	2-4
Figure 2-2 Troubleshooting flowchart of the OSPF neighbor fault.....	2-8
Figure 2-3 OSPF Vlink networking.....	2-10
Figure 3-1 Typical networking of IS-IS.....	3-5
Figure 3-2 Networking diagram of IS-IS neighbor relationship.....	3-7
Figure 3-3 Flowchart for troubleshooting the IS-IS routing table.....	3-11
Figure 3-4 Flowchart for troubleshooting the IS-IS interface.....	3-13
Figure 3-5 Typical networking of IS-IS link.....	3-14
Figure 3-6 Flowchart for troubleshooting the change of the link status.....	3-15
Figure 4-1 Typical networking diagram of BGP.....	4-5
Figure 4-2 BGP peer relationship troubleshooting flowchart.....	4-8
Figure 4-3 BGP peer relationship troubleshooting flowchart.....	4-11
Figure 4-4 BGP route loss troubleshooting flowchart.....	4-15
Figure 4-5 Typical networking diagram of BGP.....	4-17
Figure 4-6 Networking diagram that peer relationship is torn down but the number of routes does not exceed the threshold.....	4-20
Figure 5-1 Typical networking diagram of the routing policy troubleshooting in a public network.....	5-3
Figure 5-2 Troubleshooting flowchart of the routing policy.....	5-6

Tables

Table 2-1 OSPF configuration notes.....	2-4
Table 2-2 OSPF display commands.....	2-16
Table 2-3 OSPF debugging commands.....	2-17
Table 3-1 IS-IS Configuration Notes.....	3-5
Table 3-2 IS-IS routing table configuration notes.....	3-10
Table 3-3 IS-IS interface configuration notes.....	3-12
Table 3-4 IS-IS link configuration notes.....	3-15
Table 3-5 Relationship between the IS-IS interface cost and the bandwidth.....	3-18
Table 3-6 Commands for configuring IS-IS packet timers.....	3-18
Table 3-7 Commands for configuring IS-IS timers.....	3-19
Table 3-8 Is-Is display commands.....	3-21
Table 3-9 Is-Is debugging commands.....	3-22
Table 4-1 Type of BGP route attributes.....	4-2
Table 4-2 Main BGP route attributes.....	4-3
Table 4-3 Faults and solutions on large-scale BGP networks.....	4-3
Table 4-4 BGP configuration notes.....	4-5
Table 4-5 Error code of Open messages.....	4-10
Table 4-6 Prerequisites for setting up BGP peer.....	4-11
Table 4-7 Error code of Open messages.....	4-12
Table 4-8 Priority of policies for modifying the MED.....	4-23
Table 4-9 BGP display commands.....	4-25
Table 4-10 BGP debugging commands.....	4-27
Table 5-1 Routing policy configuration notes.....	5-4
Table 5-2 Routing policy display commands.....	5-10
Table 5-3 Routing policy debugging commands.....	5-10

About This Document

Purpose

This part describes the organization of this document, product version, intended audience, conventions, and update history.

Related Versions

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

Product Name	Version
S9300	V100R001C03

Intended Audience

This document is intended for:

- System Maintenance Engineer
- Commissioning Engineer
- Network Monitoring Engineer

Organization

This document consists of four chapters and is organized as follows.






Chapter	Describes
1 RIP Troubleshooting	This chapter describes the knowledge related to RIP troubleshooting, including RIP overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases and diagnostic tools and FAQs.

Chapter	Describes
2 OSPF Troubleshooting	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.
3 IS-IS Troubleshooting	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.
4 BGP Troubleshooting	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.
5 Routing Policy Troubleshooting	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.

Conventions

Symbol Conventions

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

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

General Conventions

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

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in boldface . For example, log in as user root .
<i>Italic</i>	Book titles are in <i>italics</i> .
Courier New	Examples of information displayed on the screen are in Courier New.

Command Conventions

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

Convention	Description
Boldface	The keywords of a command line are in boldface .
<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.

GUI Conventions

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

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in boldface . For example, click OK .

Convention	Description
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard Operations

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

Format	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+Alt+A means the three keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, A means the two keys should be pressed in turn.

Mouse Operations

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

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Update History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Updates in Issue 01 (2009-07-28)

Initial commercial release.

1 RIP Troubleshooting

About This Chapter

This chapter describes the knowledge related to RIP troubleshooting, including RIP overview, troubleshooting flowchart and troubleshooting procedure in typical networking, troubleshooting cases and diagnostic tools 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 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 or 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](#)

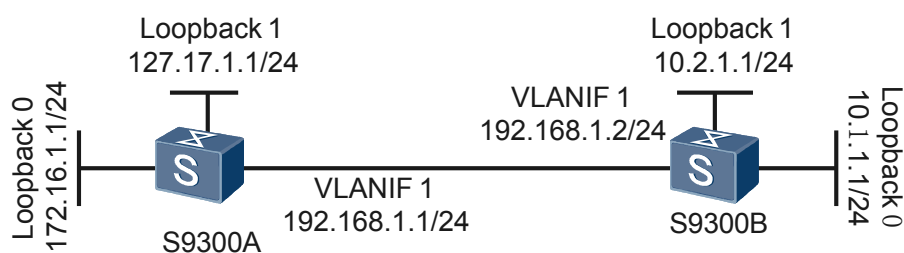
[1.2.4 Troubleshooting Procedure](#)

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 S9300—A and S9300—B.
- Loopback interfaces are used to simulate the related network segment.

Through the RIP protocol, the S9300s 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 rip [<i>process-id</i>] [vpn-instance <i>vpn-instance-name</i>] command in the system view.</p>
	Configuring a network	<p>Enable RIP in the specified network segment.</p> <p>The network address that is enabled by the network command must be an address of the natural network segment.</p> <p>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 network <i>network-address</i> command in the RIP view.</p>
	Configuring RIP to import routes	<p>Import routes 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 import-route <i>protocol</i> [cost <i>cost</i>] [route-policy <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.</p> <p>RIP-1 is a type of classful routing protocol. The RIP-1 routes are advertised through broadcast. 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 identify only 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 version { 1 2 } command in the RIP view.</p>

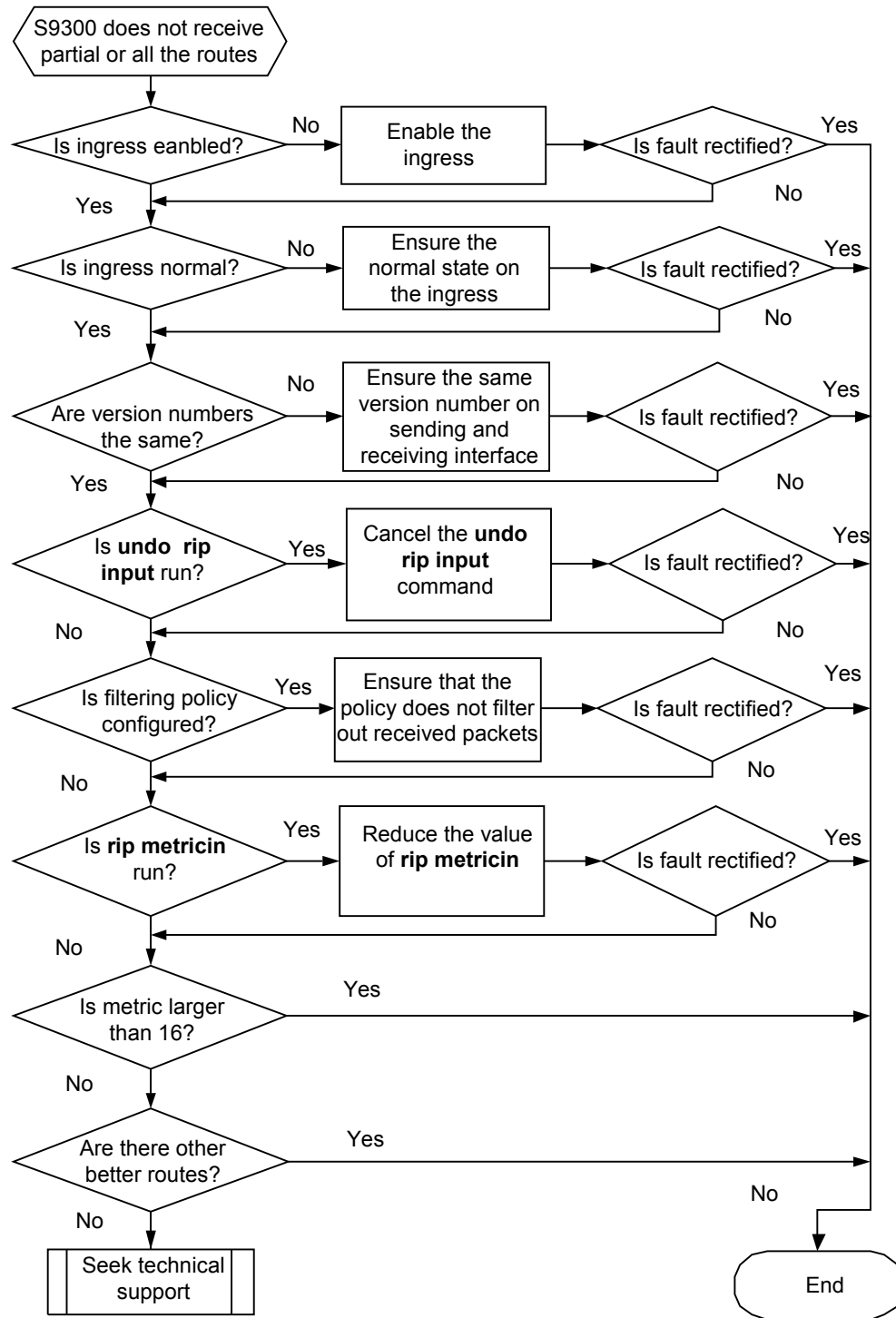
1.2.3 Troubleshooting Flowchart

In the networking shown in [Figure 1-1](#), you may find the following symptoms when all S9300s are configured:

- Certain S9300s do not learn partial or all the routes.
- The output of the **display ip routing-table** command shows that 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 network segment of the interface. Only the interface enabled with RIP can receive and send the RIP routing information.

Run the **display current-configuration configuration rip** command to check whether the incoming interface exists in the display about the current enabled RIP.

The network address enabled by the **network** command must be an address 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 learned by RIP from the interface changes to 16, and then is deleted.

Therefore, you must ensure that the status of the interface is normal.

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 RIP version configured on the incoming interface and the version of RIP packets are different, the RIP routing information may not be received.

Step 4 Check whether the **undo rip input** command is run 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 run 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 check 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 metric in** command and the metric is larger than 16.

The **rip metric in** 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.

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 learn 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 case 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 the weight of RIP. The route learned through OSPF or IS-IS is preferred.

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

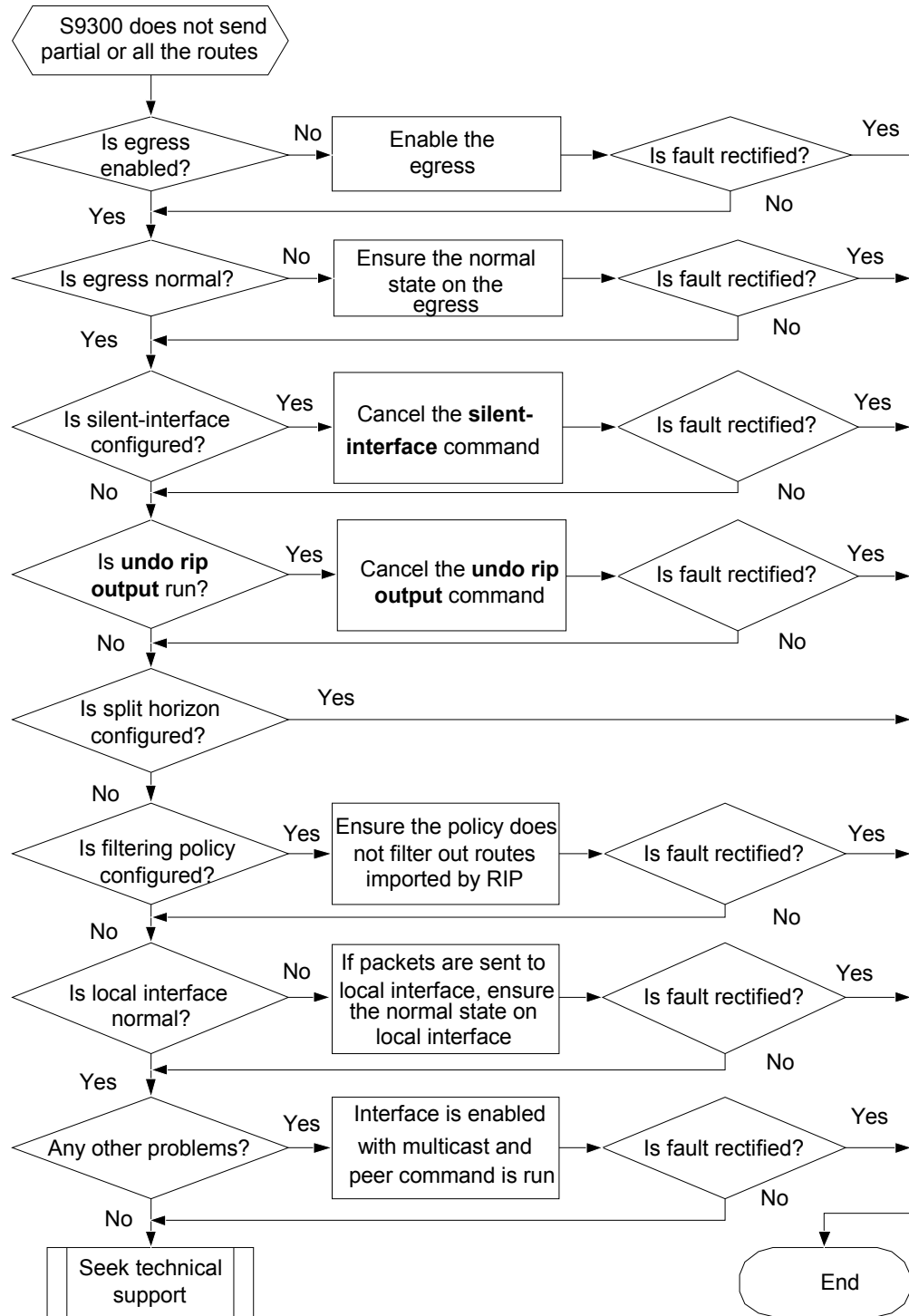
See section [Configuration Notes](#).

1.3.3 Troubleshooting Flowchart

In the networking shown in [Figure 1-1](#), the S9300 cannot send partial or all of the routes after the configuration on each S9300 is complete.

[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.

Enable the interface if it is disabled.

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 input** 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. If the command is configured, the split-horizon is enabled on the outgoing interface.

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 S9300s 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.

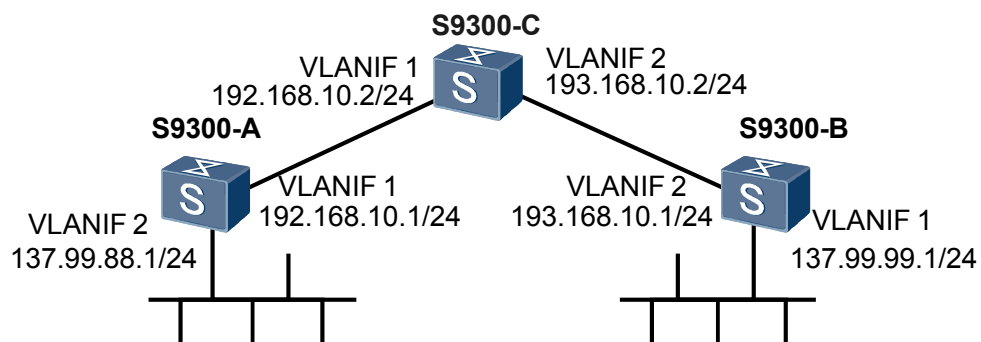
1.4.1 Discontinuous Subnet Fault

1.4.1 Discontinuous Subnet Fault

Fault Symptom

As shown in [Figure 1-4](#), the RIP 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 S9300C.
- The next hop of the route is 192.168.10.1 or 193.168.10.1.

```
<S9300C> display ip routing-table
Routing Tables: Public
    Destinations : 9          Routes : 10
Destination/Mask    Proto  Pre  Cost    Flags NextHop         Interface
   127.0.0.0/8      Direct 0    0        D 127.0.0.1       InLoopBack0
   127.0.0.1/32     Direct 0    0        D 127.0.0.1       InLoopBack0
   137.99.0.0/16    RIP    100  1        D 192.168.10.1    vlanif 1
                   RIP    100  1        D 193.168.10.1    vlanif 2
   192.168.10.0/24  Direct 0    0        D 192.168.10.2    vlanif 1
   192.168.10.1/32  Direct 0    0        D 192.168.10.1    vlanif 1
   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    vlanif 2
   193.168.10.1/32  Direct 0    0        D 193.168.10.1    vlanif 2
   193.168.10.2/32  Direct 0    0        D 127.0.0.1       InLoopBack0
```

In **Figure 1-4**, S9300C should have two routes:

- 137.99.88.0/24 that is forwarded to S9300A
- 137.99.99.0/24 that is forwarded to S9300B

Fault Analysis

1. Run the **debugging rip send** command on S9300A and S9300B respectively. Then by observing the RIP packet that is sent from POS 2/0/0, you can find:
 - S9300A sends classful 137.99.0.0 to S9300C.
 - S9300B sends classful 137.99.0.0 to S9300C.
2. The routing table of S9300C shows that S9300C receives only one of the two routes. 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.

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 RIP version.
- Step 4** Run the **undo summary** command to cancel the classful aggregation.

----End

Summary

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

- (Recommended) Configure RIP-2 on the network and cancel the classful aggregation on S9300A and S9300B.
- (Not recommended) 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 S9300A and S9300C and configure the network segment 137.99.77.0/24 between S9300C and S9300B.

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

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 Up state. 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 Cannot the RIP Database 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 run on the switch. If the command is run, the default routing information sourced from other routes cannot be received.
- Check whether the RIP receives other routes with smaller costs.
- Check whether the number of equal-cost routes received by RIP reaches the maximum.

- Check whether the sum of the routing cost and additional cost 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. By default, the host route is enabled.

Q: Configure the Interface to Send RIP-2 Routes. Debugging Information Shows That the Routes Sent by RIP-2 Carrying the Class A, Class B, or Class C Masks. 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 disable the aggregation. Thus, the route with the classless mask is produced.

Q: After the silent-interface all Command Is Run in the RIP View, Why is the RIP Route Still Received?

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

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

A: The length of tag field specified by RIP is 16 bits, while the length of tag field specified 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 and the incorrect match is produced.

Q: Why Is the summary Command Invalid After It Is Run to Perform Route Aggregation?

A: For RIP-2, the **summary** command takes effect on the condition that the split-horizon and poison reverse are disabled 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 Route Flapping?

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

- If the values of the four timers are set improperly, route flapping occurs. To solve this problem, set the values of timers properly. The relations between the values are as follows:
 - The update timer is smaller than the aging timer.
 - The suppress timer is smaller than the garbage-collect timer.
- 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 RIP-enabled interface changes frequently, route flapping occurs. To address this problem, find out why the status of the interface changes frequently.

Q: What Are the Requirements for Configuring RIP Authentication Key?

A: A RIP authentication key is expressed in plain text or cipher text by complying with the following rules:

- An authentication key in plain text is a string of 1 to 16 bytes.
- An authentication key in cipher text can be either a plain text string of 1 to 16 bytes or a cipher text string of 24 bytes.
- Space is not allowed in all authentication keys.

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

1.6.2 debugging Commands

Command	Description
debugging rip backup	Enables the debugging of RIP backup.
debugging rip <i>process-id</i> brief	Enables the debugging of brief information about RIP packets.
debugging rip <i>process-id</i> error	Enables the debugging of incorrect brief information about RIP.

Command	Description
debugging rip <i>process-id</i> event	Enables the debugging of RIP events.
debugging rip <i>process-id</i> job	Enables the debugging of RIP job.
debugging rip miscellaneous	Enables the debugging of RIP packets that are not related to the process.
debugging rip <i>process-id</i> packet	Enables the debugging of RIP packets. You can then know the process of transmitting RIP packets.
debugging rip <i>process-id</i> receive	Enables the debugging of the process of receiving RIP packets.
debugging rip <i>process-id</i> route-processing	Enables the debugging of the RIP route calculation.
debugging rip <i>process-id</i> send	Enables the debugging of the process of sending RIP packets.
debugging rip <i>process-id</i> timer	Enables the debugging of RIP timers.

2 OSPF Troubleshooting

About This Chapter

This chapter describes the procedure and diagnostic tools of OSPF troubleshooting.

[2.1 OSPF Overview](#)

This section describes the information 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 Troubleshooting Cases](#)

This section presents several troubleshooting cases.

[2.4 FAQs](#)

This section lists frequently asked questions and their answers.

[2.5 Diagnostic Tools](#)

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

2.1 OSPF Overview

This section describes the information 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).

When configuring OSPF, you first need to enable OSPF on an interface and specify the area ID. When OSPF is disabled, the interface parameters related to OSPF become invalid immediately.

2.1.2 Basic Concepts

Router ID

Router ID indicates the ID of the router.

To run the OSPF protocol, an S9300 must have the router ID. If the ID is not configured, the system chooses an ID from the IP addresses of the current interfaces.

Designated Router

The designated router (DR) is not specified by the user, but elected by the nodes on the network segment. All the nodes send messages to the DR. The DR advertises the status of the network link.

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

No neighbor relationship is set up between DR Others and no routing information is exchanged between them.

Backup Designated Router

The backup designated router (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 nodes 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 S9300s in the AS into different groups. The S9300 resides on the border of the area. Thus, certain S9300s belong to different areas.

The S9300 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.

Virtual link

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

Backbone Area

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

Summary

Summary indicates route aggregation.

The route aggregation can reduce the routing information exchanged between areas, diminish the size of the routing table, and speed up the calculation of the S9300.

Graceful Restart

To avoid unnecessary SPF calculation, the switch informs its adjacent node that it recovers in a few seconds after it restarts. Thus, the adjacent node does not delete it from the neighbor list. The other routers are not informed of the restarting of the switch.

Traffic Engineering

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

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](#)

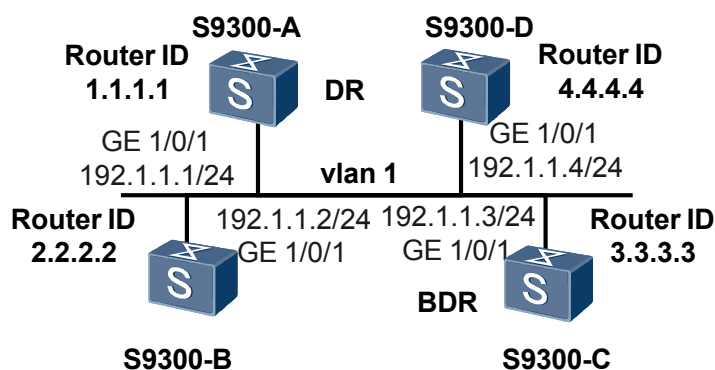
[2.2.4 Troubleshooting Procedure](#)

2.2.1 Typical Networking

Figure 2-1 shows the typical OSPF networking.

Figure 2-1 is a networking diagram for OSPF troubleshooting.

Figure 2-1 OSPF typical networking



In **Figure 2-1**:

- S9300-A has the highest priority of 100. It is elected as the DR.
- The priority of S9300-C is second to that of S9300-A. It is elected as the BDR.
- The priority of S9300-B is 0.
- S9300-D uses the default priority of 1.

S9300-A, S9300-B, S9300-C, and S9300-D set up OSPF neighbor with each other.

2.2.2 Configuration Notes

Table 2-1 OSPF configuration notes

Item	Sub-item	Notes and Configuration Commands
Enabling OSPF	Configuring a router ID	The router IDs of all nodes in the same AS are different. To configure a router ID, run the OSPF [process-id] router-id router-id * command in the system view.
	Configuring a peer	On a Non-Broadcast Multi-Access (NBMA) network, you can configure mapping to make the entire network fully-meshed. That is, there is a Virtual Link (Vlink) between any two S9300s on the network. In this case, the processing mode of OSPF is the same as that on broadcast networks, such as electing a DR or a BDR. OSPF, however, cannot discover neighboring nodes by broadcasting Hello packets. You must manually assign an IP address to the neighboring node and set the election for the neighboring node. To configure a peer, run the peer ip-address [dr-priority priority] command in the OSPF view.

Item	Sub-item	Notes and Configuration Commands
	Configuring OSPF to import routes	<p>The routes of different OSPF processes are isolated from each other.</p> <p>To configure OSPF to import routes, run the import-route protocol [<i>process-id</i>] [cost cost tag tag type type] * [route-policy route-policy-name] command in the OSPF view.</p>
	Configuring an area	<p>There must be a backbone area (area 0) on a network.</p> <p>To configure an area, run the area { <i>area-id-integer</i> <i>area-id-address</i> } command in the OSPF view.</p>
	Configuring a network	<p>It is used to specify the OSPF-enabled interface and the area to which the interface belongs.</p> <p>An interface can only belong to a specified area.</p> <p>To configure a network, run the network ip-address wildcard-mask command in the OSPF area view.</p>
	Configuring the authentication mode	<p>It is used to set the authentication mode and authentication key.</p> <p>To configure the authentication mode, run the following commands in related views:</p> <ul style="list-style-type: none"> ● authentication-mode simple { [plain] <i>plain-text</i> cipher cipher-text } (OSPF area view) ● authentication-mode { md5 hmac-md5 } [<i>key-id</i> { plain plain-text [cipher] <i>cipher-text</i> }] (OSPF area view) ● OSPF authentication-mode simple { [plain] <i>plain-text</i> cipher cipher-text } (VLANIF interface view and loopback interface view) ● OSPF authentication-mode { md5 hmac-md5 } [<i>key-id</i> { plain plain-text [cipher] <i>cipher-text</i> }] (VLANIF interface view and loopback interface view) ● OSPF authentication-mode null (VLANIF interface view and loopback interface view)
	Configuring an NSSA area	<p>Configure an NSSA area.</p> <p>To configure an NSSA area, run the nssa [default-route-advertise flush-waiting-timer time no-import-route no-summary set-n-bit] * command in the OSPF area view.</p>
	Configuring a stub area	<p>Configure a Stub area.</p> <p>To configure a stub area, run the stub [no-summary] command in the OSPF area view.</p>
	Setting the cost of an OSPF interface	<p>Set the cost of the OSPF protocol on the interface.</p> <p>To set the cost of the OSPF protocol on the interface, run the OSPF cost cost command in VLANIF interface view or loopback interface view.</p>

Item	Sub-item	Notes and Configuration Commands
	Configuring the DR priority	The interface with the highest priority is elected as the DR. To configure the DR priority, run the OSPF dr-priority priority command in the VLANIF interface view or loopback interface view.
	Setting a network type	It is used to set the network type of the OSPF interface. To set a network type, run the OSPF network-type { broadcast nbma p2mp } command in the VLANIF interface view or loopback interface view.
	Configuring a timer	It is used to set the interval for sending such packets as the Hello packets and the Dead packets on the interface. To configure a timer, run the following commands: <ul style="list-style-type: none"> • OSPF timer dead interval (VLANIF interface view and loopback interface view) • OSPF timer hello interval (VLANIF interface view and loopback interface view) • OSPF timer poll interval (VLANIF interface view and loopback interface view) • OSPF timer retransmit interval (VLANIF interface view and loopback interface view)

 **NOTE**

The following configuration commands are related to OSPF. For details, refer to the *Quidway S9300 Terabit Routing Switch Configuration Guide - IP Routing*.

The configuration is described as follows:

Configure S9300-A.

```
[S9300-A] interface gigabitethernet 1/0/1
[S9300-A-GigabitEthernet1/0/1] port trunk allow-pass vlan 1
[S9300-A-GigabitEthernet1/0/1] quit
[S9300-A] interface vlanif 1
[S9300-A-Vlanif1] ip address 192.1.1.1 255.255.255.0
[S9300-A-Vlanif1] OSPF dr-priority 100
[S9300-A-Vlanif1] quit
[S9300-A] router id 1.1.1.1
[S9300-A] OSPF
[S9300-A-OSPF-1] area 0
[S9300-A-OSPF-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

Configure S9300-B.

```
[S9300-B] interface gigabitethernet 1/0/1
[S9300-B-GigabitEthernet1/0/1] port trunk allow-pass vlan 1
[S9300-B-GigabitEthernet1/0/1] quit
[S9300-B] interface vlanif 1
[S9300-B-Vlanif1] ip address 192.1.1.2 255.255.255.0
[S9300-B-Vlanif1] OSPF dr-priority 0
[S9300-B-Vlanif1] quit
[S9300-B] router id 2.2.2.2
[S9300-B] OSPF
[S9300-B-OSPF-1] area 0
```

```
[S9300-B-OSPF-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255

# Configure S9300-C.

[S9300-C] interface gigabitethernet 1/0/1
[S9300-C-GigabitEthernet1/0/1] port trunk allow-pass vlan 1
[S9300-C-GigabitEthernet1/0/1] quit
[S9300-C] interface vlanif 1
[S9300-C-Vlanif1] ip address 192.1.1.3 255.255.255.0
[S9300-C-Vlanif1] OSPF dr-priority 2
[S9300-C-Vlanif1] quit
[S9300-C] router id 3.3.3.3
[S9300-C] OSPF
[S9300-C-OSPF-1] area 0
[S9300-C-OSPF-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255

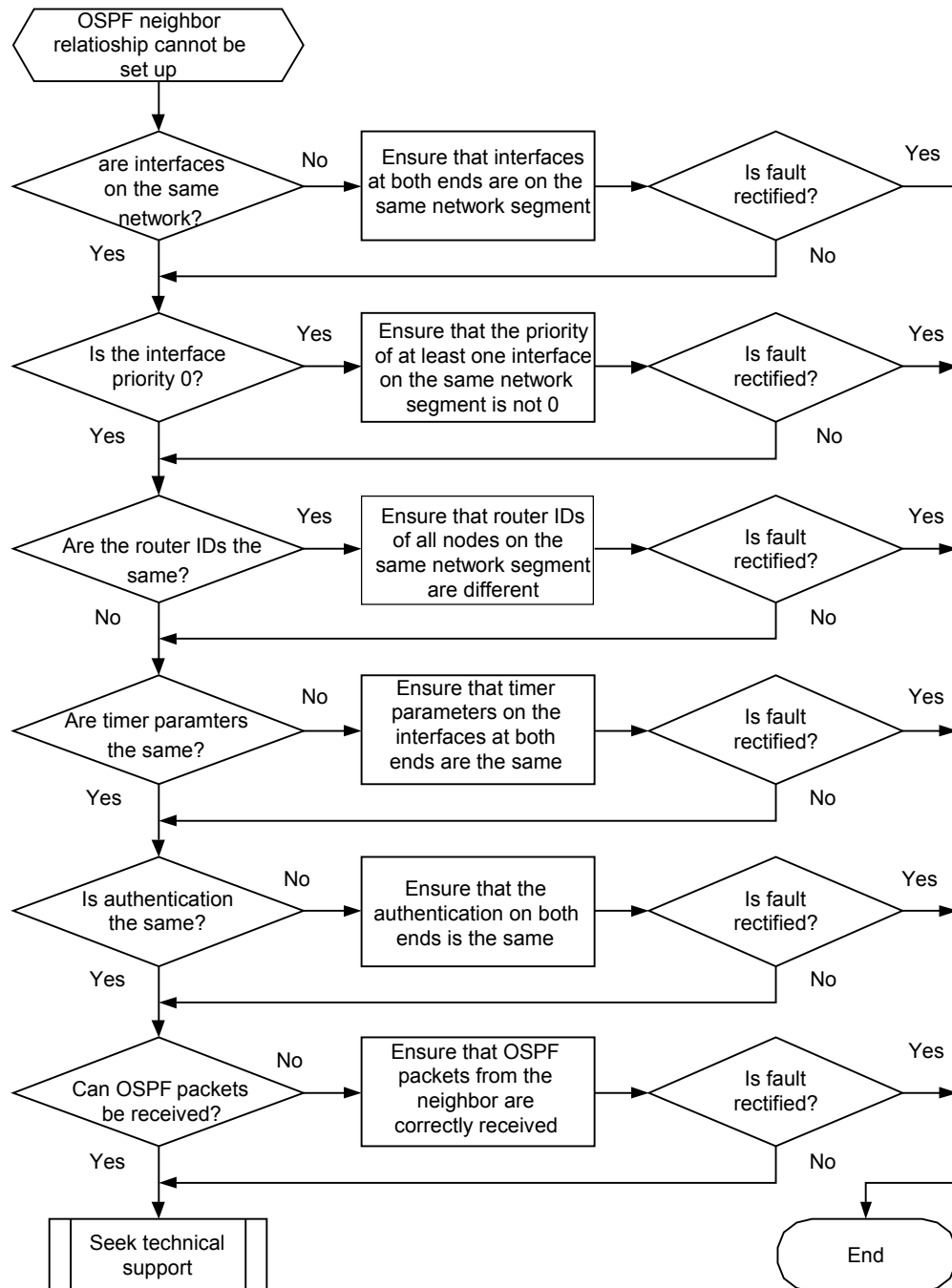
# Configure S9300-D.

[S9300-D] interface gigabitethernet 1/0/1
[S9300-D-GigabitEthernet1/0/1] port trunk allow-pass vlan 1
[S9300-D-GigabitEthernet1/0/1] quit
[S9300-D] interface vlanif 1
[S9300-D-Vlanif1] ip address 192.1.1.4 255.255.255.0
[S9300-D-Vlanif1] quit
[S9300-D] router id 4.4.4.4
[S9300-D] OSPF
[S9300-D-OSPF-1] area 0
[S9300-D-OSPF-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

2.2.3 Troubleshooting Flowchart

In the networking shown in [Figure 2-1](#), the OSPF neighbor cannot be set up after the configuration.

[Figure 2-2](#) shows the flowchart of troubleshooting the OSPF neighbor fault.

Figure 2-2 Troubleshooting flowchart of the OSPF neighbor fault

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 on 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, 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 the DR to 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 that the router ID is unique on the network segment.

The router IDs on the same network segment 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), Point-to-Multipoint (P2MP) and broadcast interfaces send the Hello packet at the interval of 10 seconds, while the NBMA interface sends 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, P2MP, and broadcast interfaces is 40 seconds, while that on the NBMA interface is 120 seconds.

The same Timer parameters must be set on the corresponding interfaces. Otherwise, the adjacency cannot be set up.

You can run the **display OSPF interface** 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 the interface is neither configured with authentication nor configured as Null, authentication configured on the area is adopted.
- If the authentication is configured on neither the interface nor the 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 fail to be received, run the **debug ip packet** command to check the debugging information of IP packets and confirm whether the packets are forwarded successfully on the IP layer. You can use the ACL filter to filter the debugging information.

If the fault persists, contact the Huawei technical personnel.

----End

2.3 Troubleshooting Cases

This section presents several troubleshooting cases.

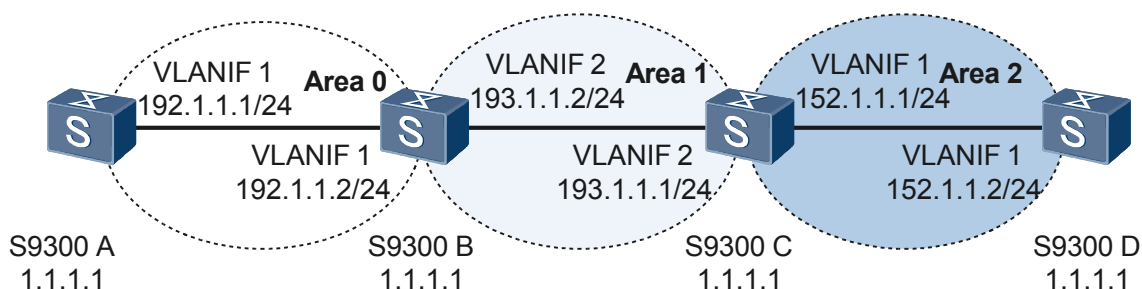
2.3.1 S9300s Cannot Learn the Internal Route After the Vlink is Configured

2.3.1 S9300s Cannot Learn the Internal Route After the Vlink is Configured

Fault Symptom

Figure 2-3 shows the OSPF Vlink networking.

Figure 2-3 OSPF Vlink networking



After the configurations are complete, the S9300s 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 on S9300-C to view the Summary LSA generated on ABR S9300-C. You can find that the Summary LSA is normal.
2. Run the **display ospf peer** command on S9300-B to view the neighbor relations. You can find that the neighbor relations between S9300-A, S9300-B, and S9300-C are normal.
3. Run the **ospf** command on S9300-D to enter the OSPF view and view the configuration of the Vlink.

OSPF prescribes that all the areas must be connected with the backbone area, namely, area 0. Run the **vlink-peer** command to set the logical connectivity. Check the Vlink configuration and you can find that the configuration of the Vlink 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 status.

The fault occurs in the process of specifying the router ID of the Vlink peer.

Procedure

- Step 1** Run the **system-view** command on S9300-D to enter the system view.
- Step 2** Run the **OSPF [process-id | router-id router-id] *** 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.

After the preceding configurations are complete, run the **display OSPF vlink** command to check the status of the peer. You can find the ID of the peer on the other end of the Vlink. The S9300s in area 2 can learn internal routes of area 0. The fault is thus rectified.

----End

Summary

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

2.4 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.

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 can form a network address.
- Ensure that there is no repeated host addresses on the network.
- Ensure that there is no repeated network addresses on the network.

Q: Why Does LSDB Not Show the Imported External Routes?

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

- Run the **display OSPF interface** command to check that the interface importing the external route is not Down.
- Run the **display OSPF brief** command to check that the node 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 whether the neighbor status is Full.
- Check whether the **lsdb-overflow-limit** command is run 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 run to aggregate the external routes.

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

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 continuous, divide them into several groups of continuous network segment addresses.
- Run the **abr-summary** command to configure route summary on the ABR for each group of continuous network segment addresses.
- Run the **filter { acl | ip-ip prefix | route-policy } { import | export }** command in the OSPF area view to check that the LSA aggregated by the ABR is not filtered out.

Q: Why Cannot the OSPF Route Contained in LSDB Be Found?

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 routes are 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 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 S9300.
- 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 whether the network connection is normal.
- Check whether there are repeated IP addresses on the network.
- If the network is busy, increase the retransmission interval and retransmission timeout period of the MIB browser.

- Check whether the OSPF instance is enabled with MIB-Binding.
- The trap address specified by the **snmp-agent target-host** command must be the same as the IP address of the MIB browser. In addition, ensure that there is a route to 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 status of the interface on the Restarter end changes.

Q: Why Cannot the External Route Be Imported If the Limit of LSDB Is Reached?

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

- Check whether the **Lsdb-Overflow-Limit** is configured on the S9300.
- Check the configuration of the **maximum-routes { intra | inter | external }** command.

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:
Reference bandwidth/Interface bandwidth.

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

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

A: OSPF sends the acknowledgement packet after receiving the LSA packet. If no acknowledgement packet is received, the S9300 resends the LSA packet to the peer.

The interval between two LSA packets 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 data link status to all the S9300s on the network.

The BDR refers to the backup designated router.

The DR Other refers to the device that is neither the DR nor BDR. The priority of the DR Other is 0.

Q: Why the DR and BDR in Full State Cannot Be Viewed on the P2P Link?

A: It is a normal situation. There is no DR or BDR on P2P and P2MP networks.

Q: Can the S9300 in an OSPF Area Set Up the Neighbor Relationship with the S9300 That Resides on Another Subnet?

A: The two S9300s on different subnets can set up the neighbor relationship if they are connected through the P2P link. In other situations, the two S9300s must reside on the same subnet if they need to set up the neighbor relationship.

Q: What Is the Interval for Sending LSAs in OSPF?

A: When the LSA of OSPF is up to the time of refreshing the link status (18005 seconds), OSPF updates its LSA and advertises the LSA outside. On a stable network, if the speed of route convergence is required to be fast, you can cancel the interval for updating LSA by using the **lsa-originate-interval 0** command. Then, the changes of the topology or routes are advertised to the network through LSA immediately.

Q: How to Disable an S9300 on an Interface from Setting Up Neighbor Relations?

A: Running the **silent-interface** command in the OSPF view can prohibit S9300s from setting up neighbor relations through interfaces. 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. Then, run the **undo silent-interface** command to enable the specified interfaces.

Q: What Is the Function of the Domain ID?

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

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

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

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

- For AS-External-LSA:
 - If OSPF is not enabled on the next hop interface of the imported route, the FA that is related to the imported route is 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, the FA is filled with the next hop address.
 - If the imported route is the static route that is configured by specifying the outgoing interface, 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 Broadcast type.
 - If OSPF is not enabled on the next hop interface of the S9300 that imports routes, 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 Principle of OSPF Authentication?

A: OSPF authentication is classified into area-based authentication and interface-based authentication:

- The type of area-based authentication can be simple, MD5, or HMAC-MD5.
- The type of interface-based authentication can be Null, simple, MD5, or HMAC-MD5.

The OSPF authentication is adopted according to the following principles:

- 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 keys are as follows:

- Plain text authentication key: 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 16 bytes.
- Cipher text authentication key: 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 16 bytes or a cipher string of 24 bytes.
- Space is not allowed in the two types of authentication keys.

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 set on the interface. These parameters must be consistent with the parameters on the neighboring node. That is, area ID, network segment, and mask must be consistent. (For P2P connection and virtual connection, the network and mask can be inconsistent.)

The network types of interfaces of two neighboring devices must be consistent. If the network is a broadcast network or an 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 run the **Ping** command. If you cannot ping the other device from the local device, 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 broadcast, 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 to all other areas. If an S9300 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. The devices in the Stub area cannot receive routes from external ASs. If an area is configured as a Stub area, all devices which connect with the area should configure the area as Stub.

Do as follows to solve the problem:

- Check the status of OSPF neighbor relation 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 run in the backbone area.
- If an area is a Stub area, the **stub** command needs to be run on all devices in the area.
- If the virtual connection is configured, check whether the neighbor is in the normal state by running the **display OSPF vlink** command.

2.5 Diagnostic Tools

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

[2.5.1 display Commands](#)

[2.5.2 debugging Commands](#)

2.5.1 display Commands

Table 2-2 OSPF display commands

Command	Description
display OSPF asbr-summary	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.
display OSPF brief	Displays the OSPF summary information.
display OSPF cumulative	Displays the OSPF statistics.
display OSPF error	Displays the OSPF errors.

Command	Description
display OSPF graceful-restart	Displays the restart status of OSPF GR.
display OSPF interface	Displays the OSPF interface information.
display OSPF lsdb	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"> ● Summary information ● LSA information of specified type ● LSA information sent by the local switch
display OSPF nexthop	Displays information about the next hop.
display OSPF peer	Displays the OSPF neighbor information. The output of the command can help you diagnose the OSPF fault and check the effect of the configuration.
display OSPF request-queue	Displays information about the OSPF request queue. The output of the command can help you diagnose and remove the OSPF fault.
display OSPF retrans-queue	Displays information about the OSPF retransmission queue. The output can help you diagnose and remove OSPF faults.
display OSPF routing	Displays information about the OSPF routing table. By choosing different parameters, you can check the route to the specified interface or the next hop.
display OSPF sham-link	Displays information about all the sham links belonging to the specified OSPF process or area and all the attributes related to those sham links.
display OSPF vlink	Displays information about the OSPF Vlink.

2.5.2 debugging Commands

Table 2-3 OSPF debugging commands

Command	Description
debugging OSPF event	Enables the debugging of OSPF event.
debugging OSPF hot-standby	Enables the debugging of the OSPF hot standby. Hot standby is also called incremental backup.
debugging OSPF graceful-restart	Enables GR debugging of the specified OSPF process to debug the process of setting up GR.

Command	Description
debugging OSPF lsa-originate	Displays the original information about the LSA.
debugging OSPF packet	Debugs 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.
debugging OSPF spf	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

[3.1 IS-IS Overview](#)

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

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

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

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

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

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

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

[3.5 Troubleshooting Link Status Advertisement](#)

This section describes the notes about configuring BFD for IS-IS, and provides the BFD for IS-IS troubleshooting flowchart and the troubleshooting procedure on a typical IS-IS network.

[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 describes 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

IS-IS is a link state protocol. It uses the Shortest Path First (SPF) algorithm to calculate routes in the autonomous systems (ASs). The IS-IS protocol is similar to the OSPF protocol.

3.1.2 IS-IS Features Supported by the S9300

Multi-instance and Multi-process

Multi-process associates a specified IS-IS process with a group of interfaces. This ensures that all the protocol-related operations for this process take effect only on the group of interfaces.

When supporting the VPN feature, each IS-IS process of an S9300 should be associated with a VPN instance.

IS-IS HSB

The S9300 supports IS-IS Hot Standby (HSB). The S9300 backs up the IS-IS configuration during the switchover of the Active Main Board (AMB) and Standby Main Board (SMB) and the graceful restart (GR) feature prevents traffic from being affected.

NOTE

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

IS-IS GR

The GR feature of the IS-IS protocol prevents traffic from being affected during switchover. In addition, route flapping does not occur when a device on the network restarts.

NOTE

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

IS-IS TE

IS-IS Traffic Engineering (TE) applies when the Multiprotocol Label Switching (MPLS) protocol establishes and maintains Label Switched Paths (LSPs). When constructing the Constraint-based Routed LSP (CR-LSP), MPLS needs to learn the traffic attributes of all the links in this area. MPLS can obtain TE information about the links through IS-IS.

NOTE

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

Administrative Tag

The value of an administrative tag is associated with certain attributes. This simplifies management of routing information. The administrative tag is advertised in the entire IS-IS routing domain through an IP address prefix to control routes. The administrative tag carries administrative information about an IP address prefix and controls the routes of different levels and routes imported from different areas, different routing protocols, multiple IS-IS instances running on a S9300, and tags.

LSP Fragment Extension

IS-IS LSP fragment extension enables an IS-IS process to generate more LSP fragments. To implement this function, you can configure additional system IDs with the network manager for the S9300. Each system ID represents a virtual system that can generate 256 LSP fragments. With more additional system IDs (up to 50 virtual systems), an IS-IS process can generate a maximum of 13056 LSP fragments.

Dynamic Hostname Exchange Mechanism

The dynamic hostname exchange mechanism simplifies the management and maintenance of IS-IS networks. This mechanism provides the IS-IS S9300 with the mapping from the hostname to the system ID. After this function is enabled, the system ID is replaced with the host name of the S9300 in the output of the **display isis name-table** command related to IS-IS.

IS-IS Fast Convergence

- Incremental SPF (I-SPF)
When the network topology changes, I-SPF calculates only affected nodes 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 processes only the changed leaf message.

NOTE

On the S9300, only I-SPF and PRC are used to calculate IS-IS routes.

- LSP fast flooding
When an S9300 receives one or more new LSPs, it floods out the LSPs less than the number of the specified LSPs before route calculation. Thus, the Link State Database (LSDB) is synchronized quickly.
- Intelligent timer
If the network topology is stable, the period for the intelligent timer to trigger the route calculation can be set to several milliseconds. Thus, the intelligent timer quickly responds to the emergency (for example, the interface is Up or Down). Then, the route convergence is accelerated. If the network topology changes frequently, the interval set by the intelligent timer increases with the calculation times to avoid excessive CPU consumption.

NOTE

You should configure the intelligent timer with caution according to the network environment.

BFD for IS-IS

The S9300 can use Bidirectional Forwarding Detection (BFD) to detect IS-IS neighbor relationships. BFD can fast detect faults on the links between IS-IS neighbors and report them to IS-IS. The fast convergence of IS-IS is thus implemented.

 **NOTE**

BFD detects only single-hop links between IS-IS neighbors because IS-IS can establish only single-hop neighbor relationships.

For details about BFD for IS-IS, see the chapter "IS-IS" in the *Quidway S9300 Terabit Routing Switch Feature Description — IP Routing*.

Three-Way Handshake

In three-way handshake mode, the S9300 considers that the neighbor is Up only after confirming that the neighboring node receives the packet sent by the S9300. Then, the S9300 sets up an adjacency with the neighbor. In addition, the three-way handshake mechanism adopts the 32-bit extended circuit ID. This extends the number of Point-to-Point (P2P) links, which is 255 defined by the original 8-bit Circuit ID field.

3.2 Troubleshooting the IS-IS Neighbor Relationship

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

[3.2.1 Typical Networking](#)

[3.2.2 Configuration Notes](#)

[3.2.3 Troubleshooting Flowchart](#)

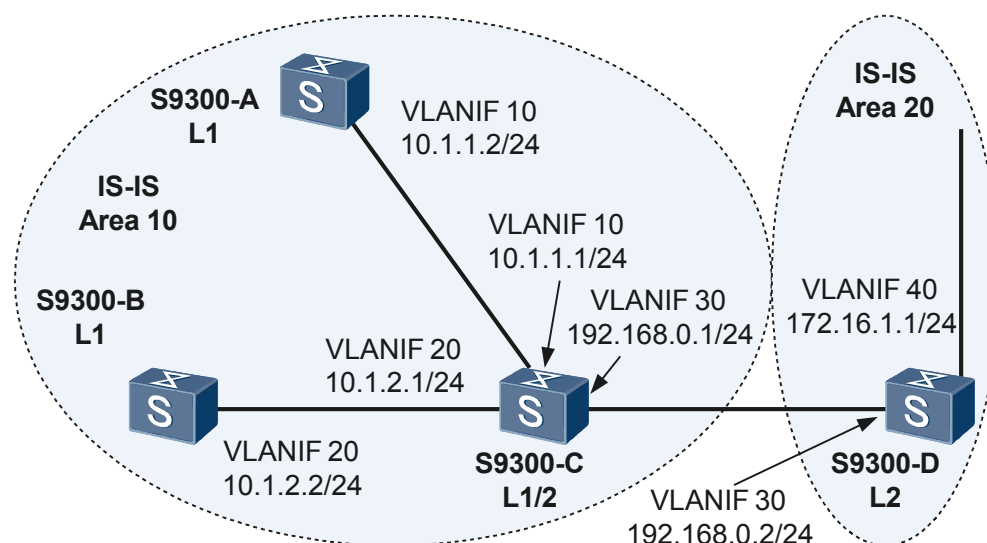
[3.2.4 Troubleshooting Procedure](#)

3.2.1 Typical Networking

Figure 3-1 shows a typical networking of IS-IS.

The following describes how to troubleshoot the IS-IS neighbor relationship based on this networking.

Figure 3-1 Typical networking of IS-IS



As shown in **Figure 3-1**:

- S9300-A, S9300-B, S9300-C, and S9300-D belong to the same AS.
- S9300-A and S9300-B are Level-1 nodes; S9300-D is a Level-2 node; S9300-C is a Level-1-2 node that connects the two areas.
- The area IDs of S9300-A, S9300-B, and S9300-C are all 10, and the area ID of S9300-D is 20.

The S9300s can communicate with each other on the network through IS-IS.

3.2.2 Configuration Notes

Table 3-1 IS-IS Configuration Notes

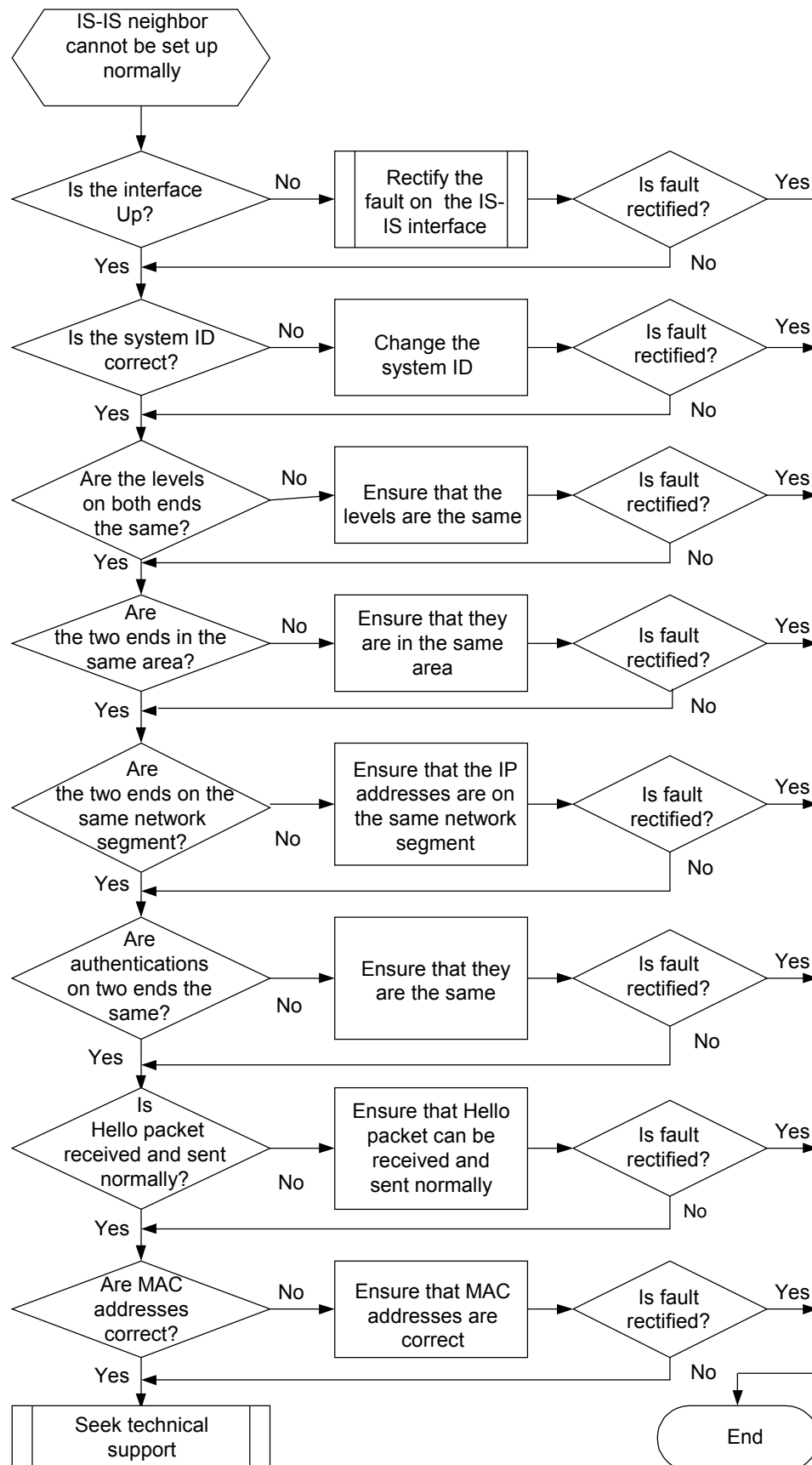
Item	Sub-item	Configuration Notes and Commands
Configuring IS-IS	Setting a level	<ul style="list-style-type: none"> • A Level-1 node establishes neighbor relationships with only Level-1 nodes or Level-1-2 nodes. • A Level-2 node establishes neighbor relationships with only Level-2 nodes or Level-1-2 nodes. • A Level-1-2 node can establish neighbor relationships with Level-1 nodes, Level-1-2 nodes, and Level-2 nodes. • A Level-1 node can establish neighbor relationships with nodes in the same area, whereas a Level-2 node can establish neighbor relationships with nodes of other areas. <p>To set a level, run the is-level { level-1 level-2 level-1-2 } command in the IS-IS view.</p>

Item	Sub-item	Configuration Notes and Commands
	Configuring a network entity (NET)	Any two nodes cannot contain the same NET. To configure an NET, run the network-entity net command in the IS-IS view.
	Assigning an IP address	Any two nodes cannot be assigned with the same IP address. To assign an IP address, run the ip address ip-address { mask mask-length } command in the VLANIF interface view.

3.2.3 Troubleshooting Flowchart

As shown in [Typical Networking](#), after the IS-IS protocol is enabled on all the S9300s on the network, you find that the S9300s cannot set up IS-IS neighbor relations with the remote ends. [Figure 3-2](#) shows the troubleshooting flowchart.

Figure 3-2 Networking diagram of IS-IS neighbor relationship



3.2.4 Troubleshooting Procedure

Context

The steps of troubleshooting are as follows:

Procedure

Step 1 Check that the interface is Up.

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

If the interface is Down, see section [3.4 Troubleshooting an IS-IS Interface](#).

Step 2 Check that the system ID is configured correctly.

Run the **display current-configuration** command to check whether the system ID of the local S9300 is the same as the system ID of the peer.

If the system IDs at both ends are the same, run the **network-entity** command to set different system IDs for the S9300s at both ends.

Step 3 Check that the levels at both ends of the neighbors are the same.

Run the **display current-configuration** command to check the level set on the S9300 and interface.

The possible cause is that the levels set at the neighbors are different.

- The levels set on IS-IS systems at both ends are different: one end is set to Level-1 and the other end is set to Level-2.
- The levels set on the interfaces at both ends are different: one end is set to Level-1 and the other end is set to Level-2.

If the preceding situation occurs, run the **isis circuit-level** command in the VLANIF interface view to modify the level configurations. Make sure that the neighbors can communicate with each other.

Step 4 Check that the two ends reside in the same area.

Run the **display current-configuration** command to check the area IDs set on the S9300 and interface.

If the two ends reside in different areas, run the **network-entity** command to modify the area ID to ensure that the two ends reside in the same area.

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

Run the **display current-configuration** command to check whether the IP address of the interface on the local S9300 and the peer IP address reside on the same network segment.

If the two ends reside on different network segments, run the **ip address** command to modify the IP address of the interface to ensure that both ends reside on the same network segment.

Step 6 Check that the two ends are configured with the same authentication mode and password.

Run the **display current-configuration** command to check whether one end is Up and the other end is not displayed. In this situation, the common cause is that the encrypted authentication on the interface fails.

To ensure that the authentication modes and passwords at both ends are matched, you can use one of the following commands to modify the encrypted authentication at both ends:

- **area-authentication-mode**
- **domain-authentication-mode**
- **isis authentication-mode**

Step 7 Check that the two ends receive and send Hello packets normally.

On a P2P network, the fault symptom is: The local end receives the Hello packets from the peer, but the peer does not receive the Hello packets from the local end. In this case, run the **debugging isis adjacency** command to check whether the Hello PDUs of the two ends can be sent and received normally.

Step 8 Check that the MAC address is configured correctly.

Check whether the status at one end is Up and the status at the other end is Init. In this case, the possible cause is that the MAC address at one end is incorrect. You need to modify the MAC address.

If the fault persists, contact the Huawei technical personnel.

----End

3.3 Troubleshooting the IS-IS Routing Table

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

[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

For the networking environment, see section [Figure 3-1](#).

3.3.2 Configuration Notes

Table 3-2 IS-IS routing table configuration notes

Item	Sub-item	Configuration Notes and Commands
Configuring the IS-IS routing table	Setting a level	If you run the import route command without specifying a level, IS-IS imports routes to the Level-2 routing table. To set a level, run the import route { level-1 level-2 level-1-2 } command in the IS-IS view.
	Setting the cost type	Set the same cost type on each S9300. To set the cost type, run the cost-style command in the IS-IS view.
	Configuring LSP fragments and virtual IDs	If the number of imported routes is more than 30345 and the MTU is 1500, you must enable LSP fragment and configure enough virtual IDs. To enable LSP fragment and configure enough virtual IDs: <ul style="list-style-type: none"> • Run the virtual-system virtual-system-id command in the IS-IS view. • Run the lsp-fragments-extend command in the IS-IS view.
	Setting the overload flag bit	After the overload flag bit is set, other nodes no longer forward packets to the S9300 except for the packets whose destination addresses are the addresses directly connected to this S9300. To set the overload flag bit, run the set-overload command in the IS-IS view.

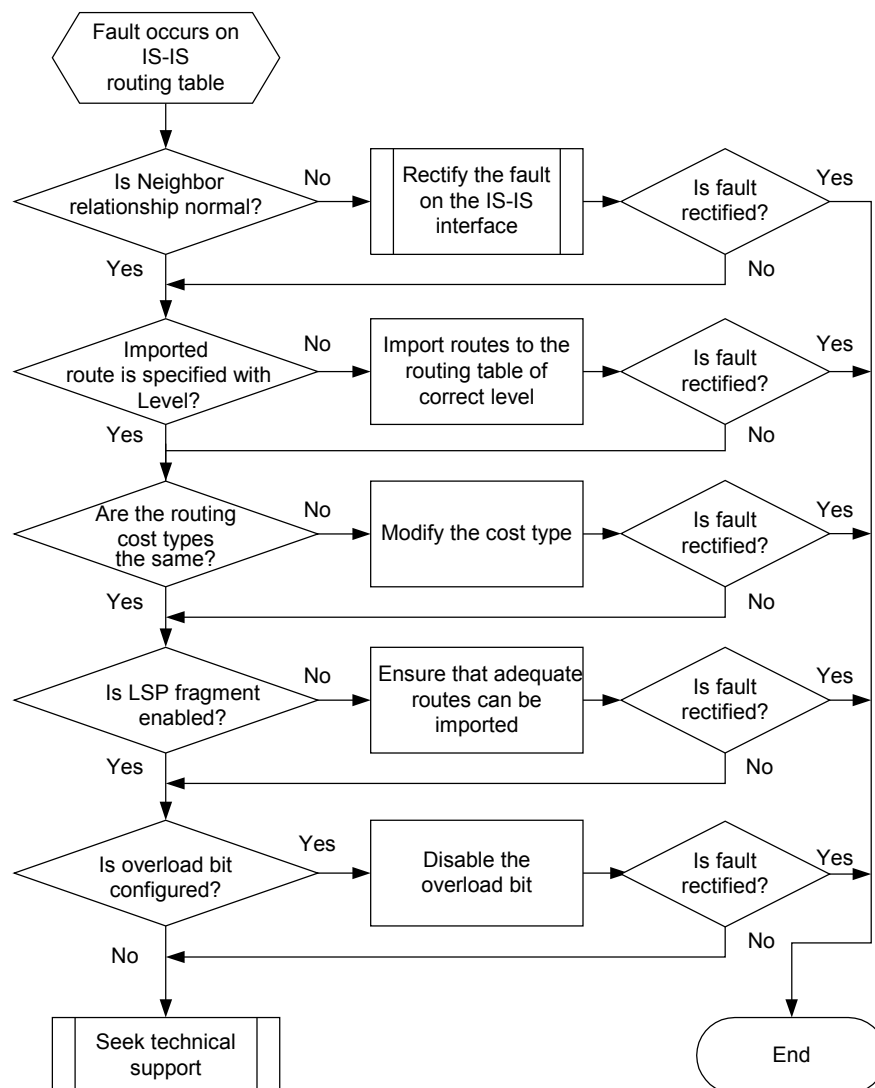
3.3.3 Troubleshooting Flowchart

After IS-IS is configured, the following situations may occur:

- The imported route is not displayed in the IS-IS Level-1 routing table.
- Only 255 fragments are displayed in the IS-IS Level-1 or Level-2 routing table.
- Only three equal-cost routes are displayed in the IS-IS routing table.

Follow the troubleshooting procedure shown in [Figure 3-3](#).

Figure 3-3 Flowchart for troubleshooting the IS-IS routing table



3.3.4 Troubleshooting Procedure

Context

The steps of troubleshooting are as follows:

Procedure

Step 1 Check that the neighbor relations are Up.

Run the **display isis peer** command to check whether the neighbor relations are Up.

If an interface is Down, see section [3.2 Troubleshooting the IS-IS Neighbor Relationship](#).

Step 2 Check that the level of the imported routes is specified.

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

Step 3 Check that all the nodes on the network use the same routing cost type.

Step 4 Check whether LSP fragment is enabled and sufficient virtual IDs are configured.

If the number of imported routes is more than 30345, LSP fragments and sufficient virtual IDs must be configured.

Step 5 Check whether the overload flag bit is set.

After the overload flag bit is set, other nodes no longer forward packets to the S9300 except for the packets whose destination addresses are the addresses directly connected to this S9300.

If the fault persists, contact the Huawei technical personnel.

---End

3.4 Troubleshooting an IS-IS Interface

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

[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](#), the IS-IS interface is Down after IS-IS is configured on all the S9300s.

3.4.2 Configuration Notes

Table 3-3 IS-IS interface configuration notes

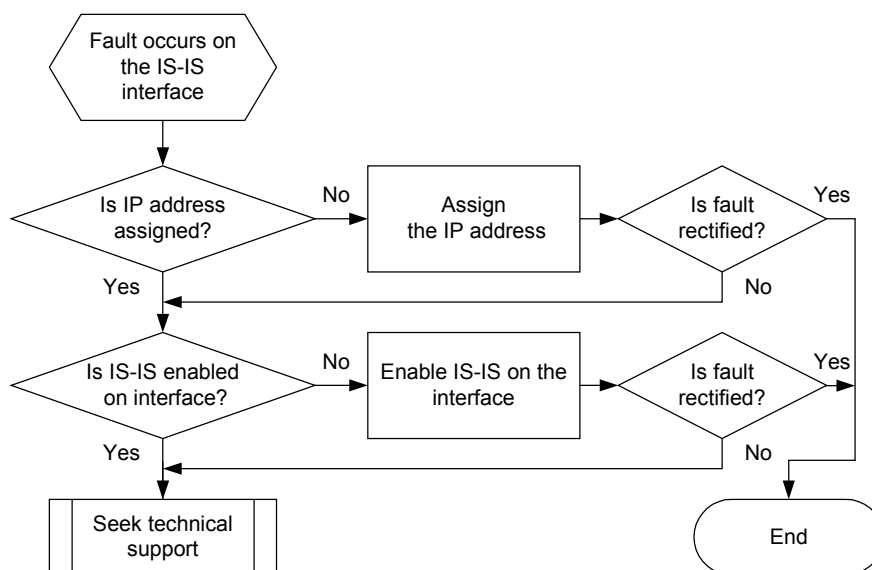
Item	Sub-item	Configuration Notes and Commands
Configuring an IS-IS interface	Setting the MTU	<p>The MTU on the physical interface must be greater than the LSP-Length value set in the IS-IS process.</p> <p>To set the MTU:</p> <ul style="list-style-type: none"> ● Run the mtu <i>mtu</i> command in the interface view. ● Run the lsp-length originate <i>max-size</i> command in the IS-IS view. ● Run the lsp-length receive <i>max-size</i> command in the IS-IS view.

Item	Sub-item	Configuration Notes and Commands
	Configuring a link	If the IS-IS link is Down, the cause may be that the correct NET is not set for the IS-IS process. To set an NET, run the network-entity net command in the IS-IS view.
	Assigning an IP address	If the IS-IS link is Up and the IP address status is Down, the cause may be that the interface is enabled with IS-IS but not assigned with an IP address. To assign an IP address, run the ip address ip-address { mask mask-length } command in the VLANIF interface view.

3.4.3 Troubleshooting Flowchart

After IS-IS is configured on all the S9300s, the IS-IS interface is Down. Follow the troubleshooting procedure shown in [Figure 3-4](#).

Figure 3-4 Flowchart for troubleshooting the IS-IS interface



3.4.4 Troubleshooting Procedure

Context

The steps of troubleshooting are as follows.

Procedure

Step 1 Check that an IP address is assigned to the interface.

Run the **display interface** command to check whether the interface is assigned with an IP address. If not, assign an IP address to the interface.

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

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

If both the physical status and protocol status are Down, check the physical connection on the interface.

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

Run the **display current-configuration** command to check whether the interface is enabled with IS-IS.

If not, run the **isis enable** command to enable IS-IS in the interface view.

If the fault persists, contact the Huawei technical personnel.

---End

3.5 Troubleshooting Link Status Advertisement

This section describes the notes about configuring BFD for IS-IS, and provides the BFD for IS-IS troubleshooting flowchart and the troubleshooting procedure on a typical IS-IS network.

[3.5.1 Typical Networking](#)

[3.5.2 Configuration Notes](#)

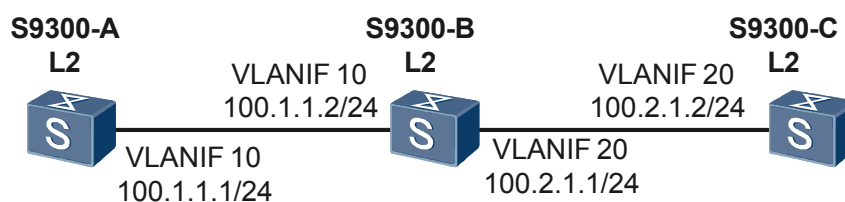
[3.5.3 Troubleshooting Flowchart](#)

[3.5.4 Troubleshooting Procedure](#)

3.5.1 Typical Networking

As shown in [Figure 3-5](#), IS-IS is run on S9300-A and S9300-B. After BFD for IS-IS is configured, no notification event is generated when the status of the link changes.

Figure 3-5 Typical networking of IS-IS link



3.5.2 Configuration Notes

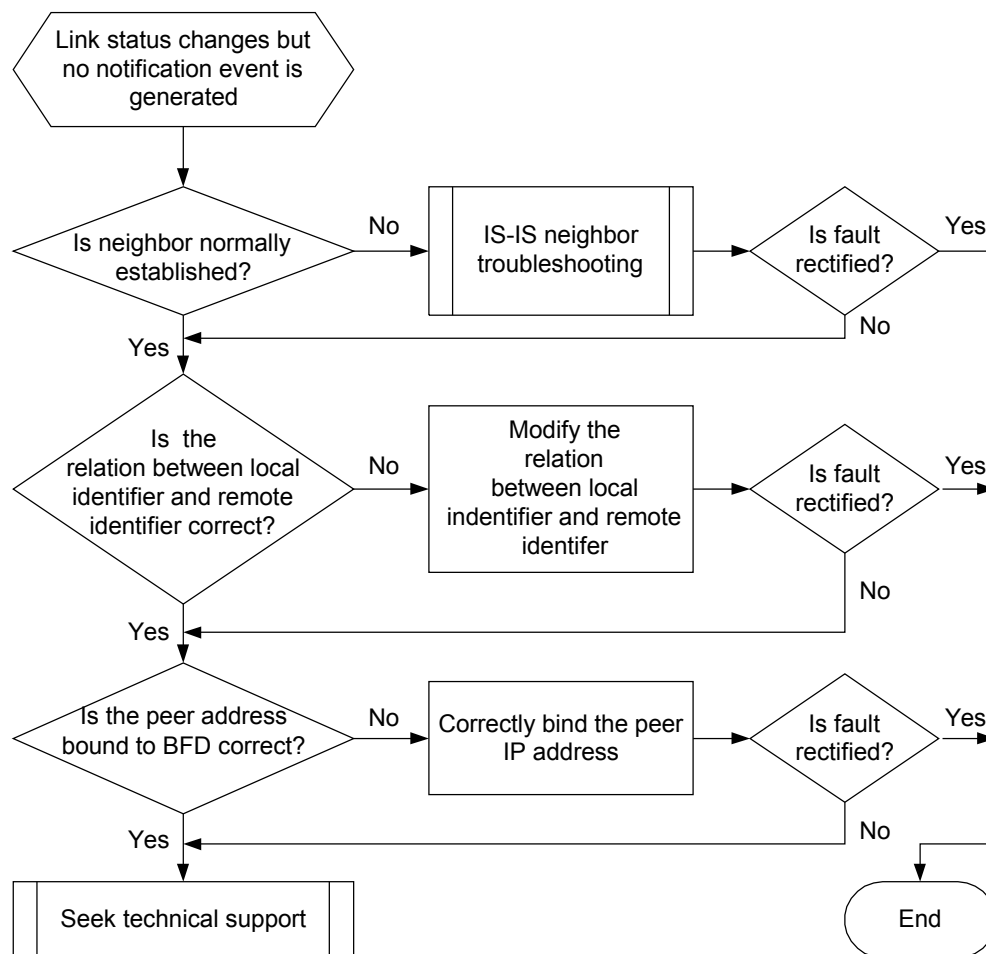
Table 3-4 IS-IS link configuration notes

Item	Sub-item	Configuration Notes and Commands
Configuring IS-IS	Configuring BFD	<ul style="list-style-type: none"> For BFD, the local discriminator and the remote discriminator need to be matched. For BFD, the peer IP address should be correctly bound. To configure BFD, run the following commands in the related views: <ul style="list-style-type: none"> discriminator local <i>discr-value</i> (BFD session view) discriminator remote <i>discr-value</i> (BFD session view) bfd cfg-name bind peer-ip <i>ip-address</i> (system view)

3.5.3 Troubleshooting Flowchart

After the S9300s are configured with BFD for IS-IS on the network, no notification event is generated when the status of the link changes. Follow the troubleshooting procedure shown in Figure 3-6.

Figure 3-6 Flowchart for troubleshooting the change of the link status



3.5.4 Troubleshooting Procedure

Context

The steps of troubleshooting are as follows:

Procedure

Step 1 Run the **ping** command to check whether the destination IP address is reachable.

If the ping fails, check whether the IP address of the interface is configured correctly.

Step 2 Check whether the IS-IS process is enabled on the interface connecting to the neighbor.

In the IS-IS view of the S9300, run the **display isis interface** command to check that the IS-IS process is enabled on the interface connecting to the neighbor.

Step 3 Check whether the area IDs of the S9300s are the same in an IS-IS process.

Run the **display isis lsdb verbose** command on each S9300 to check area ID of the local LSP, and then identify whether the S9300s reside in the same area.

Step 4 Check whether the system IDs of the S9300s are repeated in an IS-IS process.

Run the **display current-configuration** command on each S9300 to check the local system ID, and then identify whether the system IDs of the S9300s are repeated.

Step 5 Check whether the local and remote discriminators of the BFD session that is created on the S9300s at both ends match each other.

Run the **display bfd session discriminator** command to check whether the local and remote discriminators match each other.

Step 6 Check whether the peer IP address is correctly bound to the BFD session that is set up on the S9300s at both ends.

Run the **display bfd session all** command to check whether the peer IP address is correctly bound.

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 Various Features of IS-IS Be Configured?

A: The cause may be that the user is not permitted to configure various features. The user can check the licenses to confirm whether the user has obtained the licenses for configuring various features.

Q: After IS-IS Is Disabled or the Interface Is Shut Down, the LSDB Is Not Refreshed. How to Rectify the Fault?

A: After IS-IS is disabled on the interface or the interface is shut down, IS-IS refreshes the LSDB after the specified hold time.

Q: After the Physical Links of an S9300 and Those of Other S9300s Are Interconnected, Information about the Peer Neighbor Is Not Displayed When the display isis peer Command Is Run? That Is, Why Cannot the Neighbor Relationship Be Set Up?

A: The possible causes are:

The level, area ID, authentication key of the S9300s may be different.

The system IDs of the S9300s are repeated.

To remove the fault, do as follows:

1. Ensure that the IS-IS process is enabled on the connected interfaces of the two S9300s.
2. Check whether the two S9300s are of the same type. Check the TYPE configured on the S9300 by using the **display isis interface** command. If the peer end is a Level-2 node and the interface connecting the local end and the peer end is Level-1, the neighbor relationship cannot be set up. If the peer end is a Level-1 node and the interface connecting the local end and the peer end is Level-2, the neighbor relationship cannot be set up.
3. Check whether the two S9300s reside in the same area. Run the **display isis lsdb verbose** command on the two S9300s respectively to view the area ID of the local LSP.
4. Check whether the system IDs of the two S9300s are repeated. Run the **display current-configuration** command on the two S9300s respectively to check the system ID of the local S9300.
5. Check whether the interface authentication is enabled on the two interfaces and whether the keys at both ends are the same. You can use the **display this** command in each interface view to check the configurations.
6. Check whether the MTUs of the two interfaces are the same. You can run the **display isis interface** command to check the configuration of the MTU.
7. Check whether the hold time is too small. The hold time is the product of holding-Multiplier and hello interval. If the transmission delay is too long, the neighbor relationship becomes instable.

Q: The Tag Is Not Displayed in the IS-IS LSDB. How to Rectify the Fault?

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

1. If the tag cannot be found in the IS-IS LSDB after advertised in the LSP, check whether the routing metric type is set.
2. If the routing metric type is not set, set the type to Wide and ensure all the S9300s use the same type. The tag is supported by the types Wide and Wide-Compatible.

Q: The Information About the TE Link and Network Is not Displayed in the IS-IS TE Database. How to Rectify the Fault?

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

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

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

A: IS-IS determines the cost of an interface through the following methods in a descending order:

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

If the cost type is Wide or Wide-compatible, the bandwidth reference value set is valid. Then, the cost of each interface = (bandwidth-reference/interface bandwidth) x 10.

If the cost type is Narrow, Narrow-compatible, or Compatible, the cost of each interface is calculated as shown in the follow table.

Table 3-5 Relationship between the IS-IS interface cost and the bandwidth

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

NOTE

To change the cost of the loopback interface, you can run the **isis cost** command only in the interface view.

Q: What Type of IS-IS Packet Timers Can Be Configured in the Interface View?

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

Table 3-6 Commands for configuring IS-IS packet timers

Item	Configuration Command	Default Value
Interval for sending Hello packets	isis timer hello <i>hello-interval</i> [level-1 level-2	10, in seconds

Item	Configuration Command	Default Value
Number of invalid Hello packets	isis timer holding-multiplier <i>number [level-1 level-2]</i>	3
Interval for sending LSP packets	isis timer lsp-throttle <i>throttle-interval [count count]</i>	50, in milliseconds
Interval for retransmitting LSP packets on an interface	isis timer retransmit <i>retransmit-interval s</i>	5, in seconds

Q: What Type of IS-IS Timers Can Be Configured in the Interface View?

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

Table 3-7 Commands for configuring IS-IS timers

Item	Configuration Command	Default Value
Period for refreshing LSP packets	timer lsp-refresh <i>refresh-time</i>	900, in seconds
Maximum keepalive time of an LSP packet	timer lsp-max-age <i>age-time</i>	1200
Period for the SPF calculation	spf-slice-size <i>duration-time</i>	10, in seconds

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

A: DIS is abbreviated from Designated Intermediate System. The DIS is elected in preemption mode, which can be predicted. The system with the highest priority is elected as the DIS. When more than one system has the same priority, the one with the largest MAC address is the DIS. The DIS can broadcast the network link status to all the nodes on the network.

Q: How to Disable the S9300 on an Interface from Setting Up the Neighbor Relationship with Other S9300s?

A: Run the **isis silent** command on the interface to disable the S9300 on the interface from setting up the neighbor relationship with other S9300s. The network segment to which the interface belongs is advertised.

Q: Why Cannot the IS-IS Process Be Created?

A: If CPU or memory resources are excessively occupied, the IS-IS process cannot be created. In this case, you should check the usage of the CPU and memory. Release some resources if necessary.

Q: Why Cannot the Level-1 S9300 Generate the Default Route External to the Area?

A: The Level-1 node can generate the route external to the area only after it sets up a Level-1 adjacency with the Level-1-2 node in the local area. The LSP of the Level-1-2 node can set the ATT flag bit. In this case, all the Level-1 nodes generate the default route destined for the Level-1-2 node.

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

A: The possible causes are:

- The neighbor relationship cannot be set up normally.
- The cost types are different at the two ends.
- The route is filtered out by the routing policy. The route cannot be added to the URT.
- The LSP fragments are filled up. As a result, the Neighbor type-length-value (TLV) is lost. If more than 30 thousand routes need to be imported, the LSP must be configured.
- The S9300 is configured with the domain and area authentication. As a result, the authentications of the LSP are not synchronous.

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 Calculate the Route?

A: When the cost is 16777215, the Neighbor TLV generated on the link cannot be used to calculate routes. Instead, it is only used to transmit TE information.

Q: Is There Any Requirement for the Configuration of IS-IS Authentication Key?

A: An IS-IS authentication key can be either in the plain text or in the encrypted text.

The rules are described as follows:

- In plain text mode (the simple mode), the authenticator is a string of 1 to 16 characters. The string can be composed of all letters, all numbers, or combination of letters and numbers.
- In encrypted text mode, the authentication key is also a string of characters. The string can be composed of all letters, all numbers, or combination of letters and numbers.
- The string of 1 to 16 characters corresponds to the plain text; the string of 24 characters corresponds to the encrypted text.
- An authentication key cannot contain spaces.

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

A: The parameters level-1 and level-2 can be displayed only on the Ethernet interface and you must first run 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

Table 3-8 Is-Is display commands

Command	Description
display isis interface	Displays information about the IS-IS interface.
display isis lsdb	Displays information about the LSDB of IS-IS.
display isis mesh-group	Displays the configuration of the Mesh Group on the interface of the current S9300.
display isis name-table	Displays the mapping from the local S9300 name to the system ID.
display isis peer	Displays information about the IS-IS peer.
display isis graceful-restart status	Displays and debugs the restart status of IS-IS GR.
display isis route	Displays information about IS-IS routes. The default level is Level-1 and Level-2. If the Verbose parameter is used, the IS-IS routes with the preference and administrative tag is displayed.
display isis spf-log	Displays the IS-IS SPF calculation log.
display isis statistics	Displays the statistics of the IS-IS process.
display isis traffic-eng	Displays information about TE of an IS-IS process, including the IS-IS system type, cost type, and TE status.

3.7.2 debugging Commands

Table 3-9 Is-Is debugging commands

Command	Description
debugging isis adjacency	Debugs the packets sent by an IS-IS neighbor.
debugging isis all	Debugs IS-IS.
debugging isis authentication-error	Debugs IS-IS authentication errors.
debugging isis bfd	Debugs BFD for IS-IS.
debugging isis checksum-error	Debugs LSP checksum errors of IS-IS.
debugging isis circuit-information	Debugs the IS-IS interface or link.
debugging isis configuration-error	Debugs IS-IS configuration errors.
debugging isis datalink-receiving-packet	Debugs the receiving of packets on the IS-IS data link layer.
debugging isis datalink-sending-packet	Debugs the sending of packets on the IS-IS data link layer.
debugging isis event	Debugs IS-IS events.
debugging isis general-error	Debugs IS-IS errors.
debugging isis graceful-restart	Debugs IS-IS GR events.
debugging isis ha-events	Debugs IS-IS HSB events.
debugging isis interface-information	Debugs the IS-IS data link layer.
debugging isis ldp-sync	Debugs synchronization status change of LDP and IS-IS.
debugging isis memory-allocating	Debugs IS-IS memory allocation.
debugging isis miscellaneous-errors	Debugs various IS-IS errors.
debugging isis receiving-packet-regular-content	Debugs details of received IS-IS packets.
debugging isis sending-packet-regular-content	Debugs details of sent IS-IS packets.
debugging isis self-originate-update	Debugs the packets updated by IS-IS locally.
debugging isis snp-packet	Debugs SNP/PSNP packets of IS-IS.

Command	Description
debugging isis spf-event	Debugs SPF events of IS-IS.
debugging isis spf-prc	Debugs the IS-IS SPF calculation process.
debugging isis spf-summary	Debugs IS-IS SPF timing messages and statistics.
debugging isis spf-timer	Debugs IS-IS SPF triggering events.
debugging isis task-error	Debugs the IS-IS service status.
debugging isis timer	Debugs IS-IS timers.
debugging isis traffic-eng	Debugs IS-IS TE advertisement or events.
debugging isis update-packet	Debugs the displaying of IS-IS updated packets.
debugging isis update-process	Debugs the IS-IS update process.

4 BGP Troubleshooting

About This Chapter

This chapter describes the procedure and diagnostic tools of BGP troubleshooting.

[4.1 BGP Overview](#)

This section describes the information you need to know before troubleshooting BGP.

[4.2 BGP Peer Relationship Troubleshooting](#)

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

[4.3 Accidental Interruption of BGP Peer Relationship Troubleshooting](#)

This section describes the notes about configuring BGP, and provides the accidental interruption of BGP peer relationship troubleshooting flowchart and the troubleshooting procedure in a typical BGP network.

[4.4 Route Loss Troubleshooting When BGP Peers 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 network.

[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 information you need to know before troubleshooting BGP.

4.1.1 Introduction to BGP

4.1.2 BGP Route Attributes

4.1.3 Faults and Solutions on Large-Scale BGP Networks

4.1.1 Introduction to BGP

The Border Gateway Protocol (BGP) is a dynamic routing protocol used between Autonomous Systems (ASs).

4.1.2 BGP Route Attributes

BGP route attributes are a set of parameters and further describe a specific route for BGP to filter and select routes. BGP route attributes are classified into the following types.

Table 4-1 Type of BGP route attributes

Attribute Type	Description
Well-Known Mandatory	All the BGP speakers can identify this attribute. The attribute is mandatory in the Update message. Without this attribute, errors occur in the routing information.
Well-Known Discretionary	All the BGP speakers can identify this attribute. The attribute is optional in the update message and can be selected as required.
Optional transitive	This attribute can be transmitted between the ASs. A BGP speaker may not support this attribute, but still receives the routes with this attribute and advertises them to other peers.
Optional non-transitive	If a BGP speaker does not support this attribute, the Update messages with this attribute are not advertised to other peers.

Table 4-2 shows the main attributes and types of BGP routes.

Table 4-2 Main BGP route attributes

Attribute Name	Description	Attribute Type
Origin	It defines the source of the path information, including: <ul style="list-style-type: none"> • Interior Gateway Protocol (IGP): It is of the highest priority. • Exterior Gateway Protocol (EGP): It is of the secondary highest priority. • It is of the lowest preference. It indicates that the source of the route cannot be identified. 	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	<ul style="list-style-type: none"> • When the route is advertised to the External BGP (EBGP) peer, the Next_Hop is the address of the local interface connected to the peer. • When the route is advertised to the Internal BGP (IBGP) peer, Next_Hop of the routing information is not changed. 	Well-known mandatory
Local_Pref	It is only exchanged between IBGP peers, and used to determine the optimal route when the traffic leaves the AS. The greater the Local_Pref, the higher the preference.	Well-known discretionary
Community	It is a set of the destination addresses with the same attribute. The addresses have no physical boundary and are independent of ASs.	Optional transitive
MED	It is only exchanged between ASs, and used to determine the optimal route when the traffic enters the AS. The smaller the MED, the higher the preference.	Optional non-transitive

4.1.3 Faults and Solutions on Large-Scale BGP Networks

Table 4-3 Faults and solutions on large-scale BGP networks

Fault	Solution
The BGP routing table is too large.	Adopt route aggregation to aggregate multiple routes. In this case, BGP can only advertise the aggregated route to the peer. The size of the routing table is greatly reduced.

Fault	Solution
Route flapping occurs frequently.	Adopt routing damping to add up the penalty value for the flapped route. When the penalty value exceeds the suppression threshold, the route is not added to the routing table. After multiple half lives, the penalty value decreases to the reuse threshold and then the route is added to the routing table again. At the same time, Update messages are advertised to BGP peers.
A large number of peers need to be configured with the same attribute.	Adopt the peer group and configure the same attribute for members in the peer group. When a peer is added to a peer group, the configuration of this peer is the same as that of the peer group. The configuration of the peers in the group varies with that of the peer group.
The BGP speakers in multiple ASs need to be configured with the same policy.	Adopt community and configure the community attribute for BGP routes. Thus, all the members in the community share the same policy. The community attribute takes effect for BGP peers. It is not limited by the AS.
Too many IBGP peers reside in an AS.	<ul style="list-style-type: none"> ● Adopt route reflection and configure the router reflector (RR). The RR sets up IBGP connections with multiple BGP speakers, constituting a cluster where the routing information is exchanged. The BGP speakers outside the cluster set up peer relationships with the RP. ● Adopt confederation and divide the confederation into sub-ASs. The IBGP peers within the AS keep set up peer relationships with each other. The sub-ASs keep the EBGP connection with each other. <p>On a large-scale BGP network, RR and confederation can be used together.</p>

The preceding solutions can be used together.

4.2 BGP Peer Relationship Troubleshooting

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

[4.2.1 Typical Networking](#)

[4.2.2 Configuration Notes](#)

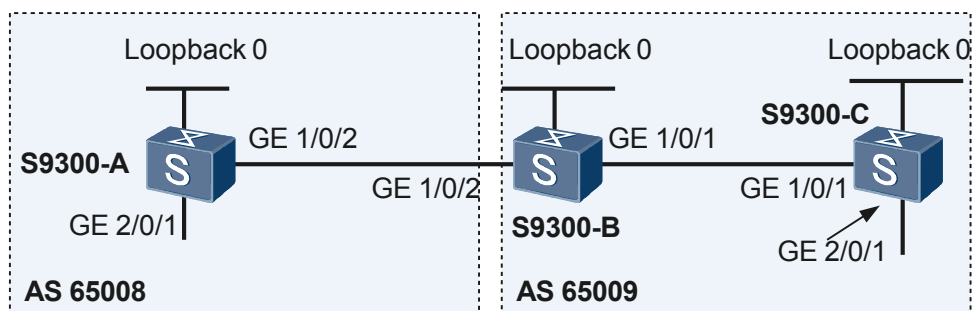
[4.2.3 Troubleshooting Flowchart](#)

[4.2.4 Troubleshooting Procedure](#)

4.2.1 Typical Networking

Figure 4-1 shows a typical BGP networking. The following describes how to troubleshoot the BGP peer relationship based on this networking.

Figure 4-1 Typical networking diagram of BGP



S9300	Interface	VLAN to which the interface belongs	IP address
S9300-A	GE 2/0/1	VLANIF 30	8.1.1.1/24
S9300-A	GE 1/0/2	VLANIF 10	3.1.1.2/24
S9300-A	Loopback0	-	10.1.1.1/32
S9300-B	GE 1/0/1	VLANIF 20	9.1.1.1/24
S9300-B	GE 1/0/2	VLANIF 10	3.1.1.1/24
S9300-B	Loopback0	-	10.1.1.2/32
S9300-C	GE 2/0/1	VLANIF 40	9.1.2.1/24
S9300-C	GE 1/0/1	VLANIF 20	9.1.1.2/24
S9300-C	Loopback0	-	10.1.1.3/32

As shown in [Figure 4-1](#):

- S9300-A resides in AS 65008; S9300-B and S9300-C reside in AS 65009. The physical interface address and Loopback0 address are shown in [Figure 4-1](#).
- An EBGP connection is set up between S9300-A and S9300-B. On both S9300-A and S9300-B, the Loopback0 addresses are configured as the peer addresses.
- An IBGP connection is set up between S9300-B and S9300-C. On both S9300-B and S9300-C, the directly connected VLANIF addresses are configured as the peer addresses.

4.2.2 Configuration Notes

Table 4-4 BGP configuration notes

Item	Sub-item	Configuration Notes and Commands
Enabling BGP	Configuring an AS	The configured AS number must be the same as that specified on the peer. To configure an AS, run the bgp as-number command in the system view.

Item	Sub-item	Configuration Notes and Commands
	Setting a router ID	<p>If a router ID is not set, the global router ID is used by default. The router ID of the local S9300 cannot be the same as that of the peer; otherwise, the connection cannot be set up.</p> <p>To set a router ID, run the router-id <i>router-id</i> command in the BGP view.</p>
Configuring BGP peers	Configuring an AS	<p>The AS number of the specified peer must be the same as that of the peer.</p> <p>To configure an AS, run the peer { <i>group-name</i> <i>ipv4-address</i> } as-number <i>as-number</i> command in the BGP view.</p>
	Configuring an interface for a BGP connection	<p>If an interface is not configured, the physical interface directly connected to the peer is used as the local interface of the TCP connection by default. The address of the specified local interface must be the same as that of the local S9300 specified on the peer.</p> <p>To configure an interface used for a BGP connection, run the peer { <i>group-name</i> <i>ipv4-address</i> } connect-interface <i>interface-type interface-number</i> command in the BGP view.</p>
	Setting the maximum number of hops for EBGP connections	<p>By default, the directly connected physical link must be available between EBGP peers. If the requirement is not met, you must use the peer ebgp-max-hop command to configure EBGP peers to establish TCP connections through multiple hops.</p> <p>To set the maximum number of hops for EBGP connections, run the peer { <i>group-name</i> <i>ipv4-address</i> } ebgp-max-hop [<i>hop-count</i>] command in the BGP view.</p>
Configuring BGP to advertise local routes	Configuring the network	<p>The local routes to be advertised must exist in the local routing table. Using routing policies can more flexibly control the routes to be advertised.</p> <p>To configure the network, run the network <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] [route-policy <i>route-policy-name</i>] command in the BGP-IPv4 unicast address family view.</p>
	Configuring BGP to import routes	<p>Configure BGP to import routes of other protocols, including IGP, Static, and Direct.</p> <p>To configure BGP to import routes, run the import-route <i>protocol</i> [<i>process-id</i>] [med <i>med</i> route-policy <i>route-policy-name</i>] * command in the BGP-IPv4 unicast address family view.</p>

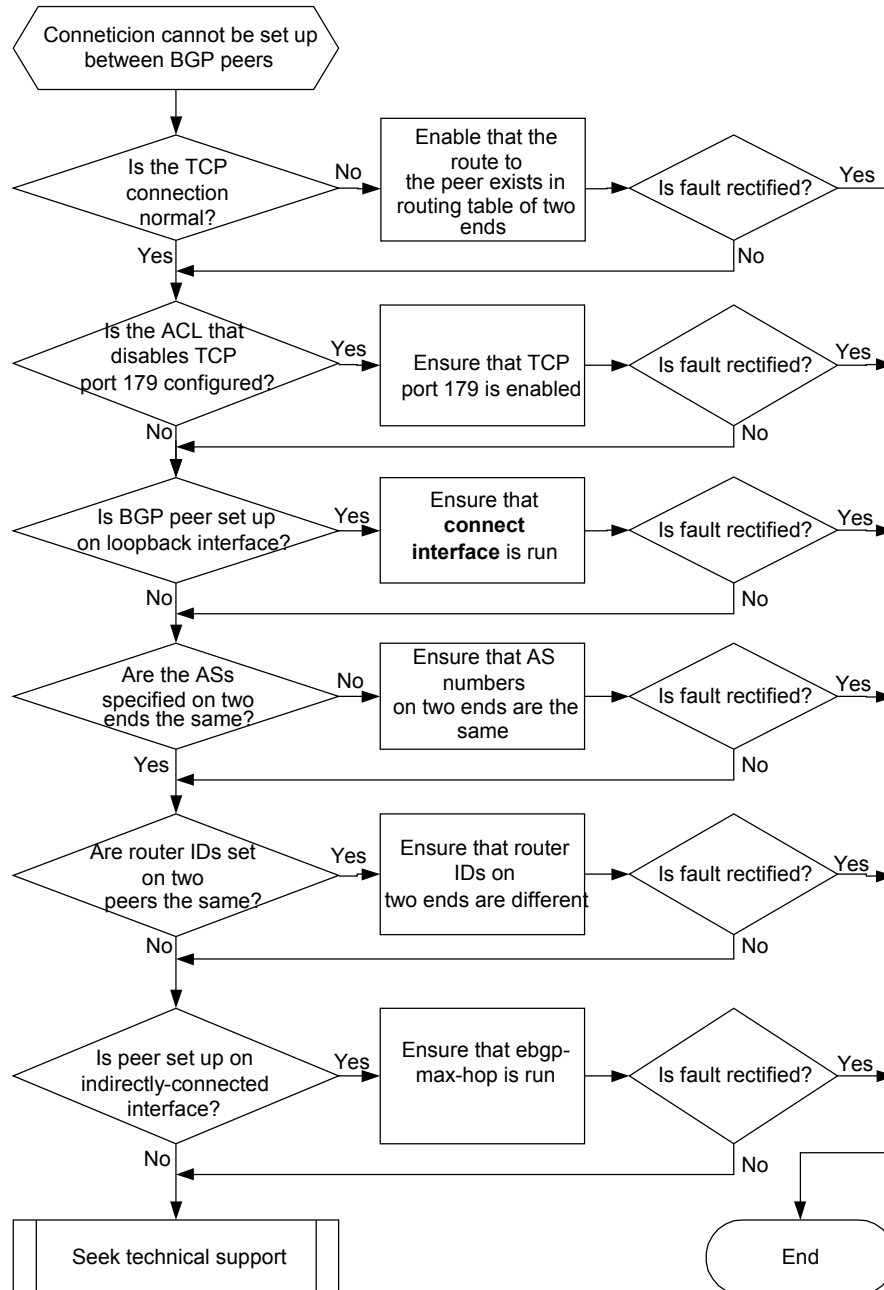
Item	Sub-item	Configuration Notes and Commands
Configuring route aggregation	Configuring automatic aggregation	Route aggregation is used to automatically aggregate only the routes imported by the import command into the route of a natural segment. To configure automatic aggregation, run the summary automatic command in the BGP-IPv4 unicast address family view.
	Configuring manual aggregation	You can manually aggregate the routes imported by the network command and the import command, and the route learned from other peers. The aggregated route does not participate in further aggregation. Manual aggregation takes precedence over automatic aggregation. To configure manual aggregation, run the aggregate ipv4-address { mask mask-length } [as-set attribute-policy route-policy-name1 detail-suppressed origin-policy route-policy-name2 suppress-policy route-policy-name3] * command in the BGP-IPv4 unicast address family view.
Configuring the routing policy for BGP to advertise routes	Configuring the policy for filtering routes to be exported	The policy takes effect when the route is advertised to all the BGP peers. To configure the policy for filtering routes to be exported, run the filter-policy { acl-number ip-prefix ip-prefix-name } export command in the BGP-IPv4 unicast address family view.
	Configuring the policy for filtering routes to be exported to a specified peer	The policy takes effect only when the route is advertised to a specified BGP peer. To configure the policy for filtering routes to be exported to a specified peer, run the peer { group-name ipv4-address } route-policy route-policy-name export command in BGP-IPv4 unicast address family view.
Configuring the routing policy for BGP to receive routes	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 filter-policy { acl-number ip-prefix ip-prefix-name } import command in the BGP-IPv4 unicast address family view.
	Configuring the policy for filtering routes to be imported from a specified peer	The policy takes effect only when the route is received from a specified BGP peer. To configure the policy for filtering routes to be imported from a specified peer, run the peer { group-name ipv4-address } route-policy route-policy-name import command in the BGP-IPv4 unicast address family view.

4.2.3 Troubleshooting Flowchart

As shown in [Figure 4-1](#), peer relationships cannot be set up between BGP peers after the BGP peer is configured for each S9300.

Perform the procedure shown in [Figure 4-2](#).

Figure 4-2 BGP peer relationship troubleshooting flowchart



4.2.4 Troubleshooting Procedure

Procedure

Step 1 Run the **ping** command with the source address 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, to check whether the route between the loopback interfaces of S9300-A and S9300-B is normal, run the following command on S9300-B:

```
ping -a 10.1.1.2 10.1.1.1
```

Step 2 Check whether an ACL disabling TCP port 179 is set.

On each S9300, run the **display current-configuration** command or the **display acl all** command to check whether an ACL that disables TCP port 179 is set. Port 179 is the listening port that is used to set up TCP connections for BGP peers. If port 179 is disabled, the TCP connections cannot be set up.

Step 3 Check that **connect-interface** is specified if the loopback interface is used to set up a 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 through debugging information when a TCP connection is set up.

Run the **debugging bgp ipv4-address all** command to debug a certain peer. For example, if S9300-B and S9300-A cannot set up the connection, run the **debugging bgp 10.1.1.2 all** command on S9300-B to enable the BGP debugging and check the cause why the connection cannot be set up.

- If "Send/Receive NOTIFICATION Err/SubErr: 2/2 (OPEN Message Error/Bad Peer AS)" is displayed, it indicates that the AS is configured incorrectly. Check whether the AS where S9300-A and S9300-B belong is the same as the AS specified on the peer.
- If "Send/Receive NOTIFICATION Err/SubErr: 2/3 (OPEN Message Error/Bad BGP Identifier)" is displayed, it indicates that the router ID is set incorrectly. Check whether the router IDs of S9300-A and S9300-B are the same.

If the error code is displayed in Send Notification, it indicates that the preceding errors occur on the BGP speaker.

If the error code is displayed in Receive Notification, it indicates that the preceding errors occur on the BGP peer.

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

If "Might miss configing ebgp-max-hop for ebgp multi-hop peer" is displayed, it indicates that the indirectly connected interface sets up the EBGP peer relation, but is not configured with Ebgp-Max-Hop. [Table 4-5](#) shows the common error codes of Open messages.

Table 4-5 Error code of Open messages

Error Code	Description
2/1	Unsupported version number
2/2	Incorrect AS number
2/3	Incorrect 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 Peer Relationship Troubleshooting

This section describes the notes about configuring BGP, and provides the accidental interruption of BGP peer relationship troubleshooting flowchart and the troubleshooting procedure in a typical BGP network.

[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

For the networking, see [Figure 4-1](#).

4.3.2 Configuration Notes

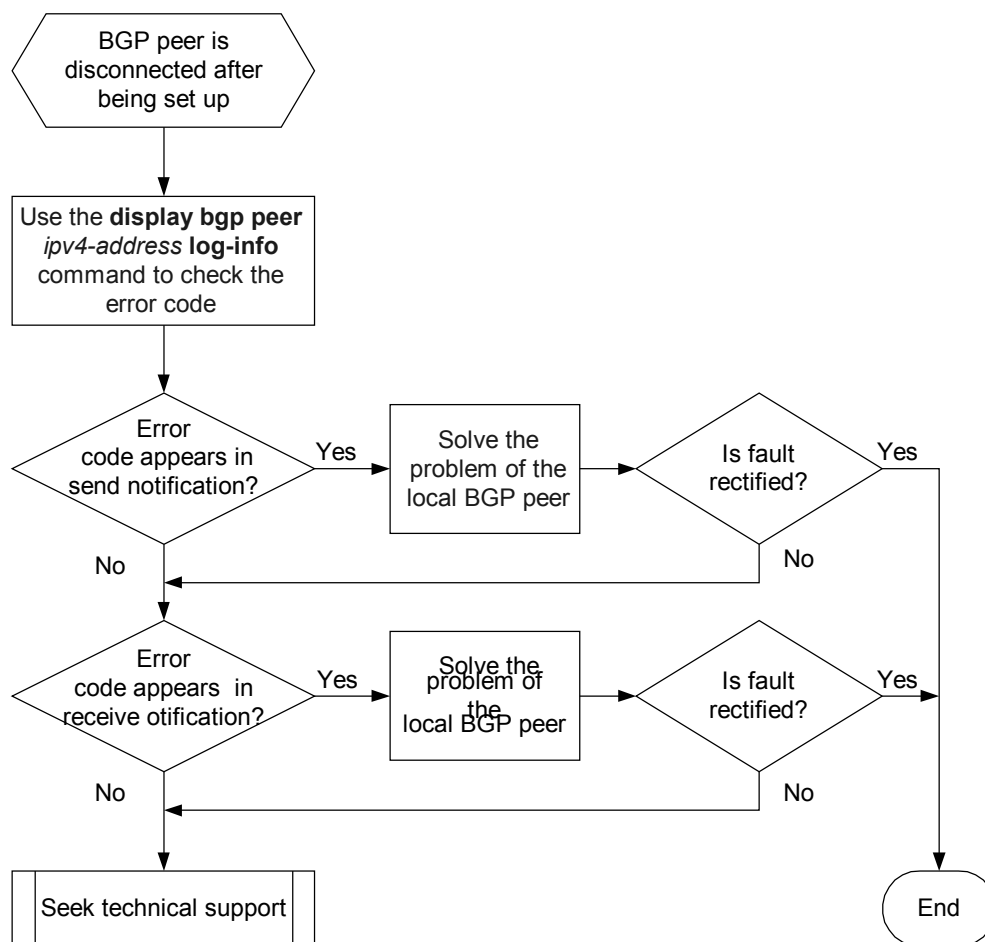
For the configuration notes, see section [4.2.2 Configuration Notes](#).

4.3.3 Troubleshooting Flowchart

As shown in [Figure 4-1](#), the BGP peer relationship is torn down after the BGP peer is configured for each S9300.

Follow the procedure shown in [Figure 4-3](#).

Figure 4-3 BGP peer relationship troubleshooting flowchart



4.3.4 Troubleshooting Procedure

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

Table 4-6 Prerequisites for setting up BGP peer

Objective	Requirement
Keep the TCP connection.	The link layer is stable.
	The reachable route is stable.
Exchange Keepalive messages correctly.	The network is not congested.
	Data packets can reach the destination.
Exchange Update messages correctly.	The network is not congested.
	Large packets can reach the destination.

Objective	Requirement
	BGP is configured correctly. The incorrect BGP configuration may lead to the incorrect attribute in Update messages.

If the preceding requirements are met, the faults of setting up the BGP peer relationship can be rectified.

Check the error code when the BGP connection is torn down.

Run the **display bgp peer ipv4-address log-info** command to check the error code when the BGP connection is torn down.

Table 4-7 Error code of Open messages

Error Code	Action
6/1	Check whether the number of prefixes reaches the upper threshold.
6/2	Check whether the administration is shut down.
6/3	Check whether the peer is deleted.
6/4	Check whether the administration is reset.
6/5	Check whether the connection fails.
6/6	Check whether other configurations change. Check whether the commands that lead to the disconnection of the BGP peer relationship are used, such as the peer { group-name ipv4-address } ignore command or the command to modify the key configurations such as router ID, RR, or confederation.
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 is reachable and the TCP connection is normal.
4/0	Check whether the routes are reachable.
	Check whether the network is congested.
	Check whether data packets can reach the destination.
3/0	Check whether the confederations are configured the on both sides and the configurations are the same.
1/1	Check whether the message header error occurs in the packet format: other errors in the message header.
1/2	Check whether the message header error occurs in the packet format: the message length error.

Error Code	Action
1/3	Check whether the message header error occurs in the packet format: the message type error.
3/1	Check whether the Update error occurs in the packet format: the attribute list error.
3/2	Check whether the Update error occurs in the packet format: the unsupported mandatory attribute.
3/3	Check whether the Update error occurs in the packet format: no mandatory attribute.
3/4	Check whether the Update error occurs in the packet format: the incorrect attribute flag.
3/5	Check whether the Update error occurs in the packet format: the incorrect 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 incorrect optional parameter.
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 incorrect AS_Path.

If the error code is displayed in Send Notification, it indicates that the preceding errors occur on the BGP speaker.

If the error code is displayed in Receive Notification, it indicates that the preceding errors occur on the BGP peer.

If the fault persists, contact the Huawei technical personnel.

4.4 Route Loss Troubleshooting When BGP Peers 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 network.

4.4.1 Typical Networking

[4.4.2 Configuration Notes](#)

[4.4.3 Troubleshooting Procedure](#)

[4.4.4 Troubleshooting Procedure](#)

4.4.1 Typical Networking

For the networking, see [Figure 4-1](#).

4.4.2 Configuration Notes

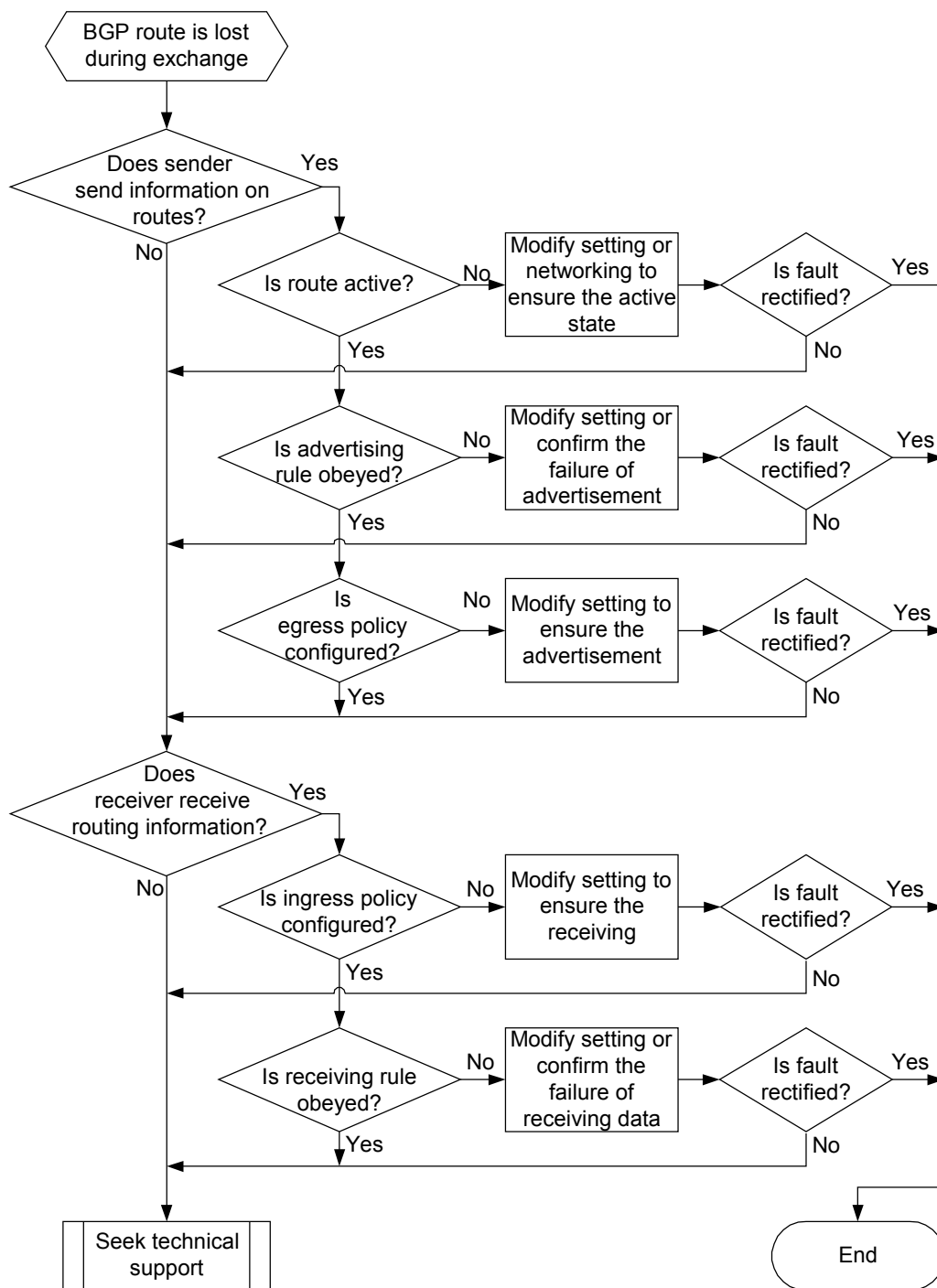
For the configuration notes, see section [4.2.2 Configuration Notes](#).

4.4.3 Troubleshooting Procedure

As shown in [Typical Networking](#), the route is lost during the exchange of Update messages after the BGP peer is configured for each S9300.

Perform the procedure shown in [Figure 4-4](#).

Figure 4-4 BGP route loss troubleshooting flowchart



4.4.4 Troubleshooting Procedure

Procedure

Step 1 Check whether the transmit end advertises the route.

Run the **display bgp routing-table peer *ipv4-address* advertised-routes** command on the transmit end to check whether the route is sent.

If the transmit end does not send the route, do as follows:

1. 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 a higher preference exists at the local end.
2. Check whether the rule for advertising routes is complied.
 - The aggregated route cannot be advertised.
Run the **display bgp routing-table** command to check which routes are aggregated routes. The route marked with s is the aggregated route.
 - The route suppressed by BGP 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 suppressed route.
 - The route learned from an IBGP peer is not forwarded to IBGP peers.
3. Check whether the policy is configured to filter the advertised route.
BGP can use the following filters:
 - IP prefix list
 - AS_Path filter
 - Community filter
 - Route-PolicyThe preceding filters can be applied to the routes 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 whether the receive end receives the route.

Run the **display bgp routing-table peer *ipv4-address* received-routes** command on the receive end to check whether the route is received.

If the receive end does not receive the route, do as follows:

1. Check whether the policy is configured to filter the received route.
Run the **display current-configuration configuration bgp** command to check the configuration.
2. Check whether the rule for receiving routes is complied with.

The route is not received when the following situation occurs:

- The **peer { *group-name* | *ipv4-address* } allow-as-loop [*number*]** command is not used and the local AS number is carried in the AS_Path of the received route.
- The **peer { *group-name* | *ipv4-address* } allow-as-loop [*number*]** command is used. Carried in the AS_Path of the received route, the number of times the AS number is repeated is greater than the value specified by *number*. By default, the value is 1.

- The first AS number in the AS_Path 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 value 0.0.0.0.
- The Cluster-List in the route received by the reflector contains the local Cluster-ID.
- The Aggregator is the invalid value 0.0.0.0.
- The 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 { group-name | ipv4-address } route-limit limit [percentage] alert-only** command is used, the received routes are denied after the threshold is reached.

If the fault persists, contact the Huawei technical personnel.

----End

4.5 Troubleshooting Cases

This section presents several troubleshooting cases.

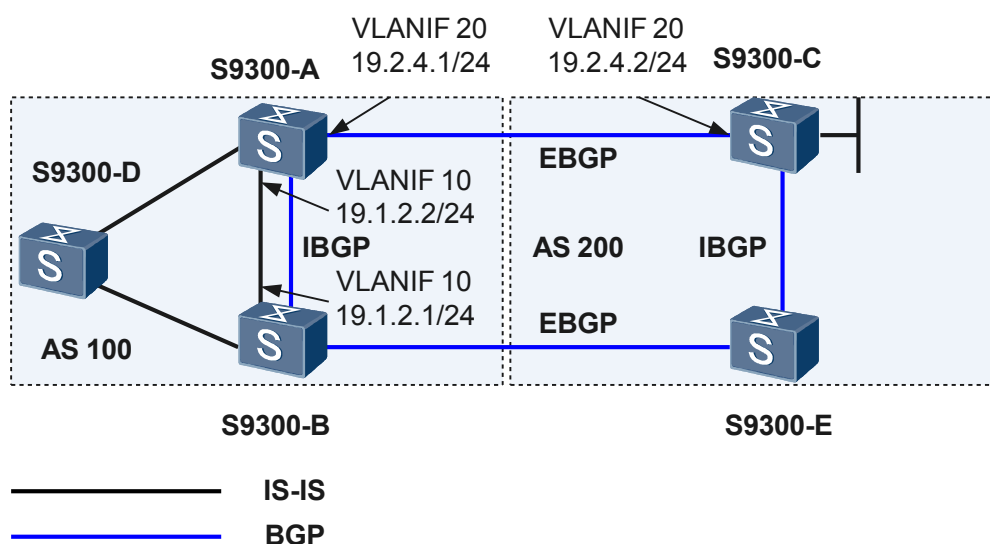
4.5.1 Routing Loop and Route Flapping

4.5.2 Peer Relationship Is Torn Down When the Number of Routes Does not Exceed the Threshold

4.5.1 Routing Loop and Route Flapping

Fault Symptom

Figure 4-5 Typical networking diagram of BGP



As shown in [Figure 4-5](#):

- In AS 100, IS-IS is run and the area has two egresses.
- S9300-A and S9300-B advertise intra-area routes after the **import-route isis** command is run in the BGP view; they receive external routes after the **import-route bgp** command is run in the IS-IS view.
- After the configuration is complete on the network, pinging 14.1.1.1 on S9300-A fails continuously. Run the **tracert -a 14.1.1.1** command to check all the gateways that the ping packet passes from S9300-A to S9300-C.

```
<S9300-A> tracert -a 14.1.1.1
traceroute to 14.1.1.1(14.1.1.1) 30 hops max, 40 bytes packet
 1 19.1.2.1 47 ms 31 ms 16 ms [S9300-B]
 2 19.1.2.2 46 ms 16 ms 31 ms [S9300-A]
 3 19.1.2.1 63 ms 47 ms 47 ms [S9300-B]
 4 19.1.2.2 62 ms 47 ms 47 ms [S9300-A]
 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 operation fails to be performed continuously. The **tracert** command output shows that a routing loop occurs between S9300-A and S9300-B. Check the route first by running the **display ip routing-table** command repeatedly on S9300-A.

```
<S9300-A> display ip routing-table 14.4.4.4
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 19.1.2.1 Vlanif10
<S9300-A> display ip routing-table 14.4.4.4
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 19.2.4.2 Vlanif20
<S9300-A> display ip routing-table 14.4.4.4
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 19.1.2.1 Vlanif10

```

It is found that the route changes continuously. The next hop of the BGP route is S9300-C, whereas the next hop of the IS-IS route is S9300-B.

On the S9300, the IS-IS route takes precedence over the BGP route by default. If the IS-IS route is stable, the flapping cannot occur.

2. Run the **display ip routing-table** command on S9300-B to check the source of the IS-IS route. Run the **display ip routing-table 14.1.1.1** command, and find that flapping also occurs between BGP and IS-IS.

Check the configuration on S9300-A and S9300-B.

```
<S9300-A> display current-configuration configuration bgp
<S9300-A> display current-configuration configuration isis
<S9300-B> display current-configuration configuration bgp
<S9300-B> display current-configuration configuration isis

```

The preceding information shows that BGP and IS-IS import routes from each other between S9300-A and S9300-B. Based on the topology, the following points can be inferred:

- The original route is transmitted to S9300-A and S9300-B through EBGP.
- S9300-A and S9300-B re-advertise the route to IS-IS. Then, the route is transmitted between S9300-A and S9300-B through IS-IS.
- By default, the IS-IS route takes precedence over the BGP route. Thus, the IS-IS route replaces the BGP route.
- The BGP route is not the optimal route. Thus, the BGP route is removed after that information is notified the peer.
- After the BGP route is removed, the IS-IS route is also removed because the IS-IS route originates from BGP.
- After the IS-IS route is removed, 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 from AS 300 is retransmitted to AS 300 through S9300-A and S9300-B. The re-selection of the external route results in flapping.

Procedure

- Step 1** Configure the policy for filtering routes on the outbound interface of S9300-A and S9300-B. Only the route in the area can be advertised.
- Step 2** Run the **preference** command to modify the preference of the route on S9300-A and S9300-B. Ensure that the precedence of the route learned from EBGP is higher than that of the IS-IS route inside the area.

---End

Summary

Routing loop or route flapping is often caused by incorrect configurations.

In the case that BGP and an IGP import routes from each other, you should identify the source. Ensure that the source route has the higher preference. In this manner, the route can keep stable.

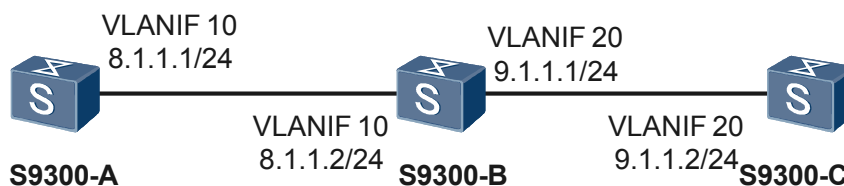
For the AS with multiple egresses, if an IGP and BGP import routes from each other, the policy for filtering the exported route is needed. This ensures that the route learned from an AS is not retransmitted to the same AS. Otherwise, the stability of the route outside the area is affected.

4.5.2 Peer Relationship Is Torn Down When the Number of Routes Does not Exceed the Threshold

Fault Symptom

As shown in [Figure 4-6](#), S9300-A resides in AS 100; S9300-B resides in AS 200; S9300-C resides in AS 300. The **peer route-limit** command is used on S9300-C to restrict the number of routes received from S9300-B. S9300-C tears down the peer relationship with S9300-B when the number of routes sent from S9300-B to S9300-C does not exceed the threshold.

Figure 4-6 Networking diagram that peer relationship is torn down but the number of routes does not exceed the threshold



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

1. Set up an EBGP connection between the S9300s.
2. Configure five static routes on S9300-A and advertise them to other S9300s through BGP.

Configure S9300-A.

```
[S9300-A] ip route-static 200.1.1.1 24 NULL 0
[S9300-A] ip route-static 200.1.2.1 24 NULL 0
[S9300-A] ip route-static 200.1.3.1 24 NULL 0
[S9300-A] ip route-static 200.1.4.1 24 NULL 0
[S9300-A] ip route-static 200.1.5.1 24 NULL 0
[S9300-A] bgp 100
[S9300-A-bgp] import-route static
```

Check the BGP routing table on S9300-C. You can find that S9300-C learns the five static routes from S9300-A.

```
[S9300-C-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 S9300-B to filter the two routes sent to S9300-C.

Configure the routing policy named **out** on S9300-B and apply the routing policy to the routes sent to S9300-C.

```
[S9300-B] acl 2001
[S9300-B-acl-basic-2001] rule permit source 200.1.1.0 0.0.0.255
[S9300-B-acl-basic-2001] rule permit source 200.1.2.0 0.0.0.255
[S9300-B-acl-basic-2001] quit
[S9300-B] route-policy out deny node 20
[S9300-B-route-policy] if-match acl 2001
[S9300-B-route-policy] quit
[S9300-B] route-policy out permit node 30
[S9300-B-route-policy] quit
[S9300-B] bgp 200
[S9300-B-bgp] peer 9.1.1.2 route-policy out export
```

Check the BGP routing table on S9300-C, and find that the routes 200.1.1.1/24 and 200.1.2.1/24 are filtered out.

```
<S9300-C> 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      200 100?
*> 200.1.4.0  9.1.1.1          0      200 100?
*> 200.1.5.0  9.1.1.1          0      200 100?
```

4. Run the **peer route-limit** command on S9300-C. Set the maximum number of routes that the S9300-C can receive from S9300-B to 4. When the number of the routes sent by S9300-B exceeds the threshold, the peer relationship is torn down.

Configure S9300-C.

```
[S9300-C] bgp 300
[S9300-C-bgp] peer 9.1.1.1 route-limit 4
```

The peer relationship between S9300-C and S9300-B is normal because S9300-B sends only three routes to S9300-C.

5. Modify the policy on S9300-B; specify the policy named **out** with the index number as 10 in **permit** mode. After only two routes that match ACL 2001 are sent to S9300-C, the peer relationship is torn down.

```
[S9300-B] route-policy out permit node 10
Info: New Sequence of this List !
%Aug 9 19:22:24 2006 S9300-B RM/4/RMLOG:
  BGP.Public: 9.1.1.2 State is changed from ESTABLISHED to IDLE.

%Aug 9 19:22:55 2006 S9300-B RM/4/RMLOG:
  BGP.Public: 9.1.1.2 State is changed from OPENCONFIRM to ESTABLISHED.

%Aug 9 19:22:55 2006 S9300-B RM/4/RMLOG:
  BGP.Public: 9.1.1.2 State is changed from ESTABLISHED to IDLE.
```

Fault Analysis

1. After the **peer route-limit** command is used, the peer relationship between S9300-B and S9300-C is torn down and re-established. The cause is that the number of routes sent by S9300-B exceeds 4. Check S9300-C, and find that the number of routes exceeds the threshold in the log.

```
[S9300-C-bgp]
%Aug 11 20:19:11 2006 S9300-C RM/4/RMLOG:
  BGP.Public: 9.1.1.1 Max number of prefix exceeded limit, maximum: 4.

%Aug 11 20:19:11 2006 S9300-C RM/4/RMLOG:
  BGP.Public: 9.1.1.1 State is changed from ESTABLISHED to IDLE.
```

Only node 10 of the routing policy is expected to be changed. In this case, two routes are sent to S9300-C, which does not exceed the threshold.

```
[S9300-B] route-policy out permit node 10
[S9300-B-route-policy] if-match acl 2001
```

After the **route-policy out permit node 10** command is used, the peer relationship is torn down. The cause is that BGP applies the routing policy immediately. When the RM uses the routing policy, the routing entry first matches the node with the smallest index number. If the route matches one node, the route does not match other nodes. Here, the index number of the node in **permit** mode is 10 and the node permits all the routes to pass through. Thus, the number of routes sent to S9300-C is 5, which exceeds the threshold.

Why is the routing policy applied before the configuration is complete?

2. Run the **display current-configuration** command on S9300-B to check the configuration.

```
<S9300-B> display current-configuration
#
 sysname S9300-B
#
 route-policy-change notify-delay 0
```

The preceding information shows that the delay for applying the policy is 0. That is, the RM immediately notifies the protocol to apply a new policy when the routing policy changes. As a result, BGP applies the routing policy when the configuration is incomplete.

Procedure

- Step 1** Run the **route-policy-change notify-delay** command to adjust the delay after the routing policy changes.
- Step 2** The delay ranges from 0 to 180. You can adjust the delay as required.
- Step 3** (Optional) Configure a new routing policy.

To check the configuration, run the **refresh bgp all export** command on S9300-B after the configuration of the routing policy is complete.

----End

Summary

If the delay for updating the routing policy is short and the **peer route-limit** command is used, the change of the routing policy may result in the excess of the routes. The BGP peer relationship is thus disconnected.

It is recommended that you set the size of the routing table to a larger value for route flapping. You can also configure the S9300 to generate alarms when the number of routes exceeds the limit, rather than disconnecting the neighbors. This can improve the system stability.

4.6 FAQs

This section lists frequently asked questions and their answers.

Q: When the **display bgp peer** Command Is Run to Check the BGP Peer, the Connection Cannot Enter the Established State. How to Rectify the Fault?

A: The prerequisites for setting up a BGP peer are as follows:

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

To rectify the fault, do as follows:

- Check whether the AS number and IP address between the peers are configured correctly by using the **display bgp peer** command.
- Check whether the router IDs set on both BGP peers conflict by using the **display bgp peer** command.
- If the loopback interface is used, check whether the **connect-interface** command is used to specify the loopback interface as the originating interface that sends BGP packets.

- If EBGP peers are physically and indirectly connected, check whether the **peer ebgp-max-hop** command is used.
- Check whether there are available routes to the peer in the routing table.
- Check whether there are reachable routes to the specified interface by using the **ping -a source-ip-address** host command.
- Check whether an ACL disabling TCP port 179 is set.

Q: When Can the peer allow-as-loop Command Be Used?

A: The command is only used to check whether there is the local AS number in the routes received from EBGP and EBGP peers in the confederation. The routes from IBGP or IBGP peers in the confederation are not checked.

Q: When Can the peer public-as-only Command Be Used?

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

- The peer is an EBGP peer or an EBGP peer in confederation.
- The AS_Path contains the AS number of the private network.
- The AS number of the private network is different from that of the peer. If the AS number of the private network is the same as that of the peer, deleting the AS number may result in loops.

Q: What Is the Priority of Policies for Modifying the MED?

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

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

Table 4-8 Priority of policies for modifying the MED

No.	Policy
1	Configure the Apply Cost clause in the export policy on the peer. It is applicable to all the BGP routes.
2	Configure the Apply Cost-Type Internal clause in the export policy on the peer.
3	Use the default MED command. It is applicable to the route to be imported such as the static, direct, and IGP route and the aggregated route.
4	Configure Apply Cost clause of the import policy.
5	Use the IGP metric for imported IGP routes. The BGP route learned from the peer carries the MED.
6	Do not set the metric.

Q: How Is the Apply Preference Clause Used in the Routing Policy of BGP?

A: The **Apply Preference** clause in the routing policy only takes effect when it is used together with the **preference** { *external internal local* | **route-policy** *route-policy-name* } command. BGP can only use the **preference** command in the BGP view to modify the preference of the route.

Q: Why Is the BGP Connection Closed After the Configuration of the BGP Peer Capability Is Changed?

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

- Label-Route-Capability is enabled or disabled.
- The BGP peer in the address family is enabled or disabled. For example, if the **peer enable** and **undo peer enable** commands are run in the VPNv4 address family, the BGP connection of the peer in other address family closes automatically.
- GR capability is enabled.

Q: Why Does Not the BGP Peer Relationship Close Immediately After the Interface Is Shut Down?

A: The EBGP peer relationship is disconnected immediately only when EBGP peers are directly connected and the **ebgp-interface-sensitive** command is run in the BGP view. By default, the command is run. Otherwise, the BGP peer relationship is not torn down until the hold time expires.

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

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

- Active IGP route in the IP routing table
You can run the **display ip routing-table protocol protocol** command to check the route.
- Direct route corresponding to the interface enabled with an IGP
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.

Q: How Is the Attribute Processed 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 or the **peer next-hop-local** command.

Q: When the Statistics of Flapped Routes Are Cleared by Running the reset bgp flap-info Command, Why Does Not the Command Take Effect If No Mask Is Added?

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 that is a Class C address is 16 bits. 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 dampened routes and release suppressed routes. If the mask is not specified, the address is processed as a classful address.

Q: Why Are the Routes Unavailable Even After the aggregate Command Is Run to Aggregate Routes?

A: Check whether the mask length of the aggregated routes is set correctly. The local outbound interface of the aggregated route is NULL0. If the mask length of the aggregated route is equal to that of the routes to be aggregated, the aggregated route destined for NULL0 overwrites the routes to be aggregated. Then, the routes are unavailable.

Q: When the import/export route-policy Command Is Applied to the Default Routes, Why Does Not the Routing Policy Take Effect?

A: On the S9300, the **import** and **export route-policy** commands are invalid for default routes.

Q: Is There Any Requirement for the Configuration of BGP Authentication Keys?

A: A BGP authentication key can be either in plain text or in encrypted text. The rules to form a BGP authentication key are as follows:

- In plain text mode, the authentication key is a string of 1 to 16 characters.
- In encrypted text mode, the authentication key is also a string of characters. The string with 1 to 16 characters corresponds to the plain text, whereas the string with 24 characters corresponds to the encrypted text.
- An authentication key cannot contain spaces.

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

Table 4-9 BGP display commands

Command	Description
display bgp peer	Displays the summary of the IPv4 peer of the public network.
display bgp peer <i>ipv4-address</i> verbose	Displays the detailed information about the specified peer.

Command	Description
display bgp peer <i>ipv4-address</i> log-info	Displays logs of the specified peer, which helps you locate the fault of accidental disconnection of the peer relationship.
display bgp group <i>group-name</i>	Displays information about the IPv4 peer group of the public network.
display bgp routing-table statistics	Displays statistics about IPv4 unicast routes of the BGP public network.
display bgp routing-table	Displays the summary about IPv4 unicast routes of the BGP public network.
display bgp routing-table peer <i>ipv4-address</i> advertised-routes	Displays the route advertised to the specified peer.
display bgp routing-table peer <i>ipv4-address</i> received-routes	Displays the route received from the specified peer.
display bgp network	Displays the BGP route imported with the network command.
display bgp paths	Displays the AS_Path of the IPv4 unicast route of the BGP public network.
display bgp multicast	Displays information about IPv4 multicast of the BGP public network. The usage of the command is the same as that of the corresponding command used for IPv4.
display ip routing-table statistics	Displays the statistics about IPv4 routes of the system public network.
display ip routing-table protocol bgp	Displays the summary about active and inactive BGP routes in the IPv4 routing table of the system public network.
display ip routing-table protocol bgp verbose	Displays the detailed information about active and inactive BGP routes in the IPv4 routing table of the system public network.
display ip routing-table protocol bgp inactive	Displays the summary about inactive BGP routes in the IPv4 routing table of the system public network.

4.7.2 debugging Commands

Table 4-10 BGP debugging commands

Command	Description
debugging bgp all	Enables the debugging of all the BGP information. The command is applied when a few routes are configured and a few routes change.
debugging bgp <i>ipv4-address</i> all	Enables the debugging of all the specified peers. The command is applied when a few routes change.
debugging bgp <i>ipv4-address</i> event	Enables the debugging of the event of the specified peer. The command is used to locate the fault of setting up the peer relationship.
debugging bgp <i>ipv4-address</i> raw-packet receive verbose	Enables the debugging of the receiving of original packets of the specified peer. The command is used to check information about original packets.
debugging bgp update ip-prefix <i>ip-prefix-name</i> receive verbose	Enables the debugging of the Update message that satisfies the matching rules of the IP prefix list. The command is used to locate the fault of the route loss.
debugging bgp graceful-restart	Enables the debugging of BGP GR.

5 Routing Policy Troubleshooting

About This Chapter

This chapter describes the procedure and diagnostic tools of routing policy troubleshooting.

[5.1 Routing Policy and Filter Overview](#)

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

[5.2 Routing Policy Troubleshooting](#)

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

[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 information you need to know before troubleshooting the routing policy.

[5.1.1 Routing Policy](#)

[5.1.2 IP Prefix List](#)

[5.1.3 Routing Policy](#)

5.1.1 Routing Policy

Routing policy is used to change the path that the traffic passes through. It is implemented by changing the route attributes such as reachability.

To implement the routing policy, you should first define the route attributes, that is, a group of matching rules. You can use the route attributes as matching rules, such as the destination address and the address of the S9300 advertising routes. The matching rules can be preset, and then they can be used to advertise, receive, and import routes.

When advertising or receiving routes, an S9300 may implement certain routing policies to filter them. For example, the S9300 receives or advertises only the routes that meet the conditions. To enrich routing information, a routing protocol such as the Open Shortest Path First (OSPF) protocol may import routes discovered by other routing protocols. When importing routes discovered by other routing protocols, an S9300 may import only the routes that meet the conditions, and sets the route attributes to meet the requirement of the protocol.

5.1.2 IP Prefix List

The IP prefix list is a flexible filter. Compared with an ACL, an IP prefix list is applied flexibly and configured easily. The IP prefix list can filter routes according to the destination address. The S9300 provides IP prefix lists for IPv4 routes.

An IP prefix list is identified by a prefix list name. Each IP prefix list can contain multiple entries, and each entry can specify the matching range in the form of a network prefix. The matching range is identified by an index number that designates the matching sequence.

During the matching, the S9300 checks entries identified by the index number in an ascending order. If one entry meets the condition, it indicates that the route matches the IP prefix list. That is, the route does not match other entries.

5.1.3 Routing Policy

A routing policy is a complex filter. A routing policy can be used to match certain attributes of specified routes, and to change the route attributes when certain conditions are met. The routing policy can use the IP prefix list to define its matching rules.

A routing policy may consist of multiple nodes. The relationship between the nodes is "OR". The system checks the nodes according to the number of the node. When a route matches a node in the routing policy, the route does not match the next node.

Each node comprises a set of **if-match** and **apply** clauses:

- The **if-match** clauses define the matching rules that are used to match certain route attributes. The relationship between the **if-match** clauses of a node is "AND". A route matches a node only when the route meets all the matching rules specified by the **if-match** clauses of the node.
- The **apply** clauses specify actions. When a route matches a node, the **apply** clauses set some attributes for the route.

5.2 Routing Policy Troubleshooting

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

5.2.1 Typical Networking

5.2.2 Configuration Notes

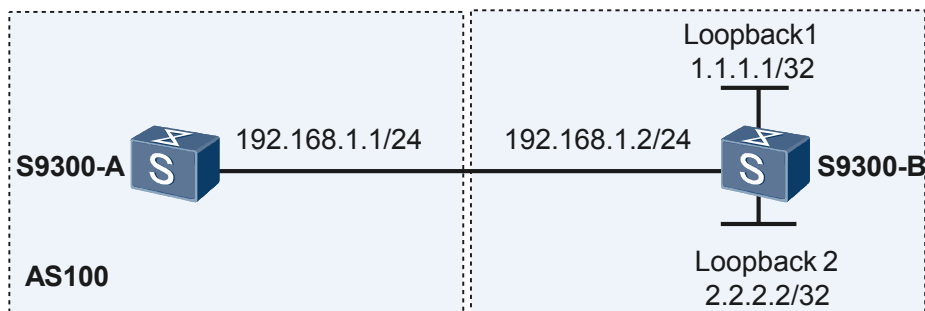
5.2.3 Troubleshooting Flowchart

5.2.4 Troubleshooting Procedure

5.2.1 Typical Networking

Figure 5-1 shows a typical networking of the routing policy. The following describes how to troubleshoot the routing policy based on this networking.

Figure 5-1 Typical networking diagram of the routing policy troubleshooting in a public network



In **Figure 5-1**, when S9300-A receives the routes advertised by S9300-B, both S9300-A and S9300-B use the routing policy.

5.2.2 Configuration Notes

Common Filters in the Routing Policy

Table 5-1 Routing policy configuration notes

Item	Sub-item	Configuration Notes and Commands
Configuring an IP prefix list	Configuring an IP prefix list	<p>To configure an IP prefix list, run the ip ip-prefix ip-prefix-name [index index-number] { permit deny } ip-address mask-length [greater-equal greater-equal-value less-equal less-equal-value] command in the system view.</p> <ul style="list-style-type: none"> • The name of the IPv4 prefix list is specified by <i>ip-prefix-name</i>. You can configure multiple matching entries for each IPv4 prefix list. Each entry may have an index number. If the index number is not specified, the number of the generated entry equals the existing maximum index number plus ten. • If the length of the specified IPv4 prefix list 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> <= <i>greater-equal</i> <= <i>less-equal</i> <= 32. • During the matching, the system checks the entries in an ascending order according to their index numbers. As long as the address or mask of one entry is the same as that of the route to be checked, the filtering mode permit or deny of the entry is returned. At the same time, the route does not match other entries. • If all entries are set in deny mode, none of the route can pass the prefix list. You can set an entry permit 0.0.0.0 greater-equal 0 less-equal 32 after multiple entries in deny mode. In this case, all IPv4 routes can pass. • The common fault is that the configuration of the IP prefix list and that of the ACL are taken as the same. Actually, if only the IP address or the 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>.

Item	Sub-item	Configuration Notes and Commands
Configuring a route policy	Configuring a route policy	<p>To configure a route policy, run the route-policy <i>route-policy-name</i> { permit deny } node { <i>node-number</i> } command in the system view.</p> <ul style="list-style-type: none"> ● The parameter permit specifies a node in permit mode. If a route matches the node, the S9300 performs the apply clauses and the matching is complete. If the route fails to match the node, the route matches the next node. If there are no if-match clauses in a node, all the routes are permitted. ● The parameter deny specifies a node in deny mode. In deny mode, the apply clauses are not used. If a route satisfies all the if-match clauses of a node, the route is denied by the node. If a route does not satisfy any if-match clause of a node, the route matches the next node. If there are no if-match clauses in a node, all the routes are denied. ● If if-match clauses of none of the nodes are unmatched, the route policy is in deny mode by default. ● If all the nodes are set in deny mode, all the routes are denied. Thus, you should configure a node in permit mode after configuring all nodes in deny mode to permit other routes to pass through.

Precautions for Applying Filters

When applying filters, note the following:

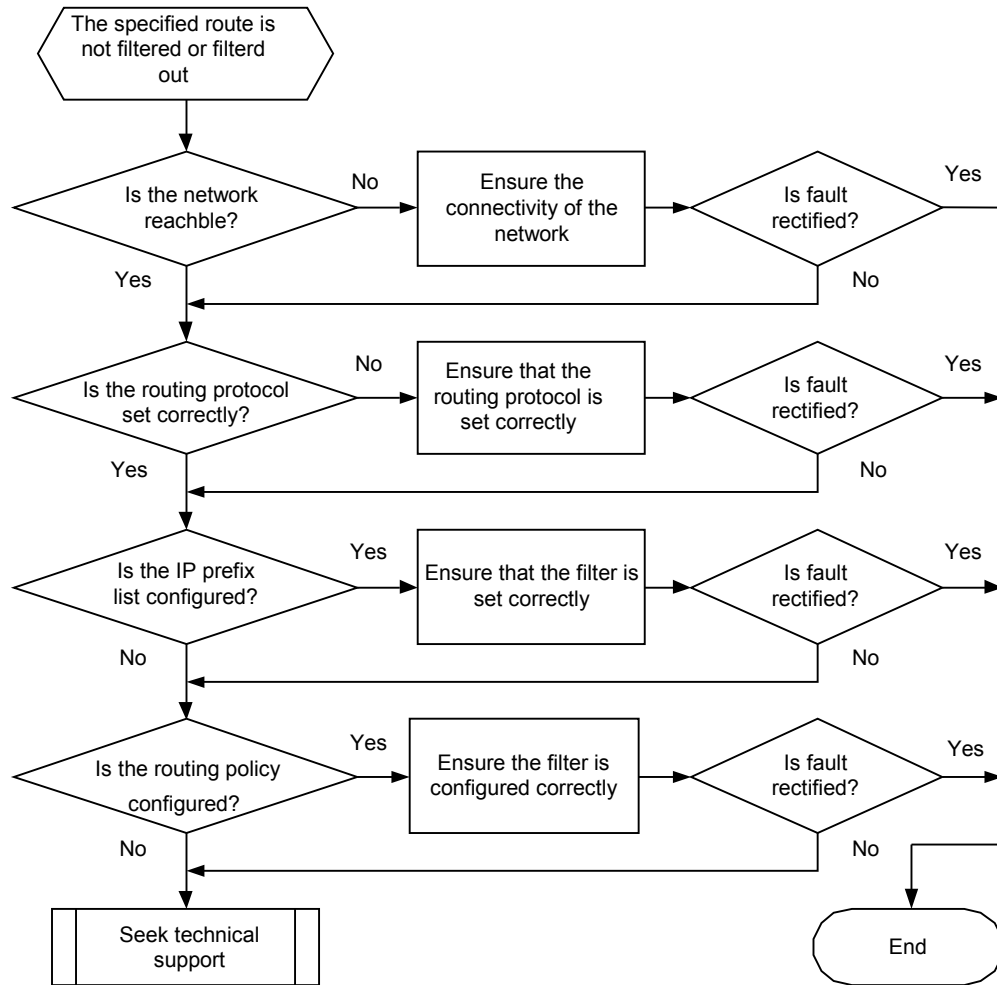
- Suppose at least one node is set either in **permit** mode or in **deny** mode for the current filter. If no node matches the address or mask range of the route that needs to be filtered, the route is denied.
- If a nonexistent filter is used in the policy, all the routes are permitted.

5.2.3 Troubleshooting Flowchart

In the networking shown in [Figure 5-1](#), the specified route is filtered or not filtered after the S9300s are configured.

Perform the troubleshooting procedure shown in [Figure 5-2](#).

Figure 5-2 Troubleshooting flowchart of the routing policy



5.2.4 Troubleshooting Procedure

Context

The steps of troubleshooting are as follows:

Procedure

Step 1 Check the network connectivity.

Run the **display ip interface brief** command to check the status of each interface. Up indicates that the interface is available, whereas Down indicates that the interface is unavailable.

If the interface is Down, check whether the link is connected properly or whether 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 whether the routing protocol is configured correctly.

If the routing protocol is configured incorrectly, refer to the troubleshooting manuals of related protocols.

Step 3 Check whether the IP prefix list is configured.

Run the **display ip ip-prefix** command to check whether the S9300 is configured with the IP prefix list. Check whether the IP prefix list takes effect by checking the number of matching times.

If the S9300 is not configured with the IP prefix list, check information about the IP prefix list in section [5.2.2 Configuration Notes](#).

Step 4 Check whether the routing policy is configured.

Run the **display route-policy** command to check whether the S9300 is configured with the routing policy.

If it is configured, check information about the routing policy in [5.2.2 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 the IP Prefix List Is Used

5.3.1 Routes Are Lost After the IP Prefix List Is Used

Fault Symptom

For the networking diagram, see [Figure 5-1](#).

In [Figure 5-1](#), S9300-A adopts the IP prefix list to filter the routes received from S9300-B.

Configure S9300-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 S9300-a import
#
ip ip-prefix S9300-a index 20 deny 2.2.2.2 32
#
```

Configure S9300-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 check the route received on S9300-A. Route 1.1.1.1/32 should be received, but the route does not exist in the routing table.

Fault Analysis

To locate the fault, perform the following steps:

1. View the routing table on S9300-B to check and ensure that all the routes are advertised to S9300-A.

On S9300-B, run the **display bgp routing-table** command to view information about the routing table. Routes 1.1.1.1/32 and 2.2.2.2/32 have been advertised to S9300-A, which indicates that a fault occurs on S9300-A.

2. Check the BGP configuration on S9300-A to check whether the filter is used when BGP receives routes.

On S9300-A, run the **display current-configuration configuration bgp** command to check the BGP configuration. You can find that S9300-A uses the IP prefix list when receiving routes from S9300-B. The IP prefix list may filter all the routes out.

3. View the configuration of the IP prefix list to check whether the route is filtered out by the IP prefix list.

On S9300-A, run the **display ip ip-prefix S9300-a** command to check the configuration of the filter. The entry in **deny** mode is set to match only 2.2.2.2/32 but the entry in **permit** mode is not set to match 1.1.1.1/32.

Thus, the fault is located. When S9300-A uses the IP prefix list to filter the routes received from S9300-B, S9300-A returns the entries in **deny** mode for the unmatched routes by default. Route 1.1.1.1/32 is, therefore, filtered out.

Procedure

Step 1 Delete the old filtering rules.

Step 2 Run the **ip ip-prefix S9300-a index 10 permit 1.1.1.1 32** command to create a new filtering rule.

After the preceding operations, run the **display ip routing-table** command to check the route received on S9300-A. If the route 1.1.1.1/32 is displayed in the routing table, the fault is rectified.

----End

Summary

When only the nodes in **deny** mode is configured in the IP prefix list, the routes that fail to match the address or mask range are denied by default. Thus, you need to configure a node in **permit** mode to permit the specified route to pass through. Or, you can define an entry **permit 0.0.0.0 greater-equal 0 less-equal 32** after configuring the nodes in **deny** mode. In this case, all the other routes can pass through. For details about the IP prefix list, see section [5.2.2 Configuration Notes](#).

5.4 FAQs

This section lists frequently asked questions and their answers.

Q: Why Cannot the Filtering Effect Be Achieved After the IPv4 Prefix List Is Configured to Filter Routes?

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

- Check whether the specified prefix list exists or is unmatched with the **display ip ip-prefix** *prefix-list-name* command.
- If the specified prefix list does not exist, the routing policy imports all the routes.
- If the specified prefix list is unmatched, the routing policy does not import the routes.
- Ensure that the default entry that permits all the routes to pass through is appended to all the filtering rules.

Q: When BGP Uses the Routing Policy to Filter the Specified Route, Why Are All the Routes Filtered?

- Run the **display current-configuration configuration bgp** command to check the BGP configuration and verify the filtering mode of the routing policy.
- Run the **display route-policy** [*route-policy-name*] command to check the configured routing policy. Configure at least one node in permit mode after all the nodes in deny mode are configured.

Q: Why Cannot BGP Accounting Be Applied When the Routing Protocol Runs Normally?

A: The possible causes are:

- The BGP routes cannot be received.
- The proper routing policy is not applied.
- BGP accounting is not enabled on the interface.

To locate the fault, follow the following steps:

- Run the **display ip route** command to check whether the route is received. If not, the fault is caused by the incorrect BGP configuration.
- Run the **display fib** command to check whether the **traffic index** parameter is delivered. If not, the fault may be caused by the incorrect configuration of the routing policy.
- Run the **display current-configuration interface** command to check whether BGP accounting is configured on the interface correctly.

BGP accounting is valid only when the S9300 needs to search the forwarding table. For example, if BGP accounting is configured for the outgoing traffic on a source 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

Table 5-2 Routing policy display commands

Command	Description
display ip ip-prefix [<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.
display route-policy [<i>route-policy-name</i>]	Displays the current configuration of the routing policy. For the application of the routing policy in different protocols, refer to corresponding protocols.

5.5.2 debugging Commands

Table 5-3 Routing policy debugging commands

Command	Description
debugging rm policy [ip-prefix <i>ip-prefix-name</i>]	Enables the debugging of packets of the routing policy. You can view information about the routing policy. If ip-prefix is specified, check the policy used for IPv4 routes.