



Quidway S9300 Terabit Routing Switch
V100R002C00

Troubleshooting - Multicast

Issue 01
Date 2009-09-10

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 IGMP Snooping Troubleshooting.....	1-1
1.1 Overview of IGMP Snooping.....	1-2
1.2 IGMP Snooping Troubleshooting.....	1-4
1.2.1 Typical Networking.....	1-4
1.2.2 Configuration Notes.....	1-5
1.2.3 Troubleshooting Flowchart.....	1-6
1.2.4 Troubleshooting Procedure.....	1-7
1.3 Troubleshooting Cases.....	1-9
1.3.1 Hosts in a Newly-Added User VLAN Cannot Receive Multicast Data.....	1-9
1.4 FAQs.....	1-11
1.5 Diagnostic Tools.....	1-12
1.5.1 display Commands.....	1-12
1.5.2 debugging Commands.....	1-12
2 IGMP Troubleshooting.....	2-1
2.1 Overview of IGMP.....	2-2
2.2 IGMP Troubleshooting.....	2-2
2.2.1 Typical Networking.....	2-2
2.2.2 Configuration Notes.....	2-3
2.2.3 Troubleshooting Flowchart.....	2-4
2.2.4 Troubleshooting Procedure.....	2-5
2.3 FAQs.....	2-7
2.4 Diagnostic Tools.....	2-9
2.4.1 display Commands.....	2-9
2.4.2 debugging Commands.....	2-9
3 PIM Troubleshooting.....	3-1
3.1 Overview of PIM.....	3-3
3.2 PIM-DM Troubleshooting.....	3-3
3.2.1 Typical Networking.....	3-3
3.2.2 Configuration Notes.....	3-4
3.2.3 Troubleshooting Flowchart.....	3-4
3.2.4 Troubleshooting Procedure.....	3-7

3.3 PIM-SM Troubleshooting.....	3-9
3.3.1 Typical Networking.....	3-9
3.3.2 Configuration Notes.....	3-10
3.3.3 Troubleshooting Flowchart.....	3-11
3.3.4 Troubleshooting Procedure.....	3-12
3.4 RPT Troubleshooting.....	3-13
3.4.1 Typical Networking.....	3-13
3.4.2 Configuration Notes.....	3-14
3.4.3 Troubleshooting Flowchart.....	3-15
3.4.4 Troubleshooting Procedure.....	3-16
3.5 Source Registering Troubleshooting.....	3-18
3.5.1 Typical Networking.....	3-18
3.5.2 Configuration Notes.....	3-19
3.5.3 Troubleshooting Flowchart.....	3-20
3.5.4 Troubleshooting Procedure.....	3-21
3.6 SPT Troubleshooting.....	3-23
3.6.1 Typical Networking.....	3-23
3.6.2 Configuration Notes.....	3-24
3.6.3 Troubleshooting Flowchart.....	3-24
3.6.4 Troubleshooting Procedure.....	3-25
3.7 Static RP Troubleshooting.....	3-28
3.7.1 Typical Networking.....	3-28
3.7.2 Configuration Notes.....	3-29
3.7.3 Troubleshooting Flowchart.....	3-29
3.7.4 Troubleshooting Procedure.....	3-30
3.8 BSR-RP Troubleshooting.....	3-31
3.8.1 Typical Networking.....	3-31
3.8.2 Configuration Notes.....	3-32
3.8.3 Troubleshooting Flowchart.....	3-32
3.8.4 Troubleshooting Procedure.....	3-34
3.9 BSR Troubleshooting.....	3-35
3.9.1 Typical Networking.....	3-36
3.9.2 Configuration Notes.....	3-36
3.9.3 Troubleshooting Flowchart.....	3-38
3.9.4 Troubleshooting Procedure.....	3-38
3.10 PIM BFD Troubleshooting.....	3-40
3.10.1 Typical Networking.....	3-40
3.10.2 Configuration Notes.....	3-40
3.10.3 Troubleshooting Flowchart.....	3-41
3.10.4 Troubleshooting Procedure.....	3-42
3.11 FAQs.....	3-43
3.12 Diagnostic Tools.....	3-46

3.12.1 display Commands.....	3-46
3.12.2 debugging Commands.....	3-46
4 MSDP Troubleshooting.....	4-1
4.1 Overview of MSDP.....	4-2
4.2 MSDP Troubleshooting.....	4-2
4.2.1 Typical Networking.....	4-2
4.2.2 Configuration Notes.....	4-3
4.2.3 Troubleshooting Flowchart.....	4-5
4.2.4 Troubleshooting Procedure.....	4-6
4.3 Troubleshooting Cases.....	4-8
4.3.1 Hosts Cannot Receive Data from an Inter-AS Multicast Source.....	4-9
4.4 FAQs.....	4-11
4.5 Diagnostic Tools.....	4-15
4.5.1 display Commands.....	4-15
4.5.2 debugging Commands.....	4-15

Figures

Figure 1-1 Forwarding of multicast data packets on a network where IGMP snooping is enabled.....	1-3
Figure 1-2 Networking diagram of IGMP snooping.....	1-5
Figure 1-3 Troubleshooting flowchart of IGMP snooping.....	1-7
Figure 1-4 Networking diagram of IGMP snooping.....	1-9
Figure 2-1 Typical networking of IGMP.....	2-3
Figure 2-2 Troubleshooting flowchart of IGMP.....	2-5
Figure 3-1 Typical PIM-DM networking.....	3-3
Figure 3-2 Troubleshooting flowchart of PIM-DM.....	3-6
Figure 3-3 Typical networking of PIM-SM.....	3-9
Figure 3-4 Troubleshooting flowchart of PIM-SM.....	3-12
Figure 3-5 Typical networking of PIM-SM.....	3-13
Figure 3-6 RPT troubleshooting flowchart.....	3-16
Figure 3-7 Typical networking of PIM-SM.....	3-19
Figure 3-8 Source registering troubleshooting flowchart.....	3-21
Figure 3-9 Typical networking of PIM-SM.....	3-23
Figure 3-10 PIM-SM SPT troubleshooting flowchart.....	3-25
Figure 3-11 Typical networking of PIM-SM.....	3-28
Figure 3-12 Static RP troubleshooting flowchart.....	3-30
Figure 3-13 Typical networking of PIM-SM.....	3-31
Figure 3-14 BSR-RP troubleshooting flowchart.....	3-33
Figure 3-15 Typical networking of PIM-SM.....	3-36
Figure 3-16 BSR troubleshooting flowchart.....	3-38
Figure 3-17 Typical networking diagram of PIM BFD.....	3-40
Figure 3-18 PIM BFD troubleshooting flowchart.....	3-42
Figure 4-1 Typical MSDP networking.....	4-3
Figure 4-2 MSDP troubleshooting flowchart.....	4-6
Figure 4-3 Typical MSDP networking.....	4-9

Tables

Table 4-1 RPF rules of MSDP.....4-11

About This Document

Purpose

This document describes the basic knowledge, troubleshooting procedures, troubleshooting cases, FAQs for IGMP snooping, IGMP proxy, IGMP, PIM, and MSDP, and diagnostic tools.

This document guides you through the troubleshooting methods of the multicast service of the S9300.

Related Versions

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

Product Name	Version
S9300	V100R002C00

Intended Audience

This document is intended for:

- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Organization






This document is organized as follows.

Chapter	Description
1 IGMP Snooping Troubleshooting	Describes the knowledge related to IGMP snooping troubleshooting, including overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases, FAQs, and diagnostic tools.
2 IGMP Troubleshooting	Describes the knowledge related to IGMP troubleshooting, including overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases, FAQs, and diagnostic tools.
3 PIM Troubleshooting	Describes the knowledge related to PIM troubleshooting, including overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases, FAQs, and diagnostic tools.
4 MSDP Troubleshooting	Describes the knowledge related to MSDP troubleshooting, including overview, troubleshooting flowchart and troubleshooting procedure in a typical networking, troubleshooting cases, FAQs, and diagnostic tools.

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

Updates in Issue 01 (2009-09-10)

Initial commercial release.

1 IGMP Snooping Troubleshooting

About This Chapter

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

[1.1 Overview of IGMP Snooping](#)

This section describes the information that you need to know before troubleshooting IGMP snooping.

[1.2 IGMP Snooping Troubleshooting](#)

This section describes the notes about configuring IGMP snooping, and provides the IGMP snooping troubleshooting flowchart and the troubleshooting procedure in a typical VLAN-based IGMP snooping networking.

[1.3 Troubleshooting Cases](#)

This section presents several troubleshooting cases.

[1.4 FAQs](#)

This section lists the frequently asked questions and their answers.

[1.5 Diagnostic Tools](#)

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

1.1 Overview of IGMP Snooping

This section describes the information that you need to know before troubleshooting IGMP snooping.

IGMP snooping runs at the data link layer. When receiving IGMP messages transmitted between a router and hosts, the S9300 enabled with IGMP snooping analyzes information carried in the messages and maintains the multicast forwarding table based on the information.

Background

When unicast IP packets are transmitted on the Ethernet, the destination Medium Access Control (MAC) addresses of the packets are the MAC addresses of packet receivers. When multicast packets are transmitted, however, the destination address of the packets is a group of unspecified members instead of a specific receiver. Therefore, when the multicast packets are forwarded from the IP layer to the data link layer, multicast forwarding entries cannot be generated. As a result, the multicast packets are broadcast at the data link layer. Transmission in broadcast mode wastes bandwidth and is inconvenient for the accounting of user services. In addition, it brings potential risks in information security.

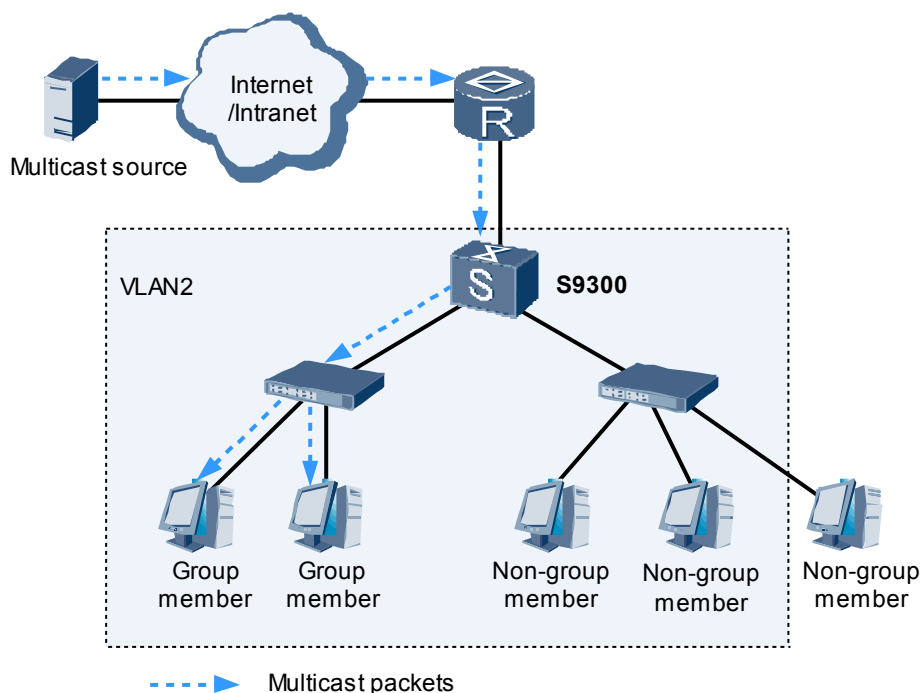
At the same time, forwarding entries are generated by exchanging Internet Group Management Protocol (IGMP) protocol packets between routers and hosts. Therefore, if there are a large number of hosts on the network, the redundant IGMP packets cause processing pressures on the routers.

After IGMP snooping is enabled on the S9300 that connects routers and hosts, the S9300 can set up a Layer 2 forwarding table for multicast packets by listening to IGMP messages exchanged between a router and hosts. In this manner, the S9300 manages and controls the forwarding of multicast packets, thus implementing Layer 2 multicast.

Basic Functions

As shown in [Figure 1-1](#), when the S9300 is enabled with IGMP snooping, it can learn the interfaces to which multicast receivers are connected by listening to IGMP messages exchanged between the multicast router and hosts. The S9300 sends the packets in multicast mode rather than in broadcast mode on the Layer 2 network. That is, only members in the multicast group can receive the packets.

Figure 1-1 Forwarding of multicast data packets on a network where IGMP snooping is enabled



Multicast Forwarding Table

The S9300 builds up a multicast forwarding table through VLAN-based IGMP snooping. The multicast forwarding table contains multiple forwarding entries. Each entry contains the following:

- ID of an inbound VLAN
- Multicast group address
- Outbound interface
- ID of an outbound VLAN

When IGMP snooping and replication of multicast data across VLANs are used together to generate forwarding entries, the ID of the multicast VLAN is used as the ID of the inbound VLAN, and the ID of a user VLAN to which a user host belongs is used as the ID of the outbound VLAN. Otherwise, the VLAN ID of a user host serves as both the inbound VLAN ID and the outbound VLAN ID.

NOTE

For details about replication of multicast data across VLANs, see the chapter "Layer 2 Multicast" in the *Quidway S9300 Terabit Routing Switch Feature Description - Multicast*.

When receiving a multicast data packet, the S9300 searches the multicast forwarding table for a matching forwarding entry based on the outbound VLAN and the destination address of the packet. The destination address of the packet is the address of a multicast group. If the multicast forwarding entry is found, the multicast packet is forwarded according to the outbound interfaces that are specified in the forwarding entry. If the multicast forwarding entry is not found:

- If neither IGMP snooping nor IGMP proxy is enabled in the VLAN, the S9300 broadcasts the unknown multicast packets in the VLAN.
- If IGMP snooping or IGMP proxy is enabled in the VLAN, the S9300 decides how to process the unknown multicast packets according to the multicast forwarding mode configured on the VLAN.
 - If the multicast forwarding mode on the VLAN is IP, the S9300 forwards the packets to the router interfaces on the VLAN.
 - If the multicast forwarding mode on the VLAN is MAC, the S9300 discards the packets.

Maintenance of the Multicast Forwarding Table

Multicast forwarding entries are classified into static and dynamic entries.

- Static entries

Static entries are manually configured and do not age.

- Dynamic entries

The S9300 enabled with IGMP snooping maintains dynamic forwarding entries by analyzing IGMP messages exchanged between a router and hosts.

- When an interface on the S9300 receives a Report message from a host, the S9300 generates a multicast forwarding entry for the interface, and then adds the forwarding entry to the multicast forwarding table.
- When an interface on the S9300 receives a Leave message from a host, the S9300 deletes the multicast forwarding entry to which the Leave message corresponds from the multicast forwarding table if prompt leave is configured in the VLAN that the packet belongs to. If prompt leave is not configured in the VLAN, the S9300 deletes the multicast forwarding entry to which the Leave message corresponds from the multicast forwarding table when no member of the group is connected to the interface.

If dynamic forwarding entries are not updated when the aging time expires, they are deleted.

Based on entries in the forwarding table, the S9300 forwards multicast packets received from an upstream router to multicast receivers.

1.2 IGMP Snooping Troubleshooting

This section describes the notes about configuring IGMP snooping, and provides the IGMP snooping troubleshooting flowchart and the troubleshooting procedure in a typical VLAN-based IGMP snooping networking.

[1.2.1 Typical Networking](#)

[1.2.2 Configuration Notes](#)

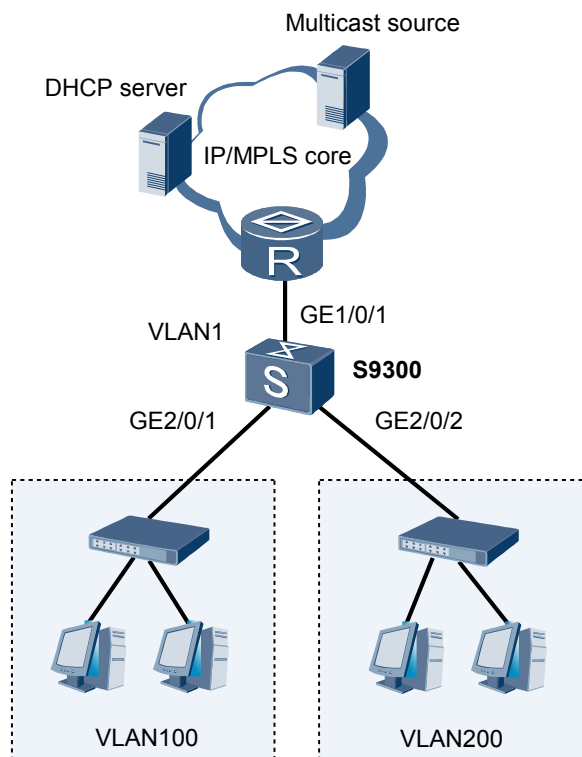
[1.2.3 Troubleshooting Flowchart](#)

[1.2.4 Troubleshooting Procedure](#)

1.2.1 Typical Networking

Figure 1-2 shows the typical multicast networking of the S9300. The following takes this networking to describe how to troubleshoot VLAN-based IGMP snooping.

Figure 1-2 Networking diagram of IGMP snooping



In the preceding networking,

- IGMP snooping is enabled on the S9300.
- GE1 /0/1 joins VLAN 1, whereas GE 2/0/1 and GE 2/0/2 join VLAN 100 and VLAN 200 respectively.
- Replication of multicast data across VLANs is enabled. VLAN 1 is the multicast VLAN, whereas VLAN 100 and VLAN 200 are user VLANs of VLAN 1.

1.2.2 Configuration Notes

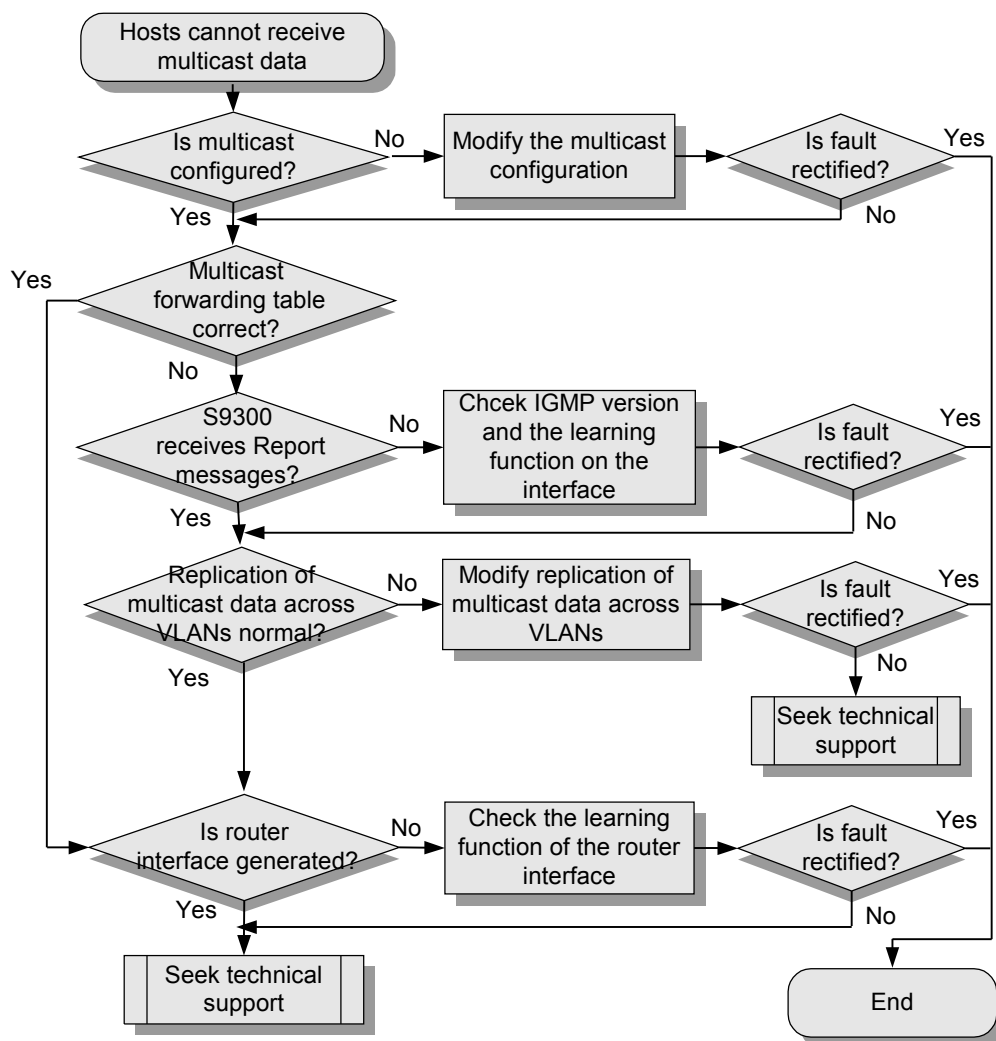
Item	Sub-item	Configuration Notes and Commands
Enabling replication of multicast data across VLANs	Enabling IGMP snooping	IGMP snooping is enabled on the S9300. By default, IGMP snooping is disabled on the S9300. To enable IGMP snooping, run the igmp-snooping enable command in the system view.

Item	Sub-item	Configuration Notes and Commands
	Configuring replication of multicast data across VLANs	<ul style="list-style-type: none"> • IGMP snooping is enabled in the VLAN. • Replication of multicast data across VLANs is enabled. <p>By default, the preceding functions are disabled.</p> <p>To enable replication of multicast data across VLANs, run the following commands in the VLAN view:</p> <ul style="list-style-type: none"> • igmp-snooping enable • multicast-vlan enable
	Configuring user VLANs	<p>The mapping between multicast VLANs and user VLANs is configured.</p> <p>By default, the mapping between multicast VLANs and user VLANs is not configured.</p> <p>To configure user VLANs, run the multicast-vlan user-vlan { { <i>vlan-id1</i> [to <i>vlan-id2</i>] } &<1-10> } command in the VLAN view.</p>
	Adding interfaces to VLANs	<ul style="list-style-type: none"> • Router interfaces need to be added to the multicast VLAN. • User interfaces need to be added to user VLANs. <p>To add interfaces to VLANs, run the interface gigabitethernet <i>interface-number</i> or interface eth-trunk <i>trunk-id</i> command in the system view, and run the port trunk allow-pass vlan { { <i>vlan-id1</i> [to <i>vlan-id2</i>] } &<1-10> all } command in the GE interface view or Eth-Trunk interface view.</p>

1.2.3 Troubleshooting Flowchart

On the network shown in "Networking diagram of IGMP snooping" in [1.2.1 Typical Networking](#), after devices are configured, it is found that hosts in VLAN 100 cannot receive multicast data. [Figure 1-3](#) shows the troubleshooting flowchart.

Figure 1-3 Troubleshooting flowchart of IGMP snooping



1.2.4 Troubleshooting Procedure

Procedure

Step 1 Check that basic multicast functions are configured correctly on the S9300.

1. Run the **display igmp-snooping [vlan vlan-id]** command on the S9300 to check whether IGMP snooping is enabled on the S9300 and in VLAN 1.
2. Run the **display vlan [vlan-id [statistics | verbose]]** command to check whether VLANs are created and interfaces are added to the VLANs correctly.
3. Run the **display interface [interface-type [interface-number]] [{ begin | exclude | include } regular-expression]** command to check that each interface is Up.
4. Run the **display multicast-vlan [vlan vlan-id]** command to check that the mapping between the multicast VLAN and user VLANs is configured correctly.

The correct configurations of the S9300 are as follows:

- GE 1/0/1 joins VLAN 1 in tagged mode through the **port trunk allow-pass vlan** command.
- GE 2/0/1 joins VLAN 100 in tagged mode after the **port trunk allow-pass vlan** command is used on GE 2/0/1.
- GE 2/0/2 joins VLAN 200 in tagged mode after the **port trunk allow-pass vlan** command is used on GE 2/0/2.
- IGMP snooping is enabled on the S9300.
- IGMP snooping is enabled in VLAN 1.
- VLAN 1 is configured as a multicast VLAN.
- User VLANs of VLAN 1 are VLAN 100 and VLAN 200.

If the configurations on the S9300 are incorrect, modify them. If configurations are correct, go to [Step 2](#).

Step 2 Check that corresponding forwarding entries exist in the multicast forwarding table.

Run the **display l2-multicast forwarding-table vlan** [*vlan-id*] [**group-address** *group-address*] [[{ **begin** | **exclude** | **include** } *regular-expression*]] command to check whether related forwarding entries exist in the multicast forwarding table.

- If the related forwarding entries do not exist, go to [Step 3](#).
- If the related forwarding entries exist, go to [Step 6](#).

Step 3 Check whether the multicast forwarding table is full.

Run the **display l2-multicast forwarding-table vlan** [*vlan-id*] [**group-address** *group-address*] [[{ **begin** | **exclude** | **include** } *regular-expression*]] command to check whether the multicast forwarding table is full.

- If the multicast forwarding table is full, delete useless entries.
- If the multicast forwarding table is not full, go to [Step 4](#).

Step 4 Check whether the S9300 receives Report messages.

Run the **display igmp-snooping statistics vlan** [*vlan-id*] command to view the IGMP Report messages in VLAN 100. You can check whether the S9300 receives Report messages.

- If the S9300 does not receive any Report message, check whether the learning function is disabled on the interfaces.
- If the S9300 receives IGMP Report messages, check whether the information about the IGMP version contained in the Report messages is correct. Devices in the same VLAN must run IGMP of the same version. If the versions of the packets are correct, go to [Step 5](#).

Step 5 Check that the mapping between the multicast VLAN and user VLANs is configured correctly.

Run the **display multicast-vlan** [**vlan** *vlan-id*] command to check whether the multicast VLAN and user VLANs are configured correctly.

After the operations through [Step 3](#) to [Step 5](#) are complete, if multicast static forwarding entries cannot be generated, contact Huawei technical personnel.

If the fault persists after multicast static forwarding entries are generated, go to [Step 6](#).

Step 6 Check whether the router interface is generated.

By default, the inbound interface of multicast data should be a router interface. The S9300 discards multicast data that enters through a non-router interface.

Run the **display igmp-snooping router-port vlan** *vlan-id* command to check whether the router interface is generated on the S9300.

- If the router interface is not generated, check whether the learning function is disabled on the related interface on the S9300.
- If the correct router interface exists, contact Huawei technical personnel.

----End

1.3 Troubleshooting Cases

This section presents several troubleshooting cases.

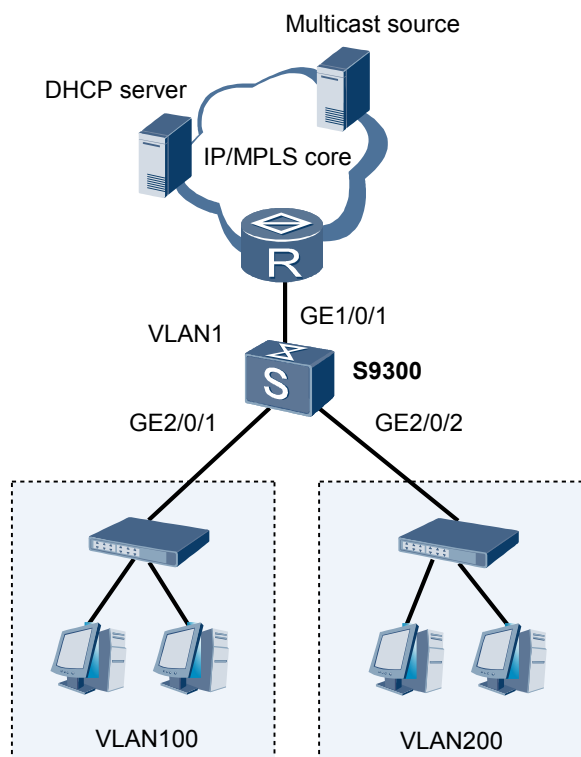
1.3.1 Hosts in a Newly-Added User VLAN Cannot Receive Multicast Data

1.3.1 Hosts in a Newly-Added User VLAN Cannot Receive Multicast Data

Fault Symptom

On the network shown in [Figure 1-4](#), GE 1/0/1 is a router interface, VLAN 1 is a multicast VLAN, and VLAN 100 and VLAN 200 are user VLANs of VLAN 1. VLAN 100 joins group 225.0.0.1 through GE 2/0/1. The hosts in VLAN 100 can receive multicast data from the source. VLAN 200 is configured to join the group through GE 2/0/2.

Figure 1-4 Networking diagram of IGMP snooping



After the preceding configurations, it is found that the hosts in VLAN 200 cannot receive multicast data sent by the source.

Fault Analysis

1. Run the **display igmp-snooping [vlan *vlan-id*]** command to check the IGMP snooping configuration. You can find that IGMP snooping is enabled on the S9300, VLAN 1, VLAN 100, and VLAN 200. Take VLAN 1 as an example.

```
<S9300> display igmp-snooping vlan 1
IGMP Snooping Vlan Information for Vlan 1
  IGMP Snooping is Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is 100
  IGMP Max Response Interval is 20
  IGMP Robustness is 5
  IGMP Last Member Query Interval is 4
  IGMP Router Port Aging Interval is 500
  IGMP Filter Group-Policy 2008
  IGMP Prompt Leave Enable, and acl number is 2008
  IGMP Require Router Alert
  IGMP Send Router Alert Enable
  IGMP Suppress Time is 15
  IGMP Router-learning Enable
  IGMP Querier Enable
```

2. Run the **display vlan *vlan-id* verbose** command to check whether the interfaces are added to the VLANs correctly. You can find that GE 2/0/2 is not added to VLAN 200.

```
<S9300> display vlan 200 verbose
VLAN ID      : 200
VLAN Type    : Common
Description  : VLAN 0200
Status       : Enable
Broadcast    : Enable
MAC learning : Enable
Statistics   : Disable
```

The multicast VLAN replicates multicast data and sends it to user VLANs, and hosts receive the multicast data through the user VLANs. Hosts cannot receive multicast data because the interface to which the hosts are connected is not added to the user VLAN.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface gigabitethernet *interface-number*** command to enter the GE interface view.
- Step 3** Run the **port trunk allow-pass vlan { { *vlan-id1* [to *vlan-id2*] } &<1-10> | all }** command to add an interface to a VLAN.

----End

Result

After the preceding operations, you can find that GE 2/0/2 is added to VLAN 200.

```
<S9300> display vlan 200 verbose
VLAN ID      : 200
VLAN Type    : Common
Description  : VLAN 0200
Status       : Enable
Broadcast    : Enable
MAC learning : Enable
Statistics   : Disable
```



```
-----  
Tagged      Port: GigabitEthernet2/0/2
```

The hosts in VLAN 200 can receive multicast data sent by the source. The fault is thus rectified.

```
<S9300> display interface gigabitEthernet 2/0/2  
GigabitEthernet2/0/2 current state : UP  
Description:HUAWEI, Quidway Series, GigabitEthernet2/0/2 Interface  
Switch Port,PVID : 200,The Maximum Frame Length is 1526  
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083  
Speed : 1000, Loopback: NONE  
Duplex: FULL, Negotiation: ENABLE  
Vlan Shaping: Not supported  
Input: 0 bytes  
  Unicast: 0, NUnicast: 0  
  Discard: 0, Error : 0  
Output: 1073407 bytes  
  Unicast: 0, NUnicast: 4332  
  Discard: 0, Error : 0
```

Summary

An interface should be correctly added to a VLAN before IGMP snooping is configured on an S9300.

1.4 FAQs

This section lists the frequently asked questions and their answers.

Q: How Does the S9300 Determine Whether Group Members Exist on the Network Segment When a Host Leaves a Multicast Group?

A: In IGMPv1, when a host leaves a multicast group, the host does not send a Leave message. When a multicast group times out, an S9300 determines that there are no members of the group exist on the network segment.

In IGMPv2, a host sends a Leave message when leaving a group. After receiving the Leave message, the querier sends a group-specific query message to the network segment. The destination address of Query messages of this type is the address of the multicast group and the group address in the message is also filled in with the address of the multicast group. If a member of this group exists on the network segment, the member sends a Report message. If no Report message is received after the forwarding entry expires, the querier considers that no member of this group exists on the network segment.

Q: Why Is Not a Forwarding Table Generated When You Configure a Static Entry?

A: If a static forwarding table of Layer 2 multicast is generated, the following conditions must be met:

- The interface belongs to a VLAN.
- The interface status is Up.
- IGMP snooping is enabled globally.
- IGMP snooping is enabled in the VLAN.
- The multicast VLAN contains at least one Up interface.

- The total number of static and dynamic entries reaches the specifications, and the static entries exceeding the total number cannot take effect.
- Global rules are configured to filter the group addresses that are manually configured.
- Product resources are unavailable. That is, other features such as VLANs also need to use product resources. If other features occupy a large number of resources, the entries of Layer 2 multicast cannot take effect.

1.5 Diagnostic Tools

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

1.5.1 display Commands

1.5.2 debugging Commands

1.5.1 display Commands

Command	Description
display igmp-snooping [<i>vlan</i> [<i>vlan-id</i>]]	Displays the configuration of IGMP snooping in a VLAN.
display igmp-snooping querier	Displays information about the IGMP snooping querier.
display igmp-snooping statistics vlan [<i>vlan-id</i>]	Displays the statistics on IGMP snooping.
display l2-multicast forwarding-mode	Displays the forwarding mode of a VLAN.
display igmp-snooping port-info [<i>vlan</i> <i>vlan-id</i> [<i>group-address</i> <i>group-address</i>]] [<i>verbose</i>]	Displays information about member interfaces of a multicast group.
display igmp-snooping router-port	Displays information about a router interface.
display l2-multicast forwarding-table <i>vlan</i> [<i>vlan-id</i>] [<i>group-address</i> <i>group-address</i>] [[{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]]	Displays the multicast forwarding table.
display multicast-vlan [<i>vlan</i> <i>vlan-id</i>]	Displays information about the multicast VLAN and its user VLANs.

1.5.2 debugging Commands

Command	Description
debugging igmp-snooping { all event leave [<i>basic-acl-number</i>] packet [<i>advance-acl-number</i>] query [<i>advance-acl-number</i>] report [advance-acl-number] timer }	Enables the debugging of IGMP snooping.

2 IGMP Troubleshooting

About This Chapter

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

[2.1 Overview of IGMP](#)

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

[2.2 IGMP Troubleshooting](#)

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

[2.3 FAQs](#)

This section lists frequently asked questions and their answers.

[2.4 Diagnostic Tools](#)

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

2.1 Overview of IGMP

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

In the TCP/IP protocol suite, the Internet Group Management Protocol (IGMP) manages IPv4 multicast members. The S9300 enabled with IGMP sets up and maintains member relations between IP hosts and their directly connected multicast routers.

NOTE

This document describes the multicast features supported by the Quidway S9300 Terabit Routing Switch. The multicast devices mentioned in the following refer to the multicast switch or S9300, not the multicast router.

Multicast hosts must support IGMP. Hosts can randomly join or leave related multicast groups. There is no limitation on the number of members of a group. Through IGMP, S9300s learn whether receivers, that is, members of a certain group, exist on the network segment connected to interfaces. The hosts running IGMP store information about the multicast groups that they join.

An S9300 and its directly connected hosts interact with each other in the following manner:

- The S9300 sends a Query message to hosts on the local network periodically.
- The hosts respond to the IGMP Query message by sending IGMP Report messages and advertise the groups that the hosts join.
- The S9300 then refreshes the local member information according to the received IGMP Report messages.
- If no Report message is received after the group-related timer on the S9300 expires, the S9300 considers that there is no member of a certain multicast group on the network segment, and does not forward related multicast data.

IGMP has the following versions:

- IGMPv1: It is defined by RFC 1112.
- IGMPv2: It is defined by RFC 2236, and is the most common version.
- IGMPv3: It is defined by RFC 3376.

2.2 IGMP Troubleshooting

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

[2.2.1 Typical Networking](#)

[2.2.2 Configuration Notes](#)

[2.2.3 Troubleshooting Flowchart](#)

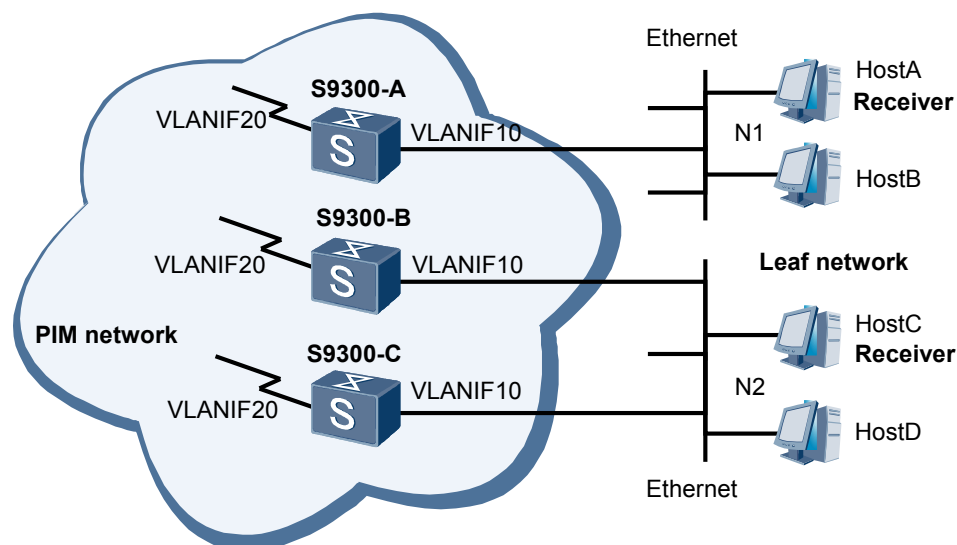
[2.2.4 Troubleshooting Procedure](#)

2.2.1 Typical Networking

Figure 2-1 shows a typical IGMP networking.

The following takes this networking to describe how to perform IGMP troubleshooting.

Figure 2-1 Typical networking of IGMP



In the preceding networking,

- Receivers receive VOD information in multicast mode. Host A and Host C are multicast receivers on the network segments N1 and N2 respectively.
- The ISP network runs PIM-SM.
- IGMPv3 runs between the S9300s and the leaf network.

Host A and Host C can receive data from S.

2.2.2 Configuration Notes

NOTE

- The physical interfaces on the S9300 are Layer 2 interfaces. To use Layer 3 multicast protocols, you need to add interfaces to a VLAN and configure Layer 3 multicast protocols on VLANIF interfaces.
- On the S9300, IGMP can be configured only on VLANIF interfaces and loopback interfaces. Generally, IGMP is not used on loopback interfaces.

Item	Sub-item	Configuration Notes and Commands
Configuring IGMP	Enabling IP multicast	Multicast is enabled on the S9300. To enable IP multicast, run the multicast routing-enable command in the system view.
	Enabling IGMP	IGMP is enabled on the interface connected to hosts and the multicast boundary cannot be configured on the interface. If the interface is enabled with PIM, enable PIM before enabling IGMP. To enable IGMP, run the igmp enable command in the interface view.

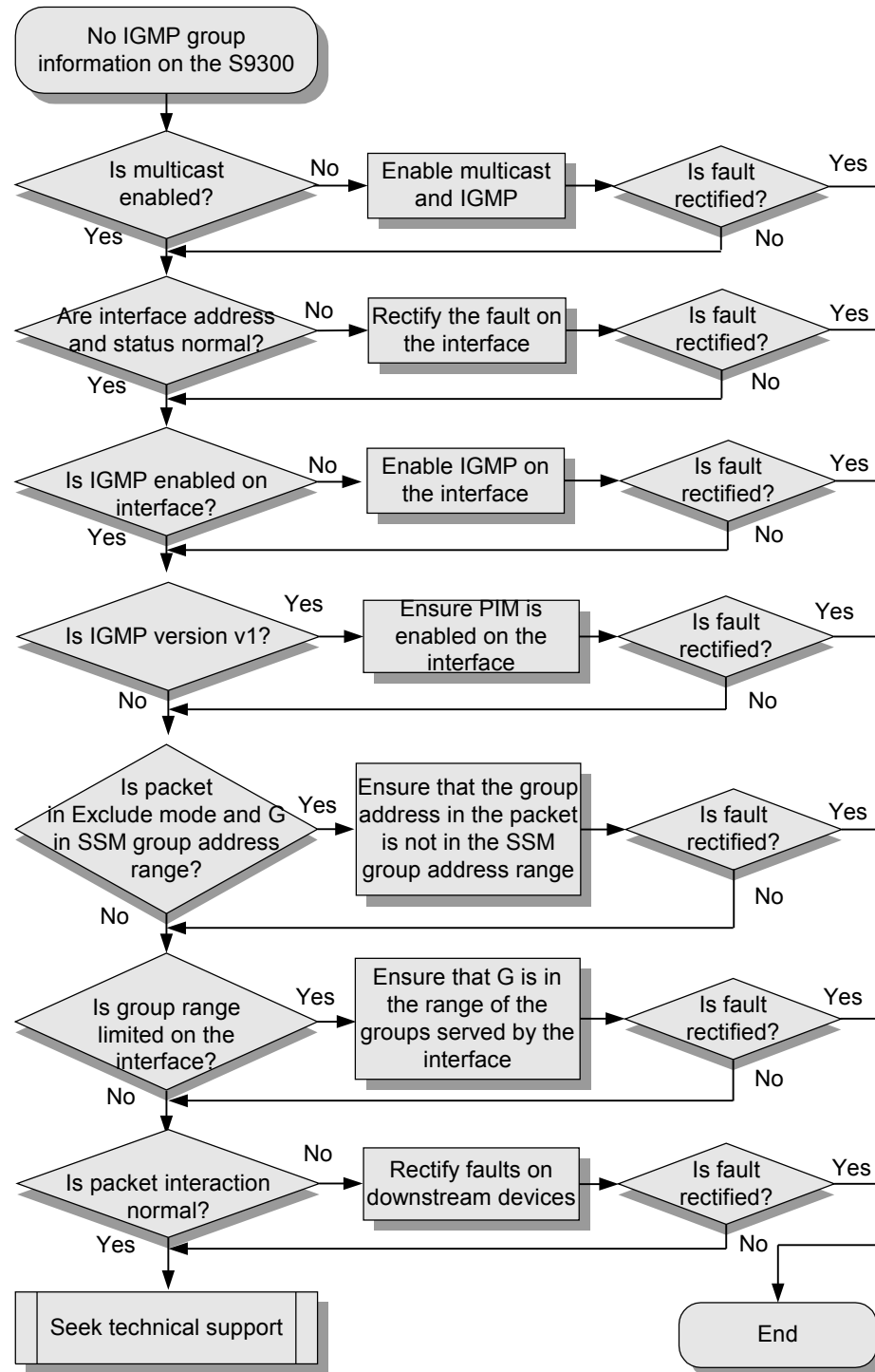
Item	Sub-item	Configuration Notes and Commands
	Configuring the IGMP version	All the S9300s on the same network segment run the same version of IGMP. By default, the IGMP version is 2. To configure the IGMP version, run the igmp version { 1 2 3 } command in the interface view.
	Configuring SSM mapping	Groups specified by static SSM mapping rules are within the SSM group address range. By default, the SSM group address range is 232.0.0.0/8. To configure SSM mapping, run the igmp ssm-mapping enable command in the interface view and the ssm-mapping group-address { mask mask-length } source-address command in the IGMP view.
	Setting IGMP parameters	Interfaces of all the S9300s on the same network segment are configured with the same IGMP parameters. To set IGMP parameters, run the following commands in the interface view: <ul style="list-style-type: none"> ● igmp lastmember-queryinterval ● igmp max-response-time ● igmp on-demand ● igmp prompt-leave ● igmp require-router-alert ● igmp robust-count ● igmp send-router-alert ● igmp timer other-querier-present ● igmp timer query
	Configuring an IGMP group policy	Configure an ACL to limit the range of groups that a host can join. To configure an IGMP group policy, run the igmp group-policy acl-number [1 2 3] command.

2.2.3 Troubleshooting Flowchart

On the network shown in "Typical networking of IGMP" in [2.2.1 Typical Networking](#), a host sends an IGMP Report message to its directly connected router requesting it to join G. But, the S9300 does not have any information about the members of G.

[Figure 2-2](#) shows the troubleshooting flowchart.

Figure 2-2 Troubleshooting flowchart of IGMP



2.2.4 Troubleshooting Procedure

Procedure

Step 1 Check whether the S9300 is enabled with the multicast function.

Run the **display current-configuration** on the S9300 directly connected to the user network segment to check the current configuration on the S9300.

- If the command output does not contain the **multicast routing-enable** command, it is recommended that you run the **multicast routing-enable** command in the system view to enable the multicast function, and then perform other IGMP configurations.

 **NOTE**

On a multicast network, it is recommended that you enable multicast on all the S9300s.

- If the command output contains the **multicast routing-enable** command, go to [Step 2](#).

Step 2 Check whether the interface status is normal.

Run the **display interface *interface-type interface-number*** command on the current S9300 to specify the interface directly connected to the host network segment and to view the information about the interface.

- If the *interface-type interface-number* **current state : Down** field is displayed, it indicates that the physical status of the interface is Down. You need to check the networking and ensure that the interface is connected correctly.
- If the **Line protocol current state : DOWN** field is displayed, it indicates that the protocol enabled on the interface is Down. Do as follows:

- Check whether the **shutdown** command is used on the interface.

Run the **display current-configuration interface *interface-type interface-number*** command to check the current configuration of the interface. If the command output contains the **shutdown** command, run the **undo shutdown** command in the interface view to cancel the configuration.

- Check whether the interface is configured with an IPv4 address.

Run the **display ip interface brief** command to check the address of the interface. If the interface is not configured with an IPv4 address, or the IPv4 address of the interface and the address of the host do not belong to the same network, reconfigure an IPv4 address for the interface.

Step 3 Check whether the interface is enabled with IGMP.

Run the **display current-configuration interface *interface-type interface-number*** command on the current S9300 to check the configuration on the interface directly connected to hosts.

- If the command output does not contain the **igmp enable** command, it indicates that IGMP is not enabled. You need to run the **igmp enable** command in the interface view to enable IGMP.
- If the command output contains the **igmp enable** command, go to [Step 4](#).

Step 4 Check whether the IGMP version is v1.

Run the **display igmp interface *interface-type interface-number*** command on the S9300 to view the IGMP configuration on the interface. If you can see **Current IGMP version is 1** in the output information, it indicates that the IGMP version is v1. Ensure that the PIM protocol is enabled on the interface so that the querier can be elected.

Step 5 Check whether G is in the SSM group range.

Run the **display current-configuration configuration pim** command on the S9300 directly connected to hosts to check the current configuration in the PIM view. If the command output contains the **ssm-policy basic-acl-number** command, it indicates that the SSM group address range is adjusted on the S9300. Then, run the **display current-configuration configuration acl-basic** command to check the ACL configuration.

- If the command output indicates that the group address range defined by the ACL contains G, it indicates that G is in the SSM group address range. Ensure that the interfaces connecting the S9300 and hosts run IGMPv3.
- If the IGMP version on a host cannot be upgraded, you need to enable SSM mapping on the S9300 interface and set the rules of static SSM mapping related to G.
- If the command output indicates that the group address range defined by the ACL does not contain G, it indicates that G is not in the SSM group address range.

Step 6 Check whether the range of groups that a host can join is limited on the interface.

Run the **display current-configuration interface interface-type interface-number** command on the current S9300 to check the configuration of the interface directly connected to hosts. If the **igmp group-policy** field in the command output is not **none**, it indicates that the range of groups a host can join is limited on the interface. IGMP filters Join messages according to the ACL. Check the range of groups defined by the ACL. If G is out of range, modify the ACL configuration or delete the command to ensure that IGMP takes effect for the members of G.

Step 7 Check whether the packet interaction is normal.

Run the **terminal monitor** and **terminal debugging** commands on the S9300 to enable the debugging and check whether packet interaction is normal. If the interaction of IGMP packets is abnormal, check the running status of downstream devices.

If the fault persists, contact Huawei technical personnel.

----End

2.3 FAQs

This section lists frequently asked questions and their answers.

Q: How Do Multiple S9300s Elect a Querier on a Shared Network Segment?

A: When a host network segment is connected to the interfaces of multiple S9300s, only one interface is allowed to send Query messages to prevent data conflict. The interface functions as the querier, and the other interfaces that run IGMP can listen to IGMP messages on the network segment.

In IGMPv1, the querier selection is determined by the DR of PIM. In IGMPv2 and IGMPv3, the interface with the smallest IP address functions as the querier.

Q: How Does an IGMP Querier Determine Whether a Member of the Group Exists on the Network Segment When a Host Leaves Its Group?

A: In IGMPv1, when a host leaves a group, the host does not send any message. By checking whether the group times out, the S9300 determines whether a member of the group exists on the network segment.

In IGMPv2 and IGMPv3, a host sends a Leave message when leaving a multicast group. After receiving the Leave message, the querier sends a group-specific query message to the network segment. The destination address of Query messages of this type is the address of the multicast group. The group address in the message is also filled in with the address of the multicast group. If a member of this group exists on the network segment, the member sends a Report message. If no Report message is received after the group timer expires, the IGMP querier considers that no member of this group exists on the network segment.

Q: Can the Versions of IGMP Running on Hosts and S9300s on the Same User Network Segment Be Different?

A: Currently, IGMP has three versions. S9300s and hosts running IGMP of different versions are compatible, but all the S9300s on the same network segment must run IGMP of the same version. If the IGMP versions of the S9300s on the same network segment are different, IGMP member relations are interrupted.

Run the **display igmp interface** *interface-type interface-number* command on all S9300s on the same network segment to check whether the IGMP versions on the S9300s are the same. When an interface on an S9300 receives a Query message with the IGMP version different from the version of the interface, the related prompt is displayed.

Q: When a User Network Segment Is Connected to Multiple S9300s, What Are the Requirements for IGMP Parameters of Interfaces?

A: There are several IGMP interface parameters and they are mutually restricted. If IGMP interface parameters of the S9300s on the same network segment are different, IGMP member relations are interrupted. As a result, IGMP interface parameters of the S9300s on the same network segment must be the same.

Run the **display igmp interface** *interface-type interface-number* command on all S9300s on the same network segment to check whether the IGMP parameters on the S9300s are the same. IGMP interface parameters are as follows:

- IGMP version
- Robustness
- Query interval
- Other querier timeout
- Maximum query response time
- Last member query count
- Last member query interval
- Startup query interval
- Startup query count

Q: An Interface Is Enabled with SSM Mapping and IGMP, and Is Configured with the Static SSM Mapping Policy. The Interface Receives IGMPv1 or IGMPv2 Report Messages. Why Does No Transformed (S, G) Entry Exist in the FIB?

A: When a querier configured with SSM mapping receives an IGMPv1 or IGMPv2 (*, G) Report message from a host, the querier transforms the (*, G) entry to (G, Include, (S1, S2, S3...)) entry only when G is in the SSM group address range and the host is configured with G-related SSM mapping rules. SSM mapping is thus implemented.

The possible causes are:

- G carried in the (*, G) Report message is not in the SSM group address range. Run the **display current-configuration configuration pim** command to check the current configuration in the PIM view. If the command output contains the **ssm-policy basic-acl-number** command, it indicates that the SSM group address range is defined on the S9300.
- Run the **display current-configuration configuration acl-basic** command to modify the ACL configuration. Ensure that G is in the SSM group address range. By default, the SSM group address range is 232.0.0.0/8.
- SSM mapping rules related to G in the (*, G) Report message are not configured. Run the **display current-configuration configuration igmp** command to check the SSM mapping rules configured on the current S9300, check whether the source address of G is specified, and check whether masks are the same.

2.4 Diagnostic Tools

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

2.4.1 display Commands

2.4.2 debugging Commands

2.4.1 display Commands

Command	Description
display igmp group	Displays information about an IGMP group.
display igmp interface	Displays the status and configuration of an IGMP interface.
display igmp routing-table	Displays information about an IGMP routing table.
display igmp ssm-mapping	Displays SSM mapping of source or group-specific addresses.
display interface	Displays the status and the configuration of a specific interface.
display current-configuration	Displays the current configuration of an S9300.
display version	Displays the information about the software version.

2.4.2 debugging Commands

Command	Description
debugging igmp all	Enables all the debugging of IGMP.
debugging igmp event	Enables the debugging of IGMP events.

Command	Description
debugging igmp leave	Enables the debugging of IGMP Leave messages. After this command is used on an S9300, the S9300 displays the debugging information when receiving a Leave message.
debugging igmp report	Enables the debugging of IGMP Report messages. After this command is used on an S9300, the S9300 displays the debugging information when receiving a Report message.
debugging igmp query	Enables the debugging of IGMP queriers. After this command is used on an IGMP querier, the querier displays the debugging information when receiving or sending a Query message.
debugging igmp timer	Enables the debugging of IGMP timers.
debugging igmp ssm-mapping	Enables the debugging of IGMP SSM mapping. When an SSM mapping event is triggered, the debugging information is displayed.

3 PIM Troubleshooting

About This Chapter

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

[3.1 Overview of PIM](#)

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

[3.2 PIM-DM Troubleshooting](#)

This section describes the notes about configuring PIM-DM, and provides the PIM-DM troubleshooting flowchart and the troubleshooting procedure in a typical PIM-DM networking.

[3.3 PIM-SM Troubleshooting](#)

This section describes the notes about configuring PIM-SM, and provides the PIM-SM troubleshooting flowchart and the troubleshooting procedure in a typical PIM-SM networking.

[3.4 RPT Troubleshooting](#)

This section describes the procedure for RPT troubleshooting.

[3.5 Source Registering Troubleshooting](#)

This section describes the procedure for source registering troubleshooting.

[3.6 SPT Troubleshooting](#)

This section describes the procedure for SPT troubleshooting.

[3.7 Static RP Troubleshooting](#)

This section describes the procedure for static RP troubleshooting.

[3.8 BSR-RP Troubleshooting](#)

This section describes the procedure for BSR-RP troubleshooting.

[3.9 BSR Troubleshooting](#)

This section describes the procedure for BSR troubleshooting.

[3.10 PIM BFD Troubleshooting](#)

This section describes the procedure for PIM BFD troubleshooting.

[3.11 FAQs](#)

This section lists frequently asked questions and their answers.

3.12 Diagnostic Tools

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

3.1 Overview of PIM

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

The Protocol Independent Multicast (PIM) contains the following independent multicast routing protocols:

- The Protocol Independent Multicast-Dense Mode (PIM-DM) is a multicast routing protocol in dense mode. It is applicable to small-scale networks with densely-distributed members. PIM-DM networks provide services for users only through the Any-Source Multicast (ASM) model. In the ASM model, hosts cannot specify a source when joining a group.
- The Protocol Independent Multicast-Sparse Mode (PIM-SM) is a multicast protocol in sparse mode. It is applicable to large-scale networks with sparsely-distributed members. PIM-SM networks provide services for users through the ASM model and the Source-Specific Multicast (SSM) model. In the SSM model, hosts can specify a source when joining a group.

3.2 PIM-DM Troubleshooting

This section describes the notes about configuring PIM-DM, and provides the PIM-DM troubleshooting flowchart and the troubleshooting procedure in a typical PIM-DM networking.

3.2.1 Typical Networking

3.2.2 Configuration Notes

3.2.3 Troubleshooting Flowchart

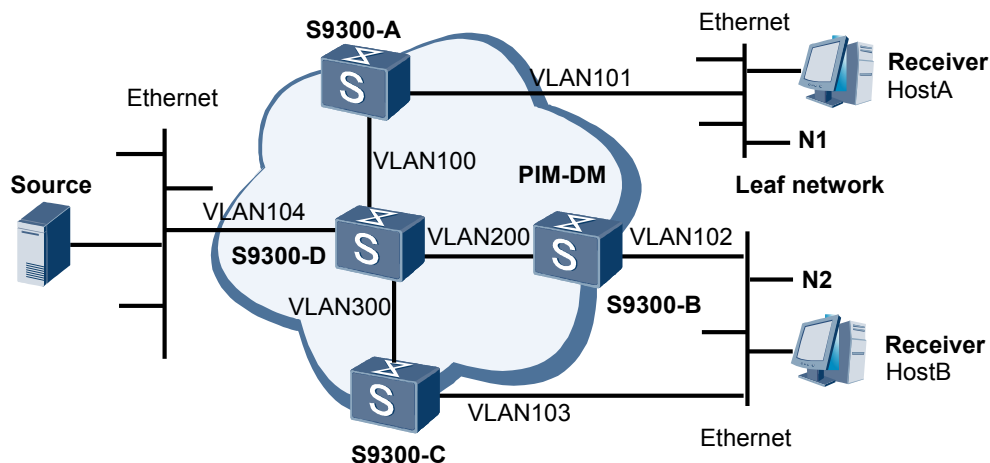
3.2.4 Troubleshooting Procedure

3.2.1 Typical Networking

Figure 3-1 shows a typical networking.

The following takes this networking to describe how to perform PIM-DM troubleshooting.

Figure 3-1 Typical PIM-DM networking



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network segment where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire PIM network runs PIM-DM.

Host A and Host B can receive data from Source.

3.2.2 Configuration Notes

NOTE

- The physical interfaces on the S9300 are Layer 2 interfaces. To use Layer 3 multicast protocols, you need to add interfaces to a VLAN and configure Layer 3 multicast protocols on VLANIF interfaces.
- On the S9300, PIM can be configured only on VLANIF interfaces and loopback interfaces. Generally, PIM is not used on loopback interfaces.

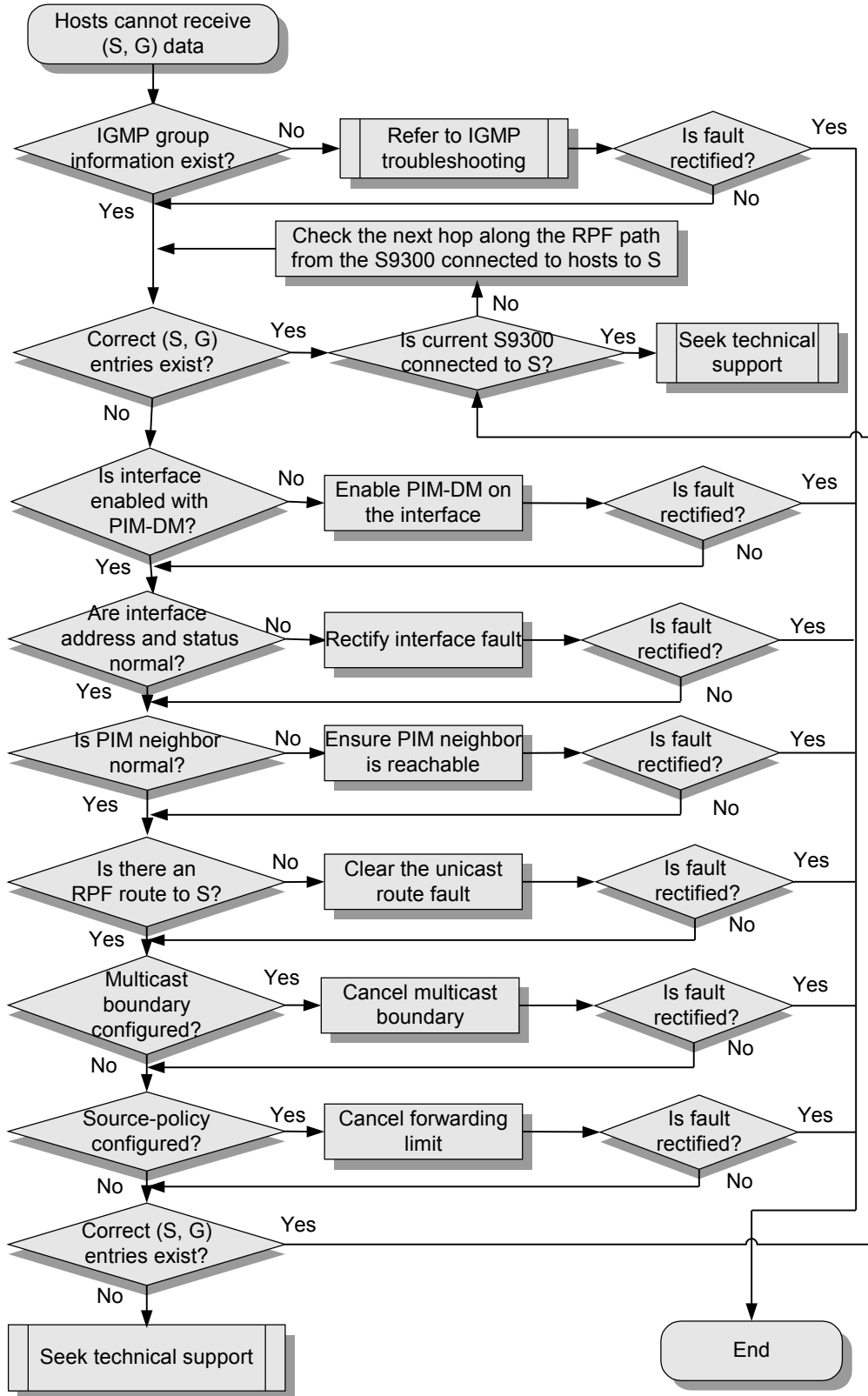
Item	Sub-item	Configuration Notes and Commands
Configuring PIM-DM	Configuring unicast routing	PIM does not maintain a separate unicast routing table. Instead, PIM uses routes in the current unicast routing table as the basis of the RPF check. To make PIM-DM work normally, ensure that unicast routes to the source are available.
	Enabling IP multicast	Multicast configuration takes effect only after the multicast function is enabled. To enable IP multicast, run the multicast routing-enable command in the system view.
	Enabling PIM-DM	PIM-DM must be enabled on the interfaces through which S9300s are interconnected, the interfaces through which S9300s are directly connected to the source, and the interfaces through which S9300s are connected to hosts. To enable PIM-DM, run the pim-dm command in the interface view.
	Configuring IGMP	The S9300 directly connected to hosts must run IGMP. To configure IGMP, run the igmp enable command in the interface view.

3.2.3 Troubleshooting Flowchart

On the network shown in "Typical PIM-DM networking" in [3.2.1 Typical Networking](#), hosts cannot receive (S, G) information.

[Figure 3-2](#) shows the troubleshooting flowchart.

Figure 3-2 Troubleshooting flowchart of PIM-DM



3.2.4 Troubleshooting Procedure

Procedure

Step 1 Check whether there is IGMP group information on the outgoing interface connected to hosts.

On the S9300 that is directly connected to hosts, run the **display igmp group interface** command to check whether there is the IGMP group information on the interface directly connected to hosts.

- If there is no IGMP group information, see [2 IGMP Troubleshooting](#).
- If information about IGMP groups exists, go to [Step 2](#).

 **NOTE**

Locate the fault from the interface directly connected to hosts to the interface directly connected to the multicast source along the RPF path hop by hop. During the troubleshooting, perform [Step 2](#) to [Step 8](#).

Step 2 Check whether the PIM routing table contains correct (S, G) entries.

Run the **display pim routing-table** command on the current S9300 to check whether there are correct (S, G) entries in the PIM routing table, especially whether the downstream interface list contains all corresponding downstream interfaces. If a downstream interface is not in the outgoing interface list of an (S, G) entry, check whether the interface is faulty.

If the routing table contains correct (S, G) entries, run the **display multicast forwarding-table** command to check whether the number of messages forwarded according to the (S, G) entry keeps increasing.

- If the number of messages forwarded according to the (S, G) entry keeps increasing, it indicates that the forwarding of upstream data is normal but the data cannot be forwarded to downstream devices. In this case, contact Huawei technical personnel.
- If the number of messages forwarded according to the (S, G) entry stops increasing, it indicates that the current S9300 does not receive multicast data. In this case, check whether the PIM routing table of the upstream S9300 contains correct (S, G) entries. If the current S9300 is directly connected to the network segment where the source resides, contact Huawei technical personnel.

Step 3 Check whether interfaces are enabled with PIM-DM.

Run the **display pim interface [verbose]** command on the current S9300 to check information about PIM on the interfaces.

If the command output does not contain a certain interface or the PIM mode is sparse on an interface, run the **pim dm** command on the interface.

If the message "Warning: Please enable multicast routing first" is displayed, run the **multicast routing-enable** command in the system view to enable multicast and then enable PIM-DM through **pim dm** command on the interfaces.

The fault often occurs when the **pim dm** command is not used on the following interfaces:

- RPF neighbor interface from which S is reachable
- RPF interface from which S is reachable
- Interface connected to the network segment where the hosts reside

- Interface connected to the network segment where the multicast source resides

Step 4 Check that the interface is in the normal state.

Run the **display interface** *interface-type interface-number* command on the S9300. *interface-type interface-number* specifies the interface that directly connects the local S9300 to another S9300. View the output information.

- If you can see "*interface-type interface-number* current state : DOWN:", it indicates that the physical status of the interface is Down. You need to check the networking and ensure that the interfaces are correctly connected.
- If you can see "Line protocol current state : DOWN", it indicates that the protocol status of the interface is Down. You need to perform the following operations:
 - Check whether the **shutdown** command is run on the interface.
Run the **display current-configuration interface** *interface-type interface-number* command to check the current configuration of the interface. If the **shutdown** command is contained in the output information, run the **undo shutdown** command in the interface view to cancel the configuration.
 - Check whether the interface is configured with an IPv4 address.
Run the **display ip interface brief** command to check the address on the interface. If the interface is not configured with an IP address or the IP address of the interface is on a different network segment from the directly connected S9300, reconfigure an IP address for the interface.

Step 5 Check whether the status of the PIM neighbor is normal.

Run the **display pim neighbor** command on the S9300 to check whether the information about the PIM neighbor is displayed. If the information about the PIM neighbor is not displayed, adjust the control parameters of the PIM neighbor. Ensure that the PIM neighbor is reachable.

Step 6 Check whether there is an RPF route to the source.

Run the **display multicast rpf-info** *source-address* command on the current S9300 to check whether there is an RPF route to S.

- If the command output indicates that the RPF route is a static multicast route or an MBGP route, run the **display current-configuration** command to check whether the configuration of the static multicast route or the MBGP route is correct.
- If the command output indicates that the RPF route is a unicast route, run the **display ip routing-table** command to check whether the unicast route is the same as the RPF route.
- If the command output indicates that the RPF route does not exist, run the **display ip routing-table** command to check the configurations of unicast routes. It is recommended that you run the **ping** command on the current S9300 and S to check whether they can ping each other.

Step 7 Check whether the multicast boundary is configured on the interface.

Run the **display current-configuration interface** *interface-type interface-number* command on the current S9300 to check the configuration of the upstream interface and the downstream interface. If the command output contains the **multicast boundary** command, it indicates that the multicast boundary is configured on the interface. It is recommended that you cancel the configuration or review the network planning.

Step 8 Check whether the **source-policy** command is used on the current S9300.

In the system view, run the **display current-configuration configuration pim** command to check the current configuration in the PIM view.

If the command output contains the **source-policy** *acl-number* command, it indicates that source-based filtering rules are configured. If the received multicast data is not in the range defined by the ACL, the multicast data is discarded. It is recommended that you cancel the configuration or configure proper ACL rules. Thus, the multicast data required by users is forwarded correctly.

Step 9 Check whether the PIM routing table contains correct (S, G) entries.

Run the **display pim routing-table** command on the current S9300 to check whether the PIM routing table contains correct (S, G) entries. For troubleshooting methods, go to step 2.

- If no (S, G) entry exists, check whether the PIM routing table of the upstream S9300 contains correct (S, G) entries.
- If existing (S, G) entries are not correct, contact Huawei technical personnel.

----End

3.3 PIM-SM Troubleshooting

This section describes the notes about configuring PIM-SM, and provides the PIM-SM troubleshooting flowchart and the troubleshooting procedure in a typical PIM-SM networking.

3.3.1 Typical Networking

3.3.2 Configuration Notes

3.3.3 Troubleshooting Flowchart

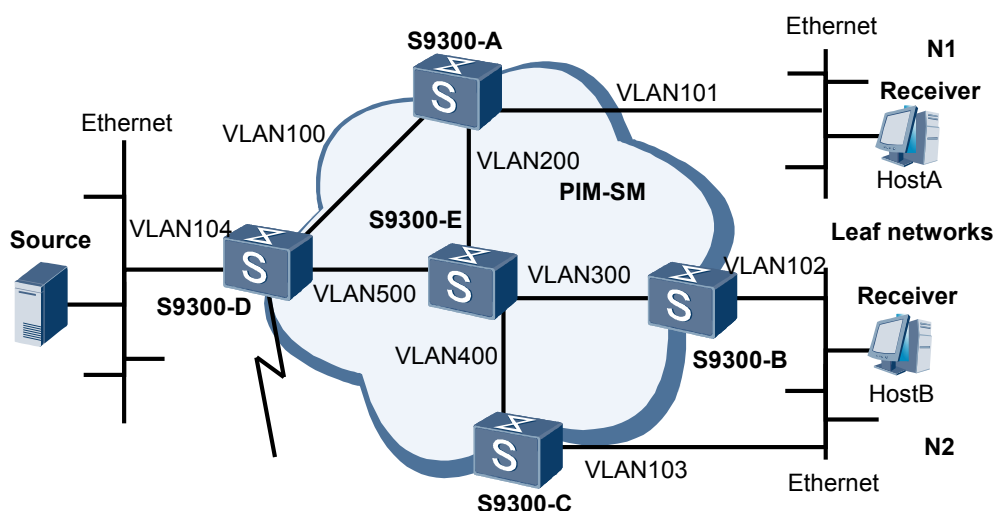
3.3.4 Troubleshooting Procedure

3.3.1 Typical Networking

Figure 3-3 shows a typical networking.

The following takes this networking to describe how to perform PIM-SM troubleshooting.

Figure 3-3 Typical networking of PIM-SM



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire network adopts a single BSR to administrate the PIM-SM domain. S9300-A is the C-BSR and the C-RP in the PIM-SM network.

Host A and Host B can receive multicast data from Source.

3.3.2 Configuration Notes

NOTE

- The physical interfaces on the S9300 are Layer 2 interfaces. To use Layer 3 multicast protocols, you need to add interfaces to a VLAN and configure Layer 3 multicast protocols on VLANIF interfaces.
- On the S9300, PIM can be configured only on VLANIF interfaces and loopback interfaces. Generally, PIM is not used on loopback interfaces.

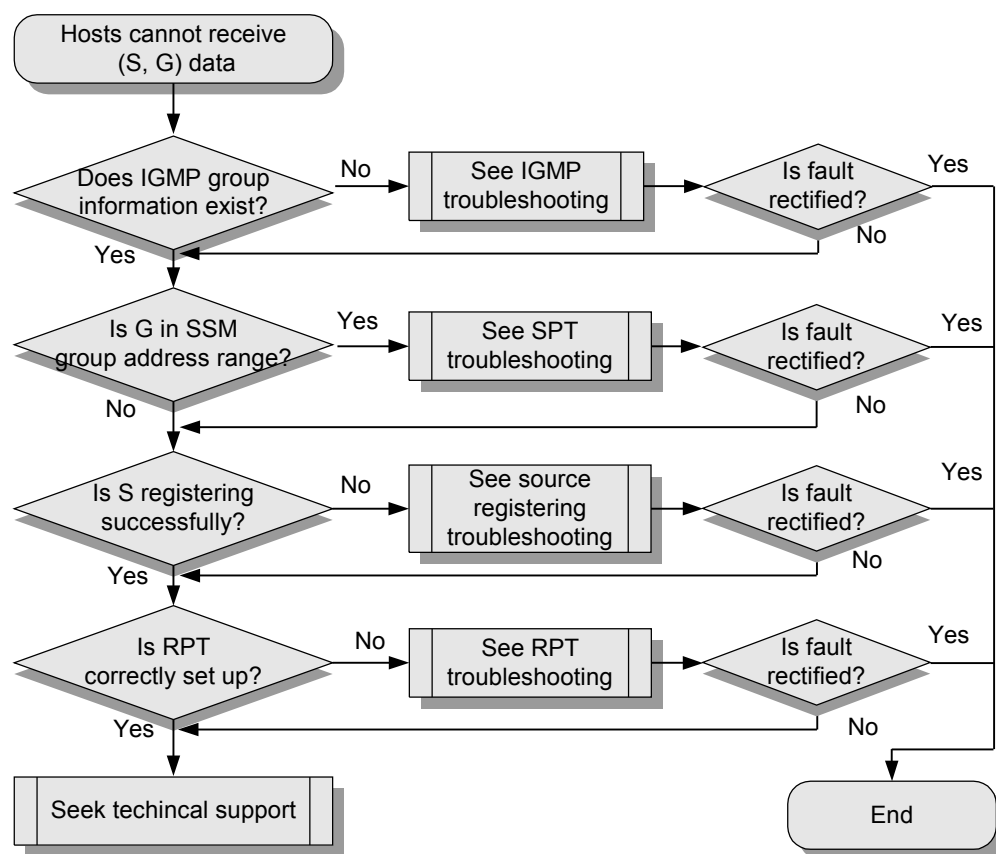
Item	Sub-item	Configuration Notes and Commands
Configuring PIM-SM	Configuring unicast routes	In PIM-SM, the RPF check is performed on the multicast source, RP, and BSR. Ensure that the unicast routes to those destinations are reachable. Ensure that all the C-RPs and BSRs can communicate in unicast mode when the BSR mechanism is applied.
	Enabling IP multicast	Multicast configuration takes effect only after the multicast function is enabled. To enable IP multicast, run the multicast routing-enable command in the system view.
	Enabling PIM-SM	PIM-SM must be enabled on the interfaces through which S9300s are connected, the interfaces through which S9300s are directly connected to the source, and the interfaces through which S9300s are connected to hosts. To enable PIM-SM, run the pim sm command in the interface view.
	Configuring an RP	When applying a static RP, ensure that the static-rp command is used on all S9300s on the network. Configure a C-BSR and C-RP when applying the BSR mechanism. To configure an RP, run the static-rp , c-br , and c-rp commands in the PIM view.

Item	Sub-item	Configuration Notes and Commands
	Configuring the SPT switchover	By default, the DR at the member side and the RP immediately trigger the SPT switchover after they receive the first multicast packet. <ul style="list-style-type: none"> ● If traffic-rate is set, the SPT switchover is triggered when the forwarding rate of an (S, G) entry is higher than the value of traffic-rate. ● If the infinity command is used, the SPT switchover is not triggered any longer. To configure the SPT switchover, run the spt-switch-threshold command in the PIM view.
	Configuring the SSM group address range	The same ssm-policy command is used on all the S9300s on a network. ASM is applicable to all multicast groups that are excluded from the SSM group address range. By default, the SSM group address range is from 232.0.0.0 to 8. To configure the SSM group address range, run the ssm-policy command in the PIM view.
	Configuring IGMP	The S9300 directly connected to hosts must run IGMP. To configure IGMP, run the igmp enable command in the interface view.

3.3.3 Troubleshooting Flowchart

On the PIM-SM network shown in "Typical networking of PIM-SM" in [3.3.1 Typical Networking](#), the configuration on each router is complete but hosts cannot receive the multicast data.

Locate the fault according to the flowchart shown in [Figure 3-4](#).

Figure 3-4 Troubleshooting flowchart of PIM-SM

3.3.4 Troubleshooting Procedure

Procedure

Step 1 Check whether there is IGMP group information on the S9300 connected to hosts.

On the S9300 directly connected to hosts, run the **display igmp group interface** command to check whether there is IGMP group information on the interface connected to hosts.

If there is no IGMP group information, see [2 IGMP Troubleshooting](#).

Step 2 Check whether G is in the SSM group address range.

Run the **display current-configuration configuration pim** command on the S9300 to check the current configuration in the PIM view. If the command output contains the **ssm-policy basic-acl-number** command, it indicates that the SSM group address range is adjusted on the S9300. Run the **display current-configuration configuration acl-basic** command to check the configuration of the ACL.

- If the command output indicates that the group range defined by the ACL contains G, it indicates that G is in the SSM group address range. Check whether the SPT is correctly set up. For more information, see [3.6 SPT Troubleshooting](#).

- If the command output indicates that the group range defined by the ACL does not contain G, it indicates that G is not in the SSM group address range. Perform the following steps to check the source registering and the RPT.

Step 3 Check whether S registering is successful.

Run the **display pim routing-table** command on the RP to check whether the PIM routing table contains (S, G) entries. If no (S, G) entry exists, it indicates that S fails to register with the RP. For more information, see [3.5 Source Registering Troubleshooting](#).

Step 4 Check whether the RPT is set up correctly.

On the S9300 connected to hosts, run the **display pim routing-table** command to check whether (*, G) forwarding entries is set up correctly. Perform the RPF check along the RPF path to S hop by hop. For details, see [3.4 RPT Troubleshooting](#).

If the fault persists, contact Huawei technical personnel.

----End

3.4 RPT Troubleshooting

This section describes the procedure for RPT troubleshooting.

[3.4.1 Typical Networking](#)

[3.4.2 Configuration Notes](#)

[3.4.3 Troubleshooting Flowchart](#)

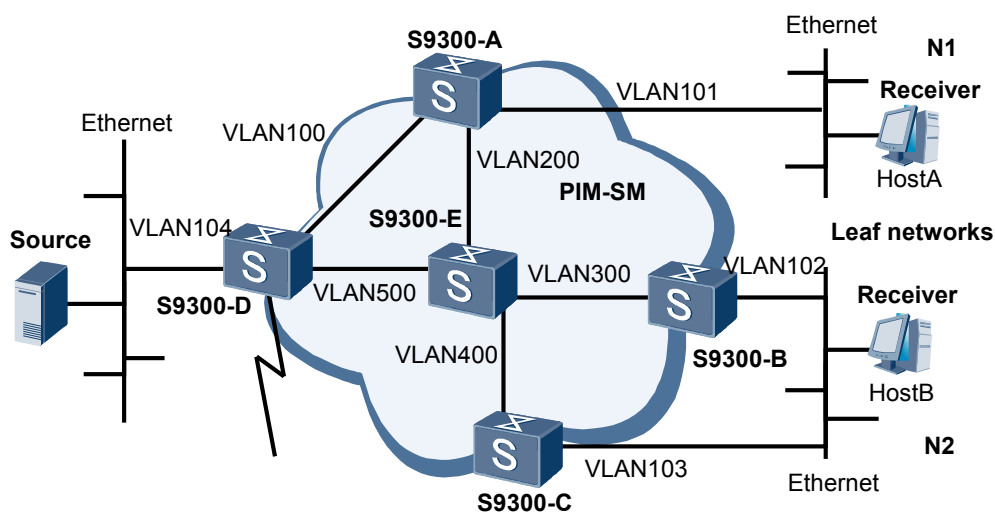
[3.4.4 Troubleshooting Procedure](#)

3.4.1 Typical Networking

[Figure 3-5](#) shows a typical networking.

The following takes this networking to describe how to perform PIM-SM troubleshooting.

Figure 3-5 Typical networking of PIM-SM



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire network adopts a single BSR to administrate the PIM-SM domain. S9300-A is the C-BSR and the C-RP in the PIM-SM network.

Host A and Host B can receive multicast data from Source.

3.4.2 Configuration Notes

NOTE

- The physical interfaces on the S9300 are Layer 2 interfaces. To use Layer 3 multicast protocols, you need to add interfaces to a VLAN and configure Layer 3 multicast protocols on VLANIF interfaces.
- On the S9300, PIM can be configured only on VLANIF interfaces and loopback interfaces. Generally, PIM is not used on loopback interfaces.

Item	Sub-item	Configuration Notes and Commands
Configuring PIM-SM	Configuring unicast routes	In PIM-SM, the RPF check is performed on the multicast source, RP, and BSR. Ensure that the unicast routes to those destinations are reachable. Ensure that all the C-RPs and BSRs can communicate in unicast mode when the BSR mechanism is applied.
	Enabling IP multicast	Multicast configuration takes effect only after the multicast function is enabled. To enable IP multicast, run the multicast routing-enable command in the system view.
	Enabling PIM-SM	PIM-SM must be enabled on the interfaces through which S9300s are connected, the interfaces through which S9300s are directly connected to the source, and the interfaces through which S9300s are connected to hosts. To enable PIM-SM, run the pim sm command in the interface view.
	Configuring an RP	When applying a static RP, ensure that the static-rp command is used on all S9300s on the network. Configure a C-BSR and C-RP when applying the BSR mechanism. To configure an RP, run the static-rp , c-br , and c-rp commands in the PIM view.

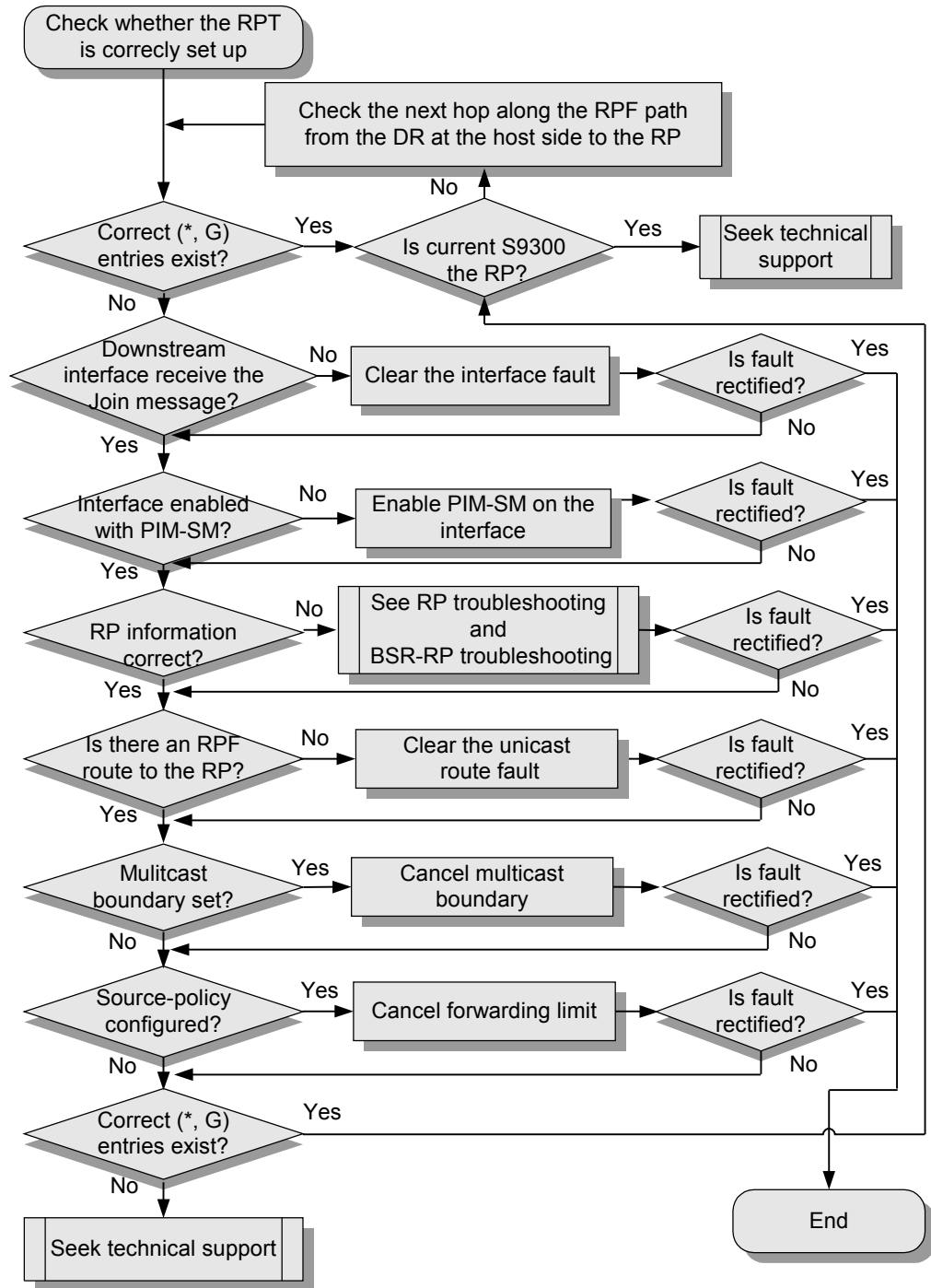
Item	Sub-item	Configuration Notes and Commands
	Configuring the SPT switchover	By default, the DR at the member side and the RP immediately trigger the SPT switchover after they receive the first multicast packet. <ul style="list-style-type: none"> ● If traffic-rate is set, the SPT switchover is triggered when the forwarding rate of an (S, G) entry is higher than the value of traffic-rate. ● If the infinity command is used, the SPT switchover is not triggered any longer. To configure the SPT switchover, run the spt-switch-threshold command in the PIM view.
	Configuring the SSM group address range	The same ssm-policy command is used on all the S9300s on a network. ASM is applicable to all multicast groups that are excluded from the SSM group address range. By default, the SSM group address range is from 232.0.0.0 to 8. To configure the SSM group address range, run the ssm-policy command in the PIM view.
	Configuring IGMP	The S9300 directly connected to hosts must run IGMP. To configure IGMP, run the igmp enable command in the interface view.

3.4.3 Troubleshooting Flowchart

On the network shown in [Figure 3-5](#), check whether the RPT is correctly set up.

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

Figure 3-6 RPT troubleshooting flowchart



3.4.4 Troubleshooting Procedure

Context

Perform the following steps from the DR on the user side to the RP hop by hop along the RPF path.

Procedure

Step 1 Check whether the PIM routing table contains correct (*, G) entries.

Run the **display pim routing-table** command on the current S9300 to check whether the PIM routing table contains correct (*, G) entries, especially whether the downstream interface list contains all downstream interfaces connected to (*, G) members.

If the routing table contains correct (*, G) entries, run the **display multicast forwarding-table** command to check whether the forwarding table contains (S, G) entries and whether the number of messages forwarded according to the (S, G) entries keeps increasing.

- If the (S, G) entries exist and the number of messages forwarded according to the (S, G) entries keeps increasing, it indicates that the forwarding of upstream data is normal but the data cannot be forwarded to downstream devices. In this case, contact Huawei technical personnel.
- If the (S, G) entries do not exist and the number of messages forwarded according to the (S, G) entries stops increasing, it indicates that the current S9300 does not receive any multicast data. The fault may occur on the upstream device. In this case, check whether the PIM routing table of the upstream device contains correct (S, G) entries. If the current S9300 is an RP, it indicates that the RPT is set up successfully, but the RP does not receive multicast data sent by the source. The fault may be that the source DR does not register successfully.

Step 2 Check whether the downstream interface receives the Join message.

Step 3 Check whether interfaces are enabled with PIM-SM.

Run the **display pim interface [verbose]** command on the current S9300 to check information about PIM on the interfaces.

If the command output does not contain a certain interface or PIM-DM is run on an interface, run the **pim sm** command on the interface.

The fault often occurs when the **pim-sm** command is not used on the following interfaces:

- RPF neighbor interface from which the RP is reachable
- RPF interface from which the RP is reachable
- Interface directly connected to the network segment where hosts reside

Step 4 Check whether the information about the RP corresponding to G is correct on the S9300.

Run the **display pim rp-info** command on the current S9300 to check whether the RP corresponding to G is learned and whether the information about the RP is the same as the information on other S9300s.

If the S9300 does not learn the RP or the information about the RP is different from the information on other S9300s, do as follows:

- If the current network uses a static RP, see [3.7 Static RP Troubleshooting](#).
- If the current network uses a BSR, see [3.8 BSR-RP Troubleshooting](#).

Step 5 Check whether the RPF route to the RP exists.

Run the **display multicast rpf-info rp-address** command on the current S9300 to check whether there is an RPF route to the RP.

- If the command output indicates that the RPF route is a static multicast route or an MBGP route, run the **display current-configuration** command to check whether the configuration of the static multicast route or MBGP route is correct.
- If the command output indicates that the RPF route is a unicast route, run the **display ip routing-table** command to check whether the unicast route is the same as the RPF route.
- If the command output indicates that the RPF route does not exist, check the configurations of unicast routes. It is recommended that you run the **ping** command on the current S9300 and the RP to check whether they can ping each other.

Step 6 Check whether the multicast boundary is configured on the interface.

Run the **display current-configuration interface** *interface-type interface-number* command on the current S9300 to check the configuration of the interface.

If the command output contains the **multicast boundary** command, it indicates that the multicast boundary is configured on the interface. To ensure that the multicast boundary is not configured on the RPF interface on the local S9300 and the interface on the RPF neighbor, it is recommended that you cancel the configuration or to review the network planning.

Step 7 Check whether the **source-policy** command is used on the current S9300.

In the system view, run the **display current-configuration configuration pim** command to check the current configuration in the PIM view.

If the command output contains the **source-policy** *acl-number* command, it indicates that the source-based filtering rules are configured. If the received multicast data is not in the range defined by the ACL, the multicast data is discarded. It is recommended that you cancel the configuration or configure proper ACL rules. Thus, the multicast data required by users are forwarded correctly.

Step 8 Check whether the PIM routing table has correct (*, G) entries.

Run the **display pim routing-table** command on the current S9300 to check whether the PIM routing table contains correct (S, G) entries. For troubleshooting methods, go to [Step 1](#).

If the PIM routing table does not contain any correct (*, G) entry, contact Huawei technical personnel.

----End

3.5 Source Registering Troubleshooting

This section describes the procedure for source registering troubleshooting.

[3.5.1 Typical Networking](#)

[3.5.2 Configuration Notes](#)

[3.5.3 Troubleshooting Flowchart](#)

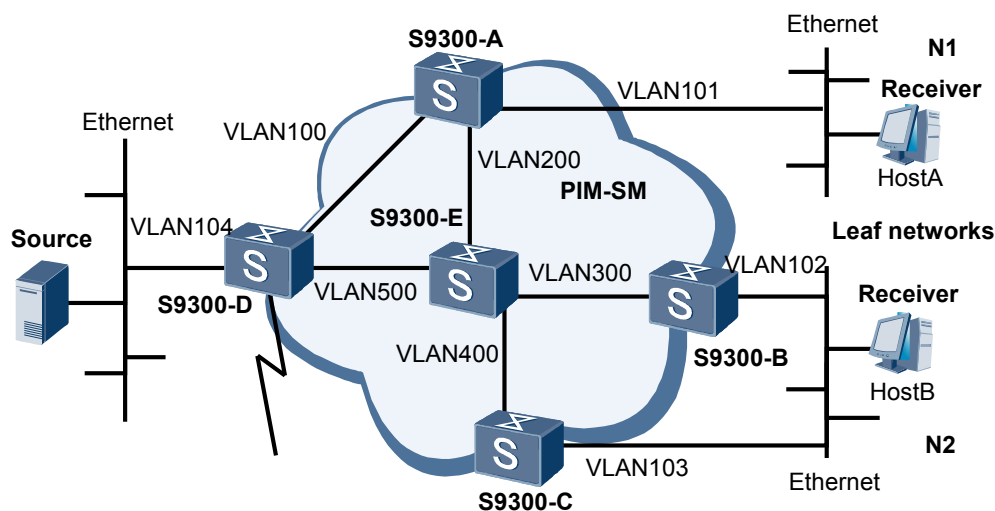
[3.5.4 Troubleshooting Procedure](#)

3.5.1 Typical Networking

[Figure 3-7](#) shows a typical networking.

The following takes this networking to describe how to perform PIM-SM troubleshooting.

Figure 3-7 Typical networking of PIM-SM



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire network adopts a single BSR to administrate the PIM-SM domain. S9300-A is the C-BSR and the C-RP in the PIM-SM network.

Host A and Host B can receive multicast data from Source.

3.5.2 Configuration Notes

NOTE

- The physical interfaces on the S9300 are Layer 2 interfaces. To use Layer 3 multicast protocols, you need to add interfaces to a VLAN and configure Layer 3 multicast protocols on VLANIF interfaces.
- On the S9300, PIM can be configured only on VLANIF interfaces and loopback interfaces. Generally, PIM is not used on loopback interfaces.

Item	Sub-item	Configuration Notes and Commands
Configuring PIM-SM	Configuring unicast routes	In PIM-SM, the RPF check is performed on the multicast source, RP, and BSR. Ensure that the unicast routes to those destinations are reachable. Ensure that all the C-RPs and BSRs can communicate in unicast mode when the BSR mechanism is applied.

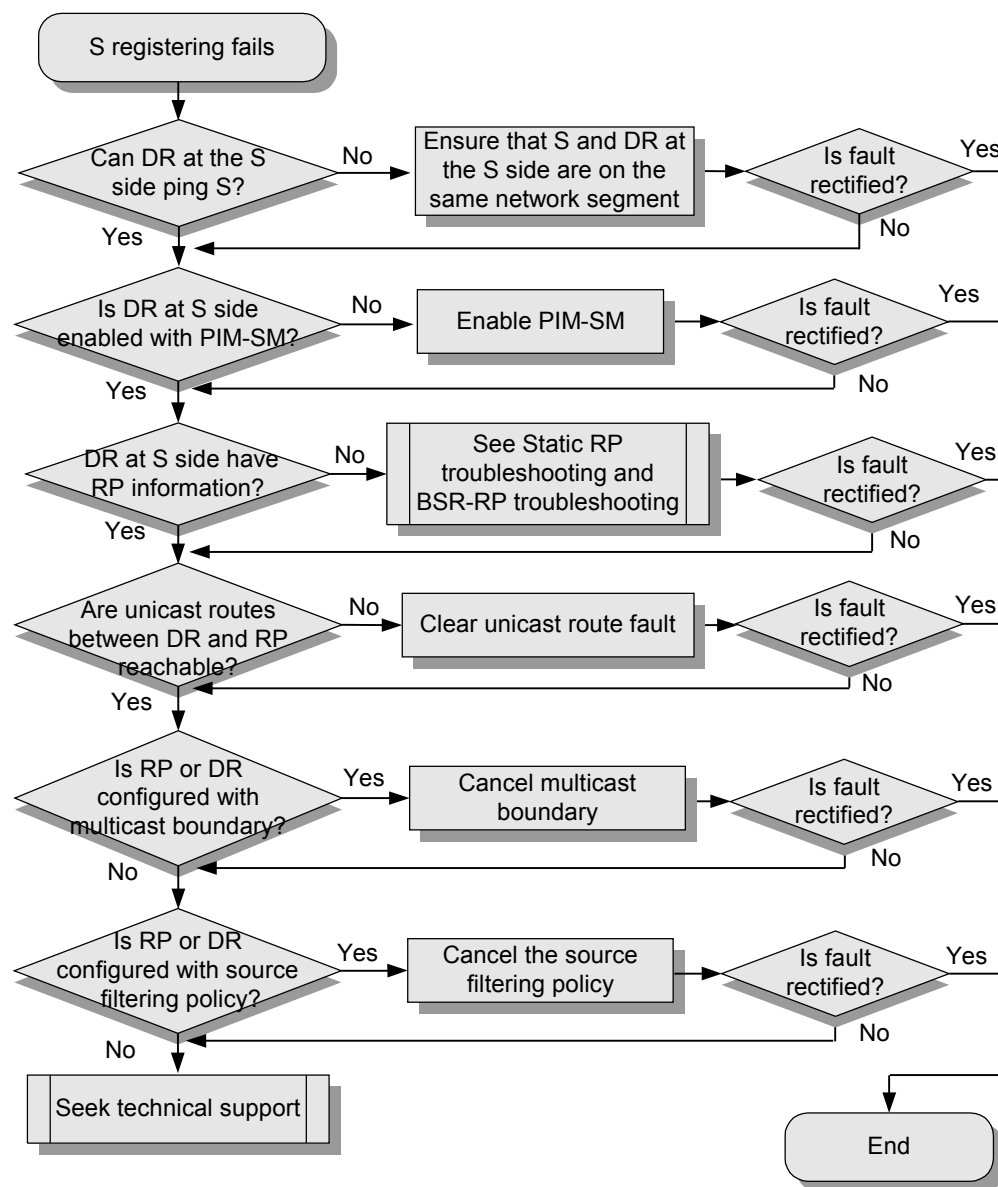
Item	Sub-item	Configuration Notes and Commands
	Enabling IP multicast	Multicast configuration takes effect only after the multicast function is enabled. To enable IP multicast, run the multicast routing-enable command in the system view.
	Enabling PIM-SM	PIM-SM must be enabled on the interfaces through which S9300s are connected, the interfaces through which S9300s are directly connected to the source, and the interfaces through which S9300s are connected to hosts. To enable PIM-SM, run the pim sm command in the interface view.
	Configuring an RP	When applying a static RP, ensure that the static-rp command is used on all S9300s on the network. Configure a C-BSR and C-RP when applying the BSR mechanism. To configure an RP, run the static-rp , c-br , and c-rp commands in the PIM view.
	Configuring the SPT switchover	By default, the DR at the member side and the RP immediately trigger the SPT switchover after they receive the first multicast packet. <ul style="list-style-type: none"> • If traffic-rate is set, the SPT switchover is triggered when the forwarding rate of an (S, G) entry is higher than the value of traffic-rate. • If the infinity command is used, the SPT switchover is not triggered any longer. To configure the SPT switchover, run the spt-switch-threshold command in the PIM view.
	Configuring the SSM group address range	The same ssm-policy command is used on all the S9300s on a network. ASM is applicable to all multicast groups that are excluded from the SSM group address range. By default, the SSM group address range is from 232.0.0.0 to 8. To configure the SSM group address range, run the ssm-policy command in the PIM view.
	Configuring IGMP	The S9300 directly connected to hosts must run IGMP. To configure IGMP, run the igmp enable command in the interface view.

3.5.3 Troubleshooting Flowchart

On the network shown in "Typical networking of PIM-SM" in [3.5.1 Typical Networking](#), S sends data to G, but no (S, G) entry exists on the RP.

Figure 3-8 shows the troubleshooting flowchart.

Figure 3-8 Source registering troubleshooting flowchart



3.5.4 Troubleshooting Procedure

Procedure

Step 1 Check whether S and the DR interface at the S side are on the same network segment.

On the DR directly connected to S, run the **ping** command to check whether the DR can ping S.

If the ping operation fails, check the address of the interface on the DR directly connected to the network segment where S resides, and the address of the interface on S directly connected to the

network segment where the DR resides. Ensure that the two interfaces are located on the same network segment.

Step 2 Check whether the DR interface at the S side is enabled with PIM-SM.

Run the **display pim interface [verbose]** command on the DR at the S side to check the information about PIM on the interface. If the command output indicates that the DR interface directly connected to S does not exist or PIM -DM is used, run the **pim sm** command on the DR interface directly connected to S.

If the message "Warning: Please enable multicast routing first" is displayed, run the **multicast routing-enable** command in the system view to enable multicast, and then enable PIM-SM on the interface.

Step 3 Check whether the information about RP corresponding to G on the DR at the S side is correct.

On the DR at the S side, run the **display pim rp-info** command to check whether the information about the RP corresponding to G is learned and whether the information about the RP is the same as the information on the other S9300s.

If the DR does not learn the RP or the information about the RP is different from the information on the other S9300s, Register messages cannot be sent to the correct RP. In this case, do as follows:

- If the current network uses a static RP, see [3.7 Static RP Troubleshooting](#).
- If the current network uses a BSR, see [3.8 BSR-RP Troubleshooting](#).

Step 4 Check whether the DR at the S side has a unicast route to the RP.

Run the **display ip routing-table** command on the DR at the S side and the RP to check whether the DR and the RP have unicast routes to each other and whether they can ping each other.

If the unicast routes are unreachable, check the unicast configuration.

Step 5 Check whether the multicast boundary is configured on the DR at the S side and the RP.

On the DR at the S side and the RP, run the **display current-configuration interface interface-type interface-number** command to check the configuration of interfaces.

If the command output contains the **multicast boundary** command, it indicates that the multicast boundary is configured on the interface. If G is in the group address range defined through the command, the interface discards the (S, G) data. To ensure that the DR at the source side and the RP can receive (S, G) data, it is recommended that you modify or cancel the configuration.

Step 6 Check whether the source-based filtering policy is configured on the DR at the S side and the RP.

Run the **display current-configuration configuration pim** command on the DR at the S side and the RP to check the current configuration in the PIM view.

If the command output contains the **source-policy acl-number** command, it indicates that source-based filtering policy is configured. If the received multicast data is not in the range defined by the ACL, the multicast data is discarded. In this case, it is recommended that you cancel the configuration or configure proper ACL rules. (S, G) data can thus be received.

If the fault persists, contact Huawei technical personnel.

----End

3.6 SPT Troubleshooting

This section describes the procedure for SPT troubleshooting.

3.6.1 Typical Networking

3.6.2 Configuration Notes

3.6.3 Troubleshooting Flowchart

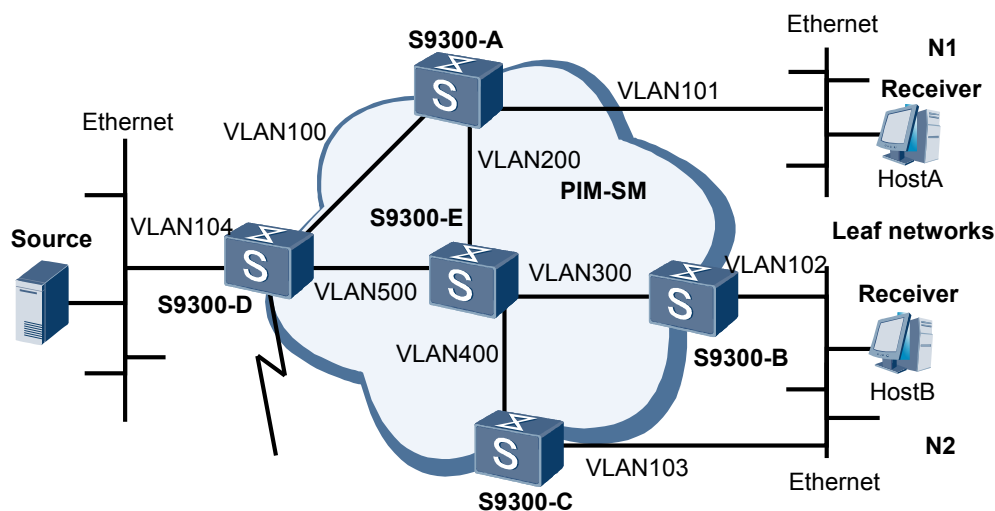
3.6.4 Troubleshooting Procedure

3.6.1 Typical Networking

Figure 3-9 shows a typical networking.

The following takes this networking to describe how to perform PIM-SM troubleshooting.

Figure 3-9 Typical networking of PIM-SM



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire network adopts a single BSR to administrate the PIM-SM domain. S9300-A is the C-BSR and the C-RP in the PIM-SM network.

Host A and Host B can receive multicast data from Source.

3.6.2 Configuration Notes

PIM-SM supports the ASM mode and the SSM mode.

- If G is in the ASM group address range, the RP or the DR at the host side can trigger the SPT switchover. The RP sends a Join message to S, and sets up an SPT from S to the RP. The DR at the host side sends a Join message to S, and sets up an SPT from S to a host. Subsequently, (S, G) data is delivered along the SPT from S to hosts.
- By default, the RP and the DR at the host side immediately trigger the SPT switchover after they receive the first multicast packet.

 **NOTE**

Configure the SPT switchover threshold on the DR at the host side. The threshold set on the RP is invalid.

- If the **spt-switch-threshold** *traffic-rate* command is used, the SPT switchover is triggered only when the (S, G) forwarding rate is greater than the value of *traffic-rate*.
- If the **spt-switch-threshold infinity** command is used, the SPT switchover is not triggered any longer.
- If G is in the SSM group address range, when a host wants to join a multicast group and specifies the source, the DR at the host side sends a Join message to S and sets up an SPT.

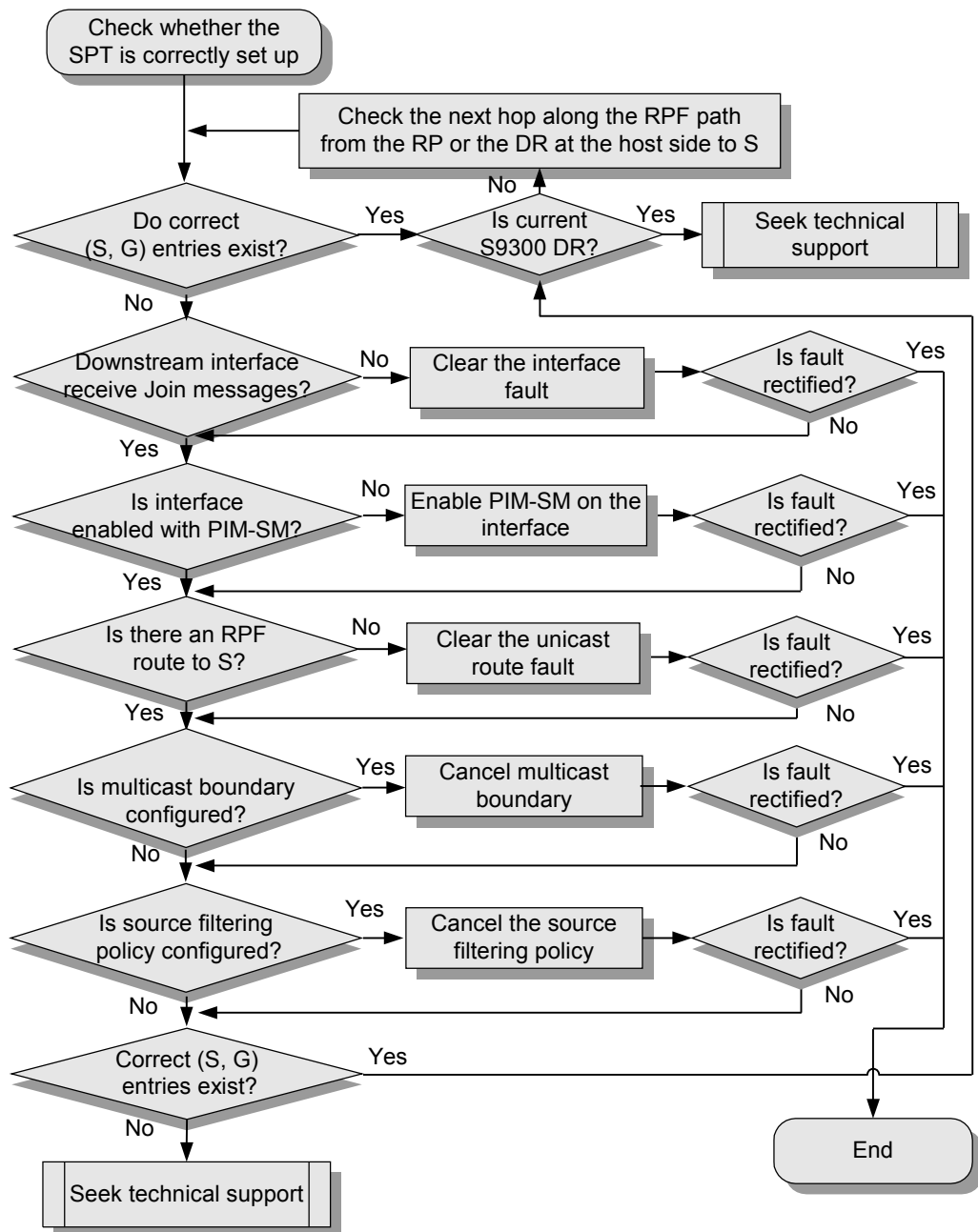
For details, see PIM-SM [3.5.2 Configuration Notes](#).

3.6.3 Troubleshooting Flowchart

On a PIM-SM network, if the following situations occur, check whether the SPT is correctly set up and locate the fault according to troubleshooting flowchart shown in [Figure 3-10](#).

- G is in the ASM group range, and hosts can normally receive (S, G) data. (S, G) data needs to be transmitted from S to the RP along the SPT and from the RP to hosts along the RPT. The (S, G) data transmitted from S to the RP, however, is always encapsulated in Register messages.
- G is in the ASM group range, and hosts can normally receive (S, G) data. (S, G) data needs to be transmitted from S to hosts along the SPT. The (S, G) data, however, is always delivered along the RPT.
- G is in the SSM group address range, and hosts can normally send IGMP (S, G) Join messages. S server can normally send (S, G) data. Hosts, however, cannot receive (S, G) data.
- (S, G) data is being delivered along the SPT, but the SPT forwarding is interrupted suddenly.

Figure 3-10 PIM-SM SPT troubleshooting flowchart



3.6.4 Troubleshooting Procedure

Context

NOTE

- If the (S, G) data from S to the RP is always encapsulated in Register messages, do as follows from the RP to the DR at the S side along the RPF path to S hop by hop.
- Otherwise, do as follows from the DR at the host side to the DR at the S side along the RPF path to S hop by hop.

Procedure

Step 1 Check whether the PIM routing table contains (S, G) entries.

Run the **display pim routing-table** command on the current S9300 to check whether the PIM routing table contains correct (S, G) entries.

- Check whether the upstream interface is the RPF interface from which S is reachable.
 - If G is in the ASM group range, the SPT switchover is triggered by the RP and the upstream interface on the RP is a "register" interface. This indicates that the RP receives the Register message sent by the DR at the S side but the SPT is not set up successfully.

Run the **display current-configuration configuration pim** command on the RP to check the current configuration in the PIM view. If the command output contains the **spt-switch-threshold { traffic-rate | infinity }** command, delete **infinity** and set the proper value of *traffic-rate*.

- If G is in the ASM group range, the SPT switchover is triggered by the DR at the host side and the upstream interface is the RPF interface from which the RP is reachable rather than the RPF interface from which S is reachable. This indicates that the SPT is not set up successfully.

Run the **display current-configuration configuration pim** command on the DR at the host side to check the current configuration in the PIM view. If the command output contains the **spt-switch-threshold { traffic-rate | infinity }** command, delete **infinity** and set the proper value of *traffic-rate*.

- Check whether the downstream interface list contains all downstream interfaces connected to all members of G.

If the routing table contains correct (S, G) entries, run the **display multicast forwarding-table** command to check whether the forwarding table contains the (S, G) entries and whether the number of messages forwarded according to the (S, G) entries keeps increasing.

- If the number of messages forwarded according to the (S, G) entries keeps increasing, it indicates that the forwarding of upstream data is normal but the data cannot be forwarded to downstream devices. In this case, contact Huawei technical personnel.
- If the number of messages forwarded according to the (S, G) entries stops increasing, it indicates that the current S9300 does not receive any multicast data. The fault may occur on the upstream device. In this case, check whether the PIM routing table of the upstream device contains correct (S, G) entries. If the current S9300 is the DR at the source side, it indicates that the SPT is set up successfully, but the DR does not forward multicast data along the SPT. In this case, contact Huawei technical personnel.

Step 2 Check whether the downstream interface receives the Join message.

NOTE

If the current S9300 is the DR at the host side, skip this step.

If the PIM routing table does not contain any (S, G) entry or any downstream interface, run the **debugging pim join-prune** command to check whether the downstream interface receives the corresponding (S, G) Join message.

If the downstream interface does not receive the corresponding (S, G) Join message, the possible causes are:

- The downstream interface is faulty.
- The downstream interface is not enabled with PIM-SM. For troubleshooting methods, go to [Step 3](#).

Step 3 Check whether the interface is enabled with PIM-SM.

Run the **display pim interface [verbose]** command on the current S9300 to check the information about PIM on the interface.

If the command output does not contain a certain interface or PIM-DM is run on an interface, run the **pim sm** command on the interface.

The fault often occurs when the **pim sm** command is not used on the following interfaces:

- RPF neighbor interface from which S is reachable
- RPF interface from which S is reachable

 **NOTE**

When setting up a PIM-SM network, ensure that multicast is enabled on all the S9300s and PIM-SM is enabled on all the interfaces.

Step 4 Check whether there is an RPF route to S on the S9300.

Run the **display multicast rpf-info source-address** command on the current S9300 to check whether there is an RPF route to S.

- If the command output indicates that the RPF route is a static multicast route or an MBGP route, run the **display current-configuration** command to check whether the configuration of the static multicast route or MBGP route is correct.
- If the command output indicates that the RPF route is a unicast route, run the **display ip routing-table** command to check whether the unicast route is the same as the RPF route.
- If the command output indicates that the RPF route does not exist, check the configurations of unicast routes. It is recommended that you run the **ping** command on the current S9300 and S to check whether they can ping each other.

 **NOTE**

When setting up a PIM-SM network, ensure that unicast routes are reachable and all S9300s have unicast routes to S.

Step 5 Check whether the multicast boundary is configured on the interface.

Run the **display current-configuration interface interface-type interface-number** command on the current S9300 to check the configuration of the interface.

If the command output contains the **multicast boundary** command, it indicates that the multicast boundary is configured on the interface. To ensure that the multicast boundary is not configured on the RPF interface of the local S9300 or the interface on neighbor interface, it is recommended that you cancel the current configuration or review the network planning.

Step 6 Check whether the source-based filtering policy is configured on the S9300.

In the system view, run the **display current-configuration configuration pim** command to check the current configuration in the PIM view.

If the command output contains the **source-policy acl-number** command, it indicates that source-based filtering policy is configured. If the received multicast data is not in the range defined by the ACL, the multicast data is discarded. It is recommended that you cancel the current configuration or configure proper ACL rules. Thus, the multicast data required by users is forwarded correctly.

Step 7 Check whether the PIM routing table contains correct (S, G) entries.

Run the **display pim routing-table** command on the current S9300 to check whether the PIM routing table contains correct (S, G) entries. For troubleshooting methods, go to [Step 1](#).

If the PIM routing table does not contain any correct (S, G) entry, contact Huawei technical personnel.

----End

3.7 Static RP Troubleshooting

This section describes the procedure for static RP troubleshooting.

[3.7.1 Typical Networking](#)

[3.7.2 Configuration Notes](#)

[3.7.3 Troubleshooting Flowchart](#)

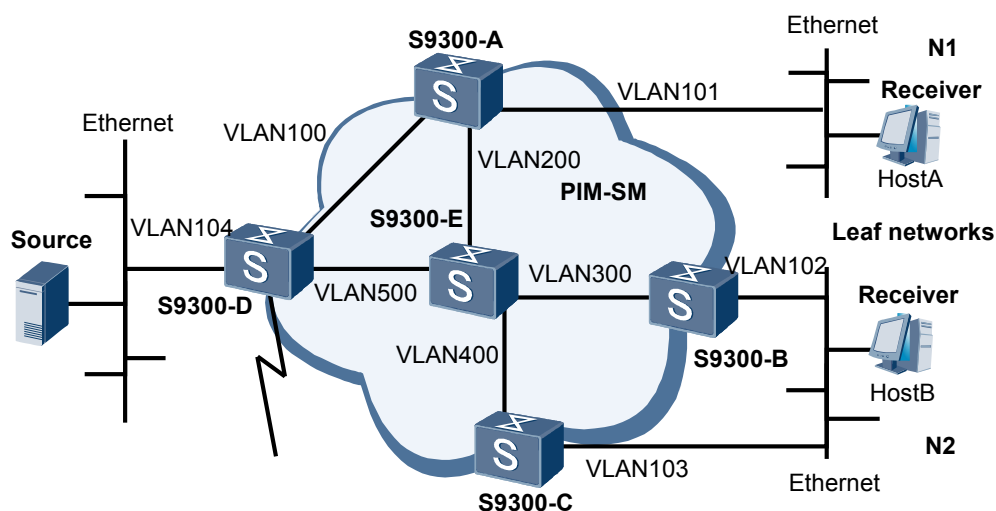
[3.7.4 Troubleshooting Procedure](#)

3.7.1 Typical Networking

[Figure 3-11](#) shows a typical networking.

The following takes this networking to describe how to perform PIM-SM troubleshooting.

Figure 3-11 Typical networking of PIM-SM



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire network adopts a single BSR to administrate the PIM-SM domain. S9300-A is the C-BSR and the C-RP in the PIM-SM network.

Host A and Host B can receive multicast data from Source.

3.7.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring a static RP	Configuring an RP address	The static RP must be configured on all the S9300s. Information about the RP corresponding to G must be the same on all the S9300s. To configure an RP address, run the static-rp command in the PIM view.
	Configuring an ACL	Filtering rules of the static RP on all the S9300s are the same. In addition, G is within the defined group address range. To configure an ACL, run the following commands: <ul style="list-style-type: none"> • acl [number] <i>acl-number</i> • rule [<i>rule-id</i>] { deny permit } [fragment source { <i>source-address</i> <i>source-wildcard</i> any } time-range <i>time-name</i>] *
	Configuring a static RP to be preferred	PIM-SM can use the static RP and the dynamic RP at the same time. By default, the dynamic RP has a higher priority. When the dynamic RP is Down, the static RP replaces the dynamic RP. You can configure a static RP to be preferred. To configure a static RP to be preferred, run the static-rp <i>rp-address</i> [<i>basic-acl-number</i>] preferred command in the PIM view. For details about the troubleshooting of a static RP, see 3.11 FAQs .

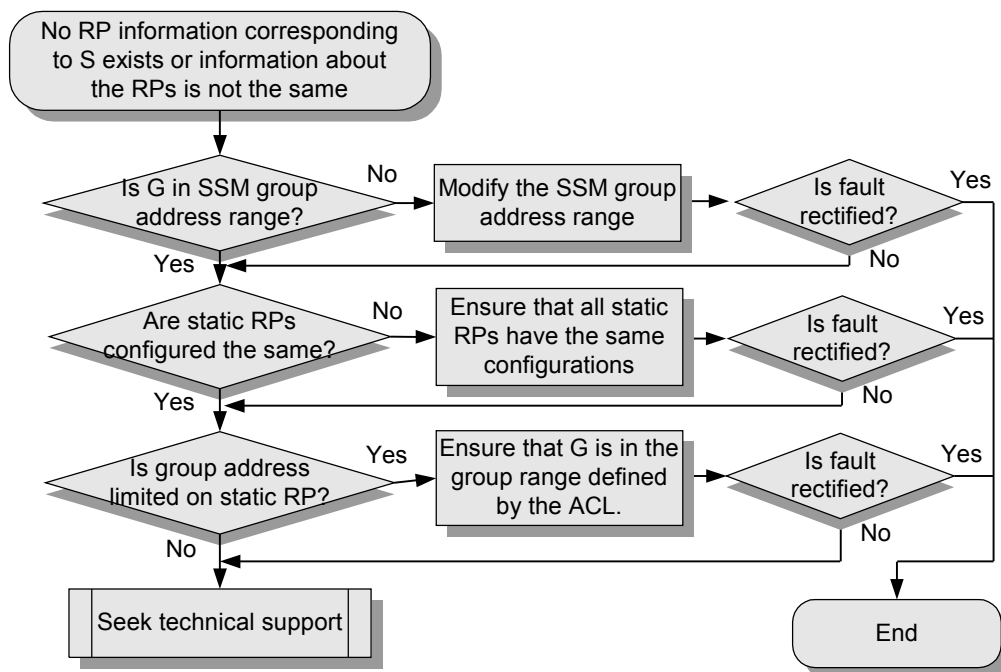
3.7.3 Troubleshooting Flowchart

On a PIM-SM network, only a static RP is configured. Run the **display pim rp-info** command on each S9300 to check the information about the RPs to which multicast groups correspond.

You can find that certain S9300s do not have information about the RP to which G corresponds, or information about RPs to which G corresponds is different.

Locate the fault as shown in [Figure 3-12](#).

Figure 3-12 Static RP troubleshooting flowchart



3.7.4 Troubleshooting Procedure

Procedure

Step 1 Check whether G is in the SSM group address range.

Groups in the SSM group address range adopt the SSM model but PIM-SM does not maintain the RPs to which they correspond.

Run the **display current-configuration configuration pim** command on the S9300 to check the current configuration in the PIM view. If the command output contains the **ssm-policy basic-acl-number** command, it indicates that the SSM group address range is adjusted on the S9300.

Run the **display current-configuration configuration acl-basic** command to check the configuration of the ACL. If the command output indicates that the group range defined by the ACL contains G, modify the configuration to ensure that the SSM group address range on all S9300s are the same.

Step 2 Check whether the configurations of static RPs on all the S9300s are the same.

Static RPs serve specific multicast groups. Multiple static RPs can exist on a network simultaneously, but information about static RPs on all S9300s must be the same. In this case, G is mapped to the same RP. If the configuration of the static RP on any S9300 in the network is different from others, the source registering or the setup of the RPT may fail.

Run the **display current-configuration** command on all S9300s to check whether the **static-rp rp-address [basic-acl-number] [preferred]** command is used on all the S9300s. If the command output indicates that information about the static RP on a S9300 is different from the information on the other S9300s, it is recommended that you run the **static-rp** command again.

Step 3 Check whether the group range is limited on a static RP.

If an ACL is specified in the **static-rp** command, run the **display current-configuration configuration acl-basic** command to check whether the group range defined by the ACL contains G. If not, modify the ACL configuration. Ensure that the ranges of groups served by static RPs are the same on all the S9300s.

If the fault persists, contact Huawei technical personnel.

----End

3.8 BSR-RP Troubleshooting

This section describes the procedure for BSR-RP troubleshooting.

[3.8.1 Typical Networking](#)

[3.8.2 Configuration Notes](#)

[3.8.3 Troubleshooting Flowchart](#)

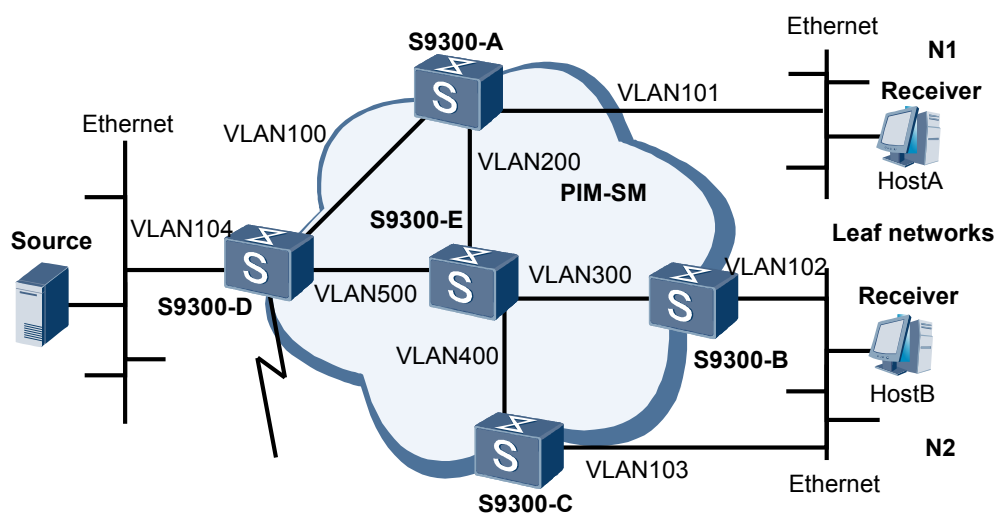
[3.8.4 Troubleshooting Procedure](#)

3.8.1 Typical Networking

Figure 3-13 shows a typical networking.

The following takes this networking to describe how to perform PIM-SM troubleshooting.

Figure 3-13 Typical networking of PIM-SM



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire network adopts a single BSR to administrate the PIM-SM domain. S9300-A is the C-BSR and the C-RP in the PIM-SM network.

Host A and Host B can receive multicast data from Source.

3.8.2 Configuration Notes

Different from a static RP, a BSR-RP usually need not be configured on all the S9300s. You can configure a C-RP only on one S9300 or on multiple S9300s.

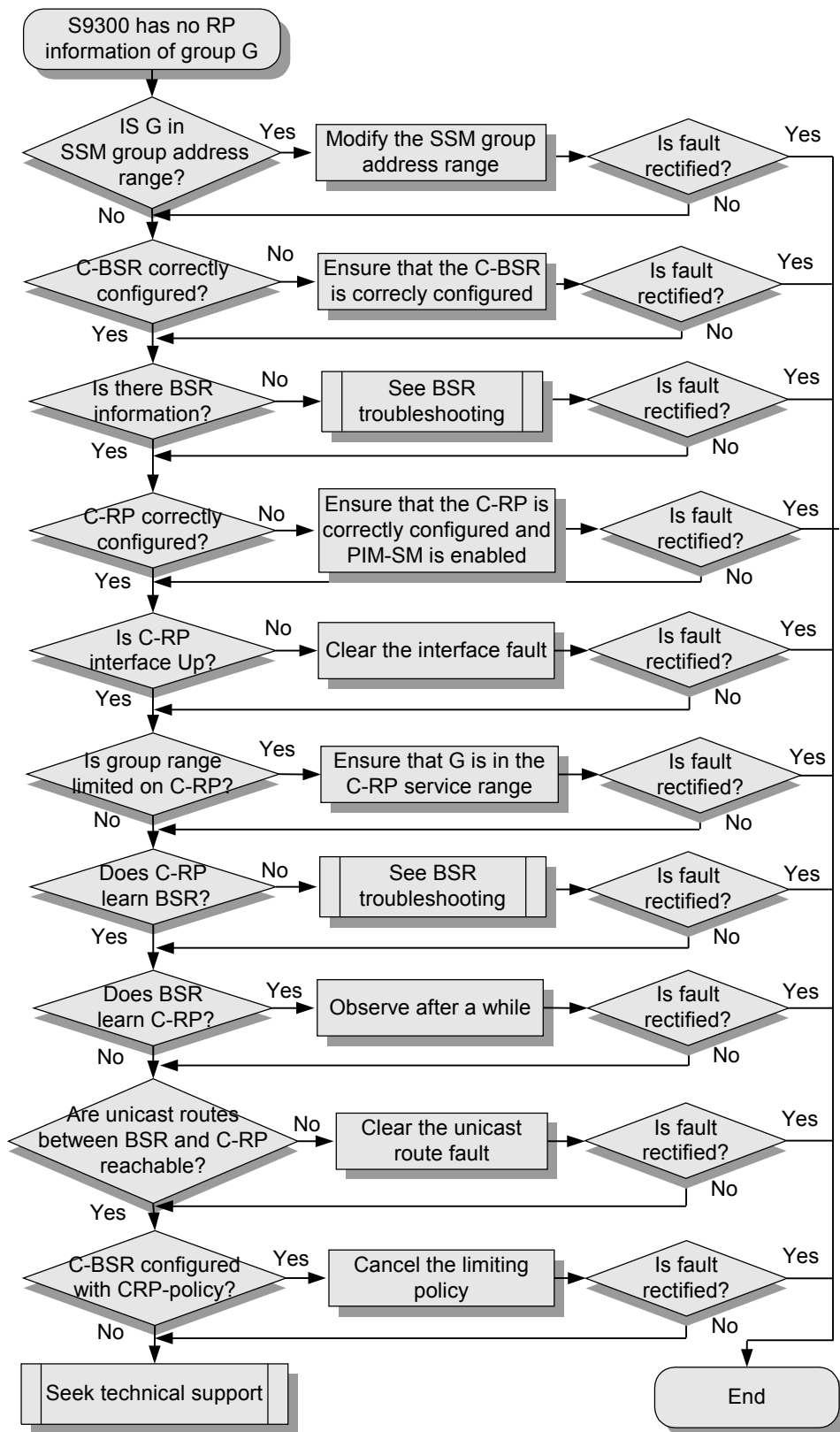
See [3.5.2 Configuration Notes](#).

3.8.3 Troubleshooting Flowchart

On a PIM-SM network, an S9300 does not have information about the RP corresponding to G.

[Figure 3-14](#) shows the troubleshooting flowchart.

Figure 3-14 BSR-RP troubleshooting flowchart



3.8.4 Troubleshooting Procedure

Procedure

Step 1 Check whether G is in the SSM group address range.

Groups in the SSM group address range adopt the SSM model but PIM-SM does not maintain the RPs to which they correspond.

Run the **display current-configuration configuration pim** command on the RP to which G corresponds to check the current configuration in the PIM view. If the command output contains the **ssm-policy basic-acl-number** command, it indicates that the SSM group address range is adjusted on the S9300.

Run the **display current-configuration configuration acl-basic** command to check the configuration of the ACL. If the command output indicates that the group range defined by the ACL contains G, modify the configuration to ensure that the SSM group address ranges on all S9300s are the same.

Step 2 Check whether a C-BSR is correctly configured on the network.

To check the current configuration in the PIM view, run the **display current-configuration configuration pim** command on the S9300 that tends to be a BSR. If the command output does not contain the **c-bsr** command, or the **c-bsr** command is not used correctly, reconfigure a C-BSR.

If the message "Info: Please enable PIM-SM on this interface to take effect" is displayed when the **c-bsr** command is used, it indicates that PIM-SM is not enabled on the C-BSR interface. Enable PIM-SM on the C-BSR interface, and then perform other BSR configurations.

Step 3 Check whether the S9300 without RP information learns BSR information.

To check whether the S9300 that has no RP information learns BSR information, run the **display pim bsr-info** command on the S9300. If the S9300 does not learn any BSR information, see [3.9 BSR Troubleshooting](#).

Step 4 Check whether a C-RP is configured correctly on the network.

Check the current configuration in the PIM view by using the **display current-configuration configuration pim** command on the S9300 that tends to be a C-RP. If the command output does not contain the **c-bsr** command or the **c-bsr** command is not used correctly, reconfigure a C-BSR.

If the message "Info: Please enable PIM-SM on this interface to take effect" is displayed when the **c-bsr** command is used, it indicates that PIM-SM is not enabled on the C-RP interface. Enable PIM-SM on the C-BSR interface, and then perform other C-RP configurations.

Step 5 Check whether the C-RP interface is Up.

Run the **display interface** command on the C-RP to check whether the C-RP interface is Up.

Step 6 Check whether the group range is limited on the C-RP.

If **group-policy basic-acl-number** is set in the **c-rp** command in [Step 3](#), it indicates that the range of groups that the C-RP serves is limited when the C-RP is configured.

Run the **display current-configuration configuration acl-basic** command to check the ACL configuration. If the command output indicates that G is not within the group range defined by the ACL, modify the ACL configuration.

Step 7 Check whether the C-RP learns BSR information.

Run the **display pim bsr-info** command to check whether the C-RP learns BSR information. If no BSR information is learned, see [3.9 BSR Troubleshooting](#).

Step 8 Check whether the BSR learns C-RP information.

Run the **display pim rp-info** command to check whether the BSR learns the C-RP information.

If BSR information is learned, it is spread over the entire network after a certain period.

Step 9 Check whether a route between the BSR and the C-RP is available and whether they can ping each other.

If the BSR and all C-RPs do not have any unicast route to each other, the BSR cannot send Bootstrap messages containing the integrated RP-set to the entire network.

- If the C-RPs do not have a unicast route to the BSR, the C-RPs cannot send Advertisement messages to the BSR in unicast mode. The BSR, therefore, cannot receive the integrated RP-set.
- If the BSR does not have a unicast route to a certain C-BSR, the BSR discards the Advertisement message received from the C-RP.

Run the **display ip routing-table** command on the BSR and the C-RP to check whether routes between them are available and whether they can ping each other.

If unicast routes are unreachable, check the unicast configuration.

Step 10 Check whether the **crp-policy** is used on the C-BSR.

Run the **display current-configuration configuration pim** command on the C-BSR to check the current configuration in the PIM view.

If the command output contains the **crp-policy acl-number** command, it indicates that the range of legal C-RPs and the range of groups that the C-RP serves are limited on the C-BSR.

Run the **display current-configuration configuration acl-adv** command to check the ACL configuration. If the command output indicates that G or the C-RP is not in the group range defined by the ACL, cancel the current configuration for reconfiguring the ACL filtering rules.

If the fault persists, contact Huawei technical personnel.

---End

3.9 BSR Troubleshooting

This section describes the procedure for BSR troubleshooting.

[3.9.1 Typical Networking](#)

[3.9.2 Configuration Notes](#)

[3.9.3 Troubleshooting Flowchart](#)

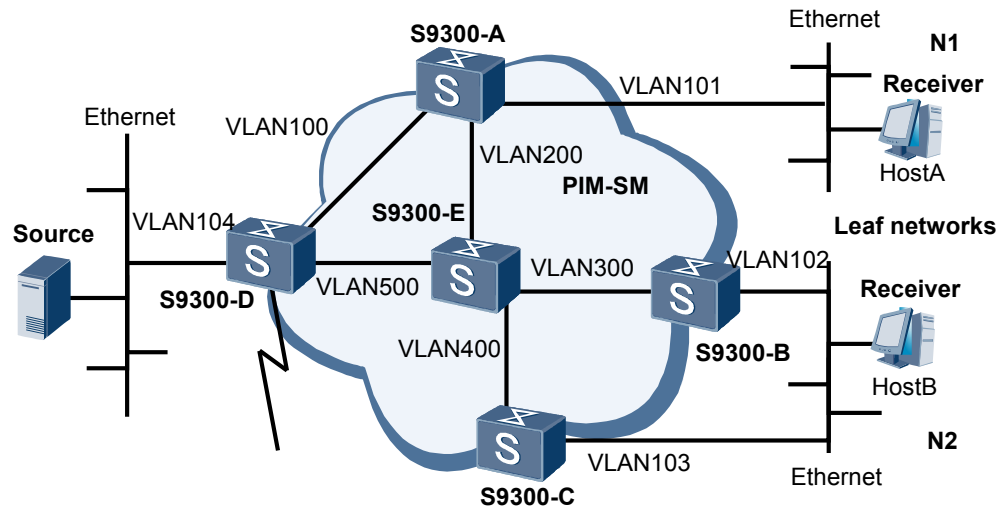
[3.9.4 Troubleshooting Procedure](#)

3.9.1 Typical Networking

Figure 3-15 shows a typical networking.

The following takes this networking to describe how to perform PIM-SM troubleshooting.

Figure 3-15 Typical networking of PIM-SM



In the networking,

- Receivers receive VOD information in multicast mode. The multicast source is Source.
- Receiver clusters of different organizations constitute leaf networks. Host A and Host B are the receivers of the multicast information on the two leaf networks.
- S9300-D is connected to the network where Source resides.
- S9300-A is connected to leaf network N1.
- S9300-B and S9300-C are connected to leaf network N2.
- The entire network adopts a single BSR to administrate the PIM-SM domain. S9300-A is the C-BSR and the C-RP in the PIM-SM network.

Host A and Host B can receive multicast data from Source.

3.9.2 Configuration Notes

NOTE

- The physical interfaces on the S9300 are Layer 2 interfaces. To use Layer 3 multicast protocols, you need to add interfaces to a VLAN and configure Layer 3 multicast protocols on VLANIF interfaces.
- On the S9300, PIM can be configured only on VLANIF interfaces and loopback interfaces. Generally, PIM is not used on loopback interfaces.

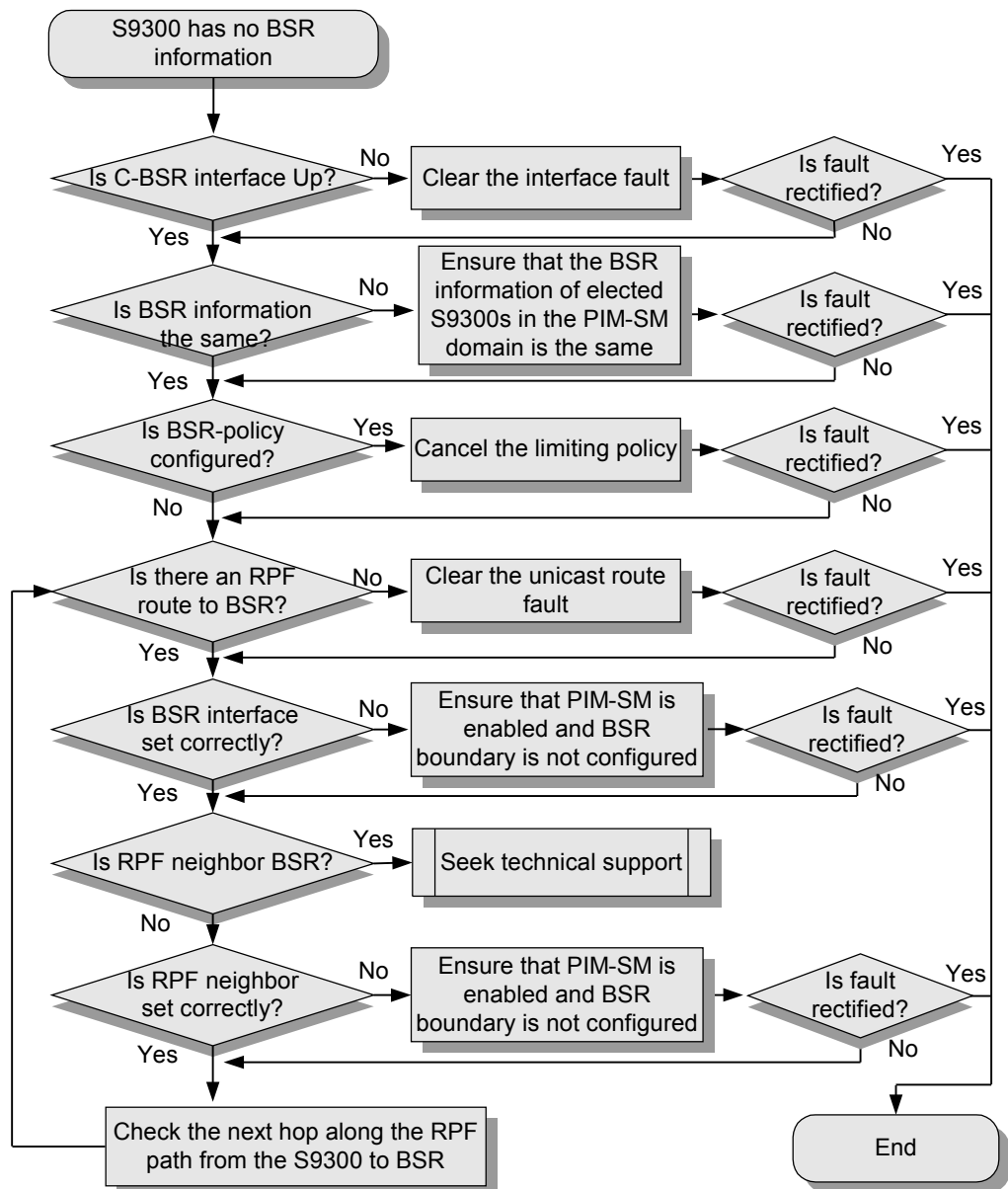
Item	Sub-item	Configuration Notes and Commands
Configuring PIM-SM	Configuring unicast routes	In PIM-SM, the RPF check is performed on the multicast source, RP, and BSR. Ensure that the unicast routes to those destinations are reachable. Ensure that all the C-RPs and BSRs can communicate in unicast mode when the BSR mechanism is applied.
	Enabling IP multicast	Multicast configuration takes effect only after the multicast function is enabled. To enable IP multicast, run the multicast routing-enable command in the system view.
	Enabling PIM-SM	PIM-SM must be enabled on the interfaces through which S9300s are connected, the interfaces through which S9300s are directly connected to the source, and the interfaces through which S9300s are connected to hosts. To enable PIM-SM, run the pim sm command in the interface view.
	Configuring an RP	When applying a static RP, ensure that the static-rp command is used on all S9300s on the network. Configure a C-BSR and C-RP when applying the BSR mechanism. To configure an RP, run the static-rp , c-br , and c-rp commands in the PIM view.
	Configuring the SPT switchover	By default, the DR at the member side and the RP immediately trigger the SPT switchover after they receive the first multicast packet. <ul style="list-style-type: none"> • If traffic-rate is set, the SPT switchover is triggered when the forwarding rate of an (S, G) entry is higher than the value of traffic-rate. • If the infinity command is used, the SPT switchover is not triggered any longer. To configure the SPT switchover, run the spt-switch-threshold command in the PIM view.
	Configuring the SSM group address range	The same ssm-policy command is used on all the S9300s on a network. ASM is applicable to all multicast groups that are excluded from the SSM group address range. By default, the SSM group address range is from 232.0.0.0 to 8. To configure the SSM group address range, run the ssm-policy command in the PIM view.
	Configuring IGMP	The S9300 directly connected to hosts must run IGMP. To configure IGMP, run the igmp enable command in the interface view.

3.9.3 Troubleshooting Flowchart

On a PIM-SM network, S9300s do not have any BSR information after the configuration on each S9300 is complete.

Figure 3-16 shows the troubleshooting flowchart.

Figure 3-16 BSR troubleshooting flowchart



3.9.4 Troubleshooting Procedure

Procedure

Step 1 Check whether the C-BSR interface is Up.

Run the **display interface** command on the C-BSR interface to check whether the C-BSR interface is Up.

Step 2 Check whether BSR information is the same.

Run the **display pim bsr-info** command on all the S9300s to check BSR information. Check whether the information about the BSR on the S9300s is the same in the same PIM-SM domain.

Step 3 Check whether the **bsr-policy** is used.

On the S9300 where there is no BSR information, run the **display current-configuration configuration pim** command to check the current configuration in the PIM view.

If the command output contains the **bsr-policy acl-number** command, the legal BSR address range is limited on the S9300.

Check the ACL configuration by using the **display current-configuration configuration acl-basic** command. If the command output indicates that the BSR is not within the range defined by the ACL, it is recommended that you reconfigure the ACL filtering rule or cancel the current configuration.

Step 4 Check whether there is an RPF path to the BSR.

Run the **display multicast rpf-info bsr-address** command on the current S9300 to check whether there is an RPF route to the BSR.

Run the **ping** command on the current S9300 and the BSR to check whether they can ping each other. If the ping operation fails, check the unicast configuration on the network.

Step 5 Check whether the RPF interface is configured correctly.

Run the **display current-configuration** command on the current S9300 to check the configuration of the RPF interface from which the BSR is reachable.

- If the command output does not contain the **pim sm** command, run the **pim sm** command on the interface to enable PIM-SM.
- If the command output contains the **pim bsr-boundary** command, it indicates that the BSR boundary is configured on the interface. It is recommended that you cancel the current configuration or review the network planning.
- If the command output contains the **multicast boundary** command, it indicates that the multicast boundary is configured on the interface. It is recommended that you cancel the current configuration or review the network planning.

Step 6 Check whether the RPF neighbor interface is configured correctly.

On the RPF neighbor to the BSR, run the **display current-configuration** command to check the configuration of the RPF neighbor interface.

- If the command output does not contain the **pim sm** command, run the **pim sm** command on the interface to enable PIM-SM.
- If the command output contains the **pim bsr-boundary** command, it indicates that the BSR boundary is configured on the interface. It is recommended to cancel the current configuration or the review the network planning.

- If the command output contains the **multicast boundary** command, it indicates that the multicast boundary is configured on the interface. It is recommended that you cancel the current configuration or review the network planning.

If the fault persists, contact Huawei technical personnel.

----End

3.10 PIM BFD Troubleshooting

This section describes the procedure for PIM BFD troubleshooting.

3.10.1 Typical Networking

3.10.2 Configuration Notes

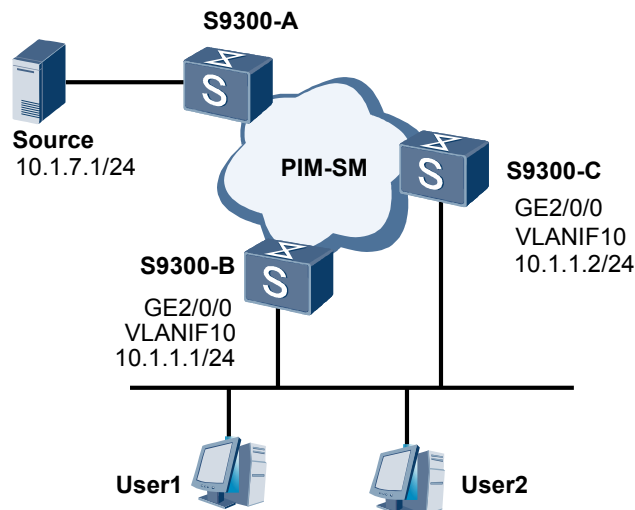
3.10.3 Troubleshooting Flowchart

3.10.4 Troubleshooting Procedure

3.10.1 Typical Networking

Figure 3-17 shows a typical networking of PIM BFD. The PIM BFD troubleshooting is based on this network.

Figure 3-17 Typical networking diagram of PIM BFD



In this networking,

- IPv4 PIM-SM is enabled on each S9300 on the network.
- PIM BFD is enabled on the interface connected to the user network segment.

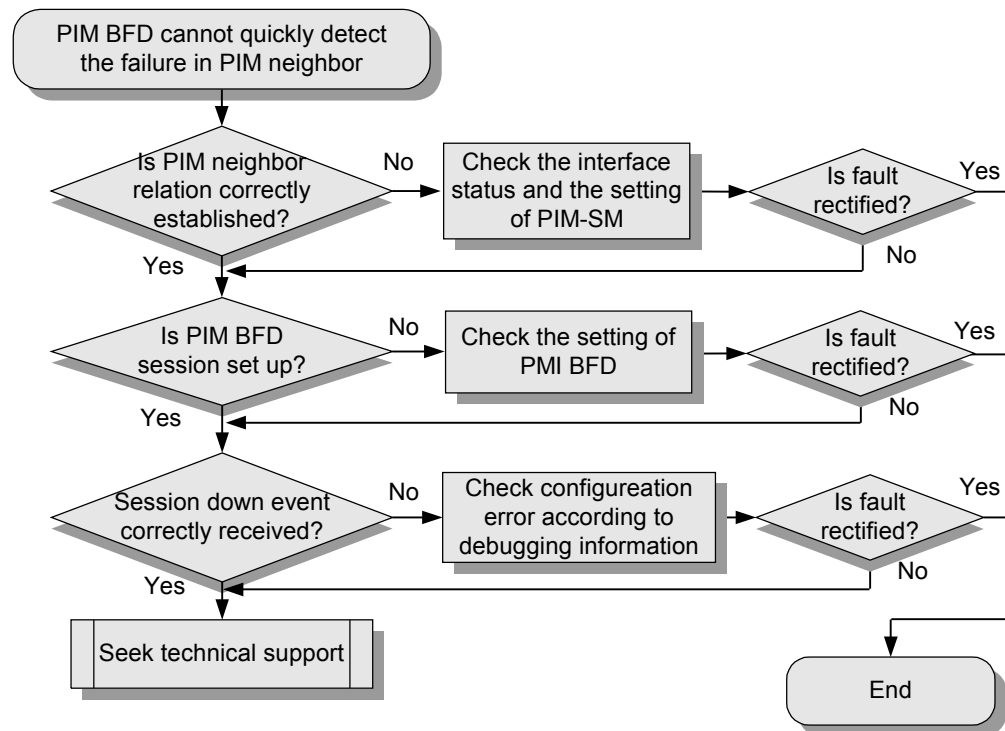
3.10.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring PIM BFD	Enabling PIM-SM	Only PIM-SM supports PIM BFD. PIM-DM does not support PIM BFD. To configure PIM-SM, run the pim sm command in the interface view.
	Configuring BFD	PIM BFD depends on BFD. If global BFD is not enabled, the status of the PIM BFD session is Down. To configure BFD, run the bfd command in the system view.
	Enabling PIM BFD	PIM BFD needs to be enabled on the interfaces at both ends of a link. To configure PIM BFD, run the pim bfd enable command in the interface view.
	Setting the parameters of a PIM BFD session	The PIM BFD session parameters are negotiated by the PIM neighbors. To set parameters of a PIM BFD session, run the pim bfd { min-tx-interval tx-value min-rx-interval rx-value detect-multiplier multiplier-value } * command in the interface view.

3.10.3 Troubleshooting Flowchart

As shown in "Typical networking diagram of PIM BFD" in [3.10.1 Typical Networking](#), a DR interface fails but the fault is not detected by the PIM BFD session between the PIM neighbor interface and the DR interface until the PIM neighbor times out.

[Figure 3-18](#) shows the troubleshooting flowchart.

Figure 3-18 PIM BFD troubleshooting flowchart

3.10.4 Troubleshooting Procedure

Procedure

Step 1 Check whether the PIM neighbor relation is set up between two S9300s.

Run the **display pim neighbor** command on the two S9300s. If the command output does not contain any information about the peer, do as follows:

- Check whether the interface status is Up.
- Check whether the IP addresses of the interfaces can be pinged.
- Check whether PIM-SM is enabled on the interfaces.
- Check whether the neighbor often times out because an improper pim hello option is configured on the interfaces.

Step 2 Check whether a PIM BFD session is established on the neighbor.

Run the **display pim bfd session** command on the two S9300s.

- If the PIM BFD session for the neighbor does not exist, check whether the **pim bfd enable** command is used on the interfaces.
- If the **pim bfd enable** command is used on the interfaces, run the **debugging pim bfd create** command. Run the **shutdown** command on the interfaces and then run the **undo shutdown** command on the interfaces. Check the debugging information after the PIM

neighbor relation is established between the interfaces. Check whether the PIM BFD session can be set up correctly at the same time.

- If the PIM BFD session for the neighbor exists but the session status is not Up, check whether the S9300 is enabled with global BFD.

Step 3 Check whether the neighbor can receive the session Down event correctly.

- Run the **debugging pim bfd event** command, and then run the **shutdown** command on the neighbor interface. Check the debugging information after the neighbor relation is interrupted. Check whether the session Down event can be received correctly.
- Check the configuration error on the S9300 according to the debugging information.

If the fault persists, contact Huawei technical personnel.

---End

3.11 FAQs

This section lists frequently asked questions and their answers.

Q: What Are the Basic Requirements for Constructing the Network That Needs to Be Configured with PIM?

A: The IP addresses of devices must be configured properly.

- The source address and the address of the interface on the S9300 directly connected to the source must be on the same network segment. If the mask lengths of the two addresses are different, the mask length of the S9300 is taken as the standard.
- The address of a host and the address of the interface on the S9300 directly connected to the host must be on the same network segment. If the mask lengths of the two addresses are different, the mask length of the S9300 is taken as the standard.

Q: Which Interface Need to Be Configured with PIM When PIM Is Configured on the Network?

A: All the RPF interfaces and RPF neighbors need to be enabled with PIM.

An S9300 always performs the RPF check before creating a forwarding entry. The S9300 finds out the optimal route to the object of the RPF check in the current unicast routing table. The outgoing interface of the optimal route functions as the RPF interface, and the next hop interface functions as the RPF neighbor. The multicast forwarding entry can be created only after PIM is enabled on the RPF interface and the RPF neighbor. A multicast distribution tree (MDT) is thus set up along the forwarding path.

Generally, the object of the RPF check is the multicast source. In PIM-SM, the object also includes the RP and the BSR.

The RPF interface and the RPF neighbor are dependent on the current unicast routes, but are independent of PIM.

It is recommended that you enable PIM on all the non-boundary interfaces in the PIM domain. Thus, no RPF interface or RPF neighbor is ignored.

The following interfaces are easily ignored:

- Interface directly connected to the source: When the RPF check aiming at the source is performed on the S9300 directly connected to the multicast source, the RPF interface is the interface connected to the multicast source.
- Interface connected to hosts: If PIM is not enabled on the interface, the interface cannot be added to the downstream interface list of the PIM routing entry. Before configuring the interface, enable PIM, and then enable IGMP.
- PIM-SM interfaces that act as C-BSRs and C-RPs.

Q: Can a PIM Domain Run PIM-DM and PIM-SM Simultaneously?

A: A PIM domain cannot run PIM-DM and PIM-SM simultaneously. If the RPF interface and the RPF neighbor are enabled with PIM of different modes, forwarding entries cannot be created correctly.

In PIM, a Hello message does not carry information about the PIM mode. The S9300 running PIM does not know the mode of PIM running on its neighbor.

If the modes of PIM enabled on the RPF interface and the RPF neighbor are different, PIM routing information cannot be exchanged. Forwarding entries cannot be set up correctly, and multicast communication thus fails.

When deploying a multicast network, configure PIM of the same mode on all the non-boundary interfaces.

Q: Why Must Unicast Routes Be Reachable Before Multicast Is Configured on the Network?

A: The multicast module on an S9300 does not maintain unicast routing information on the network. Before creating PIM routing entries, the S9300 performs the RPF check according to current routing information. If the unicast route to a certain destination does not exist, the RPF check fails.

- The reachable unicast route to the source is the prerequisite of setting up an SPT.
- The reachable unicast route to the RP is the prerequisite of source registering and the setup of an RPT.
- If a BSR is adopted on the PIM-SM network, the reachable unicast route to the BSR is the prerequisite of obtaining RP information.

Q: How Does an S9300 Running PIM-SM Perform the RPF Check During the Setup of an RPT?

A: The DR at the receiver side first performs the RPF check. The DR searches for the unicast route to the RP. The outgoing interface of the unicast route is the upstream interface and the next hop is the RPF neighbor. The DR then sends a Join message to the RPF neighbor. After receiving the Join message, the upstream S9300 performs the RPF check and continues to send the packet upstream. The Join message is thus sent to the RP hop by hop.

In the preceding process, if any S9300 on the path does not have a route to the RP, the RPT cannot be set up.

Why No (S, G) Entry Is Created in the PIM Routing Table When an Interface Receive Multicast Data?

A: The possible causes are:

- The **multicast boundary** command is used on the interface.
The **multicast boundary** *group-address* { *mask* | *mask-length* } command is used to configure the interface as the forwarding boundary of a specified multicast group. When receiving a packet for the group, the interface discards the packet and does not create any forwarding entry.
Solution: Run the **display current-configuration interface** *interface-type interface-number* command on the current S9300 to check the configuration of the interface. If the command output contains the **multicast boundary** command, it indicates that the multicast boundary is configured on the interface. It is recommended that you cancel the current configuration or review the network planning.
- On the S9300, the **source-policy** command is used in the PIM view.
After the **source-policy** *acl-number* command is used, the S9300 checks a received packet according to specified ACL rules. If the source address of the packet is not within the range defined by the ACL, the S9300 discards the packet and does not create any forwarding entry.
Solution: run the **display current-configuration configuration pim** command in the system view to check the current configuration in the PIM view. If the command output contains the **source-policy** *acl-number* command, it indicates that filtering rules based on sources are configured. It is recommended that you cancel the current configuration or reconfigure proper ACL rules.

Q: The Static RP and the Dynamic RP Are Configured. Why Is Multicast on the S9300 Configured with the Preferred Static RP Unavailable?

A: The static RP cannot respond to the change of the dynamic RP. When the dynamic RP changes, RP information on the S9300 configured with the preferred static RP is different from the information on the other S9300s.

For example, on the PIM-SM network:

- C-RP-A and C-RP-B are configured to serve all the groups.
- C-RP-A has the highest priority and is elected as RP.
- S9300-C configured with the preferred static RP is added to the network.
- The address of the static RP is configured to C-RP-A.

Due to a certain cause, C-RP-A cannot function as the dynamic RP. The C-RP-B replaces C-RP-A and acts as the dynamic RP. As a result, RP information on the S9300 configured with the preferred static RP is different from the information on the other S9300s. Multicast on the S9300 is unavailable.

To rectify the fault, do as follows:

- Adjust the configuration of the static RP on the S9300 to keep it same as the configuration on the dynamic RP.
- Cancel the preferred static RP and ensure that the configuration of RP static on all the S9300s is the same.

3.12 Diagnostic Tools

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

3.12.1 display Commands

3.12.2 debugging Commands

3.12.1 display Commands

Command	Description
display pim interface	Displays information about PIM interfaces.
display pim neighbor	Displays information about the PIM neighbors.
display pim routing-table	Displays the contents of the PIM multicast routing table.
display pim bsr-info	Displays information about the learned BSR, including the address, priority, and status of the BSR.
display pim rp-info	Displays information about the static RP and dynamic RP to which a multicast group corresponds.
display multicast routing-table	Displays multicast routing information, including routing entries and outgoing interfaces.
display multicast forwarding-table	Displays information about the multicast forwarding table.
display multicast rpf-info	Displays the RPF routing information about a specified multicast source.
display version	Displays the version of the S9300.
display current-configuration	Displays the current configuration of an S9300.
display ip routing-table	Displays unicast routes learned by an S9300.
display igmp group	Displays information about IGMP groups.
display igmp routing-table	Displays IGMP routing information.
display igmp interface	Displays information about IGMP interfaces, including the version and querier.

3.12.2 debugging Commands

Command	Description
debugging pim all	Enables all the debugging of PIM.
debugging pim assert	Enables the debugging of PIM assert.
debugging pim event	Enables the debugging of PIM events.
debugging pim join-prune	Enables the debugging of PIM Join or Prune messages.
debugging pim msdp	Enables the debugging of PIM MSDP.
debugging pim neighbor	Enables the debugging of PIM neighbors.
debugging pim register	Enables the debugging of PIM source registering.
debugging pim routing-table	Enables the debugging of a PIM multicast routing table.
debugging pim rp	Enables the debugging of a PIM RP.
debugging pim state-refresh	Enables the debugging of PIM State Refresh.
debugging pim bfd all	Enables all the debugging of PIM BFD.
debugging pim bfd create	Enables the debugging of PIM BFD session creating.
debugging pim bfd delete	Enables the debugging of PIM BFD session deleting.
debugging pim bfd event	Enables the debugging of PIM BFD events.

4 MSDP Troubleshooting

About This Chapter

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

[4.1 Overview of MSDP](#)

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

[4.2 MSDP Troubleshooting](#)

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

[4.3 Troubleshooting Cases](#)

This section presents several troubleshooting cases.

[4.4 FAQs](#)

This section lists frequently asked questions and their answers.

[4.5 Diagnostic Tools](#)

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

4.1 Overview of MSDP

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

The Multicast Source Discovery Protocol (MSDP) is used to transmit source information among multiple Rendezvous Points (RPs), which is not limited by the Protocol Independent Multicast Sparse Mode (PIM-SM) domains. The RP configured with an MSDP peer advertises information about active sources that register with the local RP to the remote MSDP peer through Source Active (SA) messages. SA messages are forwarded between MSDP peers. The source information is thus shared among multiple RPs.

4.2 MSDP Troubleshooting

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

[4.2.1 Typical Networking](#)

[4.2.2 Configuration Notes](#)

[4.2.3 Troubleshooting Flowchart](#)

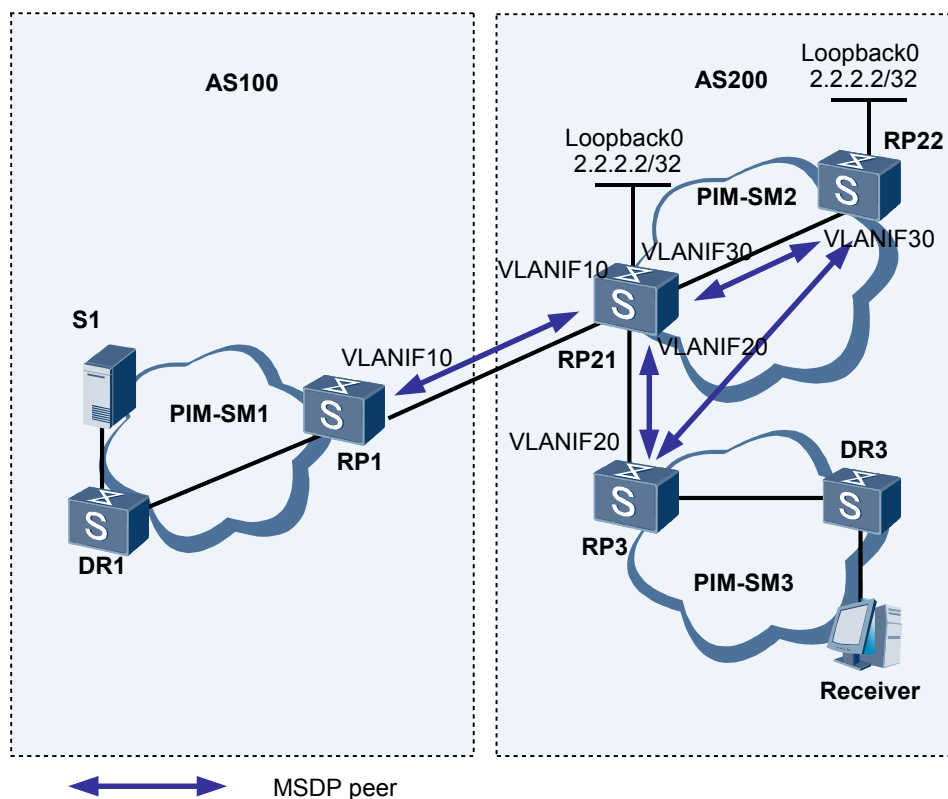
[4.2.4 Troubleshooting Procedure](#)

4.2.1 Typical Networking

Figure 4-1 shows a typical MSDP networking.

The MSDP troubleshooting is based on this network.

Figure 4-1 Typical MSDP networking



In the networking,

- The ISP maintains two ASs, that is, AS 100 and AS 200. The S9300s in the same AS are interconnected through OSPF. S9300s between ASs exchange routing information through EBGP.
- Each AS contains at least one PIM-SM domain. Each PIM-SM domain contains only one BSR, and zero or one multicast source or receiver.
- An anycast RP is configured in PIM-SM2 domain.
- MSDP peer relations are set up between RPs in each PIM-SM domain. All MSDP peers in AS 200 join the same mesh group. Inter-AS MSDP peers and EBGP peers have the same interface address.

The receivers in AS 200 can receive multicast data from the source in AS 100.

4.2.2 Configuration Notes

Item	Sub-item	Configuration Notes and Commands
Configuring an MSDP peer	Configuring PIM-SM	The multicast routing protocol within the domain must be PIM-SM. To configure PIM-SM, run the pim sm command in the interface view.

Item	Sub-item	Configuration Notes and Commands
	Configuring an RP	<p>The MSDP peer that generates MSDP messages must be the RP with which the source registers. It is recommended that you configure the MSDP peer relation only on the RPs (including static RPs and C-RPs) on the network.</p> <p>To configure an RP, run the c-rp or static-rp command in the PIM view.</p>
	Configuring an anycast RP	<p>Multiple loopback interfaces with the same IP address are configured in a PIM-SM domain. The interface is configured as the RP that serves multicast groups in the same range. The MSDP peers are set up between the S9300s.</p> <p>The MSDP peer and the RP cannot be configured on the same interface. The BSR and the RP cannot be configured on the same interface. A logical RP address must be specified for an SA message. The interface address of an MSDP peer is recommended.</p> <p>To configure an anycast RP, run the c-rp command in the PIM view and run the originating-rp interface-type interface-number command in the MSDP view.</p>
	Configuring a mesh group	<p>The MSDP peer relation must be set up between members of the same mesh group. It is recommended that you add all MSDP peers in the same AS to the same mesh group.</p> <p>To configure a mesh group, run the peer peer-address mesh-group name command in the MSDP view.</p>
	Configuring a BGP peer or an MBGP peer	<p>EBGP routes must exist between inter-AS MSDP peers; otherwise, SA messages cannot pass the RPF check. It is recommended that you set up MBGP peer relations between inter-AS MSDP peers. The addresses of the MSDP peers are the same as those of the MBGP peers.</p> <p>To configure a BGP peer or an MBGP peer, run the peer {group-name peer-address} enable command in the BGP-IPv4 multicast address family view.</p>
	Configuring a static RPF peer	<p>The RPF check is unnecessary for the SA messages sent by a static RPF peer. If two inter-AS MSDP peers consider each other as a static RPF peer, the BGP or MBGP peer relation does not need to be set up between the two MSDP peers.</p> <p>To configure a static RPF peer, run the static-rpf-peer command in the MSDP view.</p>

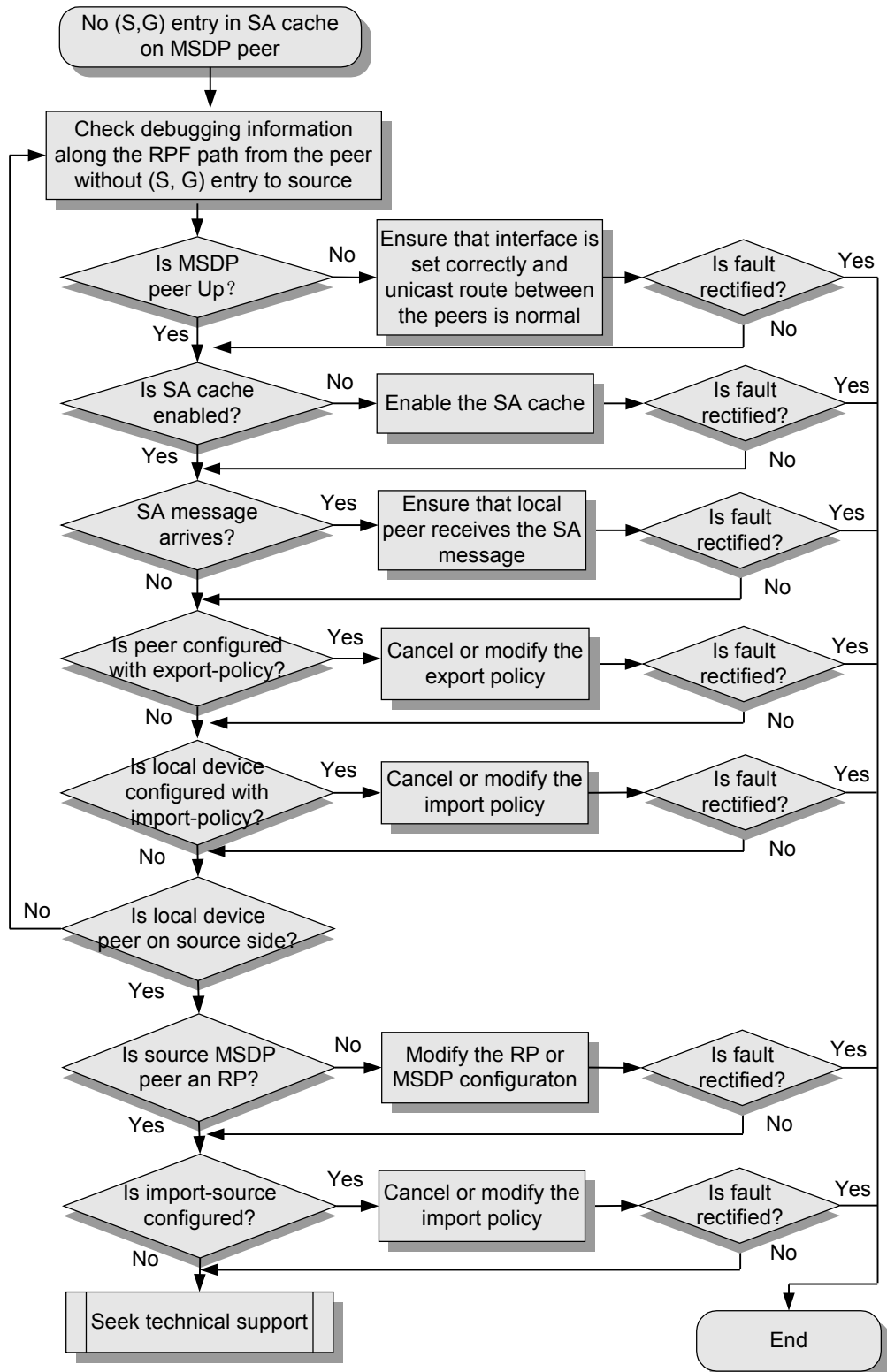
Item	Sub-item	Configuration Notes and Commands
	Configuring an import policy	<p>On the local MSDP peer, run the peer sa-policy import command to control the receiving of SA messages. If the command is used incorrectly, the received SA messages may be ignored.</p> <p>To configure an import policy, run the peer sa-policy import command in the MSDP view.</p>
	Configuring an export policy	<p>On the remote MSDP peer, run the peer sa-policy export command to control the forwarding of SA messages. If the command is used incorrectly, the SA messages may be not forwarded.</p> <p>To configure an export policy, run the peer sa-policy export command in the MSDP view.</p>
	Creating the policy for creating SA messages	<p>On the source MSDP peer, run the import-source command to control the creation of SA messages. If the command is used incorrectly, certain (S, G) entries may not be advertised.</p> <p>To create the policy for creating SA messages, run the import-source [acl acl-number] command in the MSDP view.</p>

4.2.3 Troubleshooting Flowchart

On the network shown in "Typical MSDP networking" in [4.2.1 Typical Networking](#), after the **display msdp sa-cache** command is used on the S9300 configured with an MSDP peer, no (S, G) entry exists in the SA cache.

[Figure 4-2](#) shows the troubleshooting flowchart.

Figure 4-2 MSDP troubleshooting flowchart



4.2.4 Troubleshooting Procedure

Context

Before locating the MSDP fault, clear the PIM-SM fault. For details on PIM-SM troubleshooting, see [3 PIM Troubleshooting](#). To troubleshoot the MSDP fault, you must perform the operations from [Step 1](#) to [Step 4](#) on the MSDP peers along the RPF path to the multicast source S, beginning from the MSDP peer that does not have an (S, G) entry in the SA cache and ending at the MSDP peer nearest to S. If the S9300 nearest to S is an MSDP peer, perform the operations in [Step 5](#) and [Step 6](#).

Procedure

Step 1 Check that all the MSDP peers are Up.

Run the **display msdp brief** command on the S9300 configured with an MSDP peer to check whether the MSDP peer is Up. If the peer is Down, perform the following:

- Check whether the interface of the MSDP peer is configured correctly.
- Check whether the unicast routes between the peers are reachable.

Step 2 Check that the SA cache is enabled.

Run the **display current-configuration configuration msdp** command on the S9300 configured with an MSDP peer to check the current configuration in the MSDP view.

If the command output contains the **undo cache-sa-enable** command, it indicates that the SA cache is disabled.

Run the **cache-sa-enable** command to enable the SA cache in the MSDP view.

Step 3 Check whether there is an SA message sent by a peer.

Run the **debugging msdp all** command to view the debugging of MSDP. Check whether there is an SA message sent by a peer.

If there is an SA message sent by a peer but the message does not pass the RPF check, the message is discarded. To make the RPF check successful, you can modify MBGP, BGP, and multicast static routes, or configure a static MSDP peer.

Step 4 Check whether the remote MSDP peer is configured with the export policy.

If the MSDP debugging information indicates that no SA message is received from the MSDP peer, run the **display current-configuration configuration msdp** command on the remote peer to check the current configuration in the MSDP view.

- If the command output contains the **peer peer-address sa-policy export** command, it indicates that the remote peer does not forward any SA message to the local peer.
- If the command output contains the **peer peer-address sa-policy export acl acl-number** command, it indicates that the remote peer forwards only the (S, G) entry matching the ACL. It is recommended that you check whether the S9300 is configured with an ACL and whether the (S, G) entry matches the ACL.

It is recommended that you delete the **peer sa-policy export** command or change the ACL rules specified in the command.

Step 5 Check whether the local device is configured with the import policy.

If there is an SA message sent by a peer but the message does not match the locally configured import policy, the message is discarded. In this case, run the **display current-configuration configuration msdp** command in the MSDP view to check the current configuration.

- If the command output contains the **peer peer-address sa-policy import** command, it indicates that the MSDP peer does not receive any (S, A) message.
- If the command output contains the **peer peer-address sa-policy import acl acl-number** command, it indicates that the MSDP peer receives only the (S, G) entry matching the ACL. It is recommended that you check whether the S9300 is configured with an ACL and whether the (S, G) entry matches the ACL.

It is recommended that you delete the **peer sa-policy import** command or change the ACL rules specified in the command.

Step 6 Check whether the source MSDP peer is configured as an RP.

Check the information about the routing table by running the **display pim routing-table** command on the MSDP peer nearest to the source. If an (S, G) entry does not have a 2MSDP flag, it indicates that the MSDP peer is not an RP.

To ensure that the source MSDP peer is an RP, it is recommended that you adjust the PIM-SM network or change the MSDP configuration.

Step 7 Check whether the **import-source** command is used on the MSDP peer nearest to the source.

After the **import-source [acl acl-number]** command is used, MSDP can filter an (S, G) entry according to the source address in the entry when creating an SA message. MSDP can thus control the transmission of information about multicast sources. By default, an SA message advertises information about all the known sources.

Run the **display current-configuration configuration msdp** command on the MSDP peer nearest to the source to check the current configuration in the MSDP view.

- If the command output contains the **import-source** command, it indicates that the MSDP peer does not advertise any information about the local source.
- If the command output contains the **import-source acl acl-number** command, it indicates that the MSDP peer advertises only the (S, G) entry matching the ACL. It is recommended that you check whether the S9300 is configured with an ACL and whether the (S, G) entry matches the ACL.

It is recommended that you delete the **import-source** command or change the ACL rules specified in the command.

 **NOTE**

For more information about the commands used in the previous steps, see the "Multicast Commands" in the *Quidway S9300 Terabit Routing Switch Command Reference*.

If the fault persists, contact Huawei technical personnel.

----End

4.3 Troubleshooting Cases

This section presents several troubleshooting cases.

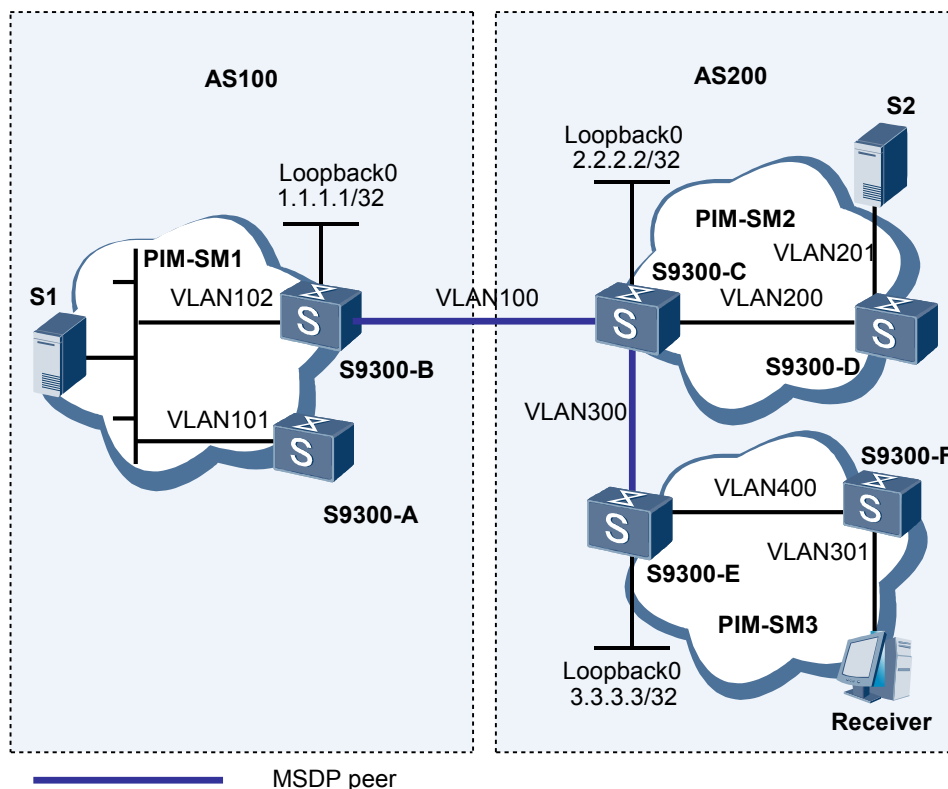
4.3.1 Hosts Cannot Receive Data from an Inter-AS Multicast Source

4.3.1 Hosts Cannot Receive Data from an Inter-AS Multicast Source

Fault Symptom

As shown in [Figure 4-3](#), users receive Video-On-Demand (VOD) information in the multicast mode.

Figure 4-3 Typical MSDP networking



Receivers in PIM-SM3 domain can receive data from S2, but cannot receive data from S1.

Fault Analysis

The fault may occur on an S9300 because receivers can receive data from S2. Do as follows to rectify the fault:

1. Run the **display pim routing-table** command on S9300-F to check routing entries. Only the (S2, G) entry is found but the (S1, G) entry is not found. In this case, the upstream S9300 does not have a multicast route.
2. Run the **display pim routing-table** command on S9300-E to check routing entries. Only the (S2, G) entry is found but the (S1, G) entry is not found.
3. Run the **display msdp sa-cache group-address source-address** command on S9300-E and specify the source address and the group address in the command. The (S1, G) entry does not exist in the SA Cache. The intra-AS MSDP peer does not send any (S1, G) information.

4. Run the **display msdp sa-cache group-address source-address** command on S9300-C. The (S1, G) entry is not found.
5. Run the **display msdp brief** command on S9300-C. The status of the MSDP peer relation between S9300-C and S9300-B is Up. Check whether S9300-C receives the SA message containing the (S1, G) entry or whether S9300-C receives the SA message but filter out the (S1, G) entry.
6. On S9300-C, run the **debugging msdp all** command to debug MSDP and to check whether S9300-C can receive SA messages correctly. S9300-C receives only the messages used to maintain the MSDP session relation but does not receive the required SA messages. Check whether S9300-B sends the required SA messages.
7. Run the **display current-configuration configuration msdp** command on S9300-B to check the MSDP configuration. There is no configuration except the configuration of an MSDP peer. That is, the **import-source** command is not used on S9300-B.
8. Run the **display pim rp-info** command on S9300-B. S9300-B is the RP of the required (S, G) entry.
9. Run the **display pim routing-table** command on S9300-B. The (S1, G) entry does not have a 2MSDP flag. As shown in the networking diagram, S9300-B is directly connected to the source. The interface through which S9300-B is directly connected to the source is not the DR of the network segment.
10. Run the **display pim interface** command on S9300-B. S9300-A rather than S9300-B is the DR directly connected to the network segment where the source resides. The DR priority of VLANIF 102 on S9300-B is 1. The fault is thus located.

Procedure

- Step 1** Run the **display pim interface** command on S9300-A. You can find that the DR priority of VLANIF 101 is 3.
- Step 2** Run the **system-view** command on S9300-B to enter the system view.
- Step 3** Run the **interface vlanif102** command on S9300-B to enter the VLANIF interface view.
- Step 4** Run the **pim hello-option dr-priority priority** command on S9300-B to change the DR priority of S9300-B to 5, which is greater than that of S9300-A.
- Step 5** Run the **display pim interface** command on S9300-B. You can find that the interface becomes a DR.
- Step 6** Return to the user view on S9300-B, and then run the **save** command to save the modification of the configuration.

After these configurations are complete, you can find that receivers can receive data from S1. The fault is thus rectified.

----End

Summary

When receiving a packet from the interface where an RP registers with the source and creating an (S, G) entry, the RP needs to label the (S, G) entry with a 2MSDP flag, indicating that the entry needs to be sent to other MSDP peers. If the RP is directly connected to the source, the RP must function as the DR on the network segment directly connected to the source. In this manner, the system labels the (S, G) entry with a 2MSDP flag and sends it to the MSDP peers.

4.4 FAQs

This section lists frequently asked questions and their answers.

Q: What Are the Requirements for Configuring an MSDP Peer?

A: The address of the local Connect-interface must be the same as the peer address of the remote peer.

- Through the **peer peer-address connect-interface interface-type interface-number** command, you can set up the MSDP peer relation between the local Connect-interface and the peer specified by the **peer peer-address** command.
- At the same time, perform the related configuration on the peer S9300. If the address of the local Connect-interface is different from the peer address of the remote S9300, the TCP connection cannot be set up.
- In addition, if there is no route between two MSDP peers, the TCP connection cannot be set up.

Q: Why Cannot an MSDP Peer Receive SA Messages?

A: After receiving an SA message from a peer, an S9300 needs to perform the RPF check on the message. If the RPF check fails, the S9300 discards the message, and does not cache the (S, G) entry contained in the SA message. Run the **debugging msdp all** command to check whether the S9300 receives an SA message.

The S9300 performs the RPF check according to the following sequence number until a matching rule is found.

Table 4-1 RPF rules of MSDP

No.	Matching Rule
1	When there is only one peer, the message passes the check.
2	When the peer is the source RP that generates SA messages, the message passes the check.
3	When the peer belongs to a mesh group, the message passes the check.
4	When the peer is a static peer, the message passes the check.
5	When MBGP is configured, either of the following situations occurs: <ul style="list-style-type: none"> • If the MSDP peer is an E-MBGP peer and the AS of the peer is the next AS to the RP, the message passes the check. • If the MSDP peer is an I-MBGP peer and the peer address is the next hop to the RP, the message passes the check. • If the MSDP peer is neither an E-MBGP peer nor an I-MBGP peer, and the AS of the peer is the next AS to the RP, the message passes the check.

No.	Matching Rule
6	When BGP is configured, either of the following situations occurs: <ul style="list-style-type: none"> • If the MSDP peer is an EBGP peer and the AS of the peer is the next AS to the RP, the message passes the check. • If the MSDP peer is an IBGP peer and the peer address is the next hop to the RP, the message passes the check. • If the MSDP peer is neither an EBGP peer nor an IBGP peer, and the AS of the peer is the next AS to the RP, the message passes the check.
7	When neither MBGP nor BGP is configured, the following situation occurs: If the route to the peer is learned from an IGP and the peer address is the next hop to RP, the message passes the check.

Q: MSDP Debugging Information Shows That the Local Node Receives an SA Message from a Peer. Why Is No Related (S, G) Entry Found in the SA Cache of the Local Node?

A: The possible cause is that the **peer peer-address sa-policy import [acl-number]** command is run on the local node, and the local node, therefore, ignores the received SA message.

After receiving an SA message from a peer, the local MSDP node matches the (S, G) entry carried in the SA message with the ACL number set in the **sa-policy import** command. If the matching is successful, the local node caches the (S, G) information and forwards the SA message. If the debugging information shows that the local node receives an SA message but there is no related (S, G) entry in the SA cache of the node, check whether the ACL parameter is set correctly.

Q: MSDP Debugging Information Shows That the Local Node Receives an SA Message from a Peer. Why Does the Local Node Not Forward the SA Message Out?

A: The possible cause is that the **peer peer-address sa-policy export [acl-number]** command is run on the local node. The local node, however, does not forward the SA message out.

After receiving an SA message from a peer, the local MSDP peer needs to forward the message to all peers except the sender of the message. Before forwarding the SA message, the local node matches the (S, G) entry carried in the SA message with **sa-policy export** configured on each peer. If the (S, G) entry does not match the SA policy of a peer, the local node does not forwarding the SA message to the peer.

Q: Why Does the Local S9300 Not Send the (S, G) Information in the Local Domain to the Remote MSDP Peer?

A: The possible causes are:

- The MSDP peer is configured on a non-RP S9300. The local S9300 sends the (S, G) information in the local domain to other MSDP peers only when the MSDP peers are configured on RPs.
- The **import-source** command is run. Therefore, the source MSDP peer does not generate any SA message.

The **import-source** command is used to control the (S, G) entries that are advertised through SA messages. The parameter **ACL** is optional. If **ACL** is not set in the command, all (S, G) entries are filtered out by default. That is, no (S, G) entry is advertised. When the **import-source** command is not run, all (S, G) information is advertised. Therefore, when the local MSDP peer does not send the (S, G) entries in the local domain to the remote MSDP peers, check whether the **import-source** command is configured correctly.

Q: What Are the Requirements for Configuring an Anycast RP?

A: When configuring an anycast RP, note the following points:

- Configure the same IP address on loopback interfaces of multiple S9300s in a PIM-SM domain, and specify the interface address as the RP.
- Set up MSDP peer relations between the S9300s. The MSDP peer address cannot be the same as the address of the RP; otherwise, the TCP connection between MSDP peers cannot be set up.
- Run the **originating-rp** command to specify a logical RP address for SA messages; otherwise, the RPs cannot exchange SA messages.
- Configure the C-BSR and C-RP on different interfaces when using BSRs.

Q: When Configuring an Anycast RP, Why Must a Logical RP Address Be Specified for SA Messages?

A: S9300s perform the RPF check on received SA messages. If an S9300 detects that the remote RP address carried in a received SA message is the same as the local RP address, the S9300 discards the SA message. Among anycast RPs, two RPs that set up the MSDP peer relation have the same IP address; therefore, you must run the **originating-rp** command to specify a logical RP address for a locally sent SA message to replace the actual RP address. The SA message can thus pass the RPF check.

The MSDP peer address is recommended when the **originating-rp** command is used to specify a logical RP address.

Q: When an Anycast RP Is Configured, Why Cannot a C-BSR and a C-RP Be Configured on the Same Interface?

A: Among anycast RPs, interfaces where C-RPs reside have the same IP address. If a C-BSR and a C-RP are configured on the same interface, the other C-RPs discard a received BSR packet. This is because the BSR packet does not pass the RPF check and the BSR address in the BSR packet is the same as the local address. As a result, the other C-RP cannot obtain the RP-set, and do not consider themselves as RPs. The function of the anycast RP cannot be implemented.

Q: How Is a Large-Scale PIM-SM Network Divided into Multiple PIM-SM Domains?

A: PIM-SM implements multicast forwarding through RPs. Dividing a large-scale PIM-SM network into multiple PIM-SM domains means using different RPs in different PIM-SM domains.

- If a static RP is used in a PIM-SM domain, all S9300s in the domain must learn the RP information through the static configuration. The range of the domain is divided if a static RP on an S9300 outside the PIM-SM domain is not set.

- If a C-RP is used in a PIM-SM domain, all S9300s in the domain must learn the RP information through BSRs. The range of the PIM-SM domain is divided if the BSR boundary is set on an S9300 at the edge of the domain by running the **pim bsr-boundary** command, because the Bootstrap message cannot pass the BSR boundary.

After a PIM-SM network is divided into domains, RP information on S9300s in different domains is different when the **display pim rp-info** command is used on the S9300s.

Q: Why Are Multicast Data Packets Encapsulated in SA Messages?

A: Certain multicast sources are bursting, and the interval for sending data is long. This leads to the timeout of (S, G) entries after source registering. In this case, the DR encapsulates the multicast data in a Register message and sends it to the source RP. After decapsulating the Register message, the source RP encapsulates the data in an SA message and sends it to the remote MSDP peer. The multicast data then reaches the receivers.

If multicast data cannot be encapsulated in SA messages because (S, G) entries time out, receivers cannot receive the multicast data.

Q: Why Cannot the Local MSDP Peer Receive SA Messages Encapsulated with Multicast Data Packets?

A: The possible causes are:

- The **encap-data-enable** command is not used on the MSDP peer (which must be an RP) connected to the source. By default, an SA message is not encapsulated with a multicast data packet.
- The TTL value in the IP header of a multicast data packet sent by the source DR is very small for the packet to reach the current MSDP.
- When an MSDP peer receives an SA message encapsulated with a multicast data packet, the MSDP peer decapsulates the message and reduces the TTL value in the header of the packet by 1. If the TTL value is 0, the MSDP peer discards the message directly. If the TTL value is greater than 0, the MSDP peer encapsulates the multicast data packet again and forwards it. If the TTL value is greater than 0, local source registering is required only when the current MSDP peer is an RP.
- The **peer minimum-ttl** command is used on peers on the path from the source to the current MSDP peer and a large TTL threshold is set.

The **peer minimum-ttl** command is only valid for SA messages encapsulated with multicast data packets. When the **peer minimum-ttl** command is used on an MSDP peer, the peer compares the TTL value reduced by 1 with the TTL threshold. If the TTL value is equal to or greater than the TTL threshold, the peer needs to encapsulate the data packet again and forward it; if the TTL value is smaller than the threshold, the peer discards the packet directly.

Q: The peer minimum-ttl Command Is Used, and the TTL Value of the Data Packet Encapsulated in an SA Message Is Smaller than the Minimum Value. Why Does the (S, G) Entry Still Exist in the SA Cache?

A: This is a normal situation.

If the TTL value in a received data packet is smaller than the value of **minimum-ttl**, an MSDP peer discards the message and does not cache the (S, G) entry. At the same time, the peer receives SA messages that carry (S, G) entries but are not encapsulated with any packet from the remote peer periodically. The MSDP peer then caches the (S, G) entries.

4.5 Diagnostic Tools

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

4.5.1 display Commands

4.5.2 debugging Commands

4.5.1 display Commands

Command	Description
display msdp brief	Displays the status of an MSDP peer.
display msdp peer-status	Displays detailed information about an MSDP peer.
display msdp sa-cache	Displays all (S, G) entries in the cache.
display msdp sa-count	Displays the number of sources and groups in the MSDP cache.
display version	Displays the version information.
display current-configuration	Displays the configuration of the current S9300.
display current-configuration configuration msdp	Displays the configuration in the MSDP view of the current S9300.
display pim routing-table	Displays all (S, G) entries and (*, G) entries.
display pim rp-info	Displays whether an address is assigned for the RP to which G corresponds and whether the RP is the local S9300.

4.5.2 debugging Commands

Command	Description
debugging msdp all	Enables all the debugging of MSDP.
debugging msdp connect	Enables the debugging of MSDP connection.
debugging msdp event	Enables the debugging of MSDP events.
debugging msdp packet	Enables the debugging of MSDP messages.
debugging msdp source-active	Enables the debugging of MSDP routes.