



Quidway S5300 Series Ethernet Switches  
V100R002C02

## **Configuration Guide - IP Multicast**

<b>Issue</b>	01
<b>Date</b>	2008-12-26
<b>Part Number</b>	

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](mailto:support@huawei.com)

**Copyright © Huawei Technologies Co., Ltd. 2008. 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

---

<b>About This Document.....</b>	<b>1</b>
<b>1 IP Multicast Configuration Guide.....</b>	<b>1-1</b>
1.1 Introduction.....	1-2
1.1.1 IP Multicast Overview.....	1-2
1.1.2 IP Multicast Features Supported by the S-switch.....	1-2
1.2 IPv4 Multicast Configuration Guide.....	1-2
1.2.1 IPv4 Multicast Addresses.....	1-2
1.2.2 IPv4 Multicast Protocols.....	1-3
1.2.3 Typical Configuration Solution.....	1-4
1.2.4 Controlling Multicast Forwarding.....	1-5
<b>2 IGMP Proxy Configuration.....</b>	<b>2-1</b>
2.1 Overview.....	2-2
2.1.1 IGMP Proxy.....	2-2
2.1.2 IGMP Proxy Supported by the S-switch.....	2-3
2.1.3 Logical Relationships Between Configuration Tasks.....	2-4
2.1.4 Update History.....	2-4
2.2 Enabling IGMP Proxy.....	2-4
2.2.1 Establishing the Configuration Task.....	2-4
2.2.2 Enabling IGMP Proxy Globally.....	2-5
2.2.3 Enabling IGMP Proxy for a VLAN.....	2-5
2.2.4 (Optional) Configuring the IGMP Version.....	2-6
2.2.5 Checking the Configuration.....	2-6
2.3 Configuring a Static Router Interface.....	2-7
2.3.1 Establishing the Configuration Task.....	2-7
2.3.2 Configuring an Interface as a Static Router Interface.....	2-7
2.3.3 Checking the Configuration.....	2-8
2.4 Configuring a Multicast Group Policy.....	2-8
2.4.1 Establishing the Configuration Task.....	2-8
2.4.2 Configuring Rules to Filter Multicast Packets.....	2-9
2.4.3 (Optional) Configuring a Multicast Group Policy.....	2-9
2.4.4 Checking the Configuration.....	2-10
2.5 Configuring Prompt Leave for Interfaces in a VLAN.....	2-11

2.5.1 Establishing the Configuration Task.....	2-11
2.5.2 (Optional) Configuring Filtering Rules for Interfaces in a VLAN.....	2-11
2.5.3 Configuring Prompt Leave for Interfaces.....	2-12
2.5.4 Checking the Configuration.....	2-12
2.6 Adjusting IGMP Proxy Parameters.....	2-13
2.6.1 Establishing the Configuration Task.....	2-13
2.6.2 (Optional) Setting the Aging Time for Router Interfaces.....	2-14
2.6.3 (Optional) Setting Parameters for Calculating the Aging Time of Member Interfaces.....	2-15
2.6.4 (Optional) Configuring the Router Alert Option of IGMP Packets.....	2-15
2.6.5 (Optional) Configuring the Source IP Address of IGMP Packets Sent by the S-switch Enabled with IGMP Proxy.....	2-16
2.6.6 Checking the Configuration.....	2-16
2.7 Maintaining IGMP Proxy.....	2-17
2.7.1 Clearing Multicast Forwarding Entries.....	2-17
2.7.2 Clearing IGMP Proxy Statistics.....	2-18
2.7.3 Debugging IGMP Proxy.....	2-18
2.8 Configuration Examples.....	2-18
2.8.1 Example for Configuring a Static Router Interface.....	2-19
2.8.2 Example for Configuring a Multicast Group Policy.....	2-20
2.8.3 Example for Configuring Prompt Leave for Interfaces in a VLAN.....	2-23
<b>3 IGMP Snooping Configuration.....</b>	<b>3-1</b>
3.1 Introduction.....	3-2
3.1.1 IGMP Snooping.....	3-2
3.1.2 References.....	3-2
3.1.3 Logical Relationships Between Configuration Tasks.....	3-2
3.2 Enabling IGMP Snooping.....	3-2
3.2.1 Establishing the Configuration Task.....	3-3
3.2.2 Enabling IGMP Snooping on the S-switch.....	3-3
3.2.3 Enabling IGMP Snooping in a VLAN.....	3-4
3.2.4 (Optional) Adding an Interface to a Multicast Group Statically.....	3-4
3.2.5 (Optional) Configuring a Static Router Interface.....	3-5
3.2.6 Checking the Configuration.....	3-5
3.3 Configuring a Multicast Policy in a VLAN.....	3-6
3.3.1 Establishing the Configuration Task.....	3-6
3.3.2 Creating an ACL.....	3-7
3.3.3 Configuring a Multicast Policy.....	3-7
3.3.4 Enabling the S-switch to Discard Unknown Multicast Packets on the Multicast Source Interface.....	3-8
3.3.5 Checking the Configuration.....	3-8
3.4 Configuring Prompt Leave of Interfaces in a VLAN.....	3-9
3.4.1 Establishing the Configuration Task.....	3-9
3.4.2 (Optional) Creating an ACL.....	3-10
3.4.3 Configuring Prompt Leave of Interfaces.....	3-10

3.4.4 Checking the Configuration.....	3-10
3.5 Adjusting IGMP Snooping Parameters.....	3-11
3.5.1 Establishing the Configuration Task.....	3-11
3.5.2 (Optional) Setting the Aging Time of the Router Interface.....	3-12
3.5.3 (Optional) Configuring Parameters for Computing the Aging Time of Member Interfaces.....	3-12
3.5.4 (Optional) Configuring the Router Alert Option in IGMP Messages.....	3-13
3.5.5 (Optional) Configuring the IGMP Snooping Module to Respond to Layer 2 Network Topology Changes.....	3-14
3.5.6 (Optional) Configuring the IGMP Version.....	3-14
3.5.7 Checking the Configuration.....	3-15
3.6 Configuring Replication of a Multicast VLAN.....	3-15
3.6.1 Establishing the Configuration Task.....	3-15
3.6.2 Configuring Replication of a Multicast VLAN on the S-switch.....	3-16
3.6.3 Configuring Replication of a Multicast VLAN in a VLAN.....	3-17
3.6.4 Setting the Mapping Between Multicast VLANs and User VLANs.....	3-17
3.6.5 Checking the Configuration.....	3-17
3.7 Maintaining IGMP Snooping.....	3-18
3.7.1 Clearing Dynamic Entries in a Multicast Forwarding Table.....	3-18
3.7.2 Clearing the Statistics on IGMP Snooping.....	3-19
3.7.3 Debugging IGMP Snooping.....	3-19
3.8 Configuration Examples.....	3-20
3.8.1 Example for Configuring Multicast Policies on the GigabitEthernet.....	3-20
3.8.2 Example for Configuring Prompt Leave of Interfaces in a VLAN.....	3-22
3.8.3 Example for Setting a Static Router Interface.....	3-24
3.8.4 Example for Configuring the IGMP Snooping Module to Respond to Layer 2 Network Topology Changes.....	3-26
3.8.5 Example for Configuring Replication of a Multicast VLAN.....	3-31
<b>4 Controllable Multicast Configuration.....</b>	<b>4-1</b>
4.1 Introduction.....	4-2
4.1.1 Overview of Controllable Multicast.....	4-2
4.1.2 Basic Principle.....	4-2
4.2 Configuring Controllable Multicast.....	4-3
4.2.1 Establishing the Configuration Task.....	4-4
4.2.2 Configuring a Multicast Group.....	4-4
4.2.3 Configuring a Multicast Group List.....	4-5
4.2.4 Configuring a Multicast Profile.....	4-5
4.2.5 Applying a Multicast Profile to a VLAN.....	4-5
4.2.6 Configuring the Preview Information of a User in a Multicast Profile.....	4-6
4.2.7 Configuring the Maximum Number of Multicast Groups That Users in a Multicast Profile Can Simultaneously Join.....	4-6
4.2.8 Checking the Configuration.....	4-7
4.3 Configuration Example.....	4-7
4.3.1 Example for Configuring Controllable Multicast.....	4-7

<b>5 PIM-DM (IPv4) Configuration.....</b>	<b>5-1</b>
5.1 Introduction.....	5-2
5.1.1 PIM-DM Overview.....	5-2
5.1.2 PIM-DM Features Supported by the S-switch.....	5-3
5.2 Configuring Basic PIM-DM Functions.....	5-3
5.2.1 Establishing the Configuration Task.....	5-4
5.2.2 Enabling IPv4 Multicast Routing.....	5-4
5.2.3 Enabling PIM-DM.....	5-4
5.2.4 Checking the Configuration.....	5-5
5.3 Adjusting Control Parameters of a Multicast Source.....	5-6
5.3.1 Establishing the Configuration Task.....	5-6
5.3.2 Configuring the Lifetime of a Source.....	5-7
5.3.3 Configuring Filtering Rules Based on Source Addresses.....	5-7
5.3.4 Checking the Configuration.....	5-8
5.4 Adjusting Control Parameters for Maintaining Neighbor Relationships.....	5-8
5.4.1 Establishing the Configuration Task.....	5-8
5.4.2 Configuring the Interval for Sending Hello Messages.....	5-9
5.4.3 Configuring the Timeout Period of a Neighbor.....	5-10
5.4.4 Refusing to Receive the Hello Message Without the Generation ID Option.....	5-11
5.4.5 Checking the Configuration.....	5-12
5.5 Adjusting Control Parameters for Prune.....	5-12
5.5.1 Establishing the Configuration Task.....	5-12
5.5.2 Configuring the Period for an Interface to Keep the Prune State.....	5-13
5.5.3 Configuring the Interval for Sending Join/Prune Messages.....	5-14
5.5.4 Configuring Control Parameters for Prune.....	5-14
5.5.5 Configuring the Interval for Overriding the Prune Action.....	5-15
5.5.6 Checking the Configuration.....	5-16
5.6 Adjusting Control Parameters for State-Refresh.....	5-16
5.6.1 Establishing the Configuration Task.....	5-16
5.6.2 Disabling State-Refresh.....	5-17
5.6.3 Configuring the Interval for Sending State-Refresh Messages.....	5-18
5.6.4 Configuring the Period for Receiving the Next State-Refresh Message.....	5-18
5.6.5 Configuring the TTL Value Carried in a State-Refresh Message.....	5-19
5.6.6 Checking the Configuration.....	5-19
5.7 Adjusting Control Parameters for Graft.....	5-20
5.7.1 Establishing the Configuration Task.....	5-20
5.7.2 Configuring the Interval for Retransmitting Graft Messages.....	5-21
5.7.3 Checking the Configuration.....	5-21
5.8 Adjusting Control Parameters for Assert.....	5-22
5.8.1 Establishing the Configuration Task.....	5-22
5.8.2 Configuring the Period for Keeping the Assert State.....	5-23
5.8.3 Checking the Configuration.....	5-24

5.9 Maintaining PIM.....	5-24
5.9.1 Clearing Statistics of PIM Control Messages.....	5-24
5.9.2 Monitoring the Running Status of PIM.....	5-25
5.9.3 Debugging PIM.....	5-25
5.10 Configuration Example.....	5-26
5.10.1 Example for Configuring Basic PIM-DM Functions.....	5-26
<b>6 PIM-SM (IPv4) Configuration.....</b>	<b>6-1</b>
6.1 Introduction.....	6-3
6.1.1 PIM-SM Overview.....	6-3
6.1.2 PIM-SM Features Supported by the S-switch.....	6-4
6.2 Configuring Basic PIM-SM Functions.....	6-5
6.2.1 Establishing the Configuration Task.....	6-5
6.2.2 Enabling IP Multicast Routing.....	6-7
6.2.3 Enabling Basic PIM-SM Functions.....	6-7
6.2.4 (Optional) Configuring a Static RP.....	6-8
6.2.5 (Optional) Configuring a Dynamic RP.....	6-9
6.2.6 (Optional) Configuring the SSM Group Address Range.....	6-10
6.2.7 Checking the Configuration.....	6-11
6.3 Adjusting Control Parameters for a Multicast Source.....	6-11
6.3.1 Establishing the Configuration Task.....	6-11
6.3.2 Configuring the Lifetime of a Source.....	6-12
6.3.3 Configuring the Filtering Rules Based on the Source Addresses.....	6-13
6.3.4 Checking the Configuration.....	6-13
6.4 Adjusting Control Parameters of the C-RP and C-BSR.....	6-13
6.4.1 Establishing the Configuration Task.....	6-14
6.4.2 Adjusting C-RP Parameters.....	6-15
6.4.3 Adjusting C-BSR Parameters.....	6-15
6.4.4 Configuring the BSR Boundary.....	6-16
6.4.5 Configuring the BSR Address Range.....	6-17
6.4.6 Configuring the Range of Valid C-RP Addresses.....	6-17
6.4.7 Checking the Configuration.....	6-18
6.5 Configuring a BSR Administrative Domain.....	6-18
6.5.1 Establishing the Configuration Task.....	6-19
6.5.2 Enabling a BSR Administrative Domain.....	6-19
6.5.3 Configuring the Boundary of a BSR Administrative Domain.....	6-20
6.5.4 Adjusting C-BSR Parameters.....	6-20
6.5.5 Checking the Configuration.....	6-22
6.6 Adjusting Control Parameters for Establishing the Neighbor Relationship.....	6-22
6.6.1 Establishing the Configuration Task.....	6-22
6.6.2 Configuring Control Parameters for Establishing the Neighbor Relationship.....	6-23
6.6.3 Configuring Control Parameters for Electing a DR.....	6-24
6.6.4 Checking the Configuration.....	6-25

6.7 Adjusting Control Parameters for Source Registering.....	6-26
6.7.1 Establishing the Configuration Task.....	6-26
6.7.2 Configuring PIM-SM Register Messages.....	6-27
6.7.3 Configuring PIM-SM Register Suppression.....	6-27
6.7.4 Checking the Configuration.....	6-28
6.8 Adjusting Control Parameters for Forwarding.....	6-28
6.8.1 Establishing the Configuration Task.....	6-28
6.8.2 Configuring Control Parameters for Keeping the Forwarding State.....	6-29
6.8.3 Configuring Control Parameters for Prune.....	6-30
6.8.4 Checking the Configuration.....	6-32
6.9 Adjusting Control Parameters for Assert.....	6-32
6.9.1 Establishing the Configuration Task.....	6-32
6.9.2 Configuring the Period for Keeping the Assert State.....	6-33
6.9.3 Checking the Configuration.....	6-34
6.10 Configuring the SPT Switchover.....	6-34
6.10.1 Establishing the Configuration Task.....	6-34
6.10.2 (Optional) Configuring the Interval for Checking the Forwarding Rate of Multicast Data.....	6-36
6.10.3 Checking the Configuration.....	6-36
6.11 Configuring PIM BFD.....	6-37
6.11.1 Establishing the Configuration Task.....	6-37
6.11.2 Configuring PIM BFD.....	6-37
6.11.3 (Optional) Adjusting BFD Parameters.....	6-38
6.11.4 Checking the Configuration.....	6-39
6.12 Maintaining PIM.....	6-39
6.12.1 Clearing Statistics of PIM Control Messages.....	6-39
6.12.2 Monitoring the Running Status of PIM-SM.....	6-39
6.12.3 Debugging PIM.....	6-40
6.13 Configuration Examples.....	6-41
6.13.1 Example for Configuring a PIM-SM Network.....	6-41
6.13.2 Example for Configuring the SPT Switchover in a PIM-SM Domain.....	6-50
6.13.3 Example for Configuring PIM BFD on Routers in Ethernet.....	6-54
<b>7 IGMP Configuration.....</b>	<b>7-1</b>
7.1 Introduction.....	7-2
7.1.1 IGMP Overview.....	7-2
7.1.2 IGMP Features Supported by the S-switch.....	7-2
7.2 Configuring Basic IGMP Functions.....	7-3
7.2.1 Establishing the Configuration Task.....	7-3
7.2.2 Enabling IP Multicast Routing.....	7-4
7.2.3 Enabling Basic IGMP Functions.....	7-5
7.2.4 Configuring IGMP Version.....	7-5
7.2.5 Configuring a Static IGMP Group.....	7-6
7.2.6 Configuring an Interface to Join a Multicast Group in a Certain Range.....	7-6

7.2.7 Checking the Configuration.....	7-7
7.3 Configuring Options of an IGMP Packet.....	7-7
7.3.1 Establishing the Configuration Task.....	7-7
7.3.2 Configuring a S-switch to Reject IGMP Packets Without the Router-Alert Option.....	7-8
7.3.3 Configuring a S-switch to Send IGMP Packets Without the Router-Alert Option.....	7-9
7.3.4 Checking the Configuration.....	7-10
7.4 Configuring IGMP Query Control.....	7-10
7.4.1 Establishing the Configuration Task.....	7-10
7.4.2 Configuring an IGMPv1 Querier.....	7-11
7.4.3 Configure an IGMPv2/v3 Querier.....	7-12
7.4.4 Checking the Configuration.....	7-15
7.5 Configuring SSM Mapping.....	7-15
7.5.1 Establishing the Configuration Task.....	7-15
7.5.2 Enabling Static SSM Mapping.....	7-16
7.5.3 Configuring a Static SSM Mapping Policy.....	7-16
7.5.4 Checking the Configuration.....	7-17
7.6 Maintaining IGMP.....	7-17
7.6.1 Clearing IGMP Group Information.....	7-17
7.6.2 Monitoring the Running Status of IGMP.....	7-18
7.6.3 Debugging IGMP.....	7-18
7.7 Configuration Examples.....	7-19
7.7.1 Example for Configuring Basic IGMP Functions.....	7-19
7.7.2 Example for Configuring SSM Mapping.....	7-22
<b>8 IPv4 Multicast Routing Management.....</b>	<b>8-1</b>
8.1 Introduction.....	8-2
8.1.1 Overview of IPv4 Multicast Routing Management.....	8-2
8.1.2 IPv4 Multicast Routing Management Features Supported by the S-switch.....	8-2
8.2 Configuring a Static Multicast Route.....	8-4
8.2.1 Establishing the Configuration Task.....	8-4
8.2.2 Configuring a Static Multicast Route.....	8-5
8.2.3 Checking the Configuration.....	8-6
8.3 Configuring a Multicast Routing Policy.....	8-6
8.3.1 Establishing the Configuration Task.....	8-6
8.3.2 Configuring Longest Match of Multicast Routes.....	8-7
8.3.3 Configuring Load Balancing of Multicast Routes.....	8-7
8.3.4 Checking the Configuration.....	8-8
8.4 Configuring the Multicast Forwarding Scope.....	8-8
8.4.1 Establish the Configuration Task.....	8-8
8.4.2 Configuring the Multicast Forwarding Boundary.....	8-9
8.4.3 Configuring the TTL Threshold of Multicast Forwarding.....	8-10
8.4.4 Checking the Configuration.....	8-10
8.5 Configuring Control Parameters of the Multicast Forwarding Table.....	8-11

8.5.1 Establishing the Configuration Task.....	8-11
8.5.2 Setting the Maximum Number of Entries in Multicast Forwarding Table.....	8-12
8.5.3 Setting the Maximum Number of Downstream Nodes of a Multicast Forwarding Entry.....	8-12
8.5.4 Checking the Configuration.....	8-13
8.6 Maintaining the Multicast Policy.....	8-13
8.6.1 Clearing Multicast Routing and Forwarding Entries.....	8-13
8.6.2 Monitoring the Status of Multicast Routing and Forwarding.....	8-14
8.6.3 Debugging Multicast Routing and Forwarding.....	8-15
8.7 Configuration Examples.....	8-15
8.7.1 Example for Changing Static Multicast Routes to RPF Routes.....	8-15
8.7.2 Example for Connecting the RPF Route Through a Static Multicast Route.....	8-18
<b>9 MSDP Configuration.....</b>	<b>9-1</b>
9.1 Introduction.....	9-2
9.1.1 MSDP Overview.....	9-2
9.1.2 MSDP Features Supported by the S-switch.....	9-2
9.2 Configuring PIM-SM Inter-domain Multicast.....	9-4
9.2.1 Establishing the Configuration Task.....	9-4
9.2.2 Configuring Intra-AS MSDP Peers.....	9-5
9.2.3 Configuring Static RPF Peers.....	9-6
9.2.4 Checking the Configuration.....	9-7
9.3 Configuring an Anycast RP in a PIM-SM Domain.....	9-8
9.3.1 Establishing the Configuration Task.....	9-8
9.3.2 Configuring the Interface Address of an RP.....	9-9
9.3.3 Configuring a C-RP.....	9-10
9.3.4 Statically Configuring an RP.....	9-10
9.3.5 Configuring an MSDP Peer.....	9-11
9.3.6 Specifying the Logical RP Address for an SA Message.....	9-12
9.3.7 Checking the Configuration.....	9-13
9.4 Managing MSDP Peer Connections.....	9-13
9.4.1 Establishing the Configuration Task.....	9-14
9.4.2 Controlling the Sessions Between MSDP Peers.....	9-14
9.4.3 Adjusting the interval for Retrying Setting up an MSDP Peer Connection.....	9-15
9.4.4 Checking the Configuration.....	9-15
9.5 Configuring SA Cache.....	9-16
9.5.1 Establishing the Configuration Task.....	9-16
9.5.2 Configuring the Maximum Number of (S, G) Entries in the Cache.....	9-17
9.5.3 Disabling the SA Cache Function.....	9-17
9.5.4 Checking the Configuration.....	9-18
9.6 Configuring an SA Request.....	9-18
9.6.1 Establishing the Configuration Task.....	9-18
9.6.2 Configuring "Sending SA Request Messages" on the Local Router.....	9-19
9.6.3 Configuring the Filtering Rules for Receiving SA Request Messages.....	9-20

9.6.4 Checking the Configuration.....	9-20
9.7 Transmitting Burst Multicast Data Between Domains.....	9-21
9.7.1 Establishing the Configuration Task.....	9-21
9.7.2 Encapsulating a Multicast Data Packet in an SA message.....	9-22
9.7.3 (Optional) Setting the TTL Threshold for Forwarding an SA Message Containing a Multicast Data Packet .....	9-23
9.7.4 Checking the Configuration.....	9-23
9.8 Configuring the Filtering Rules for SA Messages.....	9-25
9.8.1 Establishing the Configuration Task.....	9-25
9.8.2 Setting Rules for Creating an SA Message.....	9-26
9.8.3 Setting Rules for Receiving an SA Message.....	9-26
9.8.4 Setting Rules for Forwarding an SA Message.....	9-27
9.8.5 Checking the Configuration.....	9-28
9.9 Maintaining MSDP.....	9-29
9.9.1 Clearing Statistics of MSDP Peers.....	9-29
9.9.2 Clearing (S, G) Information in SA Cache.....	9-29
9.9.3 Monitoring the Running Status of MSDP.....	9-30
9.9.4 Debugging MSDP.....	9-30
9.10 Configuration Examples.....	9-31
9.10.1 Example for Configuring PIM-SM Inter-Domain Multicast.....	9-31
9.10.2 Example for Configuring Inter-AS Multicast by Using Static RPF Peers.....	9-38
9.10.3 Example for Configuring an Anycast RP.....	9-42



## Figures

<b>Figure 1-1</b> Location of each IPv4 multicast protocol.....	1-3
<b>Figure 2-1</b> Networking diagram of configuring a static router interface.....	2-19
<b>Figure 2-2</b> Networking diagram of configuring a multicast group policy.....	2-21
<b>Figure 2-3</b> Networking diagram of configuring prompt leave for interfaces in a VLAN.....	2-23
<b>Figure 3-1</b> Networking diagram for configuring multicast policies on the Gigabitethernet.....	3-20
<b>Figure 3-2</b> Networking diagram for configuring prompt leave of interfaces in a VLAN.....	3-23
<b>Figure 3-3</b> Networking diagram for configuring a static router interface.....	3-25
<b>Figure 3-4</b> Networking diagram for configuring the IGMP snooping module to respond to Layer 2 network topology changes.....	3-27
<b>Figure 3-5</b> Networking diagram for configuring replication of a multicast VLAN.....	3-31
<b>Figure 4-1</b> Hierarchical control mechanisms of controllable multicast.....	4-2
<b>Figure 4-2</b> Networking diagram of configuring controllable multicast.....	4-8
<b>Figure 5-1</b> Location of PIM-DM in the multicast network.....	5-2
<b>Figure 5-2</b> Networking diagram for configuring basic PIM-DM functions.....	5-27
<b>Figure 6-1</b> Application of PIM-SM a the multicast network.....	6-3
<b>Figure 6-2</b> Networking diagram for configuring PIM-SM multicast network.....	6-41
<b>Figure 6-3</b> Networking diagram for performing SPT switchover in a PIM-SM domain.....	6-50
<b>Figure 6-4</b> Networking diagram of applying PIM BFD on a multi-router network segment.....	6-54
<b>Figure 7-1</b> Networking diagram of configuring basic IGMP functions.....	7-20
<b>Figure 7-2</b> SSM mapping network.....	7-23
<b>Figure 8-1</b> Networking diagram for changing static multicast routes to RPF routes.....	8-16
<b>Figure 8-2</b> Networking diagram for connecting the RPF route through static multicast routes.....	8-18
<b>Figure 9-1</b> Networking diagram of configuring PIM-SM inter-domain multicast.....	9-32
<b>Figure 9-2</b> Networking diagram of configuring inter-AS multicast by using static RPF peers.....	9-39
<b>Figure 9-3</b> Networking diagram of configuring anycast RP.....	9-43



---

# Tables

---

**Table 1-1** Class D addresses.....1-3

**Table 1-2** Multicast protocols.....1-4



---

# About This Document

---

## Purpose

The document describes the configuration methods of IP multicast networks in terms of basic principles, protocol implementation, configuration procedures, and configuration examples for the IP multicast of the S-switch.

This document covers the following topics:

- Feature description
- Data preparations
- Pre-configuration tasks
- Configuration procedures
- Checking the configuration
- Configuration examples

## Related Versions

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

Product Name	Version
S5300	V100R002C02

## Intended Audience

This document is intended for:

- Commissioning engineers
- Data configuration engineers
- Network administrators
- System maintenance engineers

# Organization



This document include 9 chapters.




Chapter	Description
<b>1 IP Multicast Configuration Guide</b>	This section describes the principle and configurations of IP Multicast, and provides configuration examples.
<b>2 IGMP Proxy Configuration</b>	This section describes the principle and configurations of IGMP Proxy, and provides configuration examples.
<b>3 IGMP Snooping Configuration</b>	This section describes the principle and configurations of IGMP snooping, and provides configuration examples.
<b>4 Controllable Multicast Configuration</b>	This section describes the principle and configurations of Controllable Multicast Configuration, and provides configuration examples.
<b>5 PIM-DM (IPv4) Configuration</b>	This section describes the principle and configurations of PIM-DM in IPv4, and provides configuration examples.
<b>6 PIM-SM (IPv4) Configuration</b>	This section describes the principle and configurations of PIM-SM in IPv4, and provides configuration examples.
<b>7 IGMP Configuration</b>	This section describes the principle and configurations of IGMP, and provides configuration examples.
<b>8 IPv4 Multicast Routing Management</b>	This section describes the principle and configurations of IPv4 Multicast Routing Management, and provides configuration examples.
<b>9 MSDP Configuration</b>	This section describes the principle and configurations of MSDP, and provides configuration examples.

## Conventions

### Symbol Conventions

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

Symbol	Description
 <b>DANGER</b>	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.

Symbol	Description
 <b>CAUTION</b>	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 <b>TIP</b>	Indicates a tip that may help you address a problem or save your time.
 <b>NOTE</b>	Provides additional information to emphasize or supplement important points of the main text.

## General Conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
<b>Boldface</b>	Names of files, directories, folders, and users are in <b>Boldface</b> . For example, log in as user <b>Root</b> .
<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

Convention	Description
<b>Boldface</b>	The keywords of a command line are in <b>boldface</b> .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x   y   ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[ x   y   ... ]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none 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 alternative items are grouped in square brackets and separated by vertical bars. Several or none is 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

Convention	Description
<b>boldface</b>	Buttons, menus, parameters, tabs, windows, and dialog titles are in <b>boldface</b> . For example, click <b>OK</b> .
>	Multi-level menus are in <b>boldface</b> and separated by the ">" signs. For example, choose <b>File &gt; Create &gt; Folder</b> .

## Keyboard Operations

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

## Mouse Operations

Convention	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 version contains all updates made to previous versions.

### Updates in Issue 01 (12.26.08)

This is the first release.

# 1 IP Multicast Configuration Guide

---

## About This Chapter

This chapter describes IP multicast fundamentals, classifications, framework, and packet forwarding mechanism.

### [1.1 Introduction](#)

This section describes applications and functions of IP multicast.

### [1.2 IPv4 Multicast Configuration Guide](#)

This section describes multicast addresses, protocols, and typical configuration solutions in IPv4 networks.

## 1.1 Introduction

This section describes applications and functions of IP multicast.

### [1.1.1 IP Multicast Overview](#)

### [1.1.2 IP Multicast Features Supported by the S-switch](#)

## 1.1.1 IP Multicast Overview

Multicast is a Point to Multi-Point (P2MP) data transmission mode. During data transmission, multicast can ensure the security of information. Multicast consumes limited network bandwidth.

The multicast technology applied to IPv4 and IPv6 is called IP multicast.

The Internet services implemented through IP multicast include IPTV, Video On Demand (VOD), online meeting, e-learning, and remote medicine.

## 1.1.2 IP Multicast Features Supported by the S-switch

In the S-switch, IPv4 networks and IPv6 networks can support multicast services, but networks that runs IPv4 and IPv6 simultaneously cannot support multicast services.

## 1.2 IPv4 Multicast Configuration Guide

This section describes multicast addresses, protocols, and typical configuration solutions in IPv4 networks.

### [1.2.1 IPv4 Multicast Addresses](#)

### [1.2.2 IPv4 Multicast Protocols](#)

### [1.2.3 Typical Configuration Solution](#)

### [1.2.4 Controlling Multicast Forwarding](#)

## 1.2.1 IPv4 Multicast Addresses

The IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255. [Table 1-1](#) shows description of IPv4 multicast addresses.

The multicast group address available for multicast data services ranges from 224.0.1.0 to 239.255.255.255. Any host (or other receiving device) that joins a multicast group within this range becomes a member of the group, and can identify and receive IP packets with the IP multicast address as the destination address. The members of a group can be distributed at any position in the network. The hosts can join or leave a group at any time.

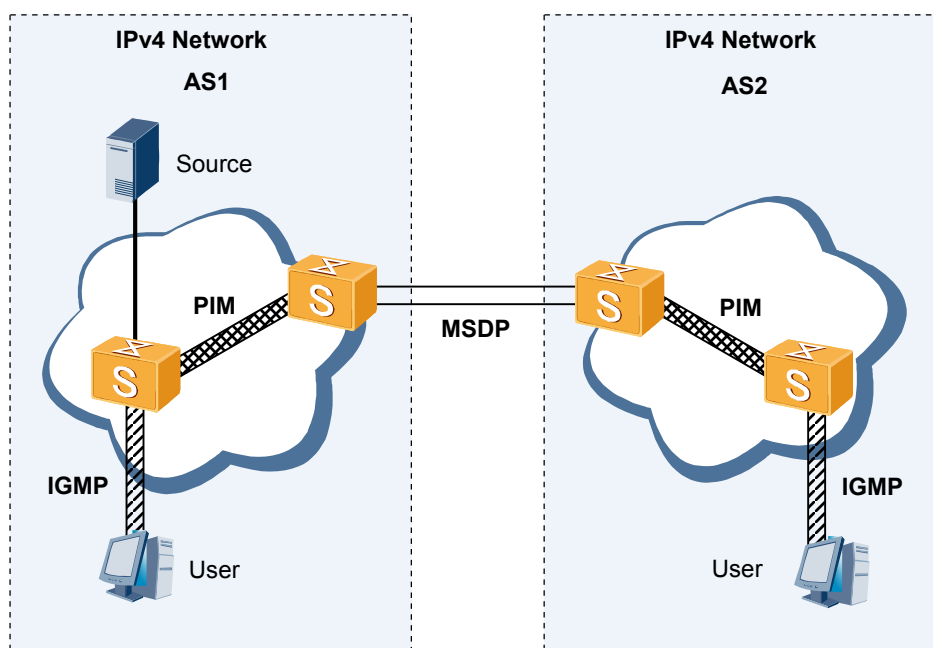
**Table 1-1** Class D addresses

Class D Address Range	Description
224.0.0.0 to 224.0.0.255	Indicates the reserved group addresses. The addresses are reserved by Internet Assigned Number Authority (IANA) for routing protocols, and are called permanent multicast group addresses. The addresses are used to identify a group of specific network devices.
224.0.1.0 to 231.255.255.255 233.0.0.0 to 238.255.255.255	Indicates Any-Source Multicast (ASM) addresses. The addresses are valid in the entire network.
232.0.0.0 to 232.255.255.255	Indicates Source-Specific Multicast (SSM) addresses. This is the default SSM group address scope, and is valid in the entire network.
239.0.0.0 to 239.255.255.255	Indicates administration multicast addresses. The default range of group addresses is valid only in the local BSR administration domain. The addresses are private addresses. You can configure the same address in different BSR administration domains.

## 1.2.2 IPv4 Multicast Protocols

To implement a complete set of IPv4 multicast services, various multicast protocols deployed in the network need to cooperate with each other, as shown in [Figure 1-1](#).

**Figure 1-1** Location of each IPv4 multicast protocol



**Table 1-2** Multicast protocols

Applied Location	Objectives	Multicast Protocol
Between hosts and multicast S-switches	Connecting hosts to a multicast network: <ul style="list-style-type: none"><li>• Ensure that the members can dynamically join and leave a group at the host side.</li><li>• Manage and maintain the member relationship at the S-switch side and exchange information with the upper-layer multicast routing protocols.</li></ul>	Internet Group Management Protocol (IGMP)
Between intra-domain multicast S-switches	Multicast routing and forwarding: <ul style="list-style-type: none"><li>• Create multicast routes on demand.</li><li>• Respond to the changes of the network topology and maintain the multicast routing table.</li><li>• Forward packets according to the routing table.</li></ul>	Protocol Independent Multicast (PIM), including Protocol Independent Multicast - Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM)
Between inter-domain multicast S-switches	Sharing information about inter-domain multicast sources: <ul style="list-style-type: none"><li>• S-switch in the domain where the source resides transmit the local source information to other S-switches in other domains.</li><li>• S-switch in different domains transmit the source information.</li></ul>	Multicast Source Discovery Protocol (MSDP)

## 1.2.3 Typical Configuration Solution



### CAUTION

Customize configuration solutions according to the actual network conditions and service requirements. The configuration solution in this section functions only as a reference.

The network environments are classified into two types, which need different configuration solutions. For details, refer to the *Quidway S5300 Series Ethernet Switches Configuration Guide - IP Multicast*.



### NOTE

Ensure that unicast routes work normally in the network before configuring IP multicast.

## Small-Scale Network

A small-scale network, such as a test network, is suitable to implement multicast data transmission in a Local Area Network (LAN), and does not interconnect with the Internet.

Perform the following configurations:

1. Enable multicast on all S-switches in the network.
2. Enable PIM-DM on all interfaces of the S-switches.
3. Enable IGMP on the interface connected to hosts.

## Large-Scale Network

A large-scale network is suitable to bear multicast services on an ISP network, and interconnects with the Internet.

Perform the following configurations:

1. Enable multicast on all S-switches in the network.
2. Enable PIM-SM on all interfaces of the S-switches.
3. Enable IGMP on the interface connected to hosts.
4. Configure an RP, specify a static RP, or elect an RP from C-RPs.
5. Divide a network into PIM-SM domains.
6. Configure MSDP in the PIM-SM domain and implement the anycast RP.

### 1.2.4 Controlling Multicast Forwarding

IP multicast guides the forwarding of multicast packets by using the multicast routing table and forwarding table. You can adjust the transmission path of multicast data by configuring the Reverse Path Forwarding (RPF) routing policy, and limit multicast forwarding by configuring the forwarding policy and the capacity of the forwarding table.



# 2 IGMP Proxy Configuration

---

## About This Chapter

This section describes the principle and configurations of IGMP proxy, and provides configuration examples.

### [2.1 Overview](#)

This section describes the advantages and functions of IGMP proxy.

### [2.2 Enabling IGMP Proxy](#)

This section describes how to enable IGMP proxy.

### [2.3 Configuring a Static Router Interface](#)

This section describes how to configure a static router interface.

### [2.4 Configuring a Multicast Group Policy](#)

This section describes how to configure a multicast group policy for a VLAN.

### [2.5 Configuring Prompt Leave for Interfaces in a VLAN](#)

This section describes how to configure prompt leave for interfaces in a VLAN.

### [2.6 Adjusting IGMP Proxy Parameters](#)

This section describes how to adjust IGMP proxy parameters.

### [2.7 Maintaining IGMP Proxy](#)

This section describes how to maintain IGMP proxy.

### [2.8 Configuration Examples](#)

This section provides several configuration examples of IGMP proxy.

## 2.1 Overview

This section describes the advantages and functions of IGMP proxy.

### 2.1.1 IGMP Proxy

### 2.1.2 IGMP Proxy Supported by the S-switch

### 2.1.3 Logical Relationships Between Configuration Tasks

### 2.1.4 Update History

## 2.1.1 IGMP Proxy

### Background

When unicast IP packets are transmitted on an Ethernet, the destination Medium Access Control (MAC) address of packets is the MAC address of the receiver. When multicast packets are transmitted, however, the destination of packets is a group of unspecific members instead of a specific receiver. Therefore, multicast forwarding entries cannot be generated when the multicast packets are forwarded to the data link layer from the IP layer. As a result, the multicast packets are broadcast on the data link layer. This wastes the bandwidth and is inconvenient for the accounting of user services. In addition, this poses a threat to information security.

At the same time, routers and hosts require forwarding entries to exchange Internet Group Management Protocol (IGMP) packets. Therefore, if there are a large number of hosts on the network, the redundant IGMP packets cause heavy pressures on the upstream routers.

To solve the preceding problems effectively, IGMP proxy is deployed on the S-switch that connects routers and hosts. In this manner, the S-switch serves as an agent server to take over certain tasks of routers.

### Main Functions

When serving as the agent server, the S-switch enabled with IGMP proxy has the following functions:

- Forming Layer 2 multicast forwarding entries to perform Layer 2 multicast  
IGMP proxy serves as a router at the host side and is responsible for sending IGMP Query messages and processing IGMP Response messages sent by hosts. In this manner, forwarding entries are formed to perform Layer 2 multicast.
- Terminating IGMP protocol packets sent to a router by hosts and replacing the hosts to send IGMP Report messages

The S-switch enabled with IGMP proxy serves as a host at the router side, responds to the Query messages, collects Report and Leave messages sent by hosts, and then notifies the router of these messages. In this manner, the number of additional IGMP protocol packets generated when many hosts frequently join or leave multicast groups is reduced. This also reduces the burden of the router.

### Advantages

IGMP proxy has the following advantages:

- Reduces broadcast packets in a Layer 2 network to save bandwidth and improve information security.
- Reduces the IGMP protocol packets exchanged between hosts and a router to lessen the pressure of the router.
- Manages and controls the forwarding of multicast packets to facilitate individual accounting for each host.

## 2.1.2 IGMP Proxy Supported by the S-switch

### IGMP Version

By default, IGMP proxy can process both IGMPv1 packets and IGMPv2 packets in a Virtual Local Area Network (VLAN).

You can configure the IGMP version according to the actual networking.

### Static Router Interface

You can configure static router interfaces by using commands. The static router interfaces do not age and are used to receive multicast packets in a steady manner for a long time.

### Multicast Group Policy

By using commands, you can configure multicast group policies. You can also configure the number of multicast groups that a host can join. This strengthens the control of IP multicast groups that a host can access.

### Prompt Leave

On the S-switch, if each interface in a VLAN connects to only one multicast receiver, you can configure the interfaces in the VLAN to promptly leave some or all multicast groups. This saves the network bandwidth.

### Aging Time of a Router Interface

A router interface is an interface through which the S-switch receives IGMP Query messages and sends IGMP Report and Leave messages. By using commands, you can configure the aging time for a router interface as required. This prevents the data interruption caused by the short aging time of the router interface when a network is unstable.

### Aging Time of Member Interfaces in a Group

Based on the actual networking, you can configure different values of aging time for member interfaces by using commands. This adjusts the aging time and optimizes the device performance.

### Router Alert Option

The S-switch processes IGMP packets based on whether the Router Alert option is contained in IGMP packets.

By default, the S-switch processes the IGMP packets received from a VLAN, regardless of whether IP headers of the packets contain the Router-Alert option. The IP headers of the IGMP packets sent to a VLAN by the S-switch contain the Router-Alert option.

You can determine whether IGMP packets received or sent should contain the Route Alert option by using commands.

## Source IP Address of Sent IGMP Packets

By using commands, you can configure source IP addresses of IGMP packets sent by the S-switch enabled with IGMP proxy as required.

By default, the source IP address of IGMP packets sent by the S-switch enabled with IGMP proxy is 192.168.0.1. When multiple S-switch devices exist on a shared network, you can set source IP addresses of IGMP packets to identify the S-switch.

## 2.1.3 Logical Relationships Between Configuration Tasks

In this chapter, you must enable IGMP proxy to validate other configurations of IGMP proxy. All other configuration tasks are optional and are not listed in sequence. You can configure them as required.

## 2.1.4 Update History

Version	Revision
V100R002C02B050	This is the first release.

## 2.2 Enabling IGMP Proxy

This section describes how to enable IGMP proxy.

To enable IGMP proxy for multiple VLANs, you can perform [2.2.3 Enabling IGMP Proxy for a VLAN](#) repeatedly as required.

[2.2.1 Establishing the Configuration Task](#)

[2.2.2 Enabling IGMP Proxy Globally](#)

[2.2.3 Enabling IGMP Proxy for a VLAN](#)

[2.2.4 \(Optional\) Configuring the IGMP Version](#)

[2.2.5 Checking the Configuration](#)

### 2.2.1 Establishing the Configuration Task

#### Applicable Environment

By default, IGMP proxy is disabled on the S-switch. You need to enable IGMP proxy for the S-switch by using commands.

After IGMP proxy is enabled globally, IGMP proxy still remains disabled for a VLAN, by default. You also need to enable IGMP proxy for a VLAN by using commands.

Based on the version of IGMP applied in a network, you can configure the S-switch enabled with IGMP proxy to process IGMP packets of the corresponding version.

## Pre-configuration Tasks

Before enabling IGMP proxy, complete the following tasks:

- Creating a VLAN
- Adding interfaces to the VLAN

## Data Preparation

To enable IGMP proxy, you need the following data.

No.	Data
1	ID of the VLAN that should be enabled with IGMP proxy
2	(Optional) Version of IGMP packets that can be processed by IGMP proxy enabled for the current VLAN

## 2.2.2 Enabling IGMP Proxy Globally

### Context

Do as follows on the S-switch that receives multicast packets from a router and forwards the multicast packets to hosts on demand:

### Procedure

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

**Step 2** Run the **igmp-proxy enable** command to enable IGMP proxy globally.

By default, IGMP proxy is disabled globally.

----End

## 2.2.3 Enabling IGMP Proxy for a VLAN

### Context

Do as follows on the VLAN that comprise hosts receiving multicast packets:

### Procedure

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

**Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.

**Step 3** Run the **igmp-proxy enable** command to enable IGMP proxy for the VLAN.

By default, IGMP proxy is disabled for a VLAN, even though IGMP proxy is enabled globally. IGMP proxy works normally only when IGMP proxy is enabled both globally and for a VLAN.

----End

## 2.2.4 (Optional) Configuring the IGMP Version

### Context

Do as follows on the S-switch enabled with IGMP proxy:

### Procedure

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

**Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.

**Step 3** Run the **igmp-proxy version *version*** command to configure the version of IGMP packets processed by the S-switch.

By default, IGMP proxy can process both IGMPv1 packets and IGMPv2 packets in a Virtual Local Area Network (VLAN).

----End

## 2.2.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the status of IGMP proxy in a VLAN.	<b>display igmp-proxy [ <i>vlan <i>vlan-id</i></i> ]</b>

### NOTE

After the **display igmp-proxy** command is run, the configuration, including the default configuration, is displayed only when the VLAN is in the Up state. That is, at least one interface in the VLAN is in the Up state.

Run the **display igmp-proxy** command to view the status of IGMP proxy in a VLAN. If IGMP proxy is enabled for the VLAN and the version of IGMP packets that can be processed is correct, it means that the configuration succeeds.

```
<Quidway> display igmp-proxy vlan 3
IGMP Proxy Vlan Information for Vlan 3
  IGMP Proxy is Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is Set to default 60
  IGMP Max Response Interval is Set to default 10
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy is Set to default : Permit All
  IGMP Prompt Leave Disable
```

IGMP Router Alert is Not Required  
IGMP Send Router Alert Enable

## 2.3 Configuring a Static Router Interface

This section describes how to configure a static router interface.

### [2.3.1 Establishing the Configuration Task](#)

### [2.3.2 Configuring an Interface as a Static Router Interface](#)

### [2.3.3 Checking the Configuration](#)

## 2.3.1 Establishing the Configuration Task

### Applicable Environment

In a stable network, if a host needs to receive certain multicast packets for a long time, you can configure a router interface on the S-switch as a static router interface. The static router interface does not age and can be deleted only by using commands. In addition, it reduces the repeated processes of aging and learning of router interfaces, saves the device resources, and improves the system performance.

### Pre-configuration Tasks

Before configuring a static router interface, complete the following task:

- [2.2 Enabling IGMP Proxy](#)

### Data Preparation

To configure a static router interface, you need the following data.

No.	Data
1	Number of the interface to be configured as a static router interface and ID of the VLAN to which the interface belongs

## 2.3.2 Configuring an Interface as a Static Router Interface

### Context

Do as follows on the interface to be configured as a static router interface:

### Procedure

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

**Step 2** Run the following command as required.

- Run the **interface** *interface-type interface-number* command to enter the Ethernet or GE interface view.
- Run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk view.

**Step 3** Run the **igmp-proxy static-router-port** *vlan vlan-id* command to configure the interface as a static router interface.

----End

## 2.3.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about static router interfaces.	<b>display igmp-proxy router-port</b> <i>vlan vlan-id</i>

### NOTE

When you use the **display igmp-proxy router-port** command, information about a static router interface is displayed only when the interface is in the Up state.

Run the **display igmp-proxy router-port** command. If information about static router interfaces is correctly displayed, it means that the configuration succeeds.

```
<Quidway> display igmp-proxy router-port vlan 2
Total Number of Router Port on Vlan 2 is 1
  Port Name      UpTime      Expires      Flags
  Ethernet0/0/2  00:01:30    --           STATIC
```

## 2.4 Configuring a Multicast Group Policy

This section describes how to configure a multicast group policy for a VLAN.

[2.4.1 Establishing the Configuration Task](#)

[2.4.2 Configuring Rules to Filter Multicast Packets](#)

[2.4.3 \(Optional\) Configuring a Multicast Group Policy](#)

[2.4.4 Checking the Configuration](#)

### 2.4.1 Establishing the Configuration Task

#### Applicable Environment

To restrict the IP multicast groups that hosts in a VLAN can access, you can configure a multicast group policy for the VLAN. You can also restrict the number of multicast groups that a host can join.

#### Pre-configuration Tasks

Before configuring a multicast group policy, complete the following tasks:

- Creating a VLAN
- Adding hosts to the VLAN
- Enabling IGMP Proxy

## Data Preparation

To configure a multicast group policy, you need the following data.

No.	Data
1	(Optional) Number of a basic ACL, ID of the VLAN to be configured with a multicast group policy, and number of multicast member interfaces in the VLAN
2	(Optional) Number of multicast groups that a host can join

## 2.4.2 Configuring Rules to Filter Multicast Packets

### Context

Do as follows on the S-switch that receives multicast packets from a router and forwards the multicast packets to hosts on demand:

### Procedure

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

**Step 2** Run the **acl [ number ] acl-number** command to create a basic Access Control List (ACL) and enter the ACL view.

The value of *acl-number* ranges from 2000 to 2999.

**Step 3** Run the **rule [ rule-id ] { permit | deny } [ fragment | source { source-address source-wildcard | any } | time-range time-name ]\*** command to create a basic ACL rule.

To configure multiple basic ACL rules, you can repeatedly perform Step 3.



#### NOTE

If the configured rules conflict with each other in the same ACL, the ACL rule with a smaller rule-id takes effect.

----End

## 2.4.3 (Optional) Configuring a Multicast Group Policy

## Context

### NOTE

- When you configure a multicast group policy for a VLAN, hosts in the VLAN cannot join any multicast group if the ACL that corresponds to basic-acl-number is not created.
- After you configure a multicast group policy for a VLAN, hosts in the VLAN cannot join any multicast group if the ACL that corresponds to basic-acl-number is deleted by using the undo acl command.
- A multicast group policy is invalid for static multicast entries.

Do as follows on the S-switch that receives multicast packets from a router and forwards the multicast packets to hosts on demand:

## Procedure

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

**Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.

**Step 3** Run the **igmp-proxy group-policy *acl-number* [ *version-number* ]** command to configure a multicast group policy for the VLAN.

By default, no multicast group policy is available for a VLAN. That is, hosts in the VLAN can join any multicast group.

----End

## 2.4.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the IGMP proxy configuration of a VLAN.	<b>display igmp-proxy [ <i>vlan</i> <i>vlan-id</i> ]</b>

After the preceding configuration, run the **display igmp proxy** command. If the correct configurations of IGMP proxy for a VLAN and of multicast group policies are displayed, it means that the configuration succeeds.

```
<Quidway> display igmp-proxy vlan 3
IGMP Proxy Vlan Information for Vlan 3
  IGMP Proxy is Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is Set to default 60
  IGMP Max Response Interval is Set to default 10
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy is Set to default : Permit All
  IGMP Prompt Leave Disable
  IGMP Router Alert is Not Required
  IGMP Send Router Alert Enable
```

## 2.5 Configuring Prompt Leave for Interfaces in a VLAN

This section describes how to configure prompt leave for interfaces in a VLAN.

### [2.5.1 Establishing the Configuration Task](#)

### [2.5.2 \(Optional\) Configuring Filtering Rules for Interfaces in a VLAN](#)

### [2.5.3 Configuring Prompt Leave for Interfaces](#)

### [2.5.4 Checking the Configuration](#)

## 2.5.1 Establishing the Configuration Task

### Applicable Environment

When an interface on the S-switch receives an IGMP Leave message from a host, the forwarding entry that corresponds to the interface is deleted from the multicast forwarding table immediately without waiting for the aging of the forwarding entry. This is called prompt leave.

When each interface in a VLAN connects to only one host, you can enable prompt leave for interfaces in the VLAN.

#### NOTE

Prompt leave for interfaces in a VLAN takes effect only when IGMPv2 packets can be processed.

### Pre-configuration Tasks

Before configuring prompt leave for interfaces in a VLAN, complete the following task:

- [2.2 Enabling IGMP Proxy](#)

### Data Preparation

To configure prompt leave for interfaces in a VLAN, you need the following data.

No.	Data
1	(Optional) Number of a basic ACL
2	ID of the VLAN to be configured with prompt leave for interfaces

## 2.5.2 (Optional) Configuring Filtering Rules for Interfaces in a VLAN

### Context

Do as follows on member interfaces that should be configured with filtering rules in a VLAN:

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **acl [ number ] acl-number** command to create a basic ACL and enter the ACL view.  
The value of *acl-number* ranges from 2000 to 2999.
- Step 3** Run the **rule [ rule-id ] { permit | deny } [ fragment | source { source-address source-wildcard | any } | time-range time-name ]\*** command to create a basic ACL rule.  
To configure multiple basic ACL rules, you can repeatedly run the command in Step 3.
- End

## 2.5.3 Configuring Prompt Leave for Interfaces

### Context

If each interface in a VLAN connects to only one host, do as follows on the VLAN:

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan vlan-id** command to enter the VLAN view.
- Step 3** Run the **igmp-proxy prompt-leave [ group-policy basic-acl-number ]** command to configure prompt leave for all interfaces in the VLAN.

If **group-policy basic-acl-number** is not specified, an interface on the S-switch promptly leaves a multicast group after receiving the Leave message from a member interface in a VLAN.

By default, no interface is allowed to promptly leave a multicast group.

----End

## 2.5.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the IGMP proxy configuration of a VLAN.	<b>display igmp-proxy [ vlan vlan-id ]</b>

After the preceding configuration, run the **display igmp proxy** command. If the correct configurations of IGMP proxy for a VLAN and of prompt leave of interfaces are displayed, it means that the configuration succeeds.

```
<Quidway> display igmp-proxy vlan 3
IGMP Proxy Vlan Information for Vlan 3
  IGMP Proxy is Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is Set to default 60
  IGMP Max Response Interval is Set to default 10
  IGMP Robustness is Set to default 2
```

```
IGMP Last Member Query Interval is Set to default 1
IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
IGMP Filter Group-Policy is Set to default : Permit All
IGMP Prompt Leave Enable, and acl number is 2008
IGMP Router Alert is Not Required
IGMP Send Router Alert Enable
```

## 2.6 Adjusting IGMP Proxy Parameters

This section describes how to adjust IGMP proxy parameters.

### 2.6.1 Establishing the Configuration Task

### 2.6.2 (Optional) Setting the Aging Time for Router Interfaces

### 2.6.3 (Optional) Setting Parameters for Calculating the Aging Time of Member Interfaces

### 2.6.4 (Optional) Configuring the Router Alert Option of IGMP Packets

### 2.6.5 (Optional) Configuring the Source IP Address of IGMP Packets Sent by the S-switch Enabled with IGMP Proxy

### 2.6.6 Checking the Configuration

## 2.6.1 Establishing the Configuration Task

### Applicable Environment

Based on the actual situations of a network, you can adjust parameters of IGMP proxy to optimize the multicast performance on the S-switch.

- A router interface is an interface through which the S-switch that receives IGMP Query messages and sends IGMP Report and Leave messages.

When a short-run congestion occurs on the network, the transmission of Query messages from the IGMP querier to the S-switch takes a longer time. Therefore, at this time, the S-switch cannot send Report or Leave messages to a router interface if the router interface ages. This may result in the interruption of multicast packets. As a result, you should set large values for the aging time for router interfaces on an unstable network.

- Based on parameters of multicast routers and actual conditions of a network, you can set parameters to change the aging time of member interfaces.

The aging time of a member interface is calculated as follows:

- When receiving an IGMP Report message from hosts, the S-switch sets the aging time by using the following formula:

IGMP robustness variable x interval for sending IGMP General Query messages + maximum response time

The interval for sending IGMP General Query messages should be greater than the maximum response time.

- When receiving an IGMP Leave message from hosts, the S-switch sets the aging time by using the following formula: Interval for sending IGMP Last Member Query messages x IGMP robustness variable

- By default, the source IP address of IGMP packets sent by the S-switch is 192.168.0.1. If 192.168.0.1 is already used by other devices in the same network segment or if multiple S-switch devices exist in a shared network, you can configure the source IP address of

IGMP packets sent by the S-switch. For example, you must specify different source IP addresses for different S-switch devices when the election mechanism is applied to the S-switch devices with different performances.

- The S-switch determines whether to process IGMP packets or not by checking the Router Alert option. You can determine whether IGMP packets received or sent should contain the Route Alert option by using commands.

## Pre-configuration Tasks

Before adjusting IGMP proxy parameters, complete the following task:

- [2.2 Enabling IGMP Proxy](#)

## Data Preparation

To adjust IGMP proxy parameters, you need the following data.

No.	Procedure
1	ID of the VLAN in which IGMP proxy parameters need to be adjusted
2	(Optional) Aging time of a router interface
3	(Optional) Interval for sending IGMP Last Member Query messages
4	(Optional) Interval for sending IGMP General Query messages
5	(Optional) Maximum response time
6	(Optional) IGMP robustness variables.
7	(Optional) Source IP address of IGMP packets sent by the S-switch enabled with IGMP proxy

## 2.6.2 (Optional) Setting the Aging Time for Router Interfaces

### Context

Do as follows on the S-switch that receives multicast packets from a router and forwards the multicast packets to hosts on demand:

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** Run the **igmp-proxy router-aging-time *router-aging-time*** command to set the aging time for router interfaces in the VLAN.

By default,

- If IGMP Query messages are received by an interface, the S-switch sets the remaining aging time of the interface to 180 seconds.
- If PIM Hello messages are received by an interface and the Holdtime value of the Hello messages is larger than the remaining aging time value of the interface, the S-switch sets the aging time of the interface to the Holdtime value contained in the PIM Hello messages.


----End

## 2.6.3 (Optional) Setting Parameters for Calculating the Aging Time of Member Interfaces

### Context

Do as follows on the S-switch that receives multicast packets from a router and forwards the multicast packets to hosts on demand:

### Procedure

- Step 1** Run the **system-view** view to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** (Optional) Run the **igmp-proxy query-interval *query-interval*** command to set the interval for sending IGMP General Query messages.
- Step 4** (Optional) Run the **igmp-proxy lastmember-queryinterval *lastmember-queryinterval*** command to set the interval for sending IGMP Last Member Query messages.
-  **NOTE**
- Setting the interval for sending IGMP Last Member Query messages takes effect in a VLAN only when IGMPv2 packets can be processed in the VLAN.
- Step 5** Run the **igmp-proxy max-response-time *max-response-time*** command to set the maximum response time.
- Step 6** (Optional) Run the **igmp-proxy robust-count *robust-count*** command to set the IGMP robustness variable.

By default, the values of the preceding parameters are as follows:

- Interval for sending IGMP General Query messages: 60 seconds
- Interval for sending Last Member Query messages: 1 second
- Maximum response time: 10 seconds
- IGMP robustness variable: 2

----End

## 2.6.4 (Optional) Configuring the Router Alert Option of IGMP Packets

## Context

Do as follows on the S-switch that receives multicast packets from a router and forwards the multicast packets to hosts on demand:

## Procedure

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

**Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.

**Step 3** (Optional) Run the **igmp-proxy require-router-alert** command to configure the S-switch to receive IGMP packets that must contain the Router Alert option in the IP header.

By default, the S-switch can receive IGMP messages that do not contain the Router Alert option in the IP header from a VLAN.

**Step 4** (Optional) Run the **igmp-proxy send-router-alert** command to configure the S-switch to send IGMP packets that must contain the Router Alert option in the IP header.

By default, the S-switch sends IGMP messages that contain the Router Alert option in the IP header.

----End

## 2.6.5 (Optional) Configuring the Source IP Address of IGMP Packets Sent by the S-switch Enabled with IGMP Proxy

## Context

Do as follows on the S-switch that receives multicast packets from a router and forwards the multicast packets to hosts on demand:

## Procedure

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

**Step 2** Run the **igmp-proxy send-query source-address *ip-address*** command to configure the source IP address for the IGMP messages sent by the S-switch enabled with IGMP proxy.

The IGMP messages sent by the S-switch consist of General Query, Group-Specific Query, Membership Report, and Leave messages.

By default, the source IP address contained in the IGMP General Query message sent by the S-switch is 192.168.0.1.

----End

## 2.6.6 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the IGMP proxy configuration of a VLAN.	<b>display igmp-proxy [ <i>vlan <i>vlan-id</i></i> ]</b>

After the preceding configuration, run the **display igmp proxy** command to check the IGMP proxy configuration of a VLAN. You can obtain the following results:

- The aging time of router interfaces is correctly configured.
- The intervals of Last Member Query messages and IGMP General Query messages, Maximum response time, and IGMP robustness variable are correctly set.
- The Router Alert option is correctly configured.

```
<Quidway> display igmp-proxy vlan 3
IGMP Proxy Vlan Information for Vlan 3
  IGMP Proxy is Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is Set to default 60
  IGMP Max Response Interval is Set to default 10
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy 2444
  IGMP Prompt Leave Enable, and acl number is 2008
  IGMP Router Alert is Not Required
  IGMP Send Router Alert Enable
```

## 2.7 Maintaining IGMP Proxy

This section describes how to maintain IGMP proxy.

### 2.7.1 Clearing Multicast Forwarding Entries

#### 2.7.2 Clearing IGMP Proxy Statistics

#### 2.7.3 Debugging IGMP Proxy

### 2.7.1 Clearing Multicast Forwarding Entries



#### CAUTION

Use this command with caution. Using this command causes temporary interruption of certain multicast flows received by hosts in a VLAN. The hosts in the VLAN receive the multicast flows again only after the forwarding entries are regenerated on the S-switch after it receives IGMP Report messages from the hosts.

To clear dynamic entries in the multicast forwarding table, run the following command in the user view.

Action	Command
Clear dynamic entries in the multicast forwarding table.	<b>reset igmp-proxy group { all   vlan <i>vlan-id</i> }</b>

**NOTE**

This command cannot clear static forwarding entries.

## 2.7.2 Clearing IGMP Proxy Statistics

**CAUTION**

The statistics of IGMP proxy cannot be restored after you clear them. So, use this command with caution.

After you confirm that the statistics of IGMP proxy need to be cleared, run the following command in the user view.

Action	Command
Clear the statistics of IGMP proxy.	<b>reset igmp-proxy statistics</b> [ <i>vlan vlan-id</i> ]

## 2.7.3 Debugging IGMP Proxy

**CAUTION**

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

When a fault occurs on IGMP proxy, you can run the following **debugging** command in the user view to debug and locate the fault.

Action	Command
Enable the debugging of IGMP proxy.	<b>debugging igmp-proxy</b> { <b>all</b>   <b>event</b>   <b>leave</b> [ <i>basic-acl-number</i> ]   <b>packet</b> [ <i>advance-acl-number</i> ]   <b>query</b> [ <i>advance-acl-number</i> ]   <b>report</b> [ <i>advance-acl-number</i> ]   <b>timer</b> }

## 2.8 Configuration Examples

This section provides several configuration examples of IGMP proxy.

[2.8.1 Example for Configuring a Static Router Interface](#)

[2.8.2 Example for Configuring a Multicast Group Policy](#)

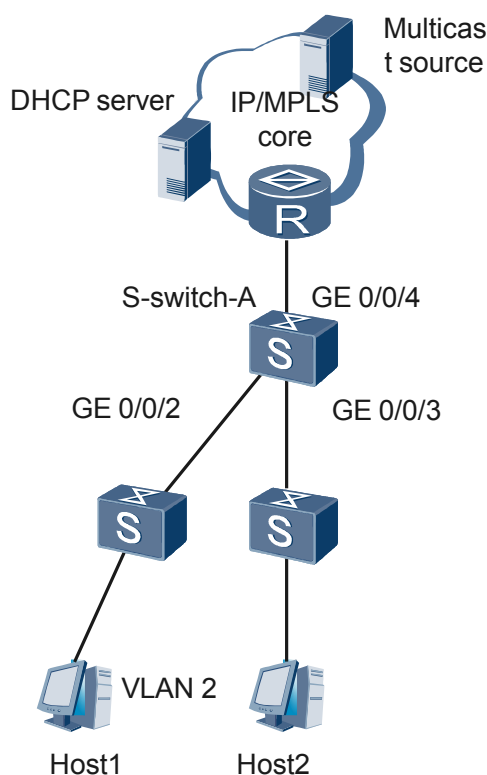
[2.8.3 Example for Configuring Prompt Leave for Interfaces in a VLAN](#)

## 2.8.1 Example for Configuring a Static Router Interface

### Networking Requirements

As shown in [Figure 2-1](#), S-switch-A is connected to a router and multiple hosts. IGMP runs on the router. It is required that S-switch-A should send multicast packets to each host steadily for a long time. At this time, you can configure a static router interface.

**Figure 2-1** Networking diagram of configuring a static router interface



### Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLAN 2 on S-switch-A and add Gigabitethernet 0/0/2, Gigabitethernet 0/0/3, and Gigabitethernet 0/0/4 to VLAN 2.
2. Enable IGMP proxy on S-switch-A.
3. Configure Gigabitethernet 0/0/4 as a static router interface in VLAN 2.
4. On S-switch-A, enable IGMP proxy for VLAN 2.

### Data Preparation

To complete the configuration, you need the following data:

- Gigabitethernet 0/0/4 to be configured as a static router interface
- Host1 and Host2 that belong to VLAN 2

## Configuration Procedure

1. Configure a VLAN.

# Create VLAN 2.

```
<S-switch-A> system-view
[S-switch-A] vlan 2
```

# Add GigabitEthernet 0/0/2, GigabitEthernet 0/0/3, and GigabitEthernet 0/0/4 to VLAN 2.

```
[S-switch-A-vlan2] port GigabitEthernet 0/0/2 to 0/0/3
[S-switch-A-vlan2] port gigabitEthernet 0/0/4
[S-switch-A-vlan2] quit
```

2. Enable IGMP proxy on S-switch-A.

```
[S-switch-A] igmp-proxy enable
```

3. Configure GigabitEthernet 0/0/4 as a static router interface in VLAN 2.

```
[S-switch-A] interface gigabitEthernet 0/0/4
[S-switch-A-GigabitEthernet0/0/4] igmp-proxy static-router-port vlan 2
[S-switch-A-GigabitEthernet0/0/4] quit
```

4. Enable IGMP proxy for VLAN 2.

```
[S-switch-A] vlan 2
[S-switch-A-vlan2] igmp-proxy enable
[S-switch-A-vlan2] quit
```

5. Verify the configuration.

Run the **display igmp-proxy router-port** command on S-switch-A.

```
[S-switch-A] display igmp-proxy router-port vlan 2
Total Number of Router Port on Vlan 3 is 1
```

Port Name	UpTime	Expires	Flags
GigabitEthernet0/0/4	00:02:32	--	STATIC

As shown in the preceding output, GigabitEthernet 0/0/4 is configured as a static router interface.

## Configuration Files

- Configuration File of S-switch-A

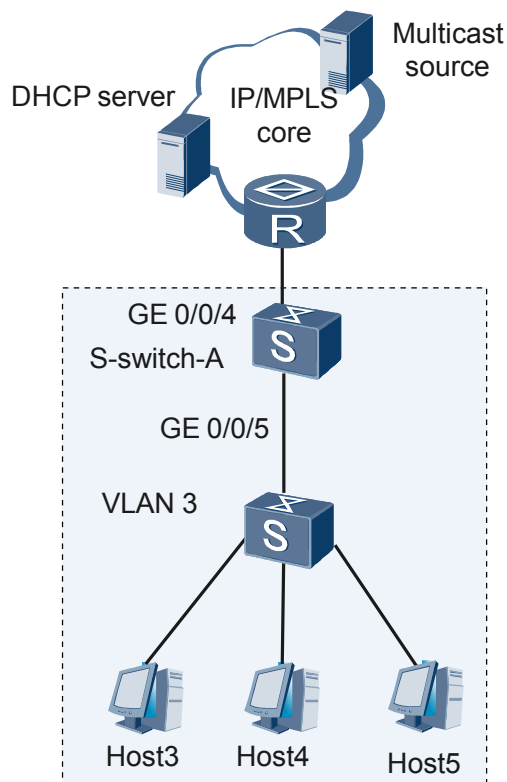
```
#
sysname S-switch-A
#
igmp-proxy enable
#
vlan batch 2
#
vlan 2
igmp-proxy enable
#
interface GigabitEthernet0/0/2
port default vlan 2
#
interface GigabitEthernet0/0/3
port default vlan 2
#
interface GigabitEthernet0/0/4
port default vlan 2
igmp-proxy static-router-port vlan 2
#
return
```

## 2.8.2 Example for Configuring a Multicast Group Policy

## Networking Requirements

As shown in [Figure 2-2](#), Host3, Host4, and Host5 belong to VLAN 3. It is required that the three hosts can not receive multicast packets from group 225.0.0.10.

**Figure 2-2** Networking diagram of configuring a multicast group policy



## Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLAN 3 on S-switch-A and add Gigabitethernet 0/0/5 and Gigabitethernet 0/0/4 to VLAN 3.
2. Enable IGMP proxy on S-switch-A.
3. Configure a multicast group policy for VLAN 3.
4. Enable IGMP proxy for VLAN 3.

## Data Preparation

To complete the configuration, you need the following data:

- Host3, Host4, and Host5 belong to VLAN 3.
- The address of multicast groups that Host3, Host4, and Host5 can not join is 225.0.0.10.

## Configuration Procedure

1. Configure a VLAN.  
# Create VLAN 3.

```
<S-switch-A> system-view
[S-switch-A] vlan 3
```

# Add Gigabitethernet 0/0/5 to Gigabitethernet 0/0/4 to VLAN 3.

```
[S-switch-A-vlan3] port Gigabitethernet 0/0/5
[S-switch-A-vlan3] port gigabitethernet 0/0/4
[S-switch-A-vlan3] quit
```

2. Enable IGMP proxy for the S-switch.

```
[S-switch-A] igmp-proxy enable
```

3. Configure a multicast group policy for VLAN 3.

# Create an ACL.

```
[S-switch-A] acl 2000
[S-switch-A-acl-basic-2000] rule deny source 225.0.0.10 0
[S-switch-A-acl-basic-2000] quit
```

# Configure a multicast group policy.

```
[S-switch-A] vlan 3
[S-switch-A-vlan3] igmp-proxy group-policy 2000
[S-switch-A-vlan3] quit
```

4. Enable IGMP proxy for a VLAN.

# Enable IGMP proxy for VLAN 3.

```
[S-switch-A] vlan 3
[S-switch-A-vlan3] igmp-proxy enable
```

5. Verify the configuration.

From Host3, Host4, or Host5, the S-switch sends IGMP Report messages with a multicast group address as 225.0.0.10. Then, run the **display igmp-proxy port-info** command on S-switch-A. You can view information about the outbound interface of the multicast group.

```
[S-switch-A-vlan3] display igmp-proxy port-info vlan 3
IGMP Proxy Group Port Information on Vlan 3 (Total 1 Groups)

Group          GrpExist PortTotal HostNum PortList          Flag
225.0.0.11     00:01:15 1          1      Gigabitethernet0/0/5  Dyn
```

As shown in the preceding output, no information about the outbound interface of multicast group 225.0.0.15 is displayed. This indicates that no interface joins the multicast group. That is, Gigabitethernet 0/0/5 does not join multicast group 225.0.0.10.

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
igmp-proxy enable
#
vlan batch 3
#
vlan 3
igmp-proxy enable
igmp-proxy group-policy 2000
#
acl number 2000
rule 5 deny source 225.0.0.10 0
#
interface Gigabitethernet0/0/5
port default vlan 3
#
interface Gigabitethernet0/0/4
port default vlan 3
#
```

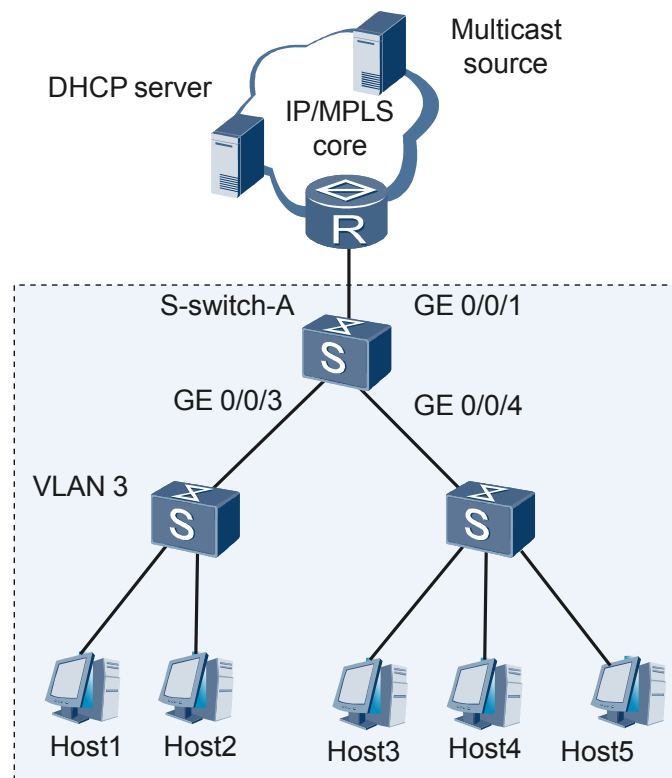
return

## 2.8.3 Example for Configuring Prompt Leave for Interfaces in a VLAN

### Networking Requirements

As shown in [Figure 2-3](#), Gigabitethernet 0/0/3 and Gigabitethernet 0/0/4 on S-switch-A are connected to only one host respectively. Other hosts connected to Gigabitethernet 0/0/3 and Gigabitethernet 0/0/4 do not need to receive multicast packets. Therefore, when receiving IGMP Leave messages from the two interfaces that connect to hosts, S-switch-A deletes the forwarding entries of multicast groups that the hosts leave, without waiting for the timeout of the aging timer. This saves the bandwidth and system resources.

**Figure 2-3** Networking diagram of configuring prompt leave for interfaces in a VLAN



### Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLAN 3 on S-switch-A and add Gigabitethernet 0/0/3, Gigabitethernet 0/0/4, and Gigabitethernet 0/0/1 on S-switch-A to VLAN 3.
2. Enable IGMP proxy on S-switch-A.
3. On S-switch-A, enable prompt leave for interfaces in VLAN 3.
4. On S-switch-A, enable IGMP proxy for VLAN 3.

## Data Preparation

To complete the configuration, you need the following data:

- ID of the VLAN to be configured with prompt leave for interfaces

## Configuration Procedure

1. Configure a VLAN.

# Create VLAN 3 on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] vlan 3
```

# Add Gigabitethernet 0/0/3, Gigabitethernet 0/0/4, and Gigabitethernet 0/0/1 on S-switch-A to VLAN 3.

```
[S-switch-A-vlan3] port Gigabitethernet 0/0/3
[S-switch-A-vlan3] port Gigabitethernet 0/0/4
[S-switch-A-vlan3] port gigabitethernet 0/0/1
[S-switch-A-vlan3] quit
```

2. Enable IGMP proxy for S-switch-A.

```
[S-switch-A] igmp-proxy enable
```

3. Configure prompt leave for interfaces in VLAN 3.

```
[S-switch-A] vlan 3
[S-switch-A-vlan3] igmp-proxy prompt-leave
```

4. Enable IGMP proxy for VLAN 3.

```
[S-switch-A-vlan3] igmp-proxy enable
[S-switch-A-vlan3] quit
```

5. Verify the configuration.

Run the **display igmp-proxy** command on S-switch-A.

```
[S-switch-A] display igmp-proxy vlan 3
IGMP Proxy Vlan Information for Vlan 3
  IGMP Proxy is Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is Set to default 60
  IGMP Max Response Interval is Set to default 10
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy is Set to default : Permit All
  IGMP Prompt Leave Enable
  IGMP Router Alert is Not Required
  IGMP Send Router Alert Enable
```

As shown in the preceding output, the prompt "IGMP Prompt Leave Enable" indicates that the configuration of prompt leave for interface in VLAN 3 succeeds.

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
igmp-proxy enable
#
vlan batch 3
#
vlan 3
  igmp-proxy enable
  igmp-proxy prompt-leave
#
```

```
interface GigabitEthernet0/0/1
 port default vlan 3
#
interface GigabitEthernet0/0/3
 port default vlan 3
#
interface GigabitEthernet0/0/4
 port default vlan 3
#
return
```



# 3 IGMP Snooping Configuration

---

## About This Chapter

This chapter describes the Internet Group Management Protocol (IGMP) snooping function and the method for configuring IGMP snooping on the S-switch.

### [3.1 Introduction](#)

This section describes the advantages of IGMP snooping.

### [3.2 Enabling IGMP Snooping](#)

This section describes how to enable IGMP snooping, how to add an interface to a multicast group statically, and how to configure a static router interface.

### [3.3 Configuring a Multicast Policy in a VLAN](#)

This section describes how to configure a multicast policy in a VLAN.

### [3.4 Configuring Prompt Leave of Interfaces in a VLAN](#)

This section describes how to configure prompt leave of interfaces in a VLAN.

### [3.5 Adjusting IGMP Snooping Parameters](#)

This section describes how to configure the aging time of router interfaces, parameters for computing the aging time of member interfaces in a multicast group, Router Alert option, IGMP snooping responding to the change of Layer 2 network topologies, and IGMP version.

### [3.6 Configuring Replication of a Multicast VLAN](#)

This section describes how to configure replication of a multicast VLAN.

### [3.7 Maintaining IGMP Snooping](#)

This section describes how to debug IGMP snooping.

### [3.8 Configuration Examples](#)

This section provides several configuration examples of the multicast function.

## 3.1 Introduction

This section describes the advantages of IGMP snooping.

### [3.1.1 IGMP Snooping](#)

### [3.1.2 References](#)

### [3.1.3 Logical Relationships Between Configuration Tasks](#)

## 3.1.1 IGMP Snooping

Through Layer 2 multicast, IGMP snooping forwards multicast data packets only to the hosts that request the packets. The advantages of IGMP snooping are as follows:

- It reduces broadcast packets on Layer 2 networks, and thus saves network bandwidth.
- It improves the security of information.
- It facilitates charging each host.

## 3.1.2 References

For more information about IGMP snooping, refer to the following documents:

- Draft-IETF-Magma-Snoop-12
- RFC 1112: Host Extensions for IP Multicasting
- RFC 2236: Internet Group Management Protocol, Version 2
- RFC 2362: Protocol Independent Multicast-Sparse Mode (PIM-SM)

## 3.1.3 Logical Relationships Between Configuration Tasks

To configure the features of IGMP snooping, see the following configurations:

- [3.2 Enabling IGMP Snooping](#)
- [3.3 Configuring a Multicast Policy in a VLAN](#)
- [3.4 Configuring Prompt Leave of Interfaces in a VLAN](#)
- [3.5 Adjusting IGMP Snooping Parameters](#)
- [3.6 Configuring Replication of a Multicast VLAN](#)

## 3.2 Enabling IGMP Snooping

This section describes how to enable IGMP snooping, how to add an interface to a multicast group statically, and how to configure a static router interface.

### [3.2.1 Establishing the Configuration Task](#)

### [3.2.2 Enabling IGMP Snooping on the S-switch](#)

### [3.2.3 Enabling IGMP Snooping in a VLAN](#)

[3.2.4 \(Optional\) Adding an Interface to a Multicast Group Statically](#)

[3.2.5 \(Optional\) Configuring a Static Router Interface](#)

[3.2.6 Checking the Configuration](#)

## 3.2.1 Establishing the Configuration Task

### Applicable Environment

By default, IGMP snooping is disabled on the S-switch. To use IGMP snooping, you must enable it first.

To use IGMP snooping in a VLAN, you also need to enable it because it is disabled in a VLAN by default even after you enable IGMP snooping on the S-switch.

If a host attached to an interface on the S-switch needs to receive the multicast data of a certain group, you can add the interface statically into the group. Then, the interface becomes a static member interface. The static member interface does not age.

In a network with a stable topology, you can set the router interface on the S-switch as the static router interface. The static router interface does not age, and can be deleted only through a command.

#### NOTE

To configure other commands related to IGMP snooping, you must enable IGMP snooping in the system view and the VLAN view.

### Pre-configuration Tasks

Before enabling IGMP snooping, complete the following tasks:

- Creating a VLAN
- Adding interfaces to the VLAN

### Data Preparation

To enable IGMP snooping, you need the following data.

No.	Data
1	ID of the VLAN in which IGMP snooping is to be enabled
2	Number of the static member interface to be configured, ID of the VLAN to which the interface is to be added, and IP address of the multicast group
3	Number of the static router interface to be configured, and ID of the VLAN to which the interface is to be added

## 3.2.2 Enabling IGMP Snooping on the S-switch

## Context

Do as follows to enable IGMP snooping on the S-switch.

## Procedure

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

**Step 2** Run the **igmp-snooping enable** command to enable IGMP snooping on the S-switch.

By default, IGMP snooping is disabled on the S-switch.

----End

## 3.2.3 Enabling IGMP Snooping in a VLAN

## Context

Do as follows to enable IGMP snooping in a VLAN.

## Procedure

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

**Step 2** Run the **igmp-snooping enable** command to enable IGMP snooping in a VLAN.

By default, IGMP snooping in a VLAN is disabled even if IGMP snooping is enabled on the S-switch.

----End

## 3.2.4 (Optional) Adding an Interface to a Multicast Group Statically

## Context

Do as follows to add an interface to a multicast group statically.

## Procedure

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

**Step 2** Run the following commands to enter the Ethernet view.

- Run the **interface interface-type interface-number** command to enter the Ethernet interface view or the GE interface view.
- Run the **interface eth-trunk trunk-id** command to enter the Eth-Trunk interface view.

**Step 3** Run the **igmp-snooping static-group group-address vlan vlan-id** command to add an interface to a multicast group statically.

 **NOTE**

- The S-switch supports up to 1024 static multicast forwarding entries.
- ? When replication of a multicast VLAN or IGMP snooping is configured on the S-switch, and selective QinQ is configured on an interface, you can run the port vlan-mapping command to configure VLAN mapping on the interface in the outbound direction. In this manner, the user VLAN ID carried in the outer VLAN tag is replicated to the inner VLAN tag. The configurations can thus take effect.

----End

## 3.2.5 (Optional) Configuring a Static Router Interface

### Context

Do as follows to configure an interface to be a static router interface.

### Procedure

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

**Step 2** Run the following commands to enter the Ethernet view.

- Run the **interface interface-type interface-number** command to enter the Ethernet interface view or the GE interface view.
- Run the **interface eth-trunk trunk-id** command to enter the Eth-Trunk interface view.

**Step 3** Run the **igmp-snooping static-router-port vlan vlan-id** command to configure an interface to be a static router interface.

 **NOTE**

When replication of a multicast VLAN is configured on the S-switch, you must configure the VLAN specified by *vlan-id* as a multicast VLAN.

----End

## 3.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the status of IGMP snooping on the S-switch.	<b>display current-configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]
Check the status of IGMP snooping in a VLAN.	<b>display igmp-snooping</b> [ <b>vlan</b> <i>vlan-id</i> ]
Check the member interfaces and router interfaces in a multicast group.	<b>display igmp-snooping port-info</b> [ <b>vlan</b> <i>vlan-id</i> ] [ <b>group</b> <i>group-address</i> ] [ <b>verbose</b> ]
Or, check the router interfaces.	<b>display igmp-snooping router-port</b> [ <b>vlan</b> <i>vlan-id</i> ]

If the configuration succeeds, you can obtain the following results by running the preceding commands:

- IGMP snooping on the S-switch is enabled.
- IGMP snooping is enabled in the VLAN.
- The interface is added to the multicast group correctly.
- The static router interface is configured correctly.

 **NOTE**

The status of a static member interface or static router interface must be Up when you run the **display igmp-snooping port-info** command. If the status is Down, you can run the **display current-configuration** command to view the configuration of the static member interface or static router interface.

## 3.3 Configuring a Multicast Policy in a VLAN

This section describes how to configure a multicast policy in a VLAN.

### [3.3.1 Establishing the Configuration Task](#)

### [3.3.2 Creating an ACL](#)

### [3.3.3 Configuring a Multicast Policy](#)

### [3.3.4 Enabling the S-switch to Discard Unknown Multicast Packets on the Multicast Source Interface](#)

### [3.3.5 Checking the Configuration](#)

## 3.3.1 Establishing the Configuration Task

### Applicable Environment

You can configure a multicast policy in a VLAN to enable hosts in the VLAN to access specific IP multicast groups.

### Pre-configuration Tasks

Before configuring a multicast policy in a VLAN, complete the following task:

- [3.2 Enabling IGMP Snooping](#)

### Data Preparation

To configure a multicast policy in a VLAN, you need the following data.

No.	Data
1	ID of the VLAN in which the multicast policy is to be configured and the ID of the multicast source interface in the VLAN
2	(Optional) IGMP version of the multicast policy

## 3.3.2 Creating an ACL

### Context

Do as follows to create an Access Control List (ACL).

### Procedure

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

**Step 2** Run the **acl [ number ] acl-number** command to create a basic ACL and enter the ACL view.

The value of *acl-number* of the basic ACL ranges from 2000 to 2999.

**Step 3** Run the **rule [ rule-id ] { permit | deny } [ fragment | source { source-address source-wildcard | any } | time-range time-name ]\*** command to add a basic ACL rule.

You can perform [Step 3](#) repeatedly to add multiple basic ACL rules.

#### NOTE

If the configured rules conflict with each other in the same ACL, the ACL rule with a smaller rule ID takes effect.

To configure a multicast policy to deny adding the users of a specified VLAN to a multicast group, you can configure the ACL rules as follows:

- Run the **rule deny source source-address source-wildcard** command to create the first rule to disable users from being added to a multicast group.
- Run the **rule permit** command to create the second rule to allow the addition of users to other multicast groups.

Ensure that the ID of the first rule must be smaller than that of the second rule.

----End

## 3.3.3 Configuring a Multicast Policy

### Prerequisite

By default, no multicast policy is available in a VLAN. That is, hosts in a VLAN can join any multicast group.

### Context

Do as follows to configure a multicast policy.

### Procedure

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

**Step 2** Run the **vlan vlan-id** command to enter the VLAN view.

**Step 3** Run the **igmp-snooping group-policy basic-acl-number [ 1 | 2 ]** command to configure a multicast policy.

----End

## Postrequisite



- When a multicast policy is configured for a VLAN, the hosts in the VLAN cannot join any multicast group if the ACL specified by the ACL number is not created.
- After the multicast policy of a VLAN is configured, the hosts in the VLAN cannot join any multicast group if the ACL being used by the multicast policy is deleted with the **undo acl** command.
- Multicast policies are invalid to static multicast entries.

## 3.3.4 Enabling the S-switch to Discard Unknown Multicast Packets on the Multicast Source Interface

### Context

To enable the S-switch to discard unknown multicast packets from a VLAN, do as follows.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** Run the **multicast drop-unknown** command to enable the S-switch to discard unknown multicast packets from a VLAN.

----End

## Postrequisite

By default, the interface is disabled from discarding unknown multicast packets.

After a multicast policy is configured, hosts in the VLAN cannot join multicast groups that are not specified in the policy. Then the S-switch adds no forwarding entries in the multicast forwarding table for other groups even when the hosts send IGMP Report packets. If the function of discarding unknown multicast packets is disabled on the multicast source interface in the VLAN, the S-switch continues to broadcast the received unknown multicast packets in the VLAN. In such a case, the hosts in the VLAN can still receive multicast packets. Therefore, you must enable the S-switch to discard unknown multicast packets on the multicast source interface in the VLAN.

## 3.3.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the configuration of IGMP snooping in a VLAN.	<b>display igmp-snooping [ <i>vlan</i> <i>vlan-id</i> ]</b>
Check information about the outbound interface of a multicast group.	<b>display igmp-snooping port-info [ <i>vlan</i> <i>vlan-id</i> [ <i>group</i> <i>group-address</i> ] ] [ <i>verbose</i> ]</b>

Action	Command
Check the configuration of the function of discarding unknown multicast packets on the multicast source interface.	<b>display current-configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]

If the configuration succeeds, you can obtain the following results by running the preceding commands:

- Multicast policies in the VLAN are configured correctly.
- Interfaces in the VLAN configured with the multicast group policy can join only the multicast group matching the specified ACL.
- The multicast source interface is enabled to discard unknown multicast packets.

## 3.4 Configuring Prompt Leave of Interfaces in a VLAN

This section describes how to configure prompt leave of interfaces in a VLAN.

### [3.4.1 Establishing the Configuration Task](#)

### [3.4.2 \(Optional\) Creating an ACL](#)

### [3.4.3 Configuring Prompt Leave of Interfaces](#)

### [3.4.4 Checking the Configuration](#)

## 3.4.1 Establishing the Configuration Task

### Applicable Environment

If every interface in a VLAN is attached to only one receiver, you can enable prompt leave for interfaces in the VLAN. This can save network bandwidth and resources.

In addition, prompt leave of interfaces makes sense only when the hosts in the VLAN can handle IGMPv2 packets.

### Pre-configuration Tasks

Before configuring prompt leave of interfaces in a VLAN, complete the following task:

- [3.2 Enabling IGMP Snooping](#)

### Data Preparation

To configure prompt leave of interfaces in a VLAN, you need the following data.

No.	Data
1	ID of the VLAN in which prompt leave of interfaces is to be configured

## 3.4.2 (Optional) Creating an ACL

### Context

Do as follows to create an ACL.

### Procedure

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

**Step 2** Run the **acl [ number ] *acl-number*** command to create a basic ACL and enter the ACL view.

The value of *acl-number* of the basic ACL ranges from 2000 to 2999.

**Step 3** Run the **rule [ rule-id ] { permit | deny } [ fragment | source { *source-address source-wildcard* | any } | time-range *time-name* ] \*** command to add a basic ACL rule.

You can perform step [Step 3](#) repeatedly to add multiple basic ACL rules.

----End

## 3.4.3 Configuring Prompt Leave of Interfaces

### Context

Do as follows to configure prompt leave of interfaces.

### Procedure

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

**Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.

**Step 3** Run the **igmp-snooping prompt-leave [ group-policy *basic-acl-number* ]** command to configure prompt leave of interfaces in the VLAN.

If **group-policy *basic-acl-number*** is not specified, the S-switch removes the forwarding entry for an interface as soon as it receives a Leave message from that interface.

By default, prompt leave of interfaces is disabled on the S-switch.

----End

## 3.4.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of IGMP snooping in a VLAN.	<b>display igmp-snooping [ vlan <i>vlan-id</i> ] configuration</b>

If the configuration succeeds, you can find that prompt leave of interfaces is configured correctly with this command.

## 3.5 Adjusting IGMP Snooping Parameters

This section describes how to configure the aging time of router interfaces, parameters for computing the aging time of member interfaces in a multicast group, Router Alert option, IGMP snooping responding to the change of Layer 2 network topologies, and IGMP version.

### 3.5.1 Establishing the Configuration Task

#### 3.5.2 (Optional) Setting the Aging Time of the Router Interface

#### 3.5.3 (Optional) Configuring Parameters for Computing the Aging Time of Member Interfaces

#### 3.5.4 (Optional) Configuring the Router Alert Option in IGMP Messages

#### 3.5.5 (Optional) Configuring the IGMP Snooping Module to Respond to Layer 2 Network Topology Changes

#### 3.5.6 (Optional) Configuring the IGMP Version

#### 3.5.7 Checking the Configuration

## 3.5.1 Establishing the Configuration Task

### Applicable Environment

Based on the actual situations of a network, you can adjust parameters of IGMP snooping to optimize the multicast performance on the S-switch.

- The router interface on the S-switch is the receiving interface of IGMP query messages. The S-switch also forwards membership report messages and group leave messages from the attached hosts to the router through the router interface. If the network is not stable, it will take a longer time for the query messages from the IGMP querier to the S-switch when short-term network congestion occurs. In this case, the S-switch will not forward membership messages or group leave messages when the aging timer of the router interface expires. This will interrupt the transmission of multicast data. Therefore, you can set a longer aging timer for the router interface on the unstable network.
- According to the parameters of the multicast router and the actual network conditions, you can set such four parameters on the S-switch as group-specify query interval, general query interval, Maximal response time, and IGMP robustness variable. The S-switch computes the aging time of multicast group members based on these four parameters.
- Configure the IGMP snooping module in the S-switch. Response to the incident of topology change in Layer 2 enables the IGMP snooping module to realize the topology change in Layer 2. The module transmits data correctly according to the new topology of the network.
- According to the IGMP version on the network, you can specify the version of IGMP messages that the IGMP snooping can process.

### Pre-configuration Tasks

Before adjusting IGMP snooping parameters, complete the following task:

- [3.2 Enabling IGMP Snooping](#)

## Data Preparation

To adjust IGMP snooping parameters, you need the following data.

No.	Procedure
1	ID of the VLAN in which IGMP snooping parameters are to be adjusted
2	(Optional) Aging time of router interfaces
3	(Optional) Group-specific query interval
4	(Optional) General query interval
5	(Optional) Maximum response time
6	(Optional) IGMP robustness variable
7	(Optional) Source IP address to which the IGMP General Query message is sent by the IGMP snooping module when the module responds to the change of Layer 2 network topologies
8	(Optional) Version of IGMP packets that can be processed by the IGMP snooping module in the current VLAN

### 3.5.2 (Optional) Setting the Aging Time of the Router Interface

#### Context

Do as follows to set the aging time of the router interface.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** Run the **igmp-snooping router-aging-time *router-aging-time*** command to set the aging time of the router interface in the VLAN.

By default, the S-switch restores the aging time of the router interface:

- To be 180 seconds when the interface receives IGMP queries
- To be the Holdtime value when the interface receives PIM Hello messages in which the Holdtime value is greater than the remaining aging time of the router interface

----End

### 3.5.3 (Optional) Configuring Parameters for Computing the Aging Time of Member Interfaces

## Context

[Step 3](#) to [Step 5](#) are optional and are not listed in sequence.

The group-specific query interval makes sense only when the hosts in the VLAN can handle IGMPv2 packets.

Do as follows to configure parameters for computing the aging time of member interfaces.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** Run the **igmp-snooping query-interval *query-interval*** command to set the general query interval.
- Step 4** Run the **igmp-snooping lastmember-queryinterval *lastmember-queryinterval*** command to set the last member query interval.
- Step 5** Run the **igmp-snooping max-response-time *max-response-time*** command to set the maximum response time.
- Step 6** Run the **igmp-snooping robust-count *robust-count*** command to set the IGMP robustness variable.

The default values of the parameters are as follows:

- General query interval: 60s
- Group-specific query interval: 1s
- Maximum response time: 10s
- IGMP robustness variable: 2

----End

## 3.5.4 (Optional) Configuring the Router Alert Option in IGMP Messages

### Context

[Step 3](#) and [Step 4](#) are optional and are not listed in sequence.

Do as follows to configure the Router Alert option in IGMP messages.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** Run the **igmp-snooping require-router-alert** command to enable the device to receive IGMP messages that must contain the Router Alert option in the IP header.
- Step 4** Run the **igmp-snooping send-router-alert** command to enable the device to send IGMP messages that must contain the Router Alert option in the IP header.

By default, the S-switch does not require the Router Alert option in the incoming IGMP messages but sends IGMP messages with the Router Alert option.

----End

### 3.5.5 (Optional) Configuring the IGMP Snooping Module to Respond to Layer 2 Network Topology Changes

#### Context

Do as follows to configure the IGMP snooping module to respond to Layer 2 network topology changes.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **igmp-snooping send-query enable** command to enable the IGMP snooping module of the S-switch to respond to Layer 2 network topology changes.
- Step 3** Run the **igmp-snooping send-query source-address ip-address** command to set the source IP address of the IGMP General Query message sent by the S-switch when the IGMP snooping module responds to Layer 2 network topology changes.

By default, the source IP address of the IGMP General Query message sent by the S-switch is 192.168.0.1.

**Step 3** is optional. Configure the IGMP snooping module to respond to Layer 2 network topology changes. After that, the S-switch sends the source IGMP General Query message when it receives the message of the topology change. The downstream S-switches of this S-switch learn the new router interface. After receiving IGMP Query messages, multicast group members respond by sending IGMP Report messages. In this manner, the S-switch and its downstream S-switches can learn new multicast forwarding entries. This function enables the S-switch to continue to transmit data correctly when the Layer 2 topology changes.

When 192.168.0.1 is already occupied by other devices in the network, run the **igmp-snooping send-query source-address** command to change the source IP address of the IGMP General Query sent by the IGMP snooping module.

----End

### 3.5.6 (Optional) Configuring the IGMP Version

#### Context

Do as follows to configure the IGMP version.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **igmp-snooping version { 1 | 2 }** command to configure the version of IGMP messages that can be processed by the IGMP snooping module of the S-switch.

By default, the IGMP snooping module can process both IGMPv1 messages and IGMPv2 messages in a VLAN.

----End

### 3.5.7 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of IGMP snooping in a VLAN.	<b>display igmp-snooping [ vlan <i>vlan-id</i> ] configuration</b>

After the preceding configuration, run the **display igmp-snooping** command to check the configuration of IGMP snooping in a VLAN. You can find the following results:

- The aging time of router interfaces is set correctly.
- The last member query interval, the general query interval, the maximum response time, and the IGMP robustness variable are set correctly.
- The Router Alert option is configured correctly.
- The version of IGMP messages that can be processed by the S-switch enabled with IGMP snooping is set correctly.

## 3.6 Configuring Replication of a Multicast VLAN

This section describes how to configure replication of a multicast VLAN.

### 3.6.1 Establishing the Configuration Task

#### 3.6.2 Configuring Replication of a Multicast VLAN on the S-switch

#### 3.6.3 Configuring Replication of a Multicast VLAN in a VLAN

#### 3.6.4 Setting the Mapping Between Multicast VLANs and User VLANs

#### 3.6.5 Checking the Configuration

### 3.6.1 Establishing the Configuration Task

#### Applicable Environment

Through replication of a multicast VLAN, you can send multicast packets to different VLANs. Thus, you can easily manage and control the multicast source and the multicast group members to reduce the waste on bandwidths.

Replication of a multicast VLAN of the S-switches bases on IGMP snooping of the S-switches. IGMP snooping of the S-switches, however, is disabled by default. Thus, you need to enable IGMP snooping of the S-switches before enabling replication of a multicast VLAN.

Replication of a multicast VLAN is also based on IGMP snooping of VLANs. IGMP snooping of VLANs is disabled by default. You need to enable IGMP snooping of VLANs before enabling replication of a multicast VLAN.

In the implementation of replication of a multicast VLAN, VLANs are classified into multicast VLANs and user VLANs. The multicast VLANs aggregate multicast traffic, and the user VLANs are the VLANs to which multicast group members belong. To implement replication of a multicast VLAN:

- For a multicast VLAN, enable IGMP snooping in the VLAN, and then enable replication of a multicast VLAN.
- For a user VLAN, enable only IGMP snooping.

Bind the multicast VLAN to the user VLAN after enabling replication of a multicast VLAN.

If a user VLAN needs to receive multicast data of a group, you can set the multicast group that the user VLAN to join as a static multicast VLAN entry. The static entry does not age.

In a network with a stable topology, you can set a router interface of a multicast VLAN on the S-switch as a static router interface. The static router interface does not age, but can be deleted only through commands.

## Pre-configuration Tasks

Before configuring replication of a multicast VLAN, complete the following tasks:

- Disabling the load balancing function of the multicast Eth-Trunk, which is disabled by default
- Creating a VLAN
- Adding interfaces to the VLAN
- [3.2 Enabling IGMP Snooping](#)

When the interface on the S-switch acts as the member interface, you must configure the default VLAN of the interface as the user VLAN. In addition, you must use the **port hybrid untagged vlan** command to add the interface to the multicast VLAN in untagged mode. Otherwise, the host on the member interface cannot receive multicast packets.

## Data Preparation

To configure replication of a multicast VLAN, you need the following data.

No.	Data
1	IDs of the VLANs to be configured with replication of a multicast VLAN

## 3.6.2 Configuring Replication of a Multicast VLAN on the S-switch

### Context

To configure replication of a multicast VLAN on the S-switch, do as follows.

## Procedure


- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **mcast-vlan enable** command to enable replication of a multicast VLAN on the S-switch.
- By default, replication of a multicast VLAN is disabled on the S-switch.
- End

### 3.6.3 Configuring Replication of a Multicast VLAN in a VLAN

#### Context

To configure replication of a multicast VLAN in a VLAN, do as follows.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** Run the **mcast-vlan enable** command to enable replication of a multicast VLAN in a VLAN.
- By default, replication of a multicast VLAN is disabled in a VLAN.
-  **NOTE**
- You cannot set the control VLAN of the Rapid Ring Protection Protocol (RRPP) and the management VLAN of the Huawei Group Management Protocol (HGMP) as a multicast VLAN.
- End

### 3.6.4 Setting the Mapping Between Multicast VLANs and User VLANs

#### Context

To set the mapping between multicast VLANs and user VLANs, do as follows.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan *vlan-id*** command to enter the VLAN view.
- Step 3** Run the **mcast user-vlan *vlan-id* to *vlan-id*** command to set the mapping between multicast VLANs and user VLANs.
- End

### 3.6.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check replication of a multicast VLAN on the S-switch.	<b>display current-configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]
Check replication of a multicast VLAN in a VLAN.	<b>display current-configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]
Check the mapping between multicast VLANs and user VLANs.	<b>display current-configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]
Check multicast VLAN entries.	<b>display multicast forwarding-table</b> [ <b>vlan</b> <i>vlan-id</i> [ <b>group</b> <i>group-address</i> ] ] [   { <b>begin</b>   <b>include</b>   <b>exclude</b> } <i>regular-expression</i> ]
Check the configurations of static router interfaces.	<b>display igmp-snooping router-port</b> [ <b>vlan</b> <i>vlan-id</i> ]

If the configuration succeeds, you can obtain the following results by running the preceding commands:

- Check replication of a multicast VLAN on the S-switch. This function is enabled.
- Check replication of a multicast VLAN in a VLAN. This function is enabled.
- Check the mapping between multicast VLANs and user VLANs. The mapping between them is set correctly.
- Check static multicast VLAN entries. The static entries are configured correctly.
- Check the configurations of static router interfaces. The static router interfaces are configured correctly.

## 3.7 Maintaining IGMP Snooping

This section describes how to debug IGMP snooping.

### [3.7.1 Clearing Dynamic Entries in a Multicast Forwarding Table](#)

### [3.7.2 Clearing the Statistics on IGMP Snooping](#)

### [3.7.3 Debugging IGMP Snooping](#)

## 3.7.1 Clearing Dynamic Entries in a Multicast Forwarding Table



### CAUTION

So, confirm the action before you use the reset igmp-snooping group command. After you run this command to clear forwarding entries of a specified VLAN in a multicast forwarding table, hosts in the VLAN are disabled from receiving multicast flows. The hosts in the VLAN receive the multicast flows again only after the forwarding entries are regenerated on the S-switch, when the S-switch receives IGMP Report messages from the hosts again.

To clear dynamic entries in a multicast forwarding table, run the following command in the user view.

Action	Command
Clear dynamic forwarding entries in a multicast forwarding table.	<b>reset igmp-snooping group</b> { <b>all</b>   <b>vlan</b> <i>vlan-id</i> }

## 3.7.2 Clearing the Statistics on IGMP Snooping



### CAUTION

The statistics on IGMP snooping cannot be restored after you clear them. So, confirm the action before you use this command.

To clear the statistics on IGMP snooping, run the following reset command in the user view.

Action	Command
Clear statistics on IGMP snooping in a VLAN.	<b>reset igmp-snooping statistics</b> [ <b>vlan</b> <i>vlan-id</i> ]

## 3.7.3 Debugging IGMP Snooping



### CAUTION

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

When an operation fault occurs on IGMP snooping, you can run the debugging command in the user view to debug IGMP snooping and locate the fault. To enable debugging, refer to the chapter "Debugging and Diagnosis" in the *Quidway S5300 Series Ethernet Switches Ethernet Switches Configuration Guide - Device Management*. For the description of the **debugging** commands, refer to the *Quidway S5300 Series Ethernet Switches Ethernet Switches Command Reference*.

Action	Command
Debug IGMP Snooping.	<b>debugging igmp-snooping</b> { <b>all</b>   <b>event</b>   <b>leave</b> [ <i>basic-acl-number</i> ]   <b>packet</b> [ <i>advance-acl-number</i> ]   <b>query</b> [ <i>advance-acl-number</i> ]   <b>report</b> [ <i>advance-acl-number</i> ]   <b>timer</b> }

## 3.8 Configuration Examples

This section provides several configuration examples of the multicast function.

[3.8.1 Example for Configuring Multicast Policies on the Gigabitethernet](#)

[3.8.2 Example for Configuring Prompt Leave of Interfaces in a VLAN](#)

[3.8.3 Example for Setting a Static Router Interface](#)

[3.8.4 Example for Configuring the IGMP Snooping Module to Respond to Layer 2 Network Topology Changes](#)

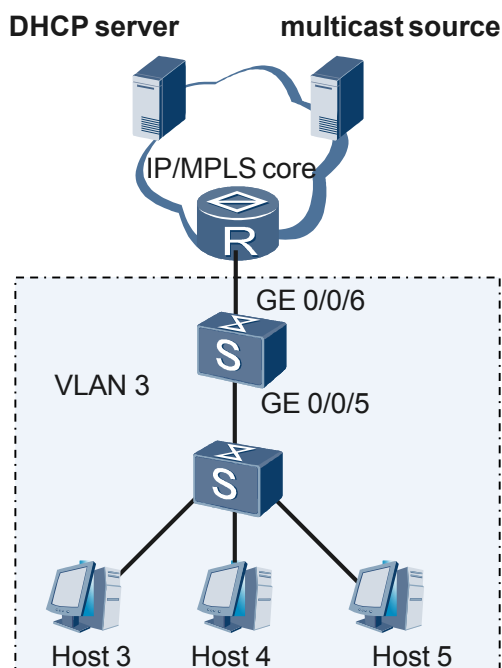
[3.8.5 Example for Configuring Replication of a Multicast VLAN](#)

### 3.8.1 Example for Configuring Multicast Policies on the Gigabitethernet

#### Networking Requirements

In [Figure 3-1](#), Host 3, Host 4, and Host 5 are all in VLAN 3. All these three hosts are allowed to receive data only from the multicast groups 225.0.0.1 to 225.0.0.10.

**Figure 3-1** Networking diagram for configuring multicast policies on the Gigabitethernet



## Configuration Roadmap

The configuration roadmap is as follows:

- Create VLAN 3 on the S-switch and add GigabitEthernet 0/0/5 and GigabitEthernet 0/0/6 to VLAN 3.
- Enable IGMP snooping on the S-switch.
- Configure multicast policies in VLAN 3.
- Enable IGMP snooping in VLAN 3.
- Enable the S-switch to discard unknown multicast packets on a router interface.

## Data Preparation

To complete the configuration, you need the following data:

- Host 3, Host 4, and Host 5 belong to VLAN 3.
- The addresses of multicast groups that Host 3, Host 4, and Host 5 can join range from 225.0.0.1 to 225.0.0.10.

## Configuration Procedure

1. Configure a VLAN.

# Create VLAN 3.

```
[Quidway] vlan 3
```

# Add GigabitEthernet 0/0/5 and GigabitEthernet 0/0/6 to VLAN 3.

```
[Quidway-vlan3] port GigabitEthernet 0/0/5 to 0/0/6
```

```
[Quidway-vlan3] quit
```

2. Enable IGMP snooping on the S-switch.

```
[Quidway] igmp-snooping enable
```

3. Configure multicast policies in VLAN 3.

# Create an ACL.

```
[Quidway] acl 2000
```

```
[Quidway-acl-basic-2000] rule permit source 225.0.0.0 0.0.0.7
```

```
[Quidway-acl-basic-2000] rule permit source 225.0.0.8 0
```

```
[Quidway-acl-basic-2000] rule permit source 225.0.0.9 0
```

```
[Quidway-acl-basic-2000] rule permit source 225.0.0.10 0
```

```
[Quidway-acl-basic-2000] quit
```

# Configure multicast policies.

```
[Quidway] vlan 3
```

```
[Quidway-vlan3] igmp-snooping group-policy 2000
```

4. Enable IGMP snooping in the VLAN.

```
[Quidway-vlan3] igmp-snooping enable
```

5. Enable the S-switch to discard unknown multicast packets in the VLAN.

```
[Quidway-vlan3] multicast drop-unknown
```

6. Verify the configuration.

# Verify that Host 3, Host 4, and Host 5 can join the multicast groups with the group addresses from 225.0.0.1 to 225.0.0.10.

Send IGMP Report messages from Host 3, Host 4, or Host 5 to the multicast group 225.0.0.2. Then, run the **display igmp-snooping port-info** command on the S-switch to view information about the outbound interface of the multicast group.

```
[Quidway-vlan3] display igmp-snooping port-info
```

```

IGMP Snooping Group Port Information on Vlan 3 (Total 1 Groups)
Group      GrpExist  PortTotal  HostNum  PortList      Flag
225.0.0.2  00:05:06  1          1        GigabitEthernet0/0/5
Dyn

```

The preceding output shows that GigabitEthernet 0/0/5 joins the multicast group 225.0.0.2.

# Verify that Host 3, Host 4, and Host 5 can join only the multicast groups that are in the range of 225.0.0.1 to 225.0.0.10.

Send IGMP Report messages from Host 3, Host 4, or Host 5 to the multicast group 225.0.0.15. Then, run the **display igmp-snooping port-info** command on the S-switch to view information about the outbound interface of the multicast group.

```

[Quidway-vlan3] display igmp-snooping port-info
IGMP Snooping Group Port Information on Vlan 3 (Total 1 Groups)
Group      GrpExist  PortTotal  HostNum  PortList      Flag
225.0.0.2  00:05:06  1          1        GigabitEthernet0/0/5      Dyn

```

The preceding output does not contain information about the outbound interface of the multicast group at 225.0.0.15. This indicates that no interface joins the multicast group. That is, GigabitEthernet 0/0/5 does not join the multicast group at 225.0.0.15.

## Configuration Files

```

#
 sysname Quidway
#
 igmp-snooping enable
#
 vlan batch 3
#
 vlan 3
  igmp-snooping enable
  igmp-snooping group-policy 2000
 multicast drop-unknown
#
 acl number 2000
 rule 5 permit source 225.0.0.0 0.0.0.7
 rule 10 permit source 225.0.0.8 0
 rule 15 permit source 225.0.0.9 0
 rule 20 permit source 225.0.0.10 0
#
 interface ethernet0/0/5
  port default vlan 3
#
 return

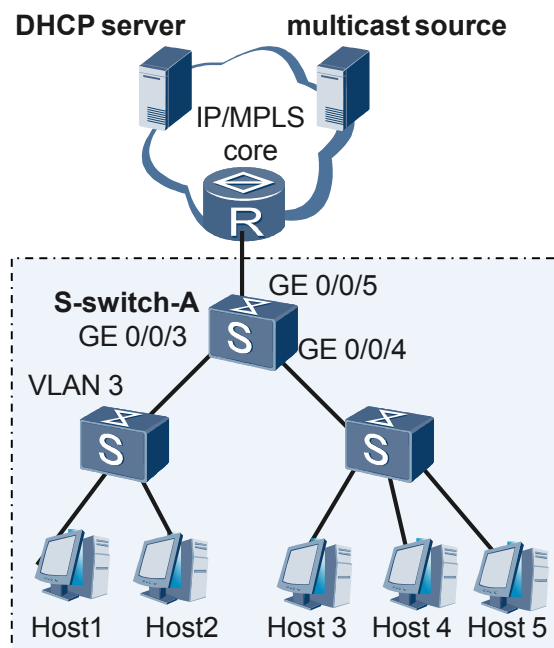
```

## 3.8.2 Example for Configuring Prompt Leave of Interfaces in a VLAN

### Networking Requirements

As shown in [Figure 3-2](#), GigabitEthernet 0/0/3 and GigabitEthernet 0/0/4 on S-switch-A are connected to only one host respectively. Other hosts connected to GigabitEthernet 0/0/3 and GigabitEthernet 0/0/4 do not need to receive multicast packets. Therefore, when receiving IGMP Leave messages from the two interfaces that connect to hosts, S-switch-A deletes the forwarding entries of the multicast groups that the hosts leave, without waiting for the timeout of the aging timer. This saves bandwidths and system resources.

**Figure 3-2** Networking diagram for configuring prompt leave of interfaces in a VLAN



## Configuration Roadmap

The configuration roadmap is as follows:

- Create VLAN 3 on S-switch-A. Add Gigabitethernet 0/0/3, Gigabitethernet 0/0/4, and Gigabitethernet 0/0/5 to VLAN 3.
- Enable IGMP snooping on S-switch-A.
- On S-switch-A, enable prompt leave of interfaces in VLAN 3.
- On S-switch-A, enable IGMP snooping in VLAN 3.

## Data Preparation

To complete the configuration, you need the following data:

- The VLAN to be configured with prompt leave of interfaces is VLAN 3.

## Configuration Procedure

1. Configure a VLAN.

# Create VLAN 3 on S-switch-A.

```
[S-switch-A] vlan 3
```

# On S-switch-A, add Gigabitethernet 0/0/3, Gigabitethernet 0/0/4, and Gigabitethernet 0/0/5 to VLAN 3.

```
[S-switch-A-vlan3] port Gigabitethernet 0/0/3 to 0/0/5
[S-switch-A-vlan3] quit
```

2. Enable IGMP snooping on S-switch-A.

```
[S-switch-A] igmp-snooping enable
```

3. Configure prompt leave of interfaces in VLAN 3.

```
[S-switch-A] vlan 3
[S-switch-A-vlan3] igmp-snooping prompt-leave
```

4. Enable IGMP snooping in VLAN 3.

```
[S-switch-A-vlan3] igmp-snooping enable
```

5. Verify the configuration.

Run the **display igmp-snooping** command on S-switch-A.

```
[S-switch-A] display igmp-snooping vlan 3 configuration
IGMP Snooping Configuration for Vlan 3
    igmp-snooping enable
    igmp-snooping prompt-leave
```

As shown in the preceding output, the prompt "IGMP Prompt Leave Enable" indicates that prompt leave of interfaces is configured successfully in VLAN 3.

## Configuration Files

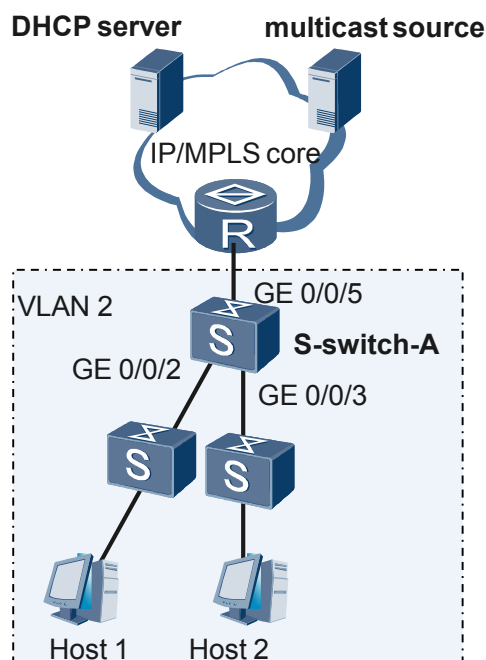
```
#
sysname S-switch-A
#
igmp-snooping enable
#
vlan batch 3
#
vlan 3
    igmp-snooping enable
    igmp-snooping prompt-leave
#
interface GigabitEthernet0/0/3
    port default vlan 3
#
interface GigabitEthernet0/0/4
    port default vlan 3
#
interface GigabitEthernet0/0/5
    port default vlan 3
#
return
```

### 3.8.3 Example for Setting a Static Router Interface

#### Networking Requirements

As shown in [Figure 3-3](#), the S-switch is connected to a router running the IGMP multicast protocol and hosts. It is required that the S-switch forward multicast data to all the hosts.

**Figure 3-3** Networking diagram for configuring a static router interface



## Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLAN 2 on S-switch-A, and add Gigabitethernet 0/0/2, Gigabitethernet 0/0/3, and Gigabitethernet 0/0/5 to VLAN 2.
2. Enable IGMP snooping on S-switch-A.
3. Set Gigabitethernet 0/0/5 as a static router interface.
4. Enable IGMP snooping in VLAN 2 on S-switch-A.

## Data Preparation

To complete the configuration, you need the following data:

- Gigabitethernet 0/0/5 is set as a static router interface.
- Host 1 and Host 2 belong to VLAN 2.

## Configuration Procedure

1. Configure a VLAN.  
# Create VLAN 2.  

```
[S-switch-A] vlan 2
```

  
# Add Gigabitethernet 0/0/2, Gigabitethernet 0/0/3, and Gigabitethernet 0/0/5 to VLAN 2.  

```
[S-switch-A-vlan2] port Gigabitethernet 0/0/2 to 0/0/3 0/0/5  
[S-switch-A-vlan2] quit
```
2. Enable IGMP snooping on S-switch-A.  

```
[S-switch-A] igmp-snooping enable
```
3. Set Gigabitethernet 0/0/5 as a static router interface.  

```
[S-switch-A] interface ethernet0/0/5
```

```
[S-switch-A-interface ethernet0/0/5] igmp-snooping static-router-port vlan 2  
[S-switch-A-interface ethernet0/0/5] quit
```

4. Enable IGMP snooping in VLAN 2.

```
[S-switch-A] vlan 2  
[S-switch-A-vlan2] igmp-snooping enable
```

5. Verify the configuration.

Run the **display igmp-snooping router-port** command on S-switch-A.

```
[S-switch-A] display igmp-snooping router-port vlan 2  
Total Number of Router Port on Vlan 2 is 1  
  Port Name      UpTime      Expires      Flags  
  Gigabitethernet0/0/5  00:00:32  --          STATIC
```

The displayed information shows that Gigabitethernet 0/0/5 has been set as a static router interface.

## Configuration Files

```
#  
sysname S-switch-A  
#  
igmp-snooping enable  
#  
vlan batch 2  
#  
vlan 2  
igmp-snooping enable  
#  
interface Gigabitethernet0/0/2  
port default vlan 2  
#  
interface Gigabitethernet0/0/3  
port default vlan 2  
#  
interface Gigabitethernet0/0/5  
port default vlan 2  
igmp-snooping static-router-port vlan 2  
#  
return
```

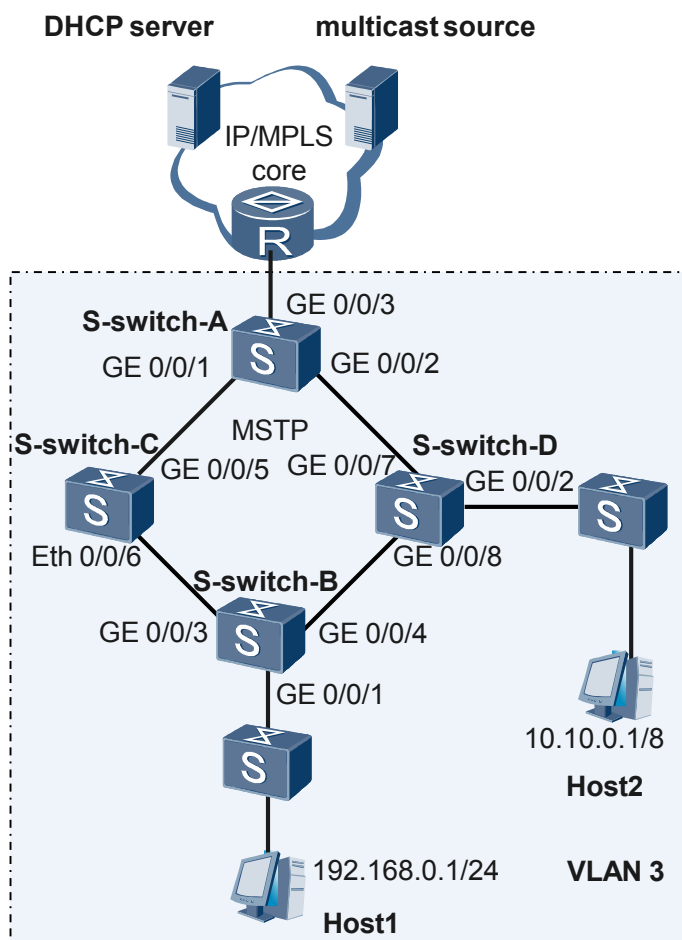
## 3.8.4 Example for Configuring the IGMP Snooping Module to Respond to Layer 2 Network Topology Changes

### Networking Requirements

In a network as shown in [Figure 3-4](#), the four S-switches connect in turn as a ring network. This increases the reliability of the network. To prevent routing loops, the Multiple Spanning Tree Protocol (MSTP) is run on the four S-switches. Host 1 and Host 2 need to receive data sent by the multicast resource. The IP address of Host 1 is 192.168.0.1 and the IP address of Host 2 is 10.10.0.1.

It is required that Host 1 and Host 2 still receive multicast data without interruption when the MSTP topology changes because of a link fault.

**Figure 3-4** Networking diagram for configuring the IGMP snooping module to respond to Layer 2 network topology changes



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure MSTP on all the S-switches.
2. Create VLAN 3 on all the S-switches and add interfaces to VLAN 3.
3. Enable IGMP snooping on all the S-switches.
4. Enable IGMP snooping in VLAN 3 on all the S-switches.
5. Configure the IGMP snooping module to respond to Layer 2 network topology changes on S-switch-A.

## Data Preparation

To complete the configuration, you need the following data:

- Set the source IP address contained in the IGMP General Query message to 192.168.0.100 when configuring the IGMP snooping module to respond to Layer 2 network topology changes.

## Configuration Procedure

1. Configure MSTP on all the S-switches.

The configuration method is not mentioned here. For the detailed method of configuring MSTP, refer to the *Quidway S5300 Series Ethernet Switches Ethernet Switches Configuration Guide - Gigabitethernet*.

2. Create VLAN 3 on all the S-switches and add interfaces to VLAN 3.

# Create VLAN 3 on S-switch-A. Add interface Gigabitethernet 0/0/1, interface Gigabitethernet 0/0/2 and interface Gigabitethernet 0/0/3 to VLAN3.

```
[S-switch-A] vlan 3
[S-switch-A-vlan3] quit
[S-switch-A] interface Gigabitethernet 0/0/1
[S-switch-A-Gigabitethernet0/0/1] port trunk allow-pass vlan 3
[S-switch-A-Gigabitethernet0/0/1] quit
[S-switch-A] interface Gigabitethernet 0/0/2
[S-switch-A-Gigabitethernet0/0/2] port trunk allow-pass vlan 3
[S-switch-A-Gigabitethernet0/0/2] quit
[S-switch-A] interface Gigabitethernet 0/0/3
[S-switch-A-Gigabitethernet0/0/3] port trunk allow-pass vlan 3
[S-switch-A-Gigabitethernet0/0/3] quit
```

# Create VLAN 3 on S-switch-B. Add interface Gigabitethernet 0/0/1, interface Gigabitethernet 0/0/3 and interface Gigabitethernet 0/0/4 to VLAN 3.

```
[S-switch-B] vlan 3
[S-switch-B-vlan3] port Gigabitethernet 0/0/1
[S-switch-B-vlan3] quit
[S-switch-B] interface Gigabitethernet 0/0/3
[S-switch-B-Gigabitethernet0/0/3] port trunk allow-pass vlan 3
[S-switch-B-Gigabitethernet0/0/3] quit
[S-switch-B] interface Gigabitethernet 0/0/4
[S-switch-B-Gigabitethernet0/0/4] port trunk allow-pass vlan 3
[S-switch-B-Gigabitethernet0/0/4] quit
```

# Create VLAN 3 on S-switch-C. Add interface Gigabitethernet 0/0/5 and interface Gigabitethernet 0/0/6 to VLAN3.

```
[S-switch-C] vlan 3
[S-switch-C-vlan3] quit
[S-switch-C] interface Gigabitethernet 0/0/5
[S-switch-C-Gigabitethernet0/0/5] port trunk allow-pass vlan 3
[S-switch-C-Gigabitethernet0/0/5] quit
[S-switch-C] interface Gigabitethernet 0/0/6
[S-switch-C-Gigabitethernet0/0/6] port trunk allow-pass vlan 3
[S-switch-C-Gigabitethernet0/0/6] quit
```

# Create VLAN 3 on S-switch-D. Add interface Gigabitethernet 0/0/2, Gigabitethernet 0/0/7 and interface Gigabitethernet 0/0/8 to VLAN3.

```
[S-switch-D] vlan 3
[S-switch-D-vlan3] port Gigabitethernet 0/0/2
[S-switch-D-vlan3] quit
[S-switch-D] interface gigabitethernet 0/0/7
[S-switch-D-Gigabitethernet0/0/7] port trunk allow-pass vlan 3
[S-switch-D-Gigabitethernet0/0/7] quit
[S-switch-D] interface gigabitethernet 0/0/8
[S-switch-D-Gigabitethernet0/0/8] port trunk allow-pass vlan 3
[S-switch-D-Gigabitethernet0/0/8] quit
```

3. Enable IGMP snooping on all the S-switches.

# Enable IGMP snooping on S-switch-A.

```
[S-switch-A] igmp-snooping enable
```

# Enable IGMP snooping on S-switch-B, S-switch-C, and S-switch-D.

The configuration method is not mentioned here. The method is the same as that for S-switch-A.

4. Enable IGMP snooping in VLAN 3 on all the S-switches.

# Enable IGMP snooping in VLAN 3 on S-switch-A.

```
[S-switch-A] vlan 3
[S-switch-A-vlan3] igmp-snooping enable
[S-switch-A-vlan3] quit
```

# Enable IGMP snooping in VLAN 3 on S-switch-B, S-switch-C, and S-switch-D.

The configuration method is not mentioned here. The method is the same as that for S-switch-A.

5. Configure the IGMP snooping module to respond to Layer 2 network topology changes on S-switch-A.

```
[S-switch-A] igmp-snooping send-query enable
[S-switch-A] igmp-snooping send-query source-address 192.168.0.100
```

6. Verify the configuration.

First, check whether Host 1 and Host 2 can receive multicast data.

Next, run the **display stp** command on all the S-switches to view which interface is congested. In this manner, you can learn the transmission route of multicast data.

Suppose the result you observe is: interface GigabitEthernet 0/0/4 is congested; the multicast data reach Host1 along the route "from S-switch-A to S-switch-C, then to S-switch-B" and reach Host2 along the route "from S-switch-A to S-switch-D". Run the command shutdown on interface GigabitEthernet 0/0/6 of S-switch-C to close the interface and change the MSTP topology.

Finally, observe whether both Host 1 and Host 2 can still receive multicast data after the network topology changes.

## Configuration Files

- S-switch-A

```
#
 sysname S-switch-A
#
 igmp-snooping enable
 igmp-snooping send-query enable
 igmp-snooping send-query source-address 192.168.0.100
#
 vlan batch 3
#
 stp enable
#
 vlan 3
  igmp-snooping enable
#
 interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 3
  bpdu enable
#
 interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 3
  bpdu enable
#
 interface GigabitEthernet0/0/3
  port trunk allow-pass vlan 3
  bpdu enable
#
 return
```

- **S-switch-B**

```
#
 sysname S-switch-B
#
 igmp-snooping enable
#
 vlan batch 3
#
 stp enable
#
 vlan 3
  igmp-snooping enable
#
 interface GigabitEthernet0/0/1
  port default vlan 3
  bpdu enable
#
 interface GigabitEthernet0/0/3
  port trunk allow-pass vlan 3
  bpdu enable
#
 interface GigabitEthernet0/0/4
  port trunk allow-pass vlan 3
  bpdu enable
#
 return
```
- **S-switch-C**

```
#
 sysname S-switch-C
#
 igmp-snooping enable
#
 vlan batch 3
#
 stp enable
#
 vlan 3
  igmp-snooping enable
#
 interface GigabitEthernet0/0/5
  port trunk allow-pass vlan 3
  bpdu enable
#
 interface GigabitEthernet0/0/6
  port trunk allow-pass vlan 3
  bpdu enable
#
 return
```
- **S-switch-D**

```
#
 sysname S-switch-D
#
 igmp-snooping enable
#
 vlan batch 3
#
 stp enable
#
 vlan 3
  igmp-snooping enable
#
 interface GigabitEthernet0/0/2
  port default vlan 3
  bpdu enable
#
 interface GigabitEthernet0/0/7
  port trunk allow-pass vlan 3
  bpdu enable
```

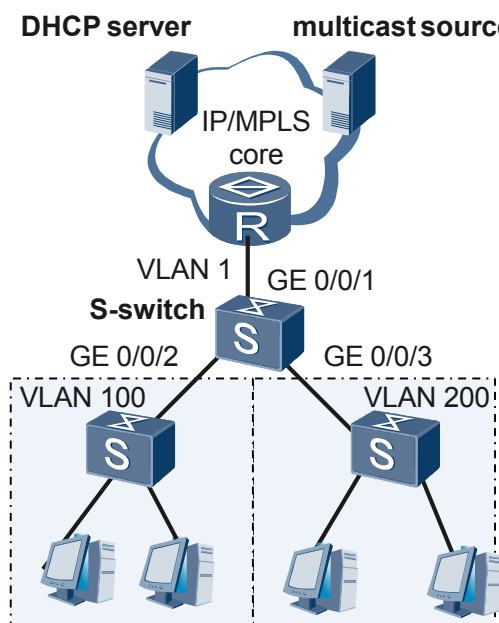
```
#
interface GigabitEthernet0/0/8
 port trunk allow-pass vlan 3
 bpdu enable
#
return
```

### 3.8.5 Example for Configuring Replication of a Multicast VLAN

#### Networking Requirements

In a network as shown in [Figure 3-5](#), four hosts are connected to the S-switch, and they belong to VLAN 100 or VLAN 200. It is required that the four hosts can receive multicast data with IP addresses from 225.0.0.1 to 225.0.0.3.

**Figure 3-5** Networking diagram for configuring replication of a multicast VLAN



#### Configuration Roadmap

The configuration roadmap is as follows:

1. Enable replication of a multicast VLAN on the S-switch.
2. Create VLAN 1, VLAN 100, and VLAN 200, and enable the multicast function in each VLAN view on the S-switch.
3. Set the mapping relationships between multicast VLANs and user VLANs.

#### NOTE

When a user VLAN is the same as a multicast VLAN, you also need to configure the mapping between the user VLAN and the multicast VLAN. Otherwise, the user VLAN cannot receive the multicast data from this VLAN.

4. Configure a static router interface and enable the interface to discard unknown multicast packets.

5. Set the interfaces types of the S-switch and the VLANs that the interfaces belong to.
6. Configure static multicast entries.

## Data Preparation

To complete the configuration, you need the following data:

- Gigabitethernet 0/0/1 is configured as a static router interface and the interface belongs to VLAN 1.
- Gigabitethernet 0/0/2 is configured as a user interface and the interface belongs to VLAN 100.
- Gigabitethernet 0/0/3 is configured as a user interface and the interface belongs to VLAN 200.
- The IP address of the multicast group in entries of static multicast VLANs ranges from 225.0.0.1 to 225.0.0.3.

## Configuration Procedure

1. Enable replication of a multicast VLAN on the S-switch.

```
<Quidway> system-view
[Quidway] igmp-snooping enable
[Quidway] multicast-vlan enable
```

2. Create a VLAN on the S-switch, and configure the corresponding function in each VLAN view.

# Enable replication of a multicast VLAN in the view of VLAN 1.

```
[Quidway] vlan 1
[Quidway-vlan1] igmp-snooping enable
[Quidway-vlan1] multicast-vlan enable
```

# Enable IGMP snooping in the view of VLAN 100.

```
[Quidway] vlan 100
[Quidway-vlan100] igmp-snooping enable
```

# Enable IGMP snooping in the view of VLAN 200.

```
[Quidway] vlan 200
[Quidway-vlan200] igmp-snooping enable
```

3. Set the mapping between a multicast VLAN and its user VLANs and enable the current interface to discard unknown packets.

```
[Quidway] vlan 1
[Quidway-vlan1] multicast user-vlan 100
[Quidway-vlan1] multicast user-vlan 200
[Quidway-vlan1] multicast drop-unknown
```

4. Set Gigabitethernet 0/0/1 as a static router interface.

```
[Quidway] interface Gigabitethernet 0/0/1
[Quidway-Gigabitethernet0/0/1] igmp-snooping static-router-port vlan 1
```

5. Configure the types of interfaces, the VLANs that the interfaces belong to, and the static multicast entries.

# In the view of Gigabitethernet 0/0/1, configure Gigabitethernet 0/0/1 to allow the packet with the VLAN tag whose VLAN ID is 1 to pass through.

```
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 1

# In the view of GigabitEthernet 0/0/2, configure the VLAN that GigabitEthernet 0/0/2
belongs to and a static multicast entry.

[Quidway] interface GigabitEthernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Quidway-GigabitEthernet0/0/2] igmp-snooping static-group 225.0.0.1 vlan 100
[Quidway-GigabitEthernet0/0/2] igmp-snooping static-group 225.0.0.2 vlan 100
[Quidway-GigabitEthernet0/0/2] igmp-snooping static-group 225.0.0.3 vlan 100

# In the view of GigabitEthernet 0/0/3, configure the VLAN that GigabitEthernet 0/0/3
belongs to and a static multicast entry.

[Quidway] interface GigabitEthernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 200
[Quidway-GigabitEthernet0/0/3] igmp-snooping static-group 225.0.0.1 vlan 200
[Quidway-GigabitEthernet0/0/3] igmp-snooping static-group 225.0.0.2 vlan 200
[Quidway-GigabitEthernet0/0/3] igmp-snooping static-group 225.0.0.3 vlan 200
```

#### 6. Verify the configuration.

First, run the **display multicast forwarding-table** command on the S-switch to view the configuration of static entries of the multicast VLAN.

```
[Quidway] display multicast forwarding-table
The total number of multicast forwarding table entries is 6.
Multicast forwarding table information on VLAN 1 (total 3 Groups)
Group                                OutPort                                OutVLAN
225.0.0.1(2 OutPorts)                GigabitEthernet0/0/2(1 OutVLAN)        VLAN 100
                                      GigabitEthernet0/0/3(1 OutVLAN)        VLAN 200
225.0.0.2(2 OutPorts)                GigabitEthernet0/0/2(1 OutVLAN)        VLAN 100
                                      GigabitEthernet0/0/3(1 OutVLAN)        VLAN 200
225.0.0.3(2 OutPorts)                GigabitEthernet0/0/2(1 OutVLAN)        VLAN 100
                                      GigabitEthernet0/0/3(1 OutVLAN)        VLAN 200

Total entries are matched : 6
```

As shown in the output, you can learn that the outbound interfaces of multicast groups with the addresses 01-00-5e-00-00-01, 01-00-5e-00-00-02, and 01-00-5e-00-00-03 are GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3. This indicates that the member interfaces GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3 are added to the multicast groups with the addresses from 225.0.0.1 to 225.0.0.3.

Secondly, check whether the hosts in VLAN 100 and VLAN 200 can receive multicast packets.

## Configuration Files

```
#
sysname Quidway
#
igmp-snooping enable
#
vlan batch 1 100 200
#
multicast-vlan enable
#
vlan 1
igmp-snooping enable
multicast-vlan enable
multicast drop-unknown
```

```
multicast user-vlan 100
multicast user-vlan 200
vlan 100
  igmp-snooping enable
vlan 200
  igmp-snooping enable
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 1
  igmp-snooping static-router-port vlan 1
#
interface GigabitEthernet0/0/2
  port link-type trunk
  port trunk allow-pass vlan 100
  igmp-snooping static-group 225.0.0.1 vlan 100
  igmp-snooping static-group 225.0.0.2 vlan 100
  igmp-snooping static-group 225.0.0.3 vlan 100
#
interface GigabitEthernet0/0/3
  port link-type trunk
  port trunk allow-pass vlan 200
  igmp-snooping static-group 225.0.0.1 vlan 200
  igmp-snooping static-group 225.0.0.2 vlan 200
  igmp-snooping static-group 225.0.0.3 vlan 200
#
return
```

# 4 Controllable Multicast Configuration

---

## About This Chapter

This chapter describes the principle of controllable multicast and procedures for configuring controllable multicast.

### [4.1 Introduction](#)

This section describes the basics of controllable multicast.

### [4.2 Configuring Controllable Multicast](#)

This section describes how to configure controllable multicast.

### [4.3 Configuration Example](#)

This section provides a configuration examples of controllable multicast.

## 4.1 Introduction

This section describes the basics of controllable multicast.

### 4.1.1 Overview of Controllable Multicast

#### 4.1.2 Basic Principle

### 4.1.1 Overview of Controllable Multicast

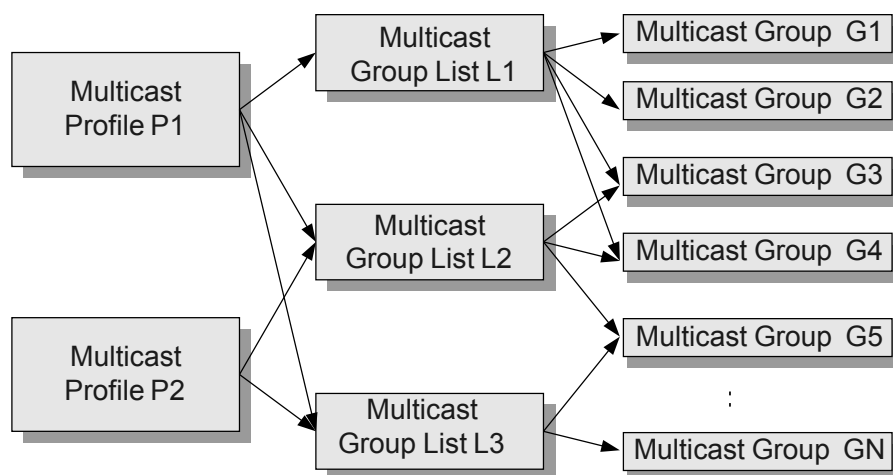
Traditional multicast services are uncontrollable. Users running traditional multicast need to send IGMP Report messages to join related multicast groups, and then receive multicast packets of the groups. With the development of IPTV services, uncontrollable multicast services cannot meet the operation requirements. IPTV services aim to make prohibits. Users can watch a program (that is, join a multicast group) only after they pay fees. If users are not authenticated, the requirements of IPTV operation cannot be met. Therefore, controllable multicast is developed to control the authorities of users to join a certain multicast group. When a user requests to join a multicast group, the S-switch must authenticate the request, and reject illegal or unauthorized requests.

## 4.1.2 Basic Principle

### Controllable Multicast Mechanism Provided by the S-switch

The S-switch provides the controllable multicast mechanism based on VLANs. Through multicast profiles, the S-switch controls the authorities of users to join related multicast groups. To flexibly configure the rights of users to join related multicast groups, the S-switch provides control mechanisms of three levels, that is, multicast group, multicast group list, and multicast profile, as shown in [Figure 4-1](#).

**Figure 4-1** Hierarchical control mechanisms of controllable multicast



## Multicast Group

A multicast group corresponds to a multicast address such as 224.1.1.1. A multicast group can be regarded as a channel or program of IPTV.

## Multicast Group List

A multicast group list is a set of multicast groups. A multicast group list can contain several multicast groups. For example, in [Figure 4-1](#), multicast group list L1 contains G1, G2, G3, and G4. A multicast group can be contained in several multicast group lists. For example, G3 is contained in L1 and L2.

## Multicast Profile

A multicast profile is a set of multicast group lists, and defines the frame of users' rights to join related multicast groups. A multicast profile can contain several multicast group lists. For example, in [Figure 4-1](#), multicast profile P1 contains L1, L2, and L3. A multicast group list can be contained in several multicast profiles. For example, L2 is contained in P1 and P2. Multicast group lists that are added to a profile have their attributes, that is, preview and watch. If a multicast group list is added to a multicast profile in watch mode, users of the multicast profile can watch all multicast groups in the list. If a multicast group list is added to a multicast profile in preview mode, users of the multicast profile can preview all multicast groups in the list.

## Usage of Multicast Profiles

Profiles of controllable multicast are applied to VLANs. A VLAN can use only one profile, but a profile can be used by multiple VLANs.

## Control Flow

The S-switch on which controllable multicast is applied can control the generation of Layer 2 multicast forwarding entries by intercepting IGMP Report messages. After receiving an IGMP Report message from a user, the S-switch obtains the profile based on the VLAN to which the message belongs. If the group is not in the list of the profile, the user cannot join the group. The S-switch intercepts the IGMP Report message and do not generate the related forwarding entry. Therefore, the user cannot receive data flows of this group. If the multicast group is in the list of the profile, check the mode through which the list is added to the profile. If the list is added to the profile in watch mode, the S-switch allows the IGMP Report message to pass through. If the list is added to the profile in preview mode, the S-switch allows the IGMP Report message to pass through and starts a timer at the same time. When the preview period expires, the S-switch deletes the forwarding entry of the group and intercepts subsequent IGMP Report messages of the group. Thus, the preview function is implemented.

## 4.2 Configuring Controllable Multicast

This section describes how to configure controllable multicast.

### [4.2.1 Establishing the Configuration Task](#)

### [4.2.2 Configuring a Multicast Group](#)

### [4.2.3 Configuring a Multicast Group List](#)

### [4.2.4 Configuring a Multicast Profile](#)

[4.2.5 Applying a Multicast Profile to a VLAN](#)[4.2.6 Configuring the Preview Information of a User in a Multicast Profile](#)[4.2.7 Configuring the Maximum Number of Multicast Groups That Users in a Multicast Profile Can Simultaneously Join](#)[4.2.8 Checking the Configuration](#)

## 4.2.1 Establishing the Configuration Task

### Applicable Environment

To control the authorities of users to join related multicast groups, you can configure controllable multicast.

### Pre-configuration Tasks

Before configuring controllable multicast, complete the following task:

- Configuring Layer 2 multicast, that is, IGMP snooping or IGMP proxy, to forward multicast packets normally

### Data Preparation

To configure controllable multicast, you need the following data.

No.	Data
1	Name and IP address of a multicast group
2	Name of a multicast list
3	Name of a multicast profile
4	IDs of the user VLANs that apply multicast profiles

## 4.2.2 Configuring a Multicast Group

### Context

Do as follows on the S-switch.

### Procedure

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

**Step 2** Run the **btv** command to enter the BTV view.

**Step 3** Run the **multicast-group group-name ip-address multicast-group-address** command to configure a multicast group.

By default, no multicast group is configured on the S-switch.

----End

## 4.2.3 Configuring a Multicast Group List

### Context

Do as follows on the S-switch.

### Procedure

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

**Step 2** Run the **btv** command to enter the BTV view.

**Step 3** Run the **multicast-list** *list-name* command to create a multicast group list and enter the view of the multicast group list.

**Step 4** Run the **add multicast-group** { **name** *group-name* | **index** *start-index* **to** *end-index* } command to add a multicast group to the multicast group list.

By default, no multicast group list is configured on the S-switch.

----End

## 4.2.4 Configuring a Multicast Profile

### Context

Do as follows on the S-switch.

### Procedure

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

**Step 2** Run the **btv** command to enter the BTV view.

**Step 3** Run the **multicast-profile** *profile-name* command to create a multicast profile and enter the view of the multicast profile.

**Step 4** Run the **add multicast-list** { **name** *list-name* | **index** *start-index* **to** *end-index* } { **watch** | **preview** } command to add a multicast group list to the multicast profile.

By default, no multicast profile is configured on the S-switch.

----End

## 4.2.5 Applying a Multicast Profile to a VLAN

### Context

Do as follows on the S-switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan** *vlan-id* command to enter the VLAN view.
- Step 3** Run the **attach multicast-profile** *profile-name* command to set the binding relationship between the VLAN and the multicast profile.
- By default, the binding relationship between the VLAN and the multicast profile is not set in S-switch.
- End

## 4.2.6 Configuring the Preview Information of a User in a Multicast Profile

### Context

Do as follows on the S-switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **btv** command to enter the BTV view.
- Step 3** Run the **multicast-profile** *profile-name* command to create a multicast profile and enter the view of the multicast profile.
- Step 4** Run the **multicast-preview** { **interval** *interval-value* | **minutes** *minutes-value* | **times** *times-value* } command to configure the preview information of a user.
- End

## 4.2.7 Configuring the Maximum Number of Multicast Groups That Users in a Multicast Profile Can Simultaneously Join

### Context

Do as follows on the S-switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **btv** command to enter the BTV view.
- Step 3** Run the **multicast-profile** *profile-name* command to create a multicast profile and enter the view of the multicast profile.
- Step 4** Run the **max-program-num** *max-value* command to configure the maximum number of multicast groups that users in the multicast profile can simultaneously join.



#### NOTE

On the S-switch, users in a multicast profile can simultaneously join a maximum of eight multicast groups. This is also the default setting.

----End

## 4.2.8 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about a multicast group.	<b>display multicast-group</b> [ <i>group-name</i> ]
Check information about a multicast group list.	<b>display multicast-list</b> [ <i>list-name</i> ]
Check information about a multicast profile.	<b>display multicast-profile</b> [ <i>profile-name</i> [ <b>verbose</b> ] ]
Check information about a VLAN where a multicast profile is applied.	<b>display multicast-profile-apply</b>

## 4.3 Configuration Example

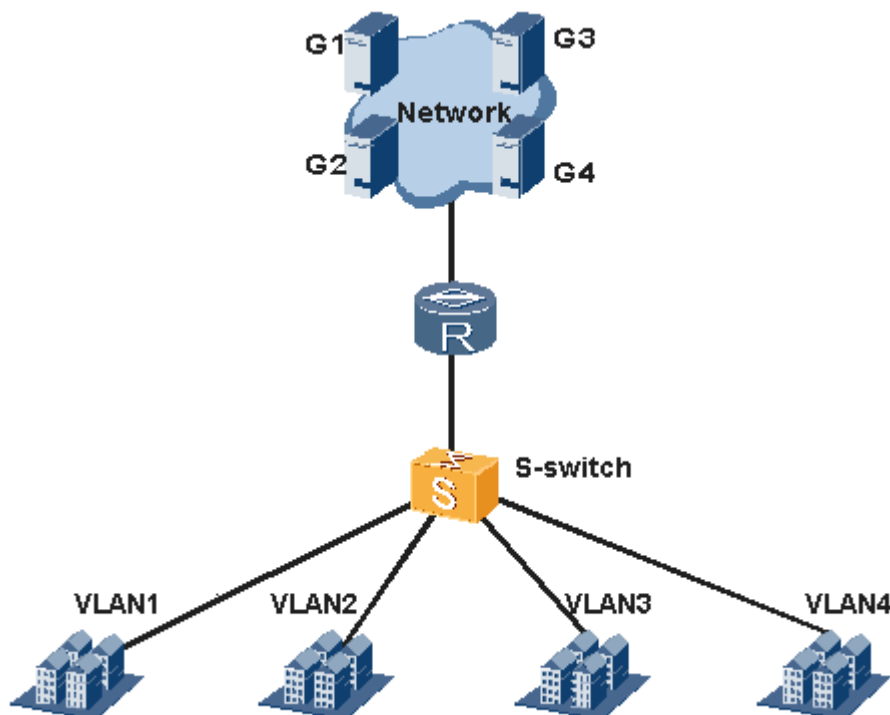
This section provides a configuration examples of controllable multicast.

### 4.3.1 Example for Configuring Controllable Multicast

## 4.3.1 Example for Configuring Controllable Multicast

### Networking Requirements

As shown in [Figure 4-2](#), multicast sources G1 (225.0.0.1), G2 (225.0.0.2), G3 (225.0.0.3), and G4 (225.0.0.4) exist in the network connected to the router. You are required to configure users in VLAN 1 to watch G1 and G2, users in VLAN 2 to watch G1 and G2 and preview G3 and G4, and users in VLAN 3 and VLAN 4 to watch all multicast groups. The users in a VLAN can simultaneously receive data of only two multicast groups. Users in VLAN 2 can preview a group for eight times each day. The period for a user to preview a group is three minutes, and the interval for a user to preview a group is five minutes.

**Figure 4-2** Networking diagram of configuring controllable multicast

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure user VLANs.
2. Configure IGMP snooping or IGMP proxy.
3. Configure controllable multicast, two multicast group lists L1 (G1, G2) and L2 (G3, G4), and three multicast profiles P1, P2, and P3.

## Data Preparation

To complete the configuration, you need the following data:

- Name of each multicast group
- Name of each multicast group list
- Name of each multicast profile

## Configuration Procedure

1. Configure user VLANs. The configuration details are not mentioned here.
2. Configure IGMP snooping or IGMP proxy. The configuration details are not mentioned here.
3. Configure controllable multicast.

# Configure multicast groups.

```
<Quidway> system-view
[Quidway] btv
[Quidway-btv] multicast-group G1 ip-address 225.0.0.1
[Quidway-btv] multicast-group G2 ip-address 225.0.0.2
```

```
[Quidway-btv] multicast-group G3 ip-address 225.0.0.3
[Quidway-btv] multicast-group G4 ip-address 225.0.0.4
```

# Configure multicast group lists.

```
[Quidway-btv] multicast-list L1
[Quidway-btv-list-L1] add multicast-group name G1
[Quidway-btv-list-L1] add multicast-group name G2
[Quidway-btv-list-L1] quit
[Quidway-btv] multicast-list L2
[Quidway-btv-list-L2] add multicast-group name G3
[Quidway-btv-list-L2] add multicast-group name G4
[Quidway-btv-list-L2] quit
```

# Configure multicast profiles.

```
[Quidway-btv] multicast-profile P1
[Quidway-btv-profile-P1] add multicast-list name L1 watch
[Quidway-btv-profile-P1] max-program-num 2
[Quidway-btv-profile-P1] quit
[Quidway-btv] multicast-profile P2
[Quidway-btv-profile-P2] add multicast-list name L1 watch
[Quidway-btv-profile-P2] add multicast-list name L2 preview
[Quidway-btv-profile-P2] max-program-num 2
[Quidway-btv-profile-P2] multicast-preview interval 5
[Quidway-btv-profile-P2] multicast-preview minutes 3
[Quidway-btv-profile-P2] multicast-preview times 8
[Quidway-btv-profile-P2] quit
[Quidway-btv] multicast-profile P3
[Quidway-btv-profile-P3] add multicast-list name L1 watch
[Quidway-btv-profile-P3] add multicast-list name L2 watch
[Quidway-btv-profile-P3] max-program-num 2
[Quidway-btv-profile-P3] quit
```

# Apply multicast profiles to VLANs.

```
[Quidway] vlan 1
[Quidway-vlan1] attach multicast-profile P1
[Quidway-vlan1] quit
[Quidway] vlan 2
[Quidway-vlan2] attach multicast-profile P2
[Quidway-vlan2] quit
[Quidway] vlan 3
[Quidway-vlan3] attach multicast-profile P3
[Quidway-vlan3] quit
[Quidway] vlan 4
[Quidway-vlan4] attach multicast-profile P3
[Quidway-vlan4] quit
```

# Verify the configuration.

```
[Quidway-btv] display multicast-profile-apply
```

Vlan-id	Index	Profile-name
Vlan1	2	P1
Vlan2	3	P2
Vlan3	4	P3
Vlan4	4	P3

Total: 4

```
[Quidway-btv] display multicast-profile
```

Index	Profile-Name	Multicast-list	Attach-VLAN
1	P1	1	1
2	P2	2	1
3	P3	2	2

Total: 3

```
[Quidway-btv] display multicast-list
```

Index	Multicast-list-name	Multicast-group
-------	---------------------	-----------------

```
-----
1          L1          2
2          L2          2
```

Total: 2

[Quidway-btv] **display multicast-group**

```
-----
Index      Multicast-group-name  Address
-----
1          G1                225.0.0.1
2          G2                225.0.0.2
3          G3                225.0.0.3
4          G4                225.0.0.4
```

Total: 4

[Quidway-btv-profile-P2] **display multicast-profile P2**

```
Profile-name      : P2
Max-program-num   : 2
Times             : 8
Minutes           : 3
Interval          : 5
```

Referenced Multicast-list (Total: 2)

```
    L1                [w]
    L2                [p]
```

Referenced VLAN: (Total: 1)

Vlan2

[Quidway-btv-profile-P2] **display multicast-profile P2 verbose**

```
Profile-name : P2
Referenced multicast-group (Total: 4)
    G1      225.0.0.1      [w]
    G2      225.0.0.2      [w]
    G3      225.0.0.3      [p]
    G4      225.0.0.4      [p]
```

## Configuration Files

```
sysname Quidway
#
vlan batch 1 to 4
#
vlan 1
 attach multicast-profile P1
vlan 2
 attach multicast-profile P2
vlan 3
 attach multicast-profile P3
vlan 4
 attach multicast-profile P3
#
btv
 multicast-group G1 ip-address 225.0.0.1
 multicast-group G2 ip-address 225.0.0.2
 multicast-group G3 ip-address 225.0.0.3
 multicast-group G4 ip-address 225.0.0.4
#
 multicast-list L1
 add multicast-group name G1
 add multicast-group name G2
 multicast-list L2
 add multicast-group name G3
 add multicast-group name G4
#
 multicast-profile P1
```

```
max-program-num 2
add multicast-list name L1 watch
multicast-profile P2
max-program-num 2
multicast-preview times 8
multicast-preview minutes 3
add multicast-list name L1 watch
add multicast-list name L2 preview
multicast-profile P3
max-program-num 2
add multicast-list name L2 watch
add multicast-list name L1 watch

#
```



# 5 PIM-DM (IPv4) Configuration

---

## About This Chapter

This chapter describes the PIM-DM (IPv4) fundamentals, configuration steps, and maintenance for PIM-DM functions, along with typical examples.

### [5.1 Introduction](#)

This section describes basic principles of PIM-DM.

### [5.2 Configuring Basic PIM-DM Functions](#)

This section describes how to configure basic PIM-DM functions.

### [5.3 Adjusting Control Parameters of a Multicast Source](#)

This section describes how to control the forwarding of multicast data based on the multicast source in a PIM network.

### [5.4 Adjusting Control Parameters for Maintaining Neighbor Relationships](#)

This section describes how to configure control parameters of a PIM-DM Hello message.

### [5.5 Adjusting Control Parameters for Prune](#)

This section describes how to configure control parameters of a PIM-DM Join/Prune message.

### [5.6 Adjusting Control Parameters for State-Refresh](#)

This section describes how to configure control parameters of a PIM-DM State-Refresh message.

### [5.7 Adjusting Control Parameters for Graft](#)

This section describes how to configure control parameters of a PIM-DM Graft message.

### [5.8 Adjusting Control Parameters for Assert](#)

This section describes how to configure control parameters of a PIM-DM Assert message.

### [5.9 Maintaining PIM](#)

This section describes how to debug PIM and clear the statistics of PIM control messages.

### [5.10 Configuration Example](#)

This section provides several configuration examples of PIM-DM.

## 5.1 Introduction

This section describes basic principles of PIM-DM.

### 5.1.1 PIM-DM Overview

#### 5.1.2 PIM-DM Features Supported by the S-switch

### 5.1.1 PIM-DM Overview



#### CAUTION

This chapter is concerned only about the PIM-DM configuration in an IPv4 network.

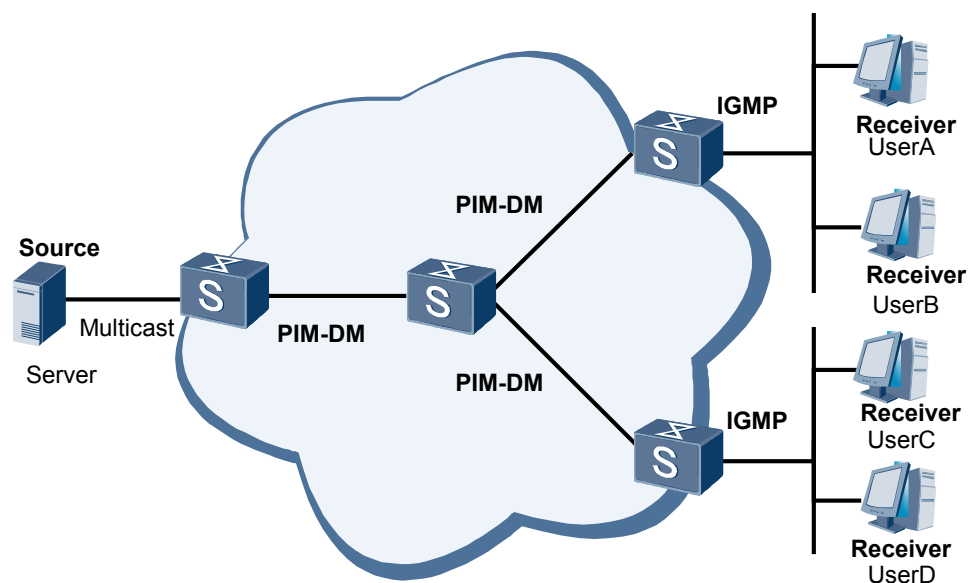
The Protocol Independent Multicast (PIM) is a multicast protocol that is independent of unicast routing protocol such as static route, RIP, OSPF, IS-IS, and BGP. Multicast routing is independent of unicast routing protocols, except that unicast routing protocols are used to generate related multicast routing entries.

Based on the Reverse Path Forwarding (RPF), PIM transmits multicast data across a network. RPF constructs a multicast forwarding tree by using the existing unicast routing information. When a multicast packet reaches a S-switch, the S-switch performs the RPF check first. If the packet does not pass the RPF check, the S-switch directly discards the packet.

The Protocol Independent Multicast-Dense Mode (PIM-DM) is a multicast routing protocol of dense node. It is applicable to a small-scale network with densely-distributed members.

The functions and location of PIM-DM in a multicast network are shown in [Figure 5-1](#).

**Figure 5-1** Location of PIM-DM in the multicast network



## 5.1.2 PIM-DM Features Supported by the S-switch

### Controlling the Forwarding of a Multicast Source

You can configure the Keepalive period of a multicast source and the filtering rules based on multicast sources by using the related commands.

### Adjusting Control Parameters for Setting Up Neighbor Relationship

You can set the interval for sending Hello messages, the period for keeping neighbors reachable, and the maximum delay for triggering Hello messages by using the related commands.

### Adjusting Control Parameters for Forwarding

You can adjust the following control parameters for forwarding by using the related commands:

- Configure the control parameters used to maintain the forwarding relationship.
  - The period for keeping the Prune state of a downstream interface
  - The interval for keeping the Prune state of the downstream interface
  - Whether the Hello messages without the Generation ID option are received
- Configure the control parameters of the Prune state.
  - The delay from the time when the current S-switch receives a Prune message from a downstream S-switch to the time when the current S-switch performs the prune action in the LAN
  - The period for overriding the prune action

### Adjusting Control Parameters for State-Refresh

You can enable or disable State-Refresh, set the interval for sending PIM State-Refresh messages, set the minimum interval for receiving the next State-Refresh message, and set the TTL value for forwarding State-Refresh messages on the S-switch directly connected to the source by using the related commands.

### Adjusting Control Parameters for Graft

You can set the interval for retransmitting Graft messages by using the related commands.

### Adjusting Control Parameters for Assert

You can set the period for a S-switch to retain the Assert state by using the related commands. The S-switch that fails in the election prevents the downstream interface from forwarding multicast data during this period. After the period expires, the downstream interface continues to forward multicast data.

## 5.2 Configuring Basic PIM-DM Functions

This section describes how to configure basic PIM-DM functions.

### [5.2.1 Establishing the Configuration Task](#)

[5.2.2 Enabling IPv4 Multicast Routing](#)[5.2.3 Enabling PIM-DM](#)[5.2.4 Checking the Configuration](#)

## 5.2.1 Establishing the Configuration Task

### Applicable Environment

PIM-DM is applicable to a small-scale network, and most network segments of the network have receivers.

### Pre-configuration Tasks

Before configuring basic PIM-DM functions, complete the following configuration tasks:

- Configuring an IPv4 unicast routing protocol

### Data Preparation

To configure basic PIM-DM functions, you need the following data.

No.	Data
1	Type and number of an interface

## 5.2.2 Enabling IPv4 Multicast Routing

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
multicast routing-enable
```

IPv4 multicast routing is enabled in the public network.

----End

## 5.2.3 Enabling PIM-DM

## Context

Do as follows on the S-switch:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

### Step 3 Run:

```
pim dm
```

PIM-DM is enabled.

After PIM-DM is enabled on the interface and the PIM neighbor relationship is set up between S-switches, the protocol packets sent by the PIM neighbors can be processed. You can run the **undo pim dm** command to disable PIM-DM on the interface.

----End

## 5.2.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check PIM on interfaces of the public network.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check PIM neighbors of the public network.	<b>display pim neighbor</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>verbose</b> ] <b>display pim neighbor neighbor-address</b> [ <b>verbose</b> ]
Check the PIM routing table of the public network.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

Run the **display pim interface verbose** command, and you can view the detailed information about PIM on the interface.

```
<Quidway> display pim interface verbose
```

```
Interface: Vlanif1, 192.168.32.11
```

```
PIM version: 2
PIM mode: Dense
PIM DR: 192.168.32.11 (local)
PIM DR Priority (configured): 1
PIM neighbor count: 0
PIM hello interval: 30 s
PIM LAN delay (negotiated): 500 ms
PIM LAN delay (configured): 500 ms
PIM hello override interval (negotiated): 2500 ms
PIM hello override interval (configured): 2500 ms
PIM generation ID: 0X878A2766
PIM hello hold interval: 105 s
PIM hello assert interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM state-refresh processing: enabled
PIM state-refresh interval: 60 s
PIM graft retry interval: 3 s
PIM BFD: disabled
PIM dr-switch-delay timer : not configured
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
```

## 5.3 Adjusting Control Parameters of a Multicast Source

This section describes how to control the forwarding of multicast data based on the multicast source in a PIM network.

### [5.3.1 Establishing the Configuration Task](#)

### [5.3.2 Configuring the Lifetime of a Source](#)

### [5.3.3 Configuring Filtering Rules Based on Source Addresses](#)

### [5.3.4 Checking the Configuration](#)

## 5.3.1 Establishing the Configuration Task

### Applicable Environment

This configuration is applicable to all PIM-DM networks.

A PIM S-switch checks the passing multicast data. By checking whether the data matches the filtering rule, the S-switch determines whether to forward the data. In this case, you can regard the S-switch as the filter of the multicast data. The filter helps to control the data flow and limit the information that downstream receivers can obtain. Network security is thus ensured.

### Pre-configuration Tasks

Before configuring control parameters of a multicast source, complete the following tasks:

- Configuring a certain unicast routing protocol
- [5.2 Configuring Basic PIM-DM Functions](#)

### Data Preparation

To configure control parameters of a multicast source, you need the following data.

No.	Data
1	Keepalive period of a multicast source
2	Filtering rules of multicast source addresses

## 5.3.2 Configuring the Lifetime of a Source

### Context

Do as follows on the first next hop S-switch connected to the source:



#### NOTE

If there is no special requirement, default values are recommended.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
source-lifetime interval
```

The lifetime of a source is set.

If a S-switch does not receive any (S, G) packet in the lifetime of the source, the S-switch considers that the source stops sending multicast data to G and the (S, G) entry becomes invalid.

When State-Refresh is enabled, the lifetime of the multicast source is prolonged to about the value of *interval*.

----End

## 5.3.3 Configuring Filtering Rules Based on Source Addresses

### Context

Do as follows on the PIM S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

**pim**

The PIM view is displayed.

**Step 3** Run:

**source-policy** *acl-number*

The filter is configured.

Only the packets with the source addresses within the range defined by filtering rules are forwarded. The effect of the filtering is more obvious if the filter is closer to the source.

----End

## 5.3.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type</i> <i>interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 5.4 Adjusting Control Parameters for Maintaining Neighbor Relationships

This section describes how to configure control parameters of a PIM-DM Hello message.

### [5.4.1 Establishing the Configuration Task](#)

### [5.4.2 Configuring the Interval for Sending Hello Messages](#)

### [5.4.3 Configuring the Timeout Period of a Neighbor](#)

### [5.4.4 Refusing to Receive the Hello Message Without the Generation ID Option](#)

### [5.4.5 Checking the Configuration](#)

## 5.4.1 Establishing the Configuration Task

### Applicable Environment

PIM S-switches exchange Hello messages to set up neighbor relationships and negotiate various control parameters.

The S-switch interface connected to hosts needs to be enabled with PIM. You can establish the PIM neighbor relationship on the interface to process various PIM packets. The configuration, however, has the security vulnerability. When a host maliciously generates PIM Hello messages and sends many packets to a S-switch, the S-switch may fail.

Enabling PIM silent on a S-switch interface connected to hosts can effectively prevent this attack and protect the S-switch. PIM silent is applicable to the S-switch interface connected to the host network segment that can be connected to only one PIM S-switch.



#### NOTE

S-switch under the control of default values can work normally. In the S-switch, users can adjust related parameters according to the specific network environment. If there is no special requirement, default values are recommended.

## Pre-configuration Tasks

Before adjusting control parameters for maintaining neighbor relationships, complete the following tasks:

- Configuring a unicast routing protocol
- [5.2 Configuring Basic PIM-DM Functions](#)

## Data Preparation

To adjust control parameters for maintaining neighbor relationships, you need the following data.

No.	Data
1	Timeout period of the neighbor
2	Interval for sending Hello messages
3	Maximum delay for triggering Hello messages

## 5.4.2 Configuring the Interval for Sending Hello Messages

### Context

Do as follows on the PIM-DM S-switch:



#### NOTE

The configuration involves the following cases:

- Global configuration: It is valid on each interface.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration

1. Run:  
`system-view`  
The system view is displayed.
  2. Run:  
`pim`  
The PIM view is displayed.
  3. Run:  
`timer hello interval`  
The interval for sending Hello messages is set.
- Configuration on an Interface
    1. Run:  
`system-view`  
The system view is displayed.
    2. Run:  
`interface interface-type interface-number`  
The interface view is displayed.
    3. Run:  
`pim timer hello interval`  
The interval for sending Hello messages is set.
    4. Run:  
`pim triggered-hello-delay interval`  
The maximum delay for triggering Hello messages is set.  
  
After the maximum delay is set, the conflict caused by multiple PIM S-switches sending Hello messages simultaneously is prevented.

----End

## 5.4.3 Configuring the Timeout Period of a Neighbor

### Context

Do as follows on the PIM-DM S-switch:

#### NOTE

The configuration involves the following two cases:

- Global configuration: It is valid on each interface.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration
  1. Run:  
`system-view`

- The system view is displayed.
2. Run:  
**pim**  
The PIM view is displayed.
  3. Run:  
**hello-option holdtime interval**  
The timeout period during which the neighbor is reachable is set.  
If no Hello message is received from a neighbor in the timeout period, the neighbor is considered unreachable.
- Configuration on an Interface
    1. Run:  
**system-view**  
The system view is displayed.
    2. Run:  
**interface interface-type interface-number**  
The interface view is displayed.
    3. Run:  
**pim hello-option holdtime interval**  
The timeout period during which the neighbor is reachable is set.  
If no Hello message is received from a neighbor in the timeout period, the neighbor is considered unreachable.
- End

## 5.4.4 Refusing to Receive the Hello Message Without the Generation ID Option

### Procedure

- Step 1** Run:  
**system-view**  
The system view is displayed.
- Step 2** Run:  
**interface interface-type interface-number**  
The interface view is displayed.
- Step 3** Run:  
**pim require-genid**  
The Generation ID option is set in a Hello message.  
The Hello message without the Generation ID option is rejected.  
When the Generation ID option in the Hello message received from an upstream neighbor changes, it indicates that the status of the upstream neighbor changes or the upstream neighbor

restarts. If a S-switch does not want to receive data from an upstream neighbor, the S-switch sends a Prune message after receiving a data packet from the upstream neighbor.

----End

## 5.4.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check information about a PIM neighbor.	<b>display pim neighbor</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>verbose</b> ] <b>display pim neighbor</b> <i>neighbor-address</i> [ <b>verbose</b> ]

## 5.5 Adjusting Control Parameters for Prune

This section describes how to configure control parameters of a PIM-DM Join/Prune message.

### 5.5.1 Establishing the Configuration Task

### 5.5.2 Configuring the Period for an Interface to Keep the Prune State

### 5.5.3 Configuring the Interval for Sending Join/Prune Messages

### 5.5.4 Configuring Control Parameters for Prune

### 5.5.5 Configuring the Interval for Overriding the Prune Action

### 5.5.6 Checking the Configuration

## 5.5.1 Establishing the Configuration Task

### Applicable Environment

When the last member leaves its group, the S-switch sends a Prune message through an upstream interface. After receiving the Prune message, the upstream S-switch performs the prune action and stops sending multicast packets to this network segment. If other downstream S-switches exist in the network, the S-switches need to send a Join message to override the prune action.

S-switches can work normally under the control of the default parameter values. Users can adjust related parameters according to the specific network environment.

### Pre-configuration Tasks

Before adjusting control parameters for prune, complete the following tasks:

- Configuring a unicast routing protocol
- [5.2.4 Checking the Configuration](#)

## Data Preparation

To adjust control parameters of forwarding, you need the following data.

No.	Data
1	Delay for transmitting Prune messages
2	Period for overriding the prune action
3	Timeout period of the Prune state
4	Size of a Join/Prune message
5	Number of (S, G) entries in Join/Prune message sent per second

## 5.5.2 Configuring the Period for an Interface to Keep the Prune State

### Context

Do as follows on the PIM-DM S-switch:

#### NOTE

The configuration involves the following two cases:

- Global configuration: It is valid on each interface.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration

1. Run:

**system-view**

The system view is displayed.

2. Run:

**pim**

The PIM view is displayed.

3. Run:

**holdtime join-prune interval**

The period during which the downstream interface is in the Prune state is set.

After the period expires, the pruned interface starts to forward packets again. Before the period expires, the S-switch refreshes the Prune state when receiving a State-Refresh message.

- Configuration on an Interface

1. Run:

**system-view**

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
pim holdtime join-prune interval
```

The period during which the downstream interface is in the Prune state is set.

After the period is expired, the pruned interface starts to forward packets again.

Before the period expires, the S-switch refreshes the Prune state when receiving a State-Refresh message.

----End

### 5.5.3 Configuring the Interval for Sending Join/Prune Messages

#### Context

Do as follows on the PIM-DM S-switch:

#### Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

- Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

- Step 3** Run:

```
pim timer join-prune interval
```

The interval for sending Join/Prune messages is set.

This command is applicable to the ASM model.

----End

### 5.5.4 Configuring Control Parameters for Prune

#### Context

Do as follows on the PIM-DM S-switch:

#### Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
pim hello-option lan-delay interval
```

The delay for transmitting messages in a LAN is set.

**Step 4** Run:

```
pim hello-option override-interval interval
```

The period for overriding the prune action is set.

----End

## 5.5.5 Configuring the Interval for Overriding the Prune Action

### Context

Do as follows on the PIM-DM S-switch:

 **NOTE**

The configuration involves the following two cases:

- Global configuration: It is valid on each interface.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
pim
```

The PIM view is displayed.

3. Run:

```
hello-option override-interval interval
```

The interval for overriding the prune action is set.

When a S-switch receives a Prune message from an upstream interface, it indicates that another downstream S-switch exists in the LAN. If the S-switch still requests the multicast data, it needs to send a Join message to the upstream S-switch in the override-interval period.

- Configuration on an Interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
pim hello-option override-interval interval
```

The interval for overriding the prune action is set.

----End

## 5.5.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the number of sent or received PIM control packets.	<b>display pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>message-type</b> <i>message-type</i> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 5.6 Adjusting Control Parameters for State-Refresh

This section describes how to configure control parameters of a PIM-DM State-Refresh message.

[5.6.1 Establishing the Configuration Task](#)

[5.6.2 Disabling State-Refresh](#)

[5.6.3 Configuring the Interval for Sending State-Refresh Messages](#)

[5.6.4 Configuring the Period for Receiving the Next State-Refresh Message](#)

[5.6.5 Configuring the TTL Value Carried in a State-Refresh Message](#)

[5.6.6 Checking the Configuration](#)

### 5.6.1 Establishing the Configuration Task

## Applicable Environment

In a PIM-DM network, periodical flooding-prune wastes a lot of network resources. To prevent a pruned interface from forwarding packets, you can enable the State-Refresh function. S-switch periodically send State-Refresh messages to refresh the prune state of interfaces and maintain the SPT.

S-switches can work normally under the control of the default parameter values. Users can adjust related parameters according to the specific network environment.

### NOTE

If there is no specific requirement, default values are recommended.

## Pre-configuration Tasks

Before adjusting control parameters for State-Refresh, complete the following tasks:

- Configuring a unicast routing protocol
- [5.2.4 Checking the Configuration](#)

## Data Preparation

To adjust control parameters for State-Refresh, you need the following data.

No.	Data
1	Interval for sending PIM State-Refresh messages
2	Period for waiting to receive the next State-Refresh message
3	TTL value for forwarding State-Refresh messages

## 5.6.2 Disabling State-Refresh

### Context

Do as follows on all the S-switches in the PIM-DM domain.

### NOTE

By default, PIM-DM State-Refresh is enabled on the interface.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
undo pim state-refresh-capable
```

PIM-DM State-Refresh is disabled.

The interface on which PIM-DM State-Refresh is disabled cannot forward any State-Refresh message.

 **NOTE**

You can run the **pim state-refresh-capable** command to re-enable PIM-DM State-Refresh on the interface.

----End

## 5.6.3 Configuring the Interval for Sending State-Refresh Messages

### Context

Do as follows on all the S-switches in the PIM-DM domain:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
state-refresh-interval interval
```

The interval for sending PIM State-Refresh messages is set.

 **NOTE**

The interval for sending PIM State-Refresh messages should be shorter than the timeout period for keeping the Prune state. You can run the **holdtime join-prune** command to set the timeout period for keeping the Prune state.

----End

## 5.6.4 Configuring the Period for Receiving the Next State-Refresh Message

### Context

Do as follows on all the PIM-DM S-switches in the PIM-DM domain:

## Procedure


- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`pim`  
The PIM view is displayed.
- Step 3** Run:  
`state-refresh-rate-limit interval`  
The period for waiting to receive the next State-Refresh message is set.  
----End

## 5.6.5 Configuring the TTL Value Carried in a State-Refresh Message

### Context

Do as follows on all the PIM-DM S-switches in the PIM-DM domain:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`pim`  
The PIM view is displayed.
- Step 3** Run:  
`state-refresh-ttl ttl-value`  
The TTL value carried in the State-Refresh message is set.
-  **NOTE**  
This command is valid only on the S-switch directly connected to the source.  
----End

## 5.6.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the number of the sent or received PIM control messages.	<b>display pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>message-type</b> <i>message-type</i> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 5.7 Adjusting Control Parameters for Graft

This section describes how to configure control parameters of a PIM-DM Graft message.

### 5.7.1 Establishing the Configuration Task

#### 5.7.2 Configuring the Interval for Retransmitting Graft Messages

#### 5.7.3 Checking the Configuration

## 5.7.1 Establishing the Configuration Task

### Applicable Environment

In a PIM-DM network, if State-Refresh is not enabled, a pruned interface can forward packets after the Prune state times out. If State-Refresh is enabled, the pruned interface may never forward packets.

To enable new members in the network to receive multicast data quickly, a PIM-DM S-switch sends a Graft message through an upstream interface. After receiving the Graft message, the upstream S-switch responds immediately with a Graft-Ack message and enables the interface that receives the Graft message to forward packets.

S-switches can work normally under the control of the default parameter values. Users can adjust the related parameters according to the specific network environment.

#### NOTE

If there is no specific requirement, default values are recommended.

### Pre-configuration Task

Before configuring control parameters for graft, complete the following tasks:

- Configuring a unicast routing protocol

- [5.2.4 Checking the Configuration](#)

## Data Preparation

To configure control parameters for graft, you need the following data.

No.	Data
1	Interval for retransmitting Graft messages

## 5.7.2 Configuring the Interval for Retransmitting Graft Messages

### Context

Do as follows on the PIM-DM S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
pim timer graft-retry interval
```

The interval for retransmitting Graft messages is set.

If the local S-switch does not receive any Graft-Ack message from the upstream S-switch in a specified period, it resends a Graft message.

----End

## 5.7.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check an unacknowledged PIM-DM graft.	<b>display pim grafts</b>

Action	Command
Check the number of the sent or received PIM control messages.	<b>display pim control-message counters</b> [ <i>interface interface-type interface-number</i> ] [ <b>message-type message-type</b> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 5.8 Adjusting Control Parameters for Assert

This section describes how to configure control parameters of a PIM-DM Assert message.

### 5.8.1 Establishing the Configuration Task

#### 5.8.2 Configuring the Period for Keeping the Assert State

#### 5.8.3 Checking the Configuration

## 5.8.1 Establishing the Configuration Task

### Applicable Environment

When a PIM-DM S-switch receives multicast data through a downstream interface, it indicates that other upstream S-switches exist in the network segment. The S-switch sends Assert messages through the interface to elect the unique upstream S-switch.

S-switches can work normally under the control of the default parameter values. Users can adjust related parameters according to the specific network environment.

#### NOTE

If there is no specific requirement, default values are recommended.

### Pre-configuration Tasks

Before adjusting control parameters for Assert, complete the following tasks:

- Configuring a unicast routing protocol
- [5.2.4 Checking the Configuration](#)

### Data Preparation

To adjust control parameters for Assert, you need the following data.

No.	Data
1	Period for keeping the Assert state

## 5.8.2 Configuring the Period for Keeping the Assert State

### Context

Do as follows on the PIM-DM S-switch:



#### NOTE

The configuration involves the following two cases:

- Global configuration: It is valid on each interface.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

#### ● Global Configuration

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
pim
```

The PIM view is displayed.

3. Run:

```
holdtime assert interval
```

The period for holding the Assert state is set.

The S-switch that fails in the election prevents its downstream interface from forwarding multicast data.

After the Holdtime of the Assert state expires, the downstream interface can forward packets.

#### ● Configuration on an Interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
pim holdtime assert interval
```

The period for holding the Assert state is set.

The S-switch that fails in the election prevents its downstream interface from forwarding multicast data.

After the Holdtime period of the Assert state expires, the downstream interface can forward packets.

----End

### 5.8.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the number of sent or received PIM control messages.	<b>display pim control-message counters</b> [ <i>interface interface-type interface-number</i> ] [ <b>message-type message-type</b> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 5.9 Maintaining PIM

This section describes how to debug PIM and clear the statistics of PIM control messages.

### 5.9.1 Clearing Statistics of PIM Control Messages

#### 5.9.2 Monitoring the Running Status of PIM

#### 5.9.3 Debugging PIM

### 5.9.1 Clearing Statistics of PIM Control Messages



#### CAUTION

The statistics of the PIM control messages on the interface cannot be restored after you reset them. Confirm the action before you run the command.

To clear the information about the PIM control messages on the interface, run the following **reset** command in the user view.

Action	Command
Clear information about the PIM control messages on an interface.	<b>reset pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ]

## 5.9.2 Monitoring the Running Status of PIM

During routine maintenance, run the following commands in any view to know the running status of PIM.

Action	Command
Check the unicast routes used by PIM.	<b>display pim claimed-route</b> [ <i>source-address</i> ]
Check the number of sent or received PIM control messages.	<b>display pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>message-type</b> <i>message-type</i> ]
Check unacknowledged PIM-DM Graft messages.	<b>display pim grafts</b>
Check information about PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check information about a PIM neighbor.	<b>display pim neighbor</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>verbose</b> ] <b>display pim neighbor</b> <i>neighbor-address</i> [ <b>verbose</b> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 5.9.3 Debugging PIM



### CAUTION

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

When a fault occurs in the running of PIM, run the **debugging** command in the user view to debug PIM and locate the fault.

Action	Command
Enable all the debugging of PIM.	<b>debugging pim all</b>
Enable the debugging of PIM events.	<b>debugging pim event</b> [ <i>advanced-acl-number</i> ]
Enable the debugging of PIM routes.	<b>debugging pim</b> [ <b>routing-table</b> [ <i>advanced-acl-number</i> ]
Enable the debugging of PIM neighbors.	<b>debugging pim</b> [ <b>neighbor</b> [ <i>basic-acl-number</i>   [ <b>receive</b>   <b>send</b> ] ] *
Enable the debugging of PIM assert.	<b>debugging pim assert</b> [ <i>advanced-acl-number</i>   [ <b>receive</b>   <b>send</b> ] ] *
Enable the debugging of PIM Join/Prune.	<b>debugging pim join-prune</b> [ <i>advanced-acl-number</i>   [ <b>receive</b>   <b>send</b> ] ] *
Enable the debugging of the PIM State-Refresh.	<b>debugging pim</b> [ <b>state-refresh</b> [ <i>advanced-acl-number</i>   [ <b>receive</b>   <b>send</b> ] ] *

## 5.10 Configuration Example

This section provides several configuration examples of PIM-DM.

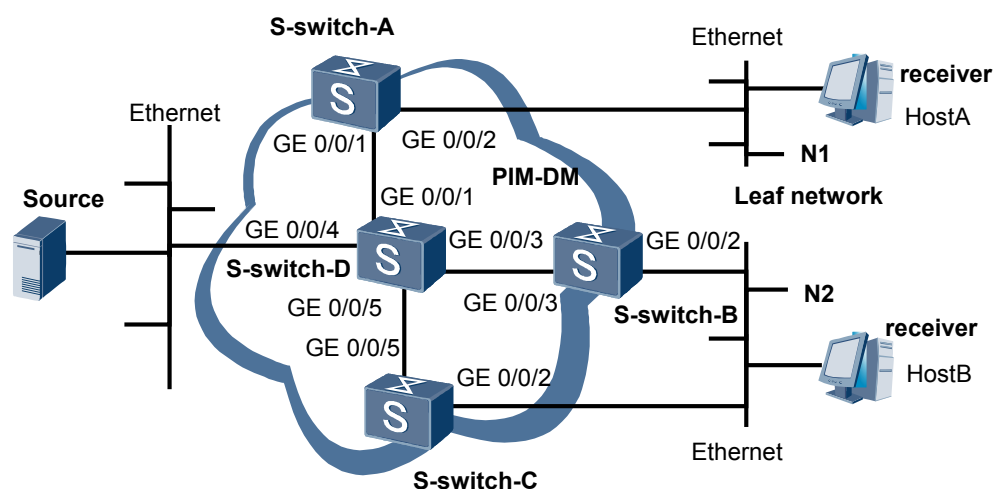
### 5.10.1 Example for Configuring Basic PIM-DM Functions

## 5.10.1 Example for Configuring Basic PIM-DM Functions

### Networking Requirements

In the test network shown in [Figure 5-2](#), multicast and an IGP are deployed, and the unicast routes work normally. It is required to configure S-switches correctly in the network to enable hosts to receive the Video On Demand (VOD) information in multicast mode.

**Figure 5-2** Networking diagram for configuring basic PIM-DM functions



S-switch	Interface	IP address	S-switch	Interface	IP address
S-switch-A	vlanif 1	192.168.1.1/24	S-switch-D	vlanif 1	192.168.2.2/24
	vlanif 2	10.110.1.1/24		vlanif 2	192.168.3.2/24
S-switch-B	vlanif 1	192.168.2.1/24	vlanif 3	vlanif 4	10.110.5.1/24
	vlanif 2	10.110.2.1/24			
S-switch-C	vlanif 1	192.168.3.1/24			
	vlanif 2	10.110.2.2/24			

## Configuration Roadmap

The network is a small-scale experiment network.

1. Enable multicast on each S-switch.-
2. Enable PIM-DM on each interface.-

## Data Preparation

To complete the configuration, you need the following data:

- Address of multicast group G is 225.1.1.1/24.
- Address of multicast source S is 10.110.5.100/24.
- Version of IGMP running on S-switches and hosts is IGMPv2.

## Configuration Procedure

### NOTE

In the configuration example, only the commands related to PIM-DM configuration are mentioned.

1. Enable multicast on each S-switch and PIM-DM on each interface.

# Enable multicast on S-switch-A and enable PIM-DM on each interface, and enable IGMP on the interface connected to the leaf network. The configuration procedures on S-switch-B, S-switch-C, and S-switch-D are similar to those on S-switch-A, and are not mentioned here.

```
[S-switch-A] multicast routing-enable
[S-switch-A] interface vlanif 2
[S-switch-A-Vlanif2] pim dm
```

```
[S-switch-A-Vlanif2] quit
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] pim dm
[S-switch-A-Vlanif1] quit
```

## 2. Configure IGMP on the interface.

# On S-switch-A, configure IGMP on the interface.

```
[S-switch-A] interface vlanif 2
[S-switch-A-Vlanif2] igmp enable
[S-switch-A-Vlanif2] quit
```

# On S-switch-B, configure IGMP on the interface. The configurations of S-switch-C are the same as that of S-switch-B, and are not mentioned here.

```
[S-switch-B] interface vlanif 2
[S-switch-B-Vlanif2] igmp enable
[S-switch-B-Vlanif2] quit
```

## 3. Verify the configuration.

# Run the **display pim interface** command to view the configuration and the running of PIM on the interface of the S-switch. Take the PIM configuration on S-switch-D as an example:

```
<S-switch-D> display pim interface
Interface      State    NbrCnt    HelloInt    DR-Pri    DR-Address
vlanif 3       up       1          30          1         192.168.1.2 (local)
vlanif 1       up       1          30          1         192.168.2.2 (local)
vlanif 2       up       1          30          1         192.168.3.2 (local)
```

# Run the **display pim neighbor** command to view the PIM neighbor relationship between S-switches. Take the PIM neighbor relationship on S-switch-D as an example:

```
<S-switch-D> display pim neighbor
Total Number of Neighbors = 3
Neighbor      Interface      Uptime      Expires      Dr-Priority    BFD-
Session
192.168.1.1   vlanif 3       00:02:22    00:01:27    1              N
192.168.2.1   vlanif 1       00:00:22    00:01:29    1              N
192.168.3.1   vlanif 2       00:00:23    00:01:31    1              N
```

# Run the **display pim routing-table** command, and you can view the PIM routing table. Assume that Host A requests the information of group G (225.1.1.1). After multicast source S (10.110.5.100) sends multicast packets to multicast group G (225.1.1.1), the SPT is established by means of flooding. All PIM multicast S-switches (including S-switch-A and S-switch-D) on the SPT have the (S, G) entry. Host A joins G, and S-switch-A generates an (\*, G) entry. The display information on S-switch-B and S-switch-C is similar to that on S-switch-A.

```
<S-switch-A> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry
(*, 225.1.1.1)
  Protocol: pim-dm, Flag: WC
  UpTime: 03:54:19
  Upstream interface: NULL
  Upstream neighbor: NULL
  RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: GigabitVlanif2
      Protocol: igmp, UpTime: 01:38:19, Expires: never

(10.110.5.100, 225.1.1.1)
  Protocol: pim-dm, Flag: ACT
  UpTime: 00:00:44
  Upstream interface: vlanif 1
  Upstream neighbor: 192.168.1.2
  RPF prime neighbor: 192.168.1.2
  Downstream interface(s) information:
  Total number of downstreams: 1
```

```

1: vlanif2
   Protocol: pim-dm, UpTime: 00:00:44, Expires: never
<S-switch-D> display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry
(10.110.5.100, 225.1.1.1)
   Protocol: pim-dm, Flag: LOC ACT
   UpTime: 01:35:25
   Upstream interface: vlanif4
   Upstream neighbor: NULL
   RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 3
  1: vlanif 3
     Protocol: pim-dm, UpTime: 00:03:27, Expires: never
  2: vlanif 1
     Protocol: pim-dm, UpTime: 00:03:27, Expires: never
  3: vlanif 2
     Protocol: pim-dm, UpTime: 00:03:27, Expires: never

```

## Configuration Files

- Configuration file of S-switch-A

```

#
 sysname S-switch-A
#
 multicast routing-enable
#
interface vlanif2
 undo shutdown
 ip address 10.110.1.1 255.255.255.0
pim dm
 pim slient
 igmp enable
#
interface vlanif 1
 undo shutdown
 link-protocol ppp
 ip address 192.168.1.1 255.255.255.0
pim dm
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
#
return

```

- Configuration file of S-switch-B

```

#
 sysname S-switch-B
#
 multicast routing-enable
#
interface vlanif2
 undo shutdown
 ip address 10.110.2.1 255.255.255.0
pim dm
 igmp enable
#
interface vlanif 1
 undo shutdown
 link-protocol ppp
 ip address 192.168.2.1 255.255.255.0
pim dm
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.110.2.0 0.0.0.255

```

```
#
return

● Configuration file of S-switch-C

#
sysname S-switch-C
#
multicast routing-enable
#
interface vlanif2
undo shutdown
ip address 10.110.2.2 255.255.255.0
pim dm
igmp enable
#
interface vlanif 1
undo shutdown
link-protocol ppp
ip address 192.168.3.1 255.255.255.0
pim dm
#
ospf 1
area 0.0.0.0
network 192.168.3.0 0.0.0.255
network 10.110.2.0 0.0.0.255
#
return

● Configuration file of S-switch-D

#
sysname S-switch-D
#
multicast routing-enable
#
interface vlanif4
undo shutdown
ip address 10.110.5.1 255.255.255.0
pim dm
#
interface vlanif 1
undo shutdown
link-protocol ppp
ip address 192.168.2.2 255.255.255.0
pim dm
#
interface vlanif 2
undo shutdown
link-protocol ppp
ip address 192.168.3.2 255.255.255.0
pim dm
#
interface vlanif 3
undo shutdown
link-protocol ppp
ip address 192.168.1.2 255.255.255.0
pim dm
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 192.168.3.0 0.0.0.255
network 192.168.1.0 0.0.0.255
network 10.110.5.0 0.0.0.255
#
return
```

# 6 PIM-SM (IPv4) Configuration

---

## About This Chapter

This chapter describes the PIM-SM (IPv4) and SSM fundamentals, configuration steps, and maintenance for PIM-SM functions, along with typical examples.

### [6.1 Introduction](#)

This section describes the PIM-SM overview and PIM-SM features supported by the S-switch.

### [6.2 Configuring Basic PIM-SM Functions](#)

This section describes how to configure PIM-SM to implement ASM and SSM models.

### [6.3 Adjusting Control Parameters for a Multicast Source](#)

This section describes how to control the forwarding of multicast data according to the multicast source in the PIM network.

### [6.4 Adjusting Control Parameters of the C-RP and C-BSR](#)

This section describes how to configure control parameters of the C-RP, advertisement messages, C-BSR, and Bootstrap messages.

### [6.5 Configuring a BSR Administrative Domain](#)

This section describes how to configure a PIM-SM administrative domain.

### [6.6 Adjusting Control Parameters for Establishing the Neighbor Relationship](#)

This section describes how to configure control parameters of PIM-SM Hello messages.

### [6.7 Adjusting Control Parameters for Source Registering](#)

This section describes how to configure control parameters of PIM-SM Register messages.

### [6.8 Adjusting Control Parameters for Forwarding](#)

This section describes how to configure control parameters of PIM-SM Join/Prune messages.

### [6.9 Adjusting Control Parameters for Assert](#)

This section describes how to configure control parameters of PIM-SM Assert messages.

### [6.10 Configuring the SPT Switchover](#)

This section describes how to configure the PIM-SM SPT switchover.

### [6.11 Configuring PIM BFD](#)

This section describes how to configure PIM BFD in a shared network segment.

### [6.12 Maintaining PIM](#)

This section describes how to clear the statistics of PIM-SM, debug PIM-SM and PIM-SSM, and monitor the running status of PIM-SM.

### [6.13 Configuration Examples](#)

This section provides several configuration examples of PIM-SM.

## 6.1 Introduction

This section describes the PIM-SM overview and PIM-SM features supported by the S-switch.

### 6.1.1 PIM-SM Overview

#### 6.1.2 PIM-SM Features Supported by the S-switch

### 6.1.1 PIM-SM Overview

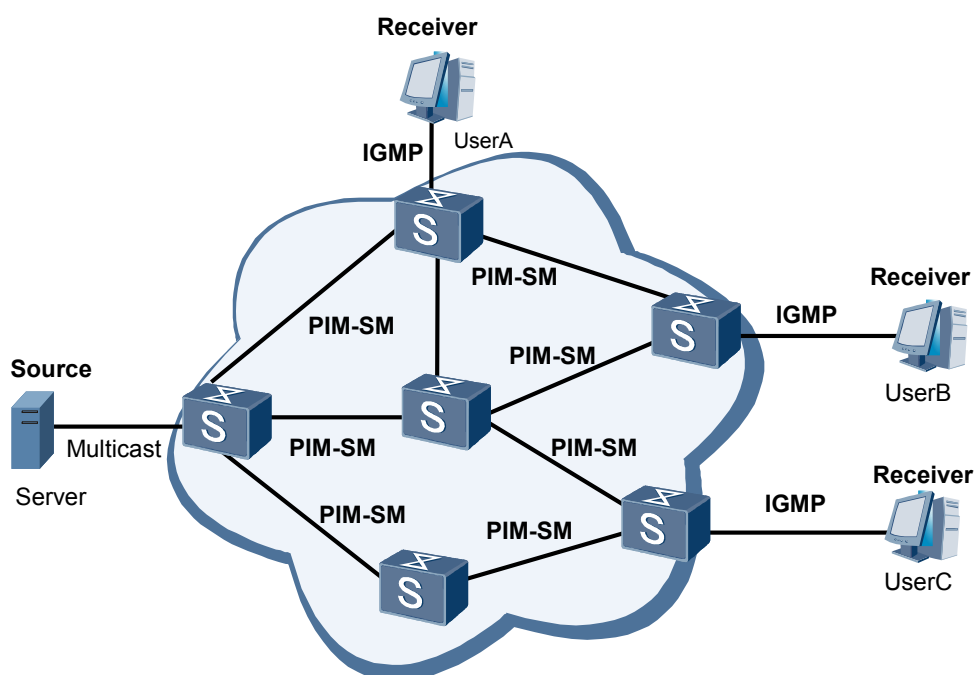
The Protocol Independent Multicast (PIM) indicates that any unicast routing protocol, such as static route, RIP, OSPF, IS-IS, or BGP, can provide the routing information for IP multicast. multicast routing is independent of unicast routing protocols, except that the unicast routing table is used to generate multicast routing entries.

PIM forwards multicast packets by using the Reverse Path Forwarding (RPF) mechanism. The RPF mechanism is used to create the multicast forwarding tree through the existing unicast routing information. When a multicast packet arrives at a S-switch, the S-switch performs the RPF check on the packet. If the RPF check succeeds, a multicast routing entry is created for forwarding the multicast packet. If the RPF check fails, the packet is discarded.

The working process of the Protocol Independent Multicast-Sparse Mode (PIM-SM) consists of neighbor discovery, assert, DR election, RP discovery, join, prune, register, and SPT switchover.

As shown in **Figure 6-1**, PIM-SM is used in a large-scale network with sparsely distributed group members.

**Figure 6-1** Application of PIM-SM in the multicast network



**NOTE**

- The Protocol Independent Multicast Dense Mode (PIM-DM) is applicable to a small-scale network with densely distributed members.
- PIM-SM can be used to construct the Any-Source Multicast (ASM) and Source-Specific Multicast (SSM) models.

## 6.1.2 PIM-SM Features Supported by the S-switch

### Basic PIM-SM Functions

PIM-SM supports the ASM and SSM models. You can configure the two models and set the range of SSM group addresses by using the related commands.

### Static RP

You can specify a static RP on all the S-switches in a PIM-SM domain. When a dynamic RP exists in the domain, the dynamic RP is preferred by default, but you can configure the static RP to be preferred by using related commands.

### Dynamic RP

You can configure C-RPs and C-BSRs in a PIM-SM domain and set the unified rules used to dynamically generate the BSR and the RP. You can specify an Access Control List (ACL) to limit the range of the multicast groups served by the C-RP, adjust the priority for C-RP election, adjust the timeout period for a BSR to wait to receive an advertisement message from the C-RP, and adjust the interval for the C-RP to send advertisement messages.

### BSR

You can specify the C-BSR in the BSR domain, adjust the hash length used by the RP for C-RP election, adjust the priority used for BSR election, and adjust the legal BSR address range. To limit the transmission of BSR messages, you can configure the BSR service boundary on an interface of the S-switch on the boundary of the BSR domain.

### Filtering Policy Based on Source Addresses

You can configure the Keepalive period of multicast sources and filtering rules of the multicast source address to control multicast sources. You can configure the policy to filter Register messages, determine whether to calculate the checksum only based on the header of a Register message, and suppress PIM-SM Register messages.

### BSR Administrative Domain

You can configure the service boundary of the BSR administrative domain and the boundary of the administrative domain by using the related commands.

### Adjusting Parameters for Maintaining PIM-SM Neighbors

You can adjust the control parameters for maintaining PIM-SM neighbors, including the interval for sending Hello messages, the timeout period for keeping neighbors reachable, the interval for triggering Hello messages, and the priority used for DR election, by using the related commands.

## PIM BFD

In the S-switch, you can dynamically set up the BFD session to detect the status of the link between PIM neighbors. Once a fault occurs on the link, BFD reports the fault to PIM.

## Configuring Control Parameters for Multicast Forwarding

You can select whether to set Generation ID in Hello messages, and configure the interval for sending Join messages, the period for keeping the forwarding status of the downstream interface, and the period for overriding the prune action by using the related commands.

## Configuring Specification of Join/Prune Message

You can configure the size of Join/Prune messages and the interval for sending Join/Prune message.

## Configuring Control Parameters for Assert

You can configure the period for retaining the Assert state of the S-switch interface.

## Adjusting Control Parameters for SPT Switchover

You can adjust conditions of the SPT switchover and the interval for checking the forwarding rate of multicast data.

## PIM-SSM

The SSM model provides a solution to multicast of specified sources. You can maintain the relation between hosts and S-switches through IGMPv3.

# 6.2 Configuring Basic PIM-SM Functions

This section describes how to configure PIM-SM to implement ASM and SSM models.

[6.2.1 Establishing the Configuration Task](#)

[6.2.2 Enabling IP Multicast Routing](#)

[6.2.3 Enabling Basic PIM-SM Functions](#)

[6.2.4 \(Optional\) Configuring a Static RP](#)

[6.2.5 \(Optional\) Configuring a Dynamic RP](#)

[6.2.6 \(Optional\) Configuring the SSM Group Address Range](#)

[6.2.7 Checking the Configuration](#)

## 6.2.1 Establishing the Configuration Task

## Applicable Environment

A PIM-SM network can adopt the ASM and SSM models to provide multicast services for user hosts. The integrated components (including the RP) of the ASM model must be configured in the network first. The SSM group address range is then adjusted as required.



### NOTE

The SSM model is only supported in IGMPv3. If user hosts must run IGMPv1 or IGMPv2, configure IGMP SSM mapping on S-switch interfaces.

Through IGMP, a S-switch knows the multicast group G that a user wants to join.

- If G is in the SSM group address range and the source S is specified when the user joins G through IGMPv3, the SSM model is used to provide multicast services.
- If G is in the SSM group address range and the S-switch is configured with the (S, G) SSM mapping rules, the SSM model is used to provide multicast services.
- If G is not in the SSM group address range, the ASM model is used to provide multicast services.

In the PIM-SM network, the ASM model supports the following methods to obtain an RP. You can select the method as required.

- dynamic RP: To obtain the dynamic RP, select several S-switches in the PIM-SM domain and configure them as C-RPs and C-BSRs, and then configure the BSR boundary on the interface on the boundary of the domain. Each S-switch in the PIM-SM domain can then automatically obtain the RP.
- Static RP: To obtain a static RP, manually configure RP on each S-switch in the PIM-SM domain. For the large-scale PIM network, configuring the static RP is complicated. To enhance the robustness and the operating management of the multicast network, the static RP is usually used as the backup of the BSR-RP.

A multicast group may be in the service range of the dynamic RP and the static RP simultaneously. By default, The S-switch prefers the dynamic RP. If the static RP precedence is configured, the static RP is preferred.

Different multicast groups correspond to different RPs. Compared with all groups corresponding to an RP, this can reduce the burden of an RP and enhance the robustness of the network.

## Pre-configuration Tasks

Before configuring basic PIM-SM functions, complete the following tasks:

- Configuring a unicast routing protocol

## Data Preparation

To configure basic PIM-SM functions, you need the following data.

No.	Data
1	Static RP address
2	ACL rule indicating the service scope of static RP
3	C-RP priority

No.	Data
4	ACL rule indicating the service scope of C-RP
5	Interval for C-RP sending Advertisement message
6	Timeout of the period during which BSR waits to receive the Advertisement message from C-RP.
7	C-BSR Hash mask length
8	C-BSR priority
9	SSM group address range

## 6.2.2 Enabling IP Multicast Routing

### Context



#### CAUTION

The configuration related to the VPN instance is applicable only to the PE router. If the interface of the VPN instance connects to the host, run the commands in step 3 and step 4.

---

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
multicast routing-enable
```

IP multicast routing is enabled in the public network instance.

----End

## 6.2.3 Enabling Basic PIM-SM Functions

### Context

Do as follows on the S-switch:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
pim sm
```

PIM SM is enabled.

After PIM SM is enabled on the interface and PIM neighbor relationships are set up between S-switches, the packets from the PIM neighbors can be processed.

----End

## 6.2.4 (Optional) Configuring a Static RP

### Context



#### CAUTION

When the static RP and the dynamicRP are configured in the PIM-SM at the same time, faults may occur in the network. So, confirm the action before you run the command. If you want to use only the dynamicRP in the PIM-SM network, skip the configuration.

---

Do as follows on all S-switches in the PIM-SM area:

## Procedure

**Step 1** Run:

```
system-view
```

The interface view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
static-rp rp-address [ basic-acl-number ] [ preferred ]
```

The static RP is specified.

You can run the command repeatedly to configure multiple static RPs for the S-switch.



#### NOTE

All S-switches in the PIM-SM area must be configured with the same **static-rp** command.

- *rp-address*: specifies the static RP address.
- *basic-acl-number*: specifies the number of the basic ACL. The ACL defines the range of the multicast group served by the static RP. When the range of multicast groups that multiple static RPs serve overlaps, the static RP with the largest IP address functions as the RP.
- **preferred**: indicates the preference of the static RP. If the C-RP is configured in the network at the same time, the S-switch prefers the RP statically specified after preferred is used. Otherwise, C-RP is preferred.

----End

## 6.2.5 (Optional) Configuring a Dynamic RP

### Context



#### CAUTION

The configuration is applicable only to the dynamic RP. If you want to use the static RP in the network, skip the configuration.

---

Do as follows on the S-switch that may become RP in the PIM-SM area:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
c-rp interface-type interface-number [ group-policy basic-acl-number | priority  
priority | holdtime hold-interval | advertisement-interval adv-interval ] *
```

The C-RP is configured.

- *interface-type interface-number*: specifies the interface where the C-RP resides. The interface must be configured with PIM-SM.
- **group-policy basic-acl-number**: specifies the multicast group permitted by ACL and served by the C-RP. *basic-acl-number* specifies the number of the basic ACL. By default, C-RP serves all multicast groups.
- **priority priority-value**: specifies the priority for electing C-RP. The greater is the value, the lower is the priority. By default, it is 0.



#### NOTE

In the RP election, the C-RP with the highest priority wins. In case of the same priority, the hash function is used and the C-RP with the greatest hash value wins. In case of the same priority and the same hash value, the C-RP with the highest IP address wins.

- **holdtime** *hold-interval*: specifies the interval during which the BSR waits for the Advertisement message from the C-RP. By default, the interval is 150 seconds.
- **advertisement-interval** *adv-interval*: specifies the interval during which the C-RP sends the Advertisement message. By default, the interval is 60 seconds.

**Step 4** Run:

```
c-bsr interface-type interface-number [ hash-length [ priority ] ]
```

The C-BSR is configured.

- *interface-type interface-number*: specifies the interface where the C-BSR resides. The interface must be configured with the PIM-SM.
- *hash-length*: specifies the length of the hash. According to the G, C-RP address, and the value of *hash-length*, S-switches calculate the C-RPs that have the same priority and require to serve G by operating hash functions, and compare the calculation results. The C-RP with the greatest calculated value functions as the RP that serves G.
- *priority*: specifies the priority used by S-switches to join the BSR election.

**NOTE**

In the BSR election, the C-BSR with the highest priority wins. In the case of the same priority, the C-BSR with the largest IP address wins.

**Step 5** (Optional) Run:

```
auto-rp listening-enable
```

The Auto-RP listening is enabled.

When the S-switch interworks with a S-switch supporting auto-RP, this command needs to be configured on the S-switch.

----End

## 6.2.6 (Optional) Configuring the SSM Group Address Range

### Context

Do as follows on all S-switches in the PIM-SM domain:

**NOTE**

This configuration is optional. By default, the SSM group address range is 232.0.0.0/8.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
ssm-policy basic-acl-number
```

The SSM group address range is configured.

 **NOTE**

Ensure that the SSM group address range of all S-switches in the network is consistent.

----End

## 6.2.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the BSR in a PIM-SM domain.	<b>display pim bsr-info</b>
Check PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check a PIM neighbor.	<b>display pim neighbor</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>verbose</b> ] <b>display pim neighbor neighbor-address</b> [ <b>verbose</b> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]
Check the RP in a PIM-SM domain.	<b>display pim rp-info</b> [ <i>group-address</i> ]

## 6.3 Adjusting Control Parameters for a Multicast Source

This section describes how to control the forwarding of multicast data according to the multicast source in the PIM network.

[6.3.1 Establishing the Configuration Task](#)

[6.3.2 Configuring the Lifetime of a Source](#)

[6.3.3 Configuring the Filtering Rules Based on the Source Addresses](#)

[6.3.4 Checking the Configuration](#)

### 6.3.1 Establishing the Configuration Task

#### Applicable Environment

All the configurations in this section are applicable to the ASM and SSM models.

S-switches check the multicast data that passes by. By checking whether the data matches the filtering rule, the S-switches determine whether to forward the data. That is, the S-switches in the PIM domain function as filters. The filters help to control the data flow, and to limit the information that the downstream receiver can obtain.

Routers can work normally under the control of default values. The S-switch allows users to adjust the parameters as required.

 **NOTE**

If there is no special requirement, default values are recommended.

## Pre-configuration Tasks

Before adjusting control parameters for a multicast source, complete the following tasks:

- Configuring a certain unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

## Data Preparation

To adjust control parameters for a multicast source, you need the following data.

No.	Data
1	Lifetime of a multicast source
2	Filtering rules based on multicast source addresses

## 6.3.2 Configuring the Lifetime of a Source

### Context

Do as follows on the S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
source-lifetime interval
```

The lifetime of a source is configured.

If the lifetime of the source expires, the (S, G) entry becomes invalid.

----End

### 6.3.3 Configuring the Filtering Rules Based on the Source Addresses

#### Context

Do as follows on the S-switch:

#### Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**pim**

The PIM view is displayed.

**Step 3** Run:

**source-policy** *acl-number*

A filter is configured.

Only the multicast packets that carry the source addresses within the range defined by the filtering rules are forwarded.

----End

### 6.3.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 6.4 Adjusting Control Parameters of the C-RP and C-BSR

This section describes how to configure control parameters of the C-RP, advertisement messages, C-BSR, and Bootstrap messages.

[6.4.1 Establishing the Configuration Task](#)[6.4.2 Adjusting C-RP Parameters](#)[6.4.3 Adjusting C-BSR Parameters](#)[6.4.4 Configuring the BSR Boundary](#)[6.4.5 Configuring the BSR Address Range](#)[6.4.6 Configuring the Range of Valid C-RP Addresses](#)[6.4.7 Checking the Configuration](#)

## 6.4.1 Establishing the Configuration Task

### Applicable Environment

This section describes how to adjust the control parameters of the C-RP and the C-BSR through commands in the ASM model.

 **NOTE**

The configuration is applicable only to a BSR-RP. If you want to use only a static RP in the network, skip the configuration.

The S-switch can work normally under the control of default values. The S-switch allows users to adjust the parameters as required.

 **NOTE**

If there is no special requirement, default values are recommended.

### Pre-configuration Tasks

Before adjusting control parameters of the C-RP and C-BSR, complete the following tasks:

- Configuring a unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

### Data Preparation

To adjust various control parameters of the C-RP and C-BSR, you need the following data.

No.	Data
1	RP priority
2	Interval for a C-RP to send Advertisement messages
3	Timeout of the period during which a BSR waits to receive Advertisement messages from a C-RP
4	Hash mask length of a C-BSR
5	Priority of a C-BSR
6	Interval for a C-BSR to send Bootstrap messages

No.	Data
7	Time of holding the Bootstrap message received from a BSR
8	ACL defining the legal BSR address scope

## 6.4.2 Adjusting C-RP Parameters

### Context

Do as follows on the S-switch configured with the C-RP:



#### NOTE

You can re-set various parameters of a C-RP. This configuration is optional. If there is no specific requirement, default values of parameters are recommended.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
pim
```

The PIM view is displayed.

#### Step 3 Run:

```
c-rp priority priority
```

The C-RP priority is set.

#### Step 4 Run:

```
c-rp advertisement-interval interval
```

The interval during which the C-RP sends Advertisement messages is set.

#### Step 5 Run:

```
c-rp holdtime interval
```

The time for holding the Advertisement message from a C-RP is set. The value must be greater than the interval for a C-RP to send advertisement messages.

The C-RP periodically sends advertisement messages to the BSR. After receiving the advertisement messages, the BSR obtains the Holdtime of the C-RP from the message. During the Holdtime, the C-RP is valid. When the Holdtime expires, the C-RP ages out.

----End

## 6.4.3 Adjusting C-BSR Parameters

## Context

Do as follows on the S-switch configured with the C-BSR:

### NOTE

You can re-set various parameters of a C-BSR. This configuration is optional. If there is no specific requirement, the default values of parameters are recommended.

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
pim
```

The PIM view is displayed.

### Step 3 Run:

```
c-bsr hash-length hash-length
```

The hash mask length of a C-BSR is set.

### Step 4 Run:

```
c-bsr priority priority
```

The priority of the C-BSR is set.

### Step 5 Run:

```
c-bsr interval interval
```

The interval for the C-BSR to send Bootstrap messages is set.

### Step 6 Run:

```
c-bsr holdtime interval
```

The time of holding the Bootstrap message received from a BSR is set.

The BSR periodically sends a Bootstrap message to the network. After receiving the Bootstrap message, the S-switches keep the message for a certain time. During the period, the BSR election stops temporarily. If the Holdtime timer times out, a new round of BSR election is triggered among C-BSRs.

### NOTE

Ensure that the value of **c-bsr holdtime** is greater than the value of **c-bsr interval**. Otherwise, the winner of BSR election cannot be fixed.

----End

## 6.4.4 Configuring the BSR Boundary

## Context

Do as follows on the S-switch that may become the BSR boundary:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`interface interface-type interface-number`  
The interface view is displayed.
- Step 3** Run:  
`pim bsr-boundary`  
The BSR boundary is configured.
- End

## 6.4.5 Configuring the BSR Address Range

### Context

Do as follows on all S-switches in the PIM-SM domain:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`pim`  
The PIM view is displayed.
- Step 3** Run:  
`bsr-policy basic-acl-number`  
The legal range of BSR addresses is set.
- After receiving a BSR message, the S-switch checks the source address of the message. If the source address is not within the range of legal addresses, the message is discarded. BSR spoofing is thus prevented.
- basic-acl-number* specifies the number of the basic ACL. The ACL defines the filtering policy for the source address range of the BSR messages.
- End

## 6.4.6 Configuring the Range of Valid C-RP Addresses

### Context

Do as follows on all the C-BSRs in the PIM-SM domain:

 **NOTE**

This configuration is optional. By default, a S-switch does not check the C-RP address and the group address contained in a received Advertisement message and adds them to the RP-set.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
crp-policy advanced-acl-number
```

The range of the valid C-RP addresses and the range of the multicast group addresses that a S-switch serves are specified. When receiving an Advertisement message, the S-switch checks the C-RP address and the addresses of the groups that the C-RP serves in the message. The C-RP address and the addresses of the groups that the C-RP serves are added to the RP-Set only when they are in the valid address range. The C-RP spoofing can thus be prevented.

*advanced-acl-number*: specifies the number of the advanced ACL. The ACL defines the filtering policy for the C-RP address range and the address range of the groups that a C-RP serves.

----End

## 6.4.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the BSR in a PIM-SM domain.	<b>display pim bsr-info</b>
Check the RP in a PIM-SM domain.	<b>display pim rp-info</b> [ <i>group-address</i> ]

## 6.5 Configuring a BSR Administrative Domain

This section describes how to configure a PIM-SM administrative domain.

[6.5.1 Establishing the Configuration Task](#)

[6.5.2 Enabling a BSR Administrative Domain](#)

[6.5.3 Configuring the Boundary of a BSR Administrative Domain](#)

[6.5.4 Adjusting C-BSR Parameters](#)

[6.5.5 Checking the Configuration](#)

## 6.5.1 Establishing the Configuration Task

### Applicable Environment

This section describes how to configure a BSR administrative domain in the ASM model through commands.

In the traditional mode, a PIM-SM network maintains only one BSR and all multicast groups in the network are in the administrative range of the BSR. To better manage the domains, the PIM-SM network is divided into multiple BSR administrative domains. Each BSR administrative domain maintains only one BSR that serves specified multicast groups. BSR administrative domains are geographically isolated. Multicast packets of a BSR administrative domain cannot pass the border of the domain.

The address of a multicast group served by a BSR administrative domain is valid only in the BSR administrative domain. The addresses of multicast groups served by different BSR administrative domains can be identical and these addresses are equal to private multicast group addresses.

Multicast groups that do not belong to any BSR administrative domain are served by the global domain. Global domain maintains only one BSR that serves the remaining multicast groups.

Dividing a PIM-SM network into multiple BSR administrative domains and a global domain effectively reduces the load of a single BSR, and provides a special service for specific multicast groups.

The S-switch can work normally under the control of default values. The S-switch allows users to adjust the parameters as required.

#### NOTE

It is recommended to adopt default values if there is no special requirement.

### Pre-configuration Tasks

Before configuring a BSR administrative domain, complete the following tasks:

- Configuring a unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

### Data Preparation

To configure a BSR administrative domain, you need the following data.

No.	Data
1	Priority and hash mask length for electing a BSR in a BSR domain
2	Priority and hash mask length of electing the global domain BSR

## 6.5.2 Enabling a BSR Administrative Domain

## Context

Do as follows on all S-switches in the PIM-SM network:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
c-bsr admin-scope
```

The division of BSR administrative domains is enabled in a PIM-SM network.

----End

## 6.5.3 Configuring the Boundary of a BSR Administrative Domain

### Context

Do as follows on all S-switches at the boundary of a BSR administrative domain:



#### NOTE

The S-switches outside the BSR administrative domain cannot forward the multicast packets of the BSR administrative domain.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
multicast boundary group-address { mask | mask-length }
```

The multicast forwarding boundary is configured.

----End

## 6.5.4 Adjusting C-BSR Parameters

## Context

Do as follows on all C-BSRs:

### NOTE

The C-BSR configuration involves three cases:

- Global configuration: For global configuration, see [6.4 Adjusting Control Parameters of the C-RP and C-BSR](#). It is valid in the global domain and each BSR administrative domain.
- Configuration in a BSR administrative domain: Because the configuration in a BSR administrative domain takes precedence over the global configuration, the global configuration is used when the configuration in a BSR administrative domain is not done.
- Configuration in the global domain: Because the configuration in the global domain takes precedence over the global configuration, the global configuration is used when the configuration in the global domain is not done.

## Procedure

- Configuration in a BSR Administrative Domain
  1. Run:  
**system-view**  
  
The system view is displayed.
  2. Run:  
**pim**  
  
The PIM view is displayed.
  3. Run:  
**c-bsr group** *group-address* { *mask* | *mask-length* } [ **hash-length** *hash-length* | **priority** *priority* ] \*  
  
The C-BSR parameters are configured.
    - *group-address* {*mask* | *mask-length*}: specifies the range of the multicast groups served by a C-BSR.
    - **hash-length** *hash-length*: specifies the hash mask length of a C-BSR.
    - **priority** *priority*: specifies the priority of a C-BSR.
- Configuration in the Global Domain
  1. Run:  
**system-view**  
  
The system view is displayed.
  2. Run:  
**pim**  
  
The PIM view is displayed.
  3. Run:  
**c-bsr global** [ **hash-length** *hash-length* | **priority** *priority* ] \*  
  
The C-BSR parameters are configured.
    - **hash-length** *hash-length*: specifies the hash mask length of a C-BSR.
    - **priority** *priority*: specifies the priority of a C-BSR.

----End

## 6.5.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the BSR in a PIM-SM domain.	<b>display pim bsr-info</b>
Check the RP in a PIM-SM domain.	<b>display pim rp-info</b> [ <i>group-address</i> ]

## 6.6 Adjusting Control Parameters for Establishing the Neighbor Relationship

This section describes how to configure control parameters of PIM-SM Hello messages.

[6.6.1 Establishing the Configuration Task](#)

[6.6.2 Configuring Control Parameters for Establishing the Neighbor Relationship](#)

[6.6.3 Configuring Control Parameters for Electing a DR](#)

[6.6.4 Checking the Configuration](#)

### 6.6.1 Establishing the Configuration Task

#### Applicable Environment

The configuration in this section is applicable to both the ASM model and the SSM model.

The PIM S-switches send Hello messages to each other to establish the neighbor relationship, negotiate the control parameters, and elect a DR.

The S-switch can work normally by default. The S-switch allows the users to adjust the parameters as required.

#### NOTE

It is recommended to adopt the default value if there is no special requirement.

#### Pre-configuration Tasks

Before configuring control parameters for establishing the neighbor relationship, complete the following tasks:

- Configuring unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

#### Data Preparation

To adjust the control parameters for establishing the neighbor relationship, you need the following data.

No.	Data
1	Priority of the DR that is elected
2	Timeout period for waiting for Hello messages from a neighbor
3	Interval for sending Hello messages
4	Maximum delay for triggering Hello messages
5	DR switchover delay, that is, the period during which the original entries are still valid when the interface changes from a DR to a non-DR.

## 6.6.2 Configuring Control Parameters for Establishing the Neighbor Relationship

### Context

Do as follows on the PIM-SM S-switch.



#### NOTE

The configuration involves the following cases:

- Global configuration: It is valid on all the interfaces.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration
  1. Run:  
**system-view**  
The system view is displayed.
  2. Run:  
**pim**  
The PIM view is displayed.
  3. Run:  
**timer hello interval**  
The interval for sending Hello messages is set.
  4. Run:  
**hello-option holdtime interval**  
The timeout period of holding the reachable state of a neighbor is set.  
  
If no Hello message is received after the interval expires, the neighbor is considered unreachable.
- Configuration on an Interface
  1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
pim timer hello interval
```

The interval for sending Hello messages is set.

4. Run:

```
pim triggered-hello-delay interval
```

The maximum delay for triggering Hello messages is set.

This can prevent the conflict of Hello messages sent by multiple PIM S-switches at the same time.

5. Run:

```
hello-option holdtime interval
```

The timeout period of holding the reachable state of a neighbor is set.

If no Hello message is received after the interval expires, the neighbor is considered unreachable.

----End

## 6.6.3 Configuring Control Parameters for Electing a DR

### Context

Do as follows on the PIM-SM S-switch:

#### NOTE

The configuration involves the following cases:

- Global configuration: It is valid on all the interfaces.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
pim
```

The PIM view is displayed.

3. Run:

```
hello-option dr-priority priority
```

The DR priority is set.

On a shared network segment where all PIM S-switches support the DR priority, the interface with the highest priority acts as the DR. In the case of the same priority, the interface with the largest IP address acts as the DR. If a minimum of one PIM S-switch does not support the DR priority, the interface with the largest IP address acts as the DR.

- Configuration on an Interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
hello-option dr-priority priority
```

The DR priority is set.

On a shared network segment where all PIM S-switches support the DR priority, the interface with the highest priority acts as the DR. In the case of the same priority, the interface with the largest IP address acts as the DR. If a minimum of one PIM S-switch does not support the DR priority, the interface with the largest IP address acts as the DR.

4. Run:

```
pim timer dr-switch-delay interval
```

The DR switchover delay is configured and the delay is specified.

When an interface changes from a DR to a non-DR, the original entries are valid till the delay expires.

By default, once an interface changes from a DR to a non-DR, the original entries are deleted immediately.

----End

## 6.6.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check information about a PIM neighbor.	<b>display pim neighbor</b> [ <b>interface</b> <i>interface-type interface-number</i>   <i>neighbor-address</i> ] [ <b>verbose</b> ]

## 6.7 Adjusting Control Parameters for Source Registering

This section describes how to configure control parameters of PIM-SM Register messages.

### [6.7.1 Establishing the Configuration Task](#)

### [6.7.2 Configuring PIM-SM Register Messages](#)

### [6.7.3 Configuring PIM-SM Register Suppression](#)

### [6.7.4 Checking the Configuration](#)

## 6.7.1 Establishing the Configuration Task

### Applicable Environment

This section describes how to configure the control parameters of the source registering through commands.

In a PIM-SM network, the DR directly connected to the source S encapsulates multicast data in a Register message and sends it to the RP in unicast mode. The RP then decapsulates the message, and forwards it along the RPT.

After the SPT switchover on the RP is complete, the multicast data reaches the RP along the source tree in the multicast mode. The RP sends a Register-stop message to the DR at the source side. The DR stops sending Register messages and enters the suppressed state. During the register suppression, the DR periodically sends null packets to inform that the source is still in the active state. After the timeout of the register suppression, the DR starts to send Register message again.

The S-switch can work normally under the control of default values. The S-switch allows the users to adjust the parameters as required.

#### NOTE

It is recommended to adopt default values if there is no special requirement.

### Pre-configuration Tasks

Before adjusting control parameters for source registering, complete the following tasks:

- Configuring a unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

### Data Preparation

To adjust control parameters for source registering, you need the following data.

No.	Data
1	ACL rules used by the RP to filter Register messages
2	Whether the checksum is calculated only according to the header of a Register message

No.	Data
3	Timeout for keeping the suppressed state of registering
4	Interval for sending null Register messages to the RP

## 6.7.2 Configuring PIM-SM Register Messages

### Context

Do as follows on all S-switches that may become an RP:

### Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**pim**

The PIM view is displayed.

**Step 3** Run:

**register-policy** *advanced-acl-number*

The policy for filtering Register messages is set.

The RP applies the policy to filter received and rejected Register messages.

**Step 4** Run:

**register-header-checksum**

The checksum is calculated only according to the header of a Register message.

By default, the checksum is calculated according to the entire message.

----End

## 6.7.3 Configuring PIM-SM Register Suppression

### Context

Do as follows on all the S-switches that may become the DR at the multicast source side:

### Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
register-suppression-timeout interval
```

The timeout for keeping the suppressed state of registering is set.

**Step 4** Run:

```
probe-interval interval
```

The interval for sending null Register messages is set.

----End

## 6.7.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the information about PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]

## 6.8 Adjusting Control Parameters for Forwarding

This section describes how to configure control parameters of PIM-SM Join/Prune messages.

### [6.8.1 Establishing the Configuration Task](#)

### [6.8.2 Configuring Control Parameters for Keeping the Forwarding State](#)

### [6.8.3 Configuring Control Parameters for Prune](#)

### [6.8.4 Checking the Configuration](#)

## 6.8.1 Establishing the Configuration Task

### Applicable Environment

The configurations in this section are applicable to the ASM model and the SSM model.

When the first member of a group appears in the network segment, the S-switch sends a Join message through an upstream interface, requiring the upstream S-switch to forward packets to the network segment.

When the last member of the group leaves, the S-switch sends a Prune message through an upstream interface, requiring the upstream S-switch to perform the Prune action and to stop forwarding packets to this network segment. If other downstream S-switches in this network segment still want to receive data of this group, they must send a Join message to override the Prune action.

In the ASM model, a S-switch periodically sends Join messages to the RP to prevent RPT branches from being deleted due to timeout.

The S-switch can work normally under the control of default values. The S-switch allows users to adjust the parameters as required.

 **NOTE**

It is recommended to adopt default values if there is no special requirement.

## Pre-configuration Tasks

Before adjusting control parameters for forwarding, complete the following tasks:

- Configuring a certain unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

## Data Preparation

To adjust control parameters for forwarding, you need the following data.

No.	Data
1	Delay for transmitting Prune messages
2	Period of overriding the Prune action
3	Timeout period of the Prune state
4	Interval for sending Join messages
5	Number of the (S, G) entries contained in the Join/Prune message sent per second

## 6.8.2 Configuring Control Parameters for Keeping the Forwarding State

### Context

Do as follows on the PIM-SM S-switch:

 **NOTE**

The configuration involves the following cases:

- Global configuration: It is valid on all the interfaces.
- Configuration on the interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration
  1. Run:
 

```
system-view
```

The system view is displayed.

2. Run:

```
pim
```

The PIM view is displayed.

3. Run:

```
timer join-prune interval
```

The interval for sending Join/Prune messages is set.

4. Run:

```
holdtime join-prune interval
```

The interval for holding the forwarding state of a downstream interface is set.

- Configuration on an Interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
timer join-prune interval
```

The interval for sending Join/Prune messages is set.

4. Run:

```
pim holdtime join-prune interval
```

The interval for holding the forwarding state of a downstream interface is set.

5. Run:

```
pim require-genid
```

The Generation ID option is contained in a Hello message. The Hello message without the Generation ID option is rejected.

By default, the S-switch handles the Hello message without the Generation option.

The change of the Generation ID in the Hello message received from an upstream neighbor indicates that the upstream neighbor is lost or the status of the upstream neighbor has changed. The S-switch immediately sends the Join/Prune message to the upstream router to refresh the status.

----End

## 6.8.3 Configuring Control Parameters for Prune

### Context

Do as follows on the PIM-SM S-switch:

 **NOTE**

The configuration involves the following cases:

- Global Configuration: It is valid on all the interfaces.
- Configuration on the interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

## Procedure

- Global Configuration

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
pim
```

The PIM view is displayed.

3. Run:

```
hello-option lan-delay interval
```

The delay for transmitting messages in a LAN is set.

A Hello message carries **lan-delay** and **override-interval**. PPT indicates the delay from the time when a S-switch receives the Prune message from a downstream interface to the time when the S-switch performs the prune action to suppress the forwarding of the downstream interface. The PPT is obtained by the lan-delay plus override-interval. If the S-switch receives a Join message from a downstream S-switch within the PPT, the S-switch does not perform the prune action.

4. Run:

```
hello-option override-interval interval
```

The interval for overriding the Prune action is set.

If a S-switch receives the Prune message through an upstream interface, this indicates that other downstream S-switches exist in this LAN. If the S-switch still needs to receive multicast data of the group, the S-switch must send a Join message to the upstream S-switch within the override-interval.

- Configuration on an Interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
pim hello-option lan-delay interval
```

The delay for transmitting messages in a LAN is set.

4. Run:

```
pim hello-option override-interval interval
```

The interval for overriding the Prune action is set.

----End

## 6.8.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the number of sent or received PIM control messages.	<b>display pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>message-type message-type</b> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 6.9 Adjusting Control Parameters for Assert

This section describes how to configure control parameters of PIM-SM Assert messages.

### 6.9.1 Establishing the Configuration Task

### 6.9.2 Configuring the Period for Keeping the Assert State

### 6.9.3 Checking the Configuration

## 6.9.1 Establishing the Configuration Task

### Applicable Environment

The configurations in this section are applicable to the ASM model and the SSM model.

If a PIM-SM S-switch receives multicast data through a downstream interface, it indicates that other upstream S-switches exist in this network segment. S-switches send Assert messages to elect the unique upstream S-switch.

The S-switch can work normally under the control of default values. The S-switch allows users to adjust the parameters as required.

#### NOTE

It is recommended to adopt default values if there is no special requirement.

## Pre-configuration Tasks

Before adjusting control parameters for assert, complete the following tasks:

- Configuring a certain unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

## Data Preparation

To adjust control parameters for assert, you need the following data.

No.	Data
1	Interval for holding the Assert state

## 6.9.2 Configuring the Period for Keeping the Assert State

### Context

Do as follows on all the S-switches in the PIM-SM domain:

#### NOTE

The configuration involves the following cases:

- Global configuration: It is valid on all the interfaces.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration
  1. Run:  
**system-view**  
  
The system view is displayed.
  2. Run:  
**pim**  
  
The PIM view is displayed.
  3. Run:  
**holdtime assert interval**  
  
The interval for holding the Assert state is set.  
  
The S-switch that fails in the election prevents the downstream interface from forwarding multicast packets within the interval. After the interval expires, the downstream interface starts to forward multicast packets.
- Configuration on the Interface
  1. Run:  
**system-view**

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
pim holdtime assert interval
```

The interval for holding the Assert state is configured.

The S-switch that fails in the election prohibits the downstream interface from forwarding multicast packets within this interval. After the interval expires, the downstream interface starts to forward multicast packets.

----End

### 6.9.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the number of the sent or received PIM control messages.	<b>display pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>message-type</b> <i>message-type</i> ]
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 6.10 Configuring the SPT Switchover

This section describes how to configure the PIM-SM SPT switchover.

### 6.10.1 Establishing the Configuration Task

#### 6.10.2 (Optional) Configuring the Interval for Checking the Forwarding Rate of Multicast Data

#### 6.10.3 Checking the Configuration

### 6.10.1 Establishing the Configuration Task

## Applicable Environment

This section describes how to configure the control parameters of the SPT switchover through commands.

In a PIM-SM network, each multicast group corresponds to an RPT. At first, all multicast sources encapsulate data in Register messages, and send them to the RP in the unicast mode. The RP decapsulates the messages and forwards them along the RPT.

Forwarding multicast data by using the RPT has the following defects:

- The DR at the source side and the RP need to encapsulate and decapsulate packets.
- Forwarding path may not be the shortest path from the source to receivers.
- Large-volume data flow increases the load of the RP, and may cause a fault.

The solution to the preceding defects is that:

- SPT switchover triggered by the RP: The RP sends a Join message to the source, and establishes a multicast route along the shortest path from the source to the RP. The subsequent packets are forwarded along the path.
- SPT switchover triggered by the DR at the member side: The DR at the member side checks the forwarding rate of multicast data. If the DR finds that the rate exceeds the threshold, the DR triggers the SPT switchover immediately. The DR sends a Join message to the source, and establishes a multicast route along the shortest path from the source to the DR. The subsequent packets are forwarded along the path.

S-switches can work normally under the control of default values. The S-switch allows users to adjust the parameters as required.

### NOTE

It is recommended to adopt default values if there is no special requirement.

## Pre-configuration Tasks

Before configuring the SPT switchover, complete the following tasks:

- Configuring a unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

## Data Preparation

To configure the SPT switchover, you need the following data.

No.	Data
1	Rate threshold that a leaf PIM S-switch switches packets from the RPT to the SPT
2	Group filtering policy and sequence policy for the switchover from the RPT to the SPT
3	Interval for checking the rate threshold of multicast data before the RPT-to-SPT switchover

## 6.10.2 (Optional) Configuring the Interval for Checking the Forwarding Rate of Multicast Data

### Context

Do as follows on all the S-switches that may become a DR at the member side:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
timer spt-switch interval
```

The interval for checking the forwarding rate of multicast data is set.

**Step 4** Run:

```
spt-switch-threshold { traffic-rate | infinity } [ group-policy basic-acl-number [
order order-value ] ]
```

The SPT switchover condition is set.

- **traffic-rate**: specifies the rate threshold of the SPT switchover.
- **infinity**: indicates that the SPT switchover is not triggered forever.
- **group-policy basic-acl-number [ order order-value]**: specifies the range of the multicast groups that use the threshold. By default, the threshold is applicable to all multicast groups.

----End

## 6.10.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the PIM routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type</i> <i>interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]

## 6.11 Configuring PIM BFD

This section describes how to configure PIM BFD in a shared network segment.

### [6.11.1 Establishing the Configuration Task](#)

### [6.11.2 Configuring PIM BFD](#)

### [6.11.3 \(Optional\) Adjusting BFD Parameters](#)

### [6.11.4 Checking the Configuration](#)

## 6.11.1 Establishing the Configuration Task

### Networking Requirements

Generally, if the current DR in a shared network segment is faulty, other PIM neighbors triggers a new round of DR election only after the neighbor relationship times out. The duration that data transmission is interrupted is not shorter than the timeout period of the neighbor relationship. Generally, it is of second level.

BFD features fast detection of faults, and is up to the millisecond level. BFD can detect statuses of PIM neighbors in the shared network segment. When BFD detects that a peer is faulty, BFD immediately reports it to PIM. PIM then triggers a new round of DR election without waiting for the timeout of the neighbor relationship. This shortens the duration of interruption of data transmission and enhances the reliability of the network.

PIM BFD is also applicable to the assert election in a shared network segment. It can fast respond to the fault of the interface that wins the assert election.

### Pre-configuration Tasks

Before configuring PIM BFD, complete the following task:

- Configuring a unicast routing protocol
- [6.2 Configuring Basic PIM-SM Functions](#)

### Data Preparation

To configure PIM BFD, you need the following data.

No.	Data
1	Minimum intervals for sending and receiving BFD detection messages, and local detection multiple

## 6.11.2 Configuring PIM BFD

## Context



### NOTE

This function is applicable to NBMA interfaces and broadcast interfaces rather than MTunnel interfaces.

Do as follows on two PIM S-switches that set up the neighbor relationship:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

### Step 3 Run:

```
pim bfd enable
```

PIM BFD is enabled.

By default, PIM BFD is disabled.

----End

## 6.11.3 (Optional) Adjusting BFD Parameters

## Context

Do as follows on two PIM S-switches that set up the neighbor relationship:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed

### Step 3 Run:

```
pim bfd { min-tx-interval tx-value | min-rx-interval rx-value | detect-multiplier  
multiplier-value }*
```

PIM BFD parameters are adjusted.

PIM BFD parameters include the minimum interval for sending PIM BFD messages, the minimum interval for receiving PIM BFD messages, and the local detection multiple.

If this command is not used, the default values of these parameters are used. When the BFD parameters configured for other protocols are the same as those configured for PIM, the configurations of the PIM BFD parameters are affected.

----End

## 6.11.4 Checking the Configuration

Action	Command
Check information about a PIM BFD session.	<b>display pim bfd session statistics</b> <b>display pim bfd session</b> [ <b>interface</b> <i>interface-type interface-number</i>   <b>neighbor</b> <i>neighbor-address</i> ] *

## 6.12 Maintaining PIM

This section describes how to clear the statistics of PIM-SM, debug PIM-SM and PIM-SSM, and monitor the running status of PIM-SM.

[6.12.1 Clearing Statistics of PIM Control Messages](#)

[6.12.2 Monitoring the Running Status of PIM-SM](#)

[6.12.3 Debugging PIM](#)

### 6.12.1 Clearing Statistics of PIM Control Messages



#### CAUTION

The statistics of PIM control messages on an interface cannot be restored after you clear it. So, confirm the action before you use the command.

To clear the statistics of PIM control messages on an interface, run the following commands in the user view.

Action	Command
Clear the statistics of PIM control messages on an interface.	<b>reset pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ]

### 6.12.2 Monitoring the Running Status of PIM-SM

During routine maintenance, run the following commands in any view to know the running status of PIM-SM.

Action	Command
Check the unicast routes used by PIM.	<b>display pim claimed-route</b> [ <i>source-address</i> ]
Check information about a PIM BFD session.	<b>display pim bfd session</b> [ <b>interface</b> <i>interface-type interface-number</i>   <b>neighbor</b> <i>neighbor-address</i> ] *
Check information about the BSR in a PIM-SM domain.	<b>display pim bsr-info</b>
Check the number of sent or received PIM control messages.	<b>display pim control-message counters</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>message-type</b> <i>message-type</i> ]
Check information about PIM on an interface.	<b>display pim interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check information about a PIM neighbor.	<b>display pim neighbor</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>verbose</b> ] <b>display pim neighbor</b> <i>neighbor-address</i> [ <b>verbose</b> ]
Check the PIM multicast routing table.	<b>display pim routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask-length</i>   <i>group-mask</i> } ] ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask-length</i>   <i>source-mask</i> } ] ] [ <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> } ] [ <b>outgoing-interface</b> { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b>   <b>none</b> } ] [ <b>mode</b> { <b>dm</b>   <b>sm</b>   <b>ssm</b> } ] [ <b>flags</b> <i>flag-value</i> ] [ <b>fsm</b> ]
Check information about the RP to which a multicast group corresponds.	<b>display pim rp-info</b> [ <i>group-address</i> ]

### 6.12.3 Debugging PIM



#### CAUTION

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

When a fault occurs in the running of PIM, run the **debugging** command in the user view to debug PIM and locate the fault.

Action	Command
Debug PIM.	<b>debugging pim</b> { <b>all</b>   <b>event</b> [ <i>advanced-acl-number</i> ]   <b>routing-table</b> [ <i>advanced-acl-number</i> ]   <b>neighbor</b> [ <i>basic-acl-number</i> ]   <b>assert</b> [ <i>advanced-acl-number</i> ]   <b>rp</b>   <b>join-prune</b> [ <i>advanced-acl-number</i> ]   <b>register</b> [ <i>advanced-acl-number</i> ]   <b>msdp</b> [ <i>advanced-acl-number</i> ]   <b>state-refresh</b> [ <i>advanced-acl-number</i> ] }

## 6.13 Configuration Examples

This section provides several configuration examples of PIM-SM.

### 6.13.1 Example for Configuring a PIM-SM Network

### 6.13.2 Example for Configuring the SPT Switchover in a PIM-SM Domain

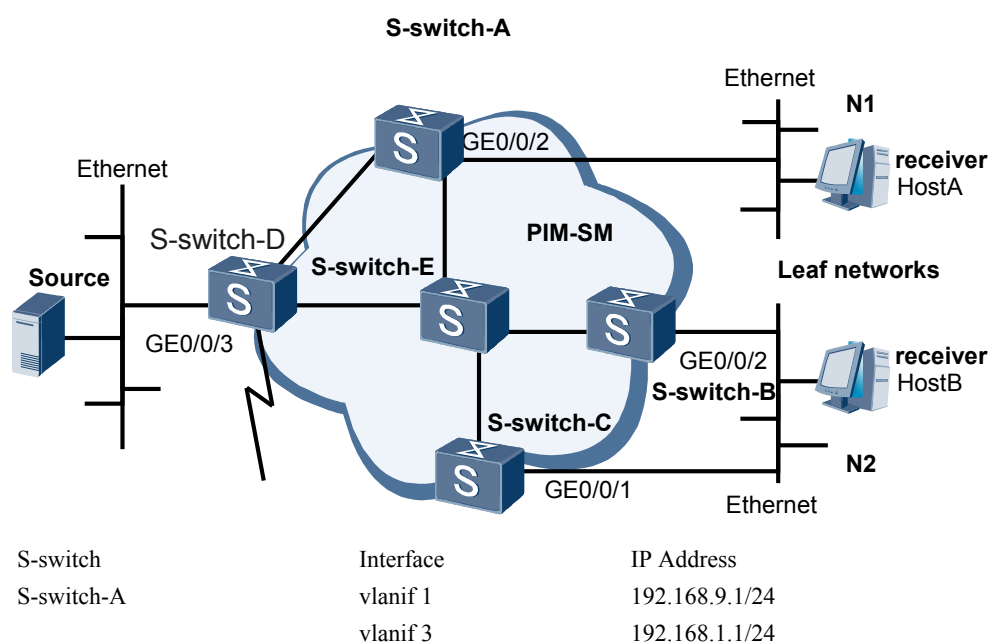
### 6.13.3 Example for Configuring PIM BFD on Routers in Ethernet

### 6.13.1 Example for Configuring a PIM-SM Network

## Networking Requirements

As shown in **Figure 6-2**, multicast is deployed in the Internet Service Provider (ISP) network. An integrated Interior Gateway Protocol (IGP) is deployed in the network. Unicast routes work normally and are connected to the Internet. It is required to perform proper configuration on S-switches in the network to enable hosts to receive the Video On Demand (VOD) information in multicast mode.

**Figure 6-2** Networking diagram for configuring PIM-SM multicast network



	vlanif 2	10.110.1.1/24
S-switch-B	vlanif 1	192.168.2.1/24
	vlanif 2	10.110.2.1/24
S-switch-C	vlanif 2	192.168.3.1/24
	vlanif 1	10.110.2.2/24
S-switch-D	vlanif 1	192.168.4.2/24
	vlanif 2	192.168.1.2/24
	vlanif 4	10.110.4.1/24
	vlanif 3	10.110.5.1/24
S-switch-E	vlanif 1	192.168.3.2/24
	vlanif 2	192.168.2.2/24
	vlanif 3	192.168.9.2/24
	vlanif 4	192.168.4.1/24

## Configuration Roadmap

The ISP network is accessed to the Internet. To expand services, PIM-SM is adopted to configure multicast functions, and ASM and SSM models are used to provide multicast services.

1. Configure an IP address for each interface on S-switches and a unicast routing protocol. PIM, an intra-domain multicast routing protocol, depends on unicast routing protocols. The multicast routing protocol can work normally only when unicast routing protocols work normally.
2. Enable the multicast function on all the S-switches providing multicast services. PIM-SM can be configured only after multicast is enabled.
3. Enable PIM-SM on all interfaces of the multicast S-switches. Other PIM-SM functions can be configured only after PIM-SM is enabled.

### NOTE

If IGMP needs to be configured on this interface, PIM-SM must be enabled before IGMP is enabled. The configuration order cannot be reversed; otherwise, the configuration of PIM-SM fails.

4. Enable IGMP on the interface connected to user hosts. A receiver can join and leave a multicast group freely by sending IGMP messages. Leaf S-switches maintain the member relationship through IGMP.
5. Enable PIM silent on the S-switch interface connected to hosts to prevent malicious hosts from attacking the S-switch by simulating and sending PIM Hello packets; therefore, the security of multicast S-switches can be ensured.

### NOTE

PIM silent is applicable only to the S-switch interface directly connected to the host network segment that is connected only to this S-switch.

6. Configure an RP. The RP is a root node of an RPT tree in a PIM-SM network. It is recommended to configure the RP on a S-switch through which many multicast flows pass, such as S-switchE in the figure.

 **NOTE**

- After creating an (\*, G) entry according to the new multicast member relationship, the DR on the user side sends Join/Prune messages to the RP, updating the shared tree.
  - When a multicast data source starts to send data to groups, the DR unicasts a Register message to the RP. After receiving the Register message, the RP decapsulates it and then forwards it to other multicast members along the shared tree. At the same time, the RP sends a Register-Stop message to the DR on the multicast source side. After the register is stopped, the traffic can be switched from RPT to the SPT.
7. (Optional) Configure the BSR boundary on the interface connected to the Internet. Bootstrap messages cannot pass through the BSR boundary; therefore, the BSR serves this PIM-SM domain only. In this manner, multicast services can be controlled effectively.
  8. (Optional) Configure the SSM group address range on each S-switch. Ensure that multicast S-switches in the PIM-SM domain provide services only for multicast groups in the SSM group address range. In this manner, multicast services can be controlled effectively.

## Data Preparation

To complete the configuration, you need the following data:

- Address of multicast group G is 225.1.1.1.
- Source address is 10.110.5.100/24.
- Version number of IGMP running between the interface and hosts is 3.
- SSM group address range is 232.1.1.0/24.

## Configuration Procedure

 **NOTE**

In the configuration example, only the commands related to PIM-SM configuration are mentioned.

1. Configure an IP address and a unicast routing protocol on each interface.
2. Enable multicast on all S-switches and PIM-SM on all interfaces.  
  
# Enable multicast on all S-switches and PIM-SM on all interfaces. The configurations of S-switch-B, S-switch-C, S-switch-D, and S-switch-E are the same as the configuration of S-switch-A, and are not mentioned here.  

```
[S-switch-A] multicast routing-enable
[S-switch-A] interface vlanif 2
[S-switch-A-Vlanif2] pim sm
[S-switch-A-Vlanif2] quit
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] pim sm
[S-switch-A-Vlanif1] quit
[S-switch-A] interface vlanif 3
[S-switch-A-Vlanif3] pim sm
[S-switch-A-Vlanif3] quit
```
3. Enable IGMP on the interface connected to hosts.  
  
# On S-switch-A, enable IGMP on the interface connected to hosts. The configurations of S-switch-B and S-switch-C are the same as the configuration of S-switch-A, and are not mentioned here.  

```
[S-switch-A] interface vlanif 2
[S-switch-A-Vlanif2] igmp enable
[S-switch-A-Vlanif2] igmp version 3
```
4. Enable PIM silent on an interface of S-switch-A.  

```
[S-switch-A] interface vlanif 2
```

```
[S-switch-A-Vlanif2] pim silent
```

## 5. Configure a C-RP.

### NOTE

- RPs are classified into two types, that is, the static RP and the dynamic RP. You can configure the static RP and the dynamic at the same time or just configure one of them.
- When the static RP and the dynamic RP are configured simultaneously, you can adjust parameters to specify the preferred RP.

This example shows how to configure the static RP and the dynamic RP, to prefer the dynamic RP, and specify the static RP as the standby RP by configuring the parameters.

# Configure the dynamic RP on one or more S-switches in the PIM-SM domain. Set the service range of the RP and configure the C-BSR and the C-RP on S-switch-E.

# On S-switch-E, configure the scope of RP advertisement and positions of a C-BSR and a C-RP.

```
[S-switch-E] acl number 2005
[S-switch-E-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[S-switch-E-acl-basic-2005] quit
[S-switch-E] pim
[S-switch-E-pim] c-bsr vlanif 3
[S-switch-E-pim] c-rp vlanif 3 group-policy 2005 priority 0
```

# Configure the static RP on all multicast S-switches. Configure S-switch-A, S-switch-B, S-switch-C, S-switch-D, and S-switch-E. The configurations on S-switch-B, S-switch-C, S-switch-D, and S-switch-E are similar to those on S-switch-A. The detailed configurations are not mentioned here.

### NOTE

If **preferred** is set in the **static-rp x.x.x.x** command, the static RP is preferred as the RP in the PIM-SM domain.

```
[S-switch-A] pim
[S-switch-A-pim] static-rp 192.168.2.2
```

## 6. On S-switch-D, configure the BSR boundary on the interface connected to the Internet.

```
[S-switch-D] interface vlanif 4
[S-switch-D-Vlanif4] pim bsr-boundary
[S-switch-D-Vlanif4] quit
```

## 7. Configure the SSM group address range.

# Set the SSM group address range to 232.1.1.0/24 on all S-switches. The configurations of S-switch-B, S-switch-C, S-switch-D, and S-switch-E are the same as the configuration of S-switch-A, and are not mentioned here.

```
[S-switch-A] acl number 2000
[S-switch-A-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[S-switch-A-acl-basic-2000] quit
[S-switch-A] pim
[S-switch-A-pim] ssm-policy 2000
```

## 8. Verify the configuration.

# Run the **display pim interface** command to view the configuration and running of PIM on an interface. The display of PIM on S-switch-C is as follows:

```
<S-switch-C> display pim interface
Interface      State    NbrCnt   HelloInt   DR-Pri    DR-Address
vlanif1        up       0         30         1         10.110.2.2   (local)
vlanif 2       up       1         30         1         192.168.3.1
```

# Run the **display pim bsr-info** command to view the BSR election on a S-switch. For example, the BSR information on S-switch-A and S-switch-E (including the C-BSR information on S-switch-E) is as follows:

```
<S-switch-A> display pim bsr-info
```

```
Elected AdminScoped BSR Count: 0
Elected BSR Address: 192.168.9.2
  Priority: 0
  Hash mask length: 30
  State: Accept Preferred
  Scope: Not scoped
  Uptime: 01:40:40
  Expires: 00:01:42
  C-RP Count: 1
```

```
<S-switch-E> display pim bsr-info
Elected AdminScoped BSR Count: 0
Elected BSR Address: 192.168.9.2
  Priority: 0
  Mask length: 30
  State: Elected
  Scope: Not scoped
  Uptime: 00:00:18
  Next BSR message scheduled at :00:01:42
  C-RP Count: 1
Candidate AdminScoped BSR Count: 0
Candidate BSR Address is: 192.168.9.2
  Priority: 0
  Hash mask length: 30
  State:Elected
  Scope: Not scoped
  Wait to be BSR: 0
```

# Run the **display pim rp-info** command to view the RP information obtained by a S-switch. For example, the RP information on S-switch-A is as follows:

```
<S-switch-A> display pim rp-info
```

```
PIM-SM BSR RP information:
Group/MaskLen: 225.1.1.0/24
  RP: 192.168.9.2
  Priority: 0
  Uptime: 00:51:45
  Expires: 00:02:22
PIM SM static RP information:
  Static RP: 192.168.2.2
```

# Run the **display pim routing-table** command to view the PIM multicast routing table on a S-switch. Host A needs to receive the information about group 225.1.1.1/24, and Host B needs to receive the information sent by source 10.110.5.100/24 to group 232.1.1.1/24. The display is as follows:

```
<S-switch-A> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
  RP: 192.168.9.2
  Protocol: pim-sm, Flag: WC
  UpTime: 00:13:46
  Upstream interface: vlanif 1,
    Upstream neighbor: 192.168.9.2
  RPF neighbor: 192.168.9.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2,
      Protocol: igmp, UpTime: 00:13:46, Expires:-

(10.110.5.100, 225.1.1.1)
  RP: 192.168.9.2
  Protocol: pim-sm, Flag: SPT ACT
  UpTime: 00:00:42
  Upstream interface: vlanif 3
    Upstream neighbor: 192.168.1.2
  RPF neighbor: 192.168.1.2
```

```
Downstream interface(s) information:
Total number of downstreams: 1
  1: vlanif2
    Protocol: pim-sm, UpTime: 00:00:42, Expires:-
<S-switch-D> display pim routing-table
Total 0 (*, G) entry; 2 (S, G) entry

(10.110.5.100, 225.1.1.1)
RP: 192.168.9.2
Protocol: pim-sm, Flag: SPT ACT
UpTime: 00:00:42
Upstream interface: vlanif3
  Upstream neighbor: 10.110.5.100
  RPF neighbor: 10.110.5.100
Downstream interface(s) information:
Total number of downstreams: 1
  1: vlanif 2
    Protocol: pim-sm, UpTime: 00:00:42, Expires:-

(10.110.5.100, 232.1.1.1)
Protocol: pim-ssm, Flag:
UpTime: 00:01:20
Upstream interface: vlanif3
  Upstream neighbor: 10.110.5.100
  RPF neighbor: 10.110.5.100
Downstream interface(s) information:
Total number of downstreams: 1
  1: vlanif 1
    Protocol: pim-ssm, UpTime: 00:01:20, Expires:-

<S-switch-E> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
RP: 192.168.9.2 (local)
Protocol: pim-sm, Flag: WC
UpTime: 00:13:16
Upstream interface: Register
  Upstream neighbor: 192.168.4.2
  RPF neighbor: 192.168.4.2
Downstream interface(s) information:
Total number of downstreams: 1
  1: vlanif 3
    Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22

(10.110.5.100, 232.1.1.1)
Protocol: pim-ssm, Flag:
UpTime: 00:01:22
Upstream interface: vlanif 4
  Upstream neighbor: 192.168.4.2
  RPF neighbor: 192.168.4.2
Downstream interface(s) information:
Total number of downstreams: 1
  1: vlanif 1
    Protocol: pim-ssm, UpTime: 00:01:22, Expires:-

<S-switch-C> display pim routing-table
Total 1 (S, G) entry

(10.110.5.100, 232.1.1.1)
Protocol: pim-ssm, Flag:
UpTime: 00:01:25
Upstream interface: vlanif 2
  Upstream neighbor: 192.168.3.2
  RPF neighbor: 192.168.3.2
Downstream interface(s) information:
Total number of downstreams: 1
  1: vlanif1
    Protocol: igmp, UpTime: 00:01:25, Expires:-
```

## Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
 multicast routing-enable
#
 acl number 2000
  rule 5 permit source 232.1.1.0 0.0.0.255
#
 interface vlanif2
  undo shutdown
  ip address 10.110.1.1 255.255.255.0
  pim sm
  igmp enable
  igmp version 3
  pim silent
#
 interface vlanif 3
  link-protocol ppp
  undo shutdown
  ip address 192.168.1.1 255.255.255.0
  pim sm
#
 interface vlanif 1
  link-protocol ppp
  undo shutdown
  ip address 192.168.9.1 255.255.255.0
  pim sm
#
 ospf 1
  area 0.0.0.0
    network 10.110.1.0 0.0.0.255
    network 192.168.1.0 0.0.0.255
    network 192.168.9.0 0.0.0.255
#
 pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
 return
```

- Configuration file of S-switch-B

```
#
 sysname S-switch-B
#
 multicast routing-enable
#
 acl number 2000
  rule 5 permit source 232.1.1.0 0.0.0.255
#
 interface vlanif2
  undo shutdown
  ip address 10.110.2.1 255.255.255.0
  pim sm
  igmp enable
  igmp version 3
#
 interface vlanif 1
  link-protocol ppp
  undo shutdown
  ip address 192.168.2.1 255.255.255.0
  pim sm
#
 ospf 1
  area 0.0.0.0
    network 10.110.2.0 0.0.0.255
    network 192.168.2.0 0.0.0.255
```

```
#
Pim
static-rp 192.168.2.2
  ssm-policy 2000
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
multicast routing-enable
#
acl number 2000
  rule 5 permit source 232.1.1.0 0.0.0.255
#
interface vlanif1
undo shutdown
ip address 10.110.2.2 255.255.255.0
  pim sm
igmp enable
igmp version 3
#
interface vlanif 2
link-protocol ppp
undo shutdown
  ip address 192.168.3.1 255.255.255.0
  pim sm
#
ospf 1
  area 0.0.0.0
    network 10.110.2.0 0.0.0.255
    network 192.168.3.0 0.0.0.255
#
pim
static-rp 192.168.2.2
  ssm-policy 2000
#
return
```

- Configuration file of S-switch-D

```
#
sysname S-switch-D
#
multicast routing-enable
#
acl number 2000
  rule 5 permit source 232.1.1.0 0.0.0.255
#
interface vlanif3
undo shutdown
ip address 10.110.5.1 255.255.255.0
  pim sm
#
interface vlanif 4
link-protocol ppp
undo shutdown
  ip address 10.110.4.1 255.255.255.0
  pim sm
pim bsr-boundary
#
interface vlanif 2
link-protocol ppp
undo shutdown
  ip address 192.168.1.2 255.255.255.0
  pim sm
#
interface vlanif 1
link-protocol ppp
undo shutdown
```

```
ip address 192.168.4.2 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 10.110.4.0 0.0.0.255
network 10.110.5.0 0.0.0.255
network 192.168.1.0 0.0.0.255
network 192.168.4.0 0.0.0.255
#
pim
static-rp 192.168.2.2
ssm-policy 2000
#
return
```

- Configuration file of S-switch-E

```
#
sysname S-switch-E
#
multicast routing-enable
#
acl number 2000
rule 5 permit source 232.1.1.0 0.0.0.255
#
acl number 2005
rule 5 permit source 225.1.1.0 0.0.0.255
#
interface vlanif 1
link-protocol ppp
undo shutdown
ip address 192.168.3.2 255.255.255.0
pim sm
#
interface vlanif 2
link-protocol ppp
undo shutdown
ip address 192.168.2.2 255.255.255.0
pim sm
#
interface vlanif 3
link-protocol ppp
undo shutdown
ip address 192.168.9.2 255.255.255.0
pim sm
#
interface vlanif 4
link-protocol ppp
undo shutdown
ip address 192.168.4.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.3.0 0.0.0.255
network 192.168.2.0 0.0.0.255
network 192.168.9.0 0.0.0.255
network 192.168.4.0 0.0.0.255
#
pim
c-bsr vlanif 3
c-rp vlanif 3 group-policy 2005 priority 0
static-rp 192.168.2.2
ssm-policy 2000
#
return
```

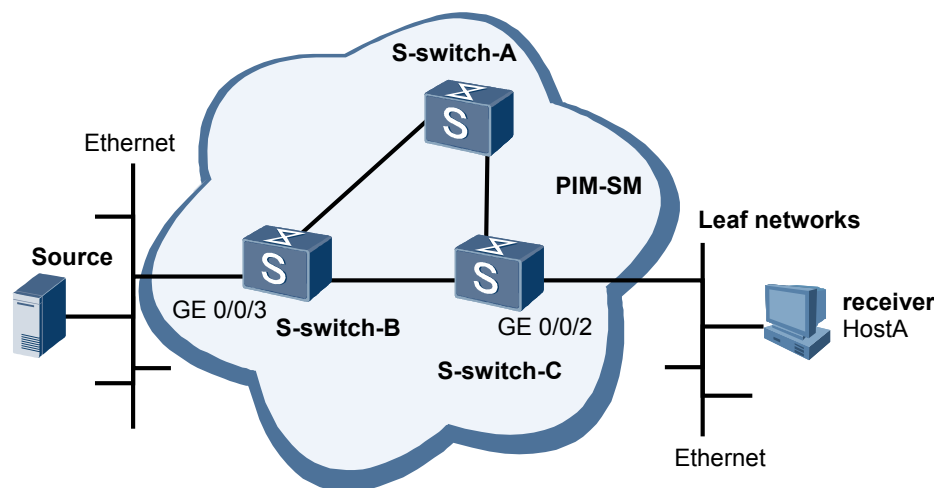
## 6.13.2 Example for Configuring the SPT Switchover in a PIM-SM Domain

### Networking Requirements

Receivers can receive the Video On Demand (VOD) information in multicast mode. The SM-single BSR administrative domain is adopted in the entire PIM network. By default, the DR at the receiver side and the RP perform the SPT switchover immediately after receiving the first multicast data packet, and choose the optimal path to receive information from the source. If a receiver wants to perform the SPT switchover after the traffic reaches the threshold, you need to configure the SPT switchover.

As shown in [Figure 6-3](#), it is required to perform proper configuration on S-switches. Host A on the leaf network can receive multicast data from the RP (vlanif 1 of S-switch-A). When the rate for forwarding multicast data reaches 1024 kbit/s, the SPT switchover is performed (After SPT switchover, the path used by Host A to receive multicast data is Source—S-switch-B—S-switch-C—Host A).

**Figure 6-3** Networking diagram for performing SPT switchover in a PIM-SM domain



S-switch	Interface	IP address
S-switch-A	vlanif 1	192.168.1.1/24
	vlanif 2	192.168.3.1/24
S-switch-B	vlanif 1	192.168.2.1/24
	vlanif 2	192.168.3.2/24
	vlanif 3	10.110.5.1/24
S-switch-C	vlanif 1	192.168.1.2/24
	vlanif 3	192.168.2.2/24
	vlanif 2	10.110.2.1/24

### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address and a unicast routing protocol for each interface.

2. Enable multicast on each S-switch, PIM-SM on each interface, and IGMP on the interface at the host side.
3. Configure vlanif 1 of S-switch-A as the C-BSR and C-RP.
4. Perform the SPT switchover on S-switch-C.

## Data Preparation

To complete the configuration, you need the following data:

- Multicast source address is 10.110.5.100/24.
- Group address is 225.1.1.1/24.
- The number of IGMP version running between S-switch-C and the leaf network is 2.

## Configuration Procedure

1. Configure an IP address and a unicast routing protocol on each interface.  
# Based on [Figure 6-3](#), configure an IP address and mask of each interface, interconnect S-switches through OSPF, ensure that S-switch-A, S-switch-B, and S-switch-C can interconnect at the network layer, and configure the three S-switches to dynamically update routes through a unicast routing protocol. The configuration details are not mentioned here.
2. Enable multicast on each S-switch, PIM-SM on each interface, and IGMP on the interface at the host side.  
# Enable multicast on each S-switch, PIM-SM on each interface, and IGMP on the interfaces through which S-switch-C is connected to the leaf network. The configurations of S-switch-A and S-switch-B are the same as the configuration of S-switch-C, and are not mentioned here.  

```
[S-switch-C] multicast routing-enable
[S-switch-C] interface vlanif 2
[S-switch-C-Vlanif2] pim sm
[S-switch-C-Vlanif2] igmp enable
[S-switch-C-Vlanif2] igmp version 2
[S-switch-C-Vlanif2] quit
[S-switch-C] interface vlanif 3
[S-switch-C-Vlanif3] pim sm
[S-switch-C-Vlanif3] quit
[S-switch-C] interface vlanif 1
[S-switch-C-Vlanif1] pim sm
[S-switch-C-Vlanif1] quit
```
3. Configure a static RP.  
# Configure the static RP on S-switch-A, S-switch-B, and S-switch-C. The configurations on S-switch-B and S-switch-C are similar to those on S-switch-A. The detailed configurations are not mentioned here.  

```
[S-switch-A] pim
[S-switch-A-pim] static-rp 192.168.1.1
```
4. Configure the threshold of the SPT switchover.  
# Perform the SPT switchover on S-switch-C when the rate of multicast data packets reaches 1024 kbit/s.  

```
[S-switch-C] pim
[S-switch-C-pim] spt-switch-threshold 1024
[S-switch-C-pim] quit
```
5. Verify the configuration.  
# The multicast source starts to send data to the group, and Host A can receive the data from the source. When the rate is smaller than 1024 kbit/s, run the **display pim routing-**

**table** command to view the PIM multicast routing table on the S-switch. You can find that the upstream neighbor is S-switch-A. The display is as follows:

```
<S-switch-C> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
  RP: 192.168.1.1
  Protocol: pim-sm, Flag: WC
  UpTime: 00:13:46
  Upstream interface: vlanif 1,
    Upstream neighbor: 192.168.1.1
    RPF neighbor: 192.168.1.1
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2,
      Protocol: igmp, UpTime: 00:13:46, Expires:-
(10.110.5.100, 225.1.1.1)
  RP: 192.168.1.1
  Protocol: pim-sm, Flag: ACT
  UpTime: 00:00:42
  Upstream interface: vlanif 1
    Upstream neighbor: 192.168.1.1
    RPF neighbor: 192.168.1.1
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2
      Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

# When the rate is greater than 1024 kbit/s, run the **display pim routing-table** command to view the PIM multicast routing table on the S-switch. You can find that the upstream neighbor is S-switch-B. The display is as follows:

```
<S-switch-C> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
  RP: 192.168.1.1
  Protocol: pim-sm, Flag: WC
  UpTime: 00:13:46
  Upstream interface: vlanif 2,
    Upstream neighbor: 192.168.2.2
    RPF neighbor: 192.168.2.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2,
      Protocol: igmp, UpTime: 00:13:46, Expires:-
(10.110.5.100, 225.1.1.1)
  RP: 192.168.1.1
  Protocol: pim-sm, Flag: RPT SPT ACT
  UpTime: 00:00:42
  Upstream interface: vlanif 2
    Upstream neighbor: 192.168.2.2
    RPF neighbor: 192.168.2.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2
      Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
multicast routing-enable
#
interface vlanif 1
link-protocol ppp
```

```
undo shutdown
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface vlanif 2
 link-protocol ppp
undo shutdown
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
pim
static-rp 192.168.1.1
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
multicast routing-enable
#
interface vlanif3
undo shutdown
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
interface vlanif 1
 link-protocol ppp
undo shutdown
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface vlanif 2
 link-protocol ppp
undo shutdown
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
pim
static-rp 192.168.1.1
#
ospf 1
 area 0.0.0.0
  network 10.110.5.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
multicast routing-enable
#
interface vlanif 1
 link-protocol ppp
undo shutdown
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface vlanif2
undo shutdown
 ip address 10.110.2.1 255.255.255.0
 pim sm
```

```

igmp enable
igmp version 2
#
interface vlanif 3
link-protocol ppp
undo shutdown
ip address 192.168.2.2 255.255.255.0
pim sm
#
pim
spt-switch-threshold 1024
static-rp 192.168.1.1
#
ospf 1
area 0.0.0.0
network 10.110.2.0 0.0.0.255
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
return

```

### 6.13.3 Example for Configuring PIM BFD on Routers in Ethernet

#### Networking Requirements

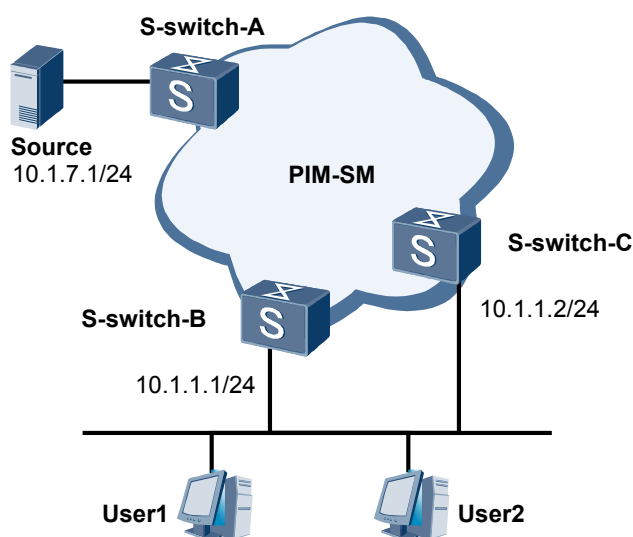
In the multicast network shown in [Figure 6-4](#), PIM-SM is run on S-switches, hosts normally receive the VOD information from the multicast source, and S-switch-B and S-switch-C are connected to the host network segment. When the DR changes, other S-switches in the network segment can detect the change of the DR quickly.

Set up the BFD session on the host network segment to quickly respond to the changes of the DR, and configure the delay of the DR switchover. In this case, when a S-switch is added to the network segment and may become a DR, the multicast routing table of the original DR is reserved till the entries of the new DR are created. The packet loss due to the delay for creating multicast entries is thus prevented.

#### NOTE

After the delay of the PIM DR switchover is set, downstream receivers may receive two copies of the same data during the DR switchover, and trigger the assert mechanism. If you do not tend to trigger the assert mechanism, you need not configure the DR switchover delay.

**Figure 6-4** Networking diagram of applying PIM BFD on a multi-router network segment



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure PIM BFD on the interface that is connected to the host network segment.
2. Configure the PIM DR switching delay on the interface that is connected to the host network segment.

## Data Preparation

To complete the configuration, you need the following data:

- Parameters of a PIM BFD session
- PIM DR switching delay

## Configuration Procedures

### NOTE

In the configuration example, only the commands related to PIM-SM BFD are mentioned.

1. Configure an IP address for each interface and a unicast routing protocol.
2. Enable BFD globally and configure PIM BFD on an interface.

# Enable BFD globally on S-switch-B and S-switch-C, enable PIM BFD on the interface that is connected to the host network segment, and configure PIM BFD parameters. Configuration procedures of S-switch-C are similar to those of S-switch-B, and are not mentioned here.

```
[S-switch-B] bfd
[S-switch-B-bfd] quit
[S-switch-B] interface vlanif 2
[S-switch-B-Vlanif2] pim bfd enable
[S-switch-B-Vlanif2] pim bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 3
```

3. Configure the PIM DR switching delay

# Configure the PIM DR switching delay on S-switch-B and S-switch-C. The configuration procedures of S-switch-C are similar to those of S-switch-B, and are not mentioned here.

```
[S-switch-B-Vlanif2] pim timer dr-switch-delay 20
[S-switch-B-Vlanif2] quit
[S-switch-B] quit
```

4. Verify the configuration

# Run the **display pim interface verbose** command, and you can view detailed information about the PIM interface. The information about the PIM interface on S-switch-B indicates that the DR on the host network segment is S-switch-C, and the interface is enabled with PIM BFD and configured with the switching delay.

```
<S-switch-B> display pim interface vlanif2 verbose
Interface: vlanif2, 10.1.1.1
  PIM version: 2
  PIM mode: Sparse
  PIM DR: 10.1.1.2
  PIM DR Priority (configured): 1
  PIM neighbor count: 1
  PIM Hello interval: 30 s
  PIM LAN delay (negotiated): 500 ms
  PIM LAN delay (configured): 500 ms
  PIM Hello override interval (negotiated): 2500 ms
  PIM Hello override interval (configured): 2500 ms
  PIM Silent: disabled
```

```

PIM neighbor tracking (negotiated): disabled
PIM neighbor tracking (configured): disabled
PIM generation ID: 0XF5712241
PIM Hello hold interval: 105 s
PIM Hello assert interval: 180 s
PIM triggered Hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
PIM BFD: enable
PIM BFD min-tx-interval: 100 ms
PIM BFD min-rx-interval: 100 ms
PIM BFD detect-multiplier: 3
PIM dr-switch-delay timer : 20 s
Number of S-switches on network not using DR priority: 0
Number of S-switches on network not using LAN delay: 0
Number of S-switches on link not using neighbor tracking: 2

```

# Run the **display pim bfd session** command to display the BFD session on each S-switch, and you can check whether the BFD session on each S-switch is set up.

```

<S-switch-B> display pim bfd session
Total 1 BFD session Created
vlanif2 (10.1.1.1): Total 1 BFD session Created

```

Neighbor	ActTx(ms)	ActRx(ms)	ActMulti	Local/Remote	State
10.1.1.2	100	100	3	8192/8192	Up

# Run the **display pim routing-table** command to view the PIM routing table. S-switch-C acts as the DR. (S, G) and (\*, G) entries exist. The display is as follows:

```

<S-switch-C> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry
(*, 225.1.1.1)
  RP: 10.1.5.2
  Protocol: pim-sm, Flag: WC
  UpTime: 00:13:46
  Upstream interface: vlanif 1,
    Upstream neighbor: 10.1.2.2
  RPF neighbor: 10.1.2.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2,
      Protocol: igmp, UpTime: 00:13:46, Expires:-
(10.1.7.1, 225.1.1.1)
  RP: 10.1.5.2
  Protocol: pim-sm, Flag: SPT ACT
  UpTime: 00:00:42
  Upstream interface: vlanif 1
    Upstream neighbor: 10.1.2.2
  RPF neighbor: 10.1.2.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2
      Protocol: pim-sm, UpTime: 00:00:42, Expires:-

```

## Configuration Files

S-switch-A needs to be configured only with basic PIM-SM functions that are not most of concern in this example. Therefore, the configuration file of S-switch-A is not mentioned here.

The configuration file of S-switch-B is as follows. The configuration file of S-switch-C is similar to that of S-switch-B and is not mentioned here.

```

#
sysname S-switch-B
#
multicast routing-enable
#
bfd

```

```
#
interface vlanif 1
 link-protocol ppp
 undo shutdown
 ip address 10.1.2.1 255.255.255.0
 pim sm
#
interface vlanif2
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 pim sm
 igmp enable
 pim bfd enable
 pim bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 3
 pim timer dr-switch-delay 20
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
return
```



# 7 IGMP Configuration

---

## About This Chapter

This chapter describes the IGMP fundamentals and configuration steps, and maintenance for IGMP functions, along with typical examples.

### [7.1 Introduction](#)

This section describes the basic principle of IGMP and IGMP features supported by the S-switch.

### [7.2 Configuring Basic IGMP Functions](#)

This section describes how to configure basic IGMP functions.

### [7.3 Configuring Options of an IGMP Packet](#)

This section describes how to configure IGMP packet options.

### [7.4 Configuring IGMP Query Control](#)

This section describes how to configure IGMPv1 and IGMPv2/v3 queriers.

### [7.5 Configuring SSM Mapping](#)

This section describes how to configure SSM mapping.

### [7.6 Maintaining IGMP](#)

This section describes how to clear IGMP statistics and debug IGMP.

### [7.7 Configuration Examples](#)

This section provides several configuration examples of IGMP.

## 7.1 Introduction

This section describes the basic principle of IGMP and IGMP features supported by the S-switch.

### 7.1.1 IGMP Overview

#### 7.1.2 IGMP Features Supported by the S-switch

### 7.1.1 IGMP Overview

With the wide applications of multicast, increasingly more hosts join the related multicast groups. Managing multicast groups and related members on S-switches becomes an important issue.

In the TCP/IP suite, the Internet Group Management Protocol (IGMP) manages IP multicast members. It establishes and maintains the relationship between IP hosts and S-switches that are directly connected to the IP hosts.

IGMP is a signaling mechanism of hosts towards S-switches on the leaf network. IGMP can be divided into two functional parts: at the host side and at the S-switch side.

#### NOTE

The Operating System (OS) used by a host determine whether the host supports IGMP.

- All hosts that participate in multicast transmission must be enabled with IGMP. Hosts can randomly join or leave the related multicast groups, and the number of hosts is not limited.
- Through IGMP, a multicast S-switch can know whether there is a member of a certain group in the network segment to which each interface of the S-switch is connected. Hosts store information only about the multicast groups they join.

At present, IGMP has three versions, that is, IGMPv1 (defined in RFC 1112), IGMPv2 (defined in RFC 2236), and IGMPv3 (defined in RFC 3376). All IGMP versions support the Any-Source Multicast (ASM) model. IGMPv3 can be directly applied to the Source-Specific Multicast (SSM) model, whereas IGMPv1 and IGMPv2 require the technical support of SSM mapping when they are applied to the SSM model.

### 7.1.2 IGMP Features Supported by the S-switch

#### Basic Functions of IGMP

The basic IGMP functions supported by the S-switch are as follows:

- Supporting IGMPv1, IGMPv2, and IGMPv3. The IGMP version can be configured.
- Supporting static IGMP.
- Configuring the range of multicast groups that an interface can join.

#### Router-Alert

Through Router-Alert, IGMP sends the messages related to the group that the local device does not join to the upper protocol for processing.

According to requirements, users can determine whether to set Router-Alert in IGMP packets to be sent, and whether to require that the received IGMP packets contain Router-Alert.

## IGMP Query Controller

For IGMPv1, users can set the interval for sending general query messages and the robustness variable.

For IGMPv2, users can configure the interval for sending general query messages, robustness variables, the maximum response time of IGMP query packets, and IGMP fast leave.

For IGMPv3, users can configure the interval for sending general query messages, robustness variables, and the maximum response time of IGMP query packets.

## SSM-Mapping

You can configure SSM mapping on S-switches to provide SSM services for hosts that run IGMPv1 or IGMPv2.

## 7.2 Configuring Basic IGMP Functions

This section describes how to configure basic IGMP functions.

### [7.2.1 Establishing the Configuration Task](#)

### [7.2.2 Enabling IP Multicast Routing](#)

### [7.2.3 Enabling Basic IGMP Functions](#)

### [7.2.4 Configuring IGMP Version](#)

### [7.2.5 Configuring a Static IGMP Group](#)

### [7.2.6 Configuring an Interface to Join a Multicast Group in a Certain Range](#)

### [7.2.7 Checking the Configuration](#)

## 7.2.1 Establishing the Configuration Task

### Applicable Environment

IGMP is applicable to the network segment where S-switches are connected to hosts. S-switches and hosts need to run IGMP. This section describes how to configure only IGMP on S-switches.

Before configuring IGMP, enable IP multicast routing. IP multicast routing is the precondition for configuring all multicast functions. If IP multicast routing is disabled, the configurations related to multicast are deleted.

You need to enable IGMP on the interface connected to hosts. Because the packet formats of IGMPv1, IGMPv2, and IGMPv3 are different, you need to specify the IGMP version for S-switches and hosts first (the later version at the S-switch side is compatible with the earlier version at the host side). After this, you can perform other IGMP configurations.

You can set an ACL rule so that the host joins specified multicast groups and receive packets from these groups. This ACL rule serves as a filter on the associated interface and limits the range of groups that an interface joins.

## Pre-configuration Tasks

Before configuring basic IGMP functions, complete the following tasks:

- Configuring the link layer protocol parameters and an IP address for each interface to make the link protocol of the interface Up
- Configuring a unicast routing protocol to make IP routes between nodes reachable

## Data Preparation

To configure basic IGMP functions, you need the following data.

No.	Data
1	IGMP version
2	Group address and source address used to configure static multicast groups
3	ACL rules used for filtering multicast groups

### NOTE

- The configuration in the IGMP view is globally effective, whereas the configuration in the interface view is effective only on the interface.
- When the command is not used in the interface view, the global values set in the IGMP view are used. When the command is used in both views, the values set in the interface view are preferred.

## 7.2.2 Enabling IP Multicast Routing

### Context

Do as follows on the S-switch connected to hosts:

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
multicast routing-enable
```

IP multicast routing is enabled in the public network instance.

By default, IPv4 multicast routing is not enabled in the public network instance.

----End

## 7.2.3 Enabling Basic IGMP Functions

### Context

Do as follows on the S-switch connected to hosts:

### Procedure

- Step 1** Run:
- ```
system-view
```
- The system view is displayed.
- Step 2** Run:
- ```
interface interface-type interface-number
```
- The interface view is displayed.
- Step 3** Run:
- ```
igmp enable
```
- IGMP is enabled.
- By default, IGMP is not enabled on the interface.
- End

## 7.2.4 Configuring IGMP Version

### Context



#### CAUTION

All the S-switches on the same subnet must be configured with the same IGMP version. By default, IGMPv2 is adopted.

---

### Procedure

- Step 1** Run:
- ```
system-view
```
- The system view is displayed.
- Step 2** Run:
- ```
interface interface-type interface-number
```
- The interface view is displayed.
- Step 3** Run:
- ```
version { 1 | 2 | 3 }
```

The IGMP version is set for the interface.

----End

## 7.2.5 Configuring a Static IGMP Group

### Context

The configuration is optional. By default, the interface does not statically join any multicast group.

Do as follows on the S-switch connected to hosts:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
igmp static-group group-address [ source source-address ]
```

The interface is configured to statically join a multicast group.

After the interface joins the multicast group, the S-switch considers that members of the group exist in the network segment where the interface resides.

----End

## 7.2.6 Configuring an Interface to Join a Multicast Group in a Certain Range

### Context

Do as follows on the S-switch connected to hosts:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
igmp group-policy acl-number [ 1 | 2 | 3 ]
```

The range of multicast groups that the interface is allowed to join is configured.

----End

## 7.2.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the configuration and running of IGMP on an interface.	<b>display igmp interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the members of a static IGMP multicast group.	<b>display igmp group</b> [ <i>group-address</i>   <b>interface interface-type interface-number</b> ] <b>static</b>
Check the members of an IGMP multicast group.	<b>display igmp group</b> [ <i>group-address</i>   <b>interface interface-type interface-number</b> ] <b>static</b>

## 7.3 Configuring Options of an IGMP Packet

This section describes how to configure IGMP packet options.

### [7.3.1 Establishing the Configuration Task](#)

### [7.3.2 Configuring a S-switch to Reject IGMP Packets Without the Router-Alert Option](#)

### [7.3.3 Configuring a S-switch to Send IGMP Packets Without the Router-Alert Option](#)

### [7.3.4 Checking the Configuration](#)

## 7.3.1 Establishing the Configuration Task

### Applicable Environment

With the help of the Router-Alert option, an IGMP S-switch can send the received packets for the group that the S-switch does not join to the upper layer protocol for processing. For details of Route-Alert, refer to RFC 2113.

### Pre-configuration Tasks

Before configuring options of an IGMP packet, complete the following task:

- Configuring a unicast routing protocol
- [7.2 Configuring Basic IGMP Functions](#)

### Data Preparation

To configure options of an IGMP packet, you need the following data.

No.	Data
1	Whether a packet should contain the Router-Alert option

## 7.3.2 Configuring a S-switch to Reject IGMP Packets Without the Router-Alert Option

### Context

By default, S-switches do not check the Router-Alert option contained in IGMP packets. That is, S-switches process all the received IGMP packets, including the IGMP packets without the Router-Alert option.

When a user does not want to receive the IGMP packets without Router-Alert option, do as follows on the S-switch connected to the user:



#### NOTE

The configuration involves the following cases:

- Global configuration: It is valid on all interfaces.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration
  1. Run:  
**system-view**  
The system view is displayed.
  2. Run:  
**igmp**  
The IGMP view is displayed.
  3. Run:  
**require-router-alert**  
The S-switch is configured to receive only the IGMP packets with the Router-Alert option.  
The IGMP packets without the Router-Alert option are discarded.
- Configuration on an Interface
  1. Run:  
**system-view**  
The system view is displayed.
  2. Run:  
**interface** *interface-type interface-number*  
The interface view is displayed.

The interface is connected to hosts or a switch.

3. Run:  
`igmp require-router-alert`

The S-switch is configured to receive only the IGMP packets with the Router-Alert option.

The IGMP packets without the Router-Alert option are discarded.

----End

### 7.3.3 Configuring a S-switch to Send IGMP Packets Without the Router-Alert Option

#### Context

By default, the IGMP packets sent by S-switches contain the Router-Alert option.

To configure a S-switch to send the IGMP packets without the Router-Alert option, do as follows on the S-switch connected to hosts:

#### NOTE

The configuration involves the following cases:

- Global configuration: It is valid on all interfaces.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

#### Procedure

- Global Configuration
  1. Run:  
`system-view`  
  
The system view is displayed.
  2. Run:  
`igmp`  
  
The IGMP view is displayed.
  3. Run:  
`undo send-router-alert`  
  
The header of a sent IGMP packet does not contain the Router-Alert option.
- Configuration on an Interface
  1. Run:  
`system-view`  
  
The system view is displayed.
  2. Run:  
`interface interface-type interface-number`  
  
The interface view is displayed.

The interface is connected to hosts or a switch.

3. Run:  
`undo igmp send-router-alert`

The header of a sent IGMP packet does not contain the Router-Alert option.

----End

## 7.3.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check an IGMP group.	<b>display igmp group</b> [ <i>group-address</i>   <b>interface</b> <i>interface-type interface-number</i> ] [ <b>static</b>   <b>verbose</b> ]
Check the configuration and running of IGMP on an interface.	<b>display igmp interface</b> [ <i>interface-type interface-number</i>   <b>up</b>   <b>down</b> ] [ <b>verbose</b> ]

## 7.4 Configuring IGMP Query Control

This section describes how to configure IGMPv1 and IGMPv2/v3 queriers.

[7.4.1 Establishing the Configuration Task](#)

[7.4.2 Configuring an IGMPv1 Querier](#)

[7.4.3 Configure an IGMPv2/v3 Querier](#)

[7.4.4 Checking the Configuration](#)

### 7.4.1 Establishing the Configuration Task

#### Applicable Environment



#### CAUTION

A great many of IGMP interfaces exist on the network and the IGMP interfaces are mutually restricted. Therefore, ensure that all the IGMP parameter values of all the IGMP S-switch interfaces on the same network segment are identical. Otherwise, the network may be faulty.

The querier periodically sends IGMP query messages on a shared network connected to receivers. When receiving a Report message from a member, the querier refreshes information about the members. The timeout period of the IGMP querier refers to the duration that another S-switch waits to become the querier after the current querier fails to send query messages.

If non-queriers do not receive any general query message within the Keepalive period of other IGMP queriers, the querier is considered faulty, and a new round of querier election is triggered automatically.

In ADSL dial-up access, the querier corresponds to only one host because a single host corresponds to one port. When a receiver frequently joins or leaves multiple multicast groups, like switchover among TV channels, you can enable the mechanism of fast leave on the querier.

## Pre-configuration Tasks

Before configuring IGMP query control, complete the following tasks:

- Configuring a unicast routing protocol to interconnect the entire multicast domain
- [7.2 Configuring Basic IGMP Functions](#)

## Data Preparation

To configure IGMP query control, you need the following data.

No.	Data
1	Interval for sending IGMP general query messages
2	Robustness variable
3	Maximum response time of IGMP query messages
4	Keepalive time of other IGMP queriers
5	Interval for sending IGMP last member query messages
6	ACL list used to control the application range of fast leave

## 7.4.2 Configuring an IGMPv1 Querier

### Context



#### CAUTION

This configuration is applicable only to IGMPv1.

This configuration is optional. Do as follows on the S-switch connected to hosts.



#### NOTE

The configuration involves the following cases:

- Global configuration: It is valid on all interfaces.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

### Procedure

- Global Configuration

1. Run:  
`system-view`  
The system view is displayed.
  2. Run:  
`igmp`  
The IGMP view is displayed.
  3. Run:  
`timer query interval`  
The interval for sending general query messages is set.  
By default, the interval for sending general query messages is 60 seconds.
  4. Run:  
`robust-count robust-value`  
The robustness variable is set.  
By default, the IGMP robustness variable is 2.
- Configuration on an Interface
    1. Run:  
`system-view`  
The system view is displayed.
    2. Run:  
`interface interface-type interface-number`  
The interface view is displayed.
    3. Run:  
`igmp timer query interval`  
The interval for sending general query messages is set.
    4. Run:  
`igmp robust-count robust-value`  
The robustness variable is set.
- End

### 7.4.3 Configure an IGMPv2/v3 Querier

#### Context



#### CAUTION

This configuration is applicable to IGMPv2 and IGMPv3. In actual configuration, ensure that the interval for sending general query messages is greater than the maximum response time but is smaller than the Keepalive time of other IGMP queriers.

---

This configuration is optional. Do as follows on the S-switch connected to hosts.

 **NOTE**

The configuration involves the following cases:

- Global configuration: It is valid on all interfaces.
- Configuration on an interface: The configuration on an interface takes precedence over the global configuration. If the configuration on an interface is not done, the global configuration is used.

## Procedure

- Global Configuration

1. Run:

**system-view**

The system view is displayed.

2. Run:

**igmp**

The IGMP view is displayed.

3. Run:

**timer query interval**

The interval for sending general query messages is set.

By default, the interval for sending general query messages is 60 seconds.

4. Run:

**robust-count robust-value**

The robustness variable is set.

By default, the robustness variable is 2.

When a S-switch starts, the S-switch sends general query messages for the number of *robust-value* times. The sending interval is 1/4 of the interval for sending IGMP general query messages. When a S-switch receives a Leave message, the S-switch sends group-specific query messages for the number of *robust-value* times. The sending interval is the interval for sending IGMP group-specific query messages. The greater the robustness variable is, the more robust the IGMP S-switch is. However, the timeout period of the group is longer.

5. Run:

**max-response-time interval**

The maximum response time is set for the Query messages on the IGMP router.

By default, the maximum IGMP response time is 10 seconds.

6. Run:

**timer other-querier-present interval**

The Keepalive time of other IGMP queriers is set.

By default, the Keepalive time of other IGMP queriers is obtained through the formula, that is, the Keepalive time of other IGMP queriers = robustness variable x the interval for sending general query messages + 1/2 x the maximum response time. When the default values of the robustness variable, the interval for sending general query messages, and the maximum response time are used, the Keepalive time of other IGMP queriers is 125 seconds.

## 7. Run:

```
lastmember-queryinterval interval
```

The interval for sending IGMP last member query messages is set.

The shorter the interval is, the more flexible the querier is.

By default, the interval for sending IGMP group-specific query messages is 1 second.

## ● Configuration on an Interface

## 1. Run:

```
system-view
```

The system view is displayed.

## 2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

## 3. Run:

```
igmp timer query interval
```

The interval for sending general query messages is set.

## 4. Run:

```
igmp max-response-time interval
```

The maximum response time to IGMP query messages is set.

## 5. Run:

```
igmp timer other-querier-present interval
```

The Keepalive time of other IGMP queriers is set.

## 6. Run:

```
igmp robust-count robust-value
```

The IGMP robustness variable is set.

## 7. Run:

```
igmp lastmember-queryinterval interval
```

The interval for sending IGMP group-specific messages is set.

## 8. Run:

```
igmp on-demand
```

The group membership on the interface is configured not to time out.

The interface does not send any IGMP query message outside.

By default, the interface takes part in the querier election and sends query messages.

 **NOTE**

This command is valid to IGMPv2 only.

## 9. Run:

```
igmp prompt-leave [ group-policy acl-number ]
```

IGMP fast leave is configured.

After receiving a Leave message from a host, the interface does not send the last-member query message, and deletes group membership on the interface immediately.

By default, the interface needs to perform the last-member query.

This command is applicable only to IGMPv2.

----End

## 7.4.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the configuration and running of IGMP on an interface.	<b>display igmp interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the IGMP routing table.	<b>display igmp routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ] ] * [ <b>static</b> ]

## 7.5 Configuring SSM Mapping

This section describes how to configure SSM mapping.

[7.5.1 Establishing the Configuration Task](#)

[7.5.2 Enabling Static SSM Mapping](#)

[7.5.3 Configuring a Static SSM Mapping Policy](#)

[7.5.4 Checking the Configuration](#)

### 7.5.1 Establishing the Configuration Task

#### Applicable Environment

In the network segment where multicast services are provided in the SSM mode, certain hosts must run IGMPv1/v2 due to various limitations. To provide SSM services for the hosts, you need to configure static SSM mapping on the S-switch.

#### Pre-configuration Tasks

To configure SSM mapping, complete the following task:

- Configuring a unicast routing protocol
- [7.2.2 Enabling IP Multicast Routing](#)

#### Data Preparation

To configure SSM mapping, you need the following data.

No.	Data
1	Interfaces that need to be configured with SSM mapping
2	Multicast group address and mask, and multicast source address and mask

## 7.5.2 Enabling Static SSM Mapping

### Context

Do as follows on the S-switch connected to hosts:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
igmp enable
```

IGMP is enabled.

**Step 4** Run:

```
igmp version 3
```

IGMPv3 is configured.

To ensure that hosts that run any IGMP version on the network segment can obtain SSM services, you are recommended to configure IGMPv3 on the interface.

**Step 5** Run:

```
igmp ssm-mapping enable
```

SSM Mapping is enabled.

----End

## 7.5.3 Configuring a Static SSM Mapping Policy

### Context

Do as follows on the S-switch connected to hosts:

## Procedure

### Step 1 Run:

```
system-view
```

The interface view is displayed.

### Step 2 Run:

```
igmp
```

The IGMP view is displayed.

### Step 3 Run:

```
ssm-mapping group-address { mask | mask-length } source-address
```

The mapping from a multicast group to the source is configured.

You can run the command for many times to configure the mapping from a group to multiple multicast sources.

- *group-address { mask | mask-length }*: specifies the group address and the mask.
- *source-address*: specifies the address of the source that sets up the mapping with the group.

----End

## 7.5.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the configuration on a specific interface.	<b>display interface</b> <i>interface-type interface-number</i>
Check information about groups involved in SSM mapping.	<b>display igmp group</b> [ <i>group-address</i>   <b>interface</b> <i>interface-type interface-number</i> ] * <b>ssm-mapping</b> [ <b>verbose</b> ]
Check SSM mapping rules of a specified group address.	<b>display igmp ssm-mapping</b> { <b>group</b> [ <i>group-address</i> ]   <b>interface</b> [ <i>interface-type interface-number</i> ] }

## 7.6 Maintaining IGMP

This section describes how to clear IGMP statistics and debug IGMP.

### 7.6.1 Clearing IGMP Group Information

#### 7.6.2 Monitoring the Running Status of IGMP

#### 7.6.3 Debugging IGMP

## 7.6.1 Clearing IGMP Group Information

**CAUTION**

The IGMP groups that an interface dynamically joins are deleted after you run the **reset igmp group** command. Therefore, receivers cannot receive multicast information normally. So, confirm the action before you run the command.

To clear information about the running of IGMP, run the following **reset** commands in the user view.

Action	Command
Delete the IGMP groups that an interface dynamically joins.	<b>reset igmp group</b> { <b>all</b>   <b>interface</b> <i>interface-type interface-number</i> { <b>all</b>   <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ] [ <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ] ] } }
Delete the IGMP groups that an interface statically joins.	<b>undo igmp static-group</b> { <b>all</b>   <i>group-address</i> [ <b>source</b> <i>source-address</i> ] }

## 7.6.2 Monitoring the Running Status of IGMP

During routine maintenance, run the following commands in the user view to view the running status of IGMP.

Action	Command
Check information about IGMP groups.	<b>display igmp group</b> [ <i>group-address</i>   <b>interface</b> <i>interface-type interface-number</i> ] [ <b>static</b>   <b>verbose</b> ]
Check information about multicast groups involved in SSM mapping.	<b>display igmp group ssm-mapping</b> [ <i>group-address</i>   <b>interface</b> <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the configuration and running of IGMP on an interface.	<b>display igmp interface</b> [ <i>interface-type interface-number</i> ] [ <b>verbose</b> ]
Check the IGMP routing table.	<b>display igmp routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ] ] * [ <b>static</b> ]
Check SSM mapping of a source/group-specific address.	<b>display igmp ssm-mapping</b> { <b>group</b> [ <i>group-address</i> ]   <b>interface</b> [ <i>interface-type interface-number</i> ] }

## 7.6.3 Debugging IGMP



## CAUTION

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

When an IGMP fault occurs, run the following **debugging** commands in the user view to debug and locate the fault.

Action	Command
Debug IGMP.	<b>debugging igmp</b> { <b>all</b>   <b>event</b>   <b>leave</b> [ <i>basic-acl-number</i> ]   <b>report</b> [ <i>advanced-acl-number</i> ]   <b>query</b> [ <i>basic-acl-number</i> ]   <b>timer</b> }
Debug SSM mapping.	<b>debugging igmp ssm-mapping</b> [ <i>advanced-acl-number</i> ]

## 7.7 Configuration Examples

This section provides several configuration examples of IGMP.

### [7.7.1 Example for Configuring Basic IGMP Functions](#)

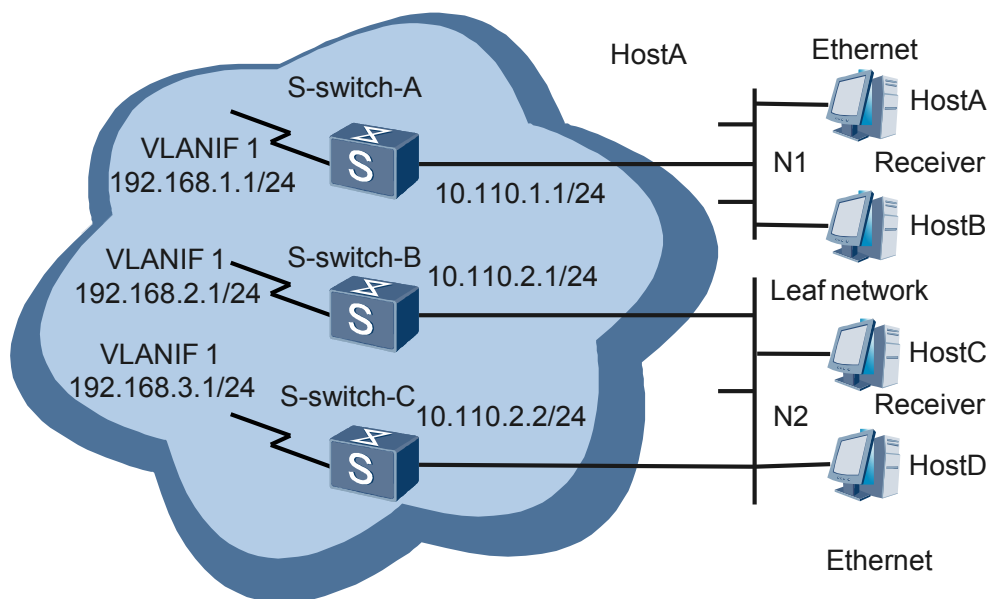
### [7.7.2 Example for Configuring SSM Mapping](#)

## 7.7.1 Example for Configuring Basic IGMP Functions

### Networking Requirements

In the IPv4 network shown in [Figure 7-1](#), unicast routes are normal. It is required to implement multicast in the network to enable hosts to receive the Video On Demand (VOD) information.

When the host connected to a certain interface of a S-switch needs to receive a very popular program for a long time, you can add the interface to a multicast group statically. As shown in the following network, if Host A and Host B need to receive the multicast data of multicast group 225.1.1.1 for a long time, add VLANIF 1 of the S-switches to multicast group 225.1.1.1 statically.

**Figure 7-1** Networking diagram of configuring basic IGMP functions

## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable multicast on all S-switches.
2. Enable PIM-SM on all interfaces.
3. Enable IGMP on the interface connected to hosts.
4. Add vlanif 1 on S-switch-A to multicast group 225.1.1.1 statically. In this manner, hosts can steadily receive the multicast data of multicast group 225.1.1.1 for a long time.

## Data Preparation

To complete the configuration, you need the following data:

- Version number of IGMP run on S-switch and hosts
- Static multicast group address that is 225.1.1.1

## Configuration Procedure

### NOTE

Only the commands related to IGMP configuration are mentioned here.

1. Enable multicast on each S-switch, and configure IGMP and PIM-SM on the interface connected to hosts.

# Enable multicast on S-switch-A; enable IGMP and PIM-SM on Gigabit vlanif 1; configure the IGMP version to 2.

The configurations of S-switch-B and S-switch-C are the same as the configuration of S-switch-A, and are not mentioned here.

```
[S-switch-A] multicast routing-enable
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] pim sm
[S-switch-A-Vlanif1] igmp enable
```

- [S-switch-A-Vlanif1] **quit**
2. Add vlanif 1 on S-switch-A to multicast group 225.1.1.1 statically. In this manner, the hosts connected to vlanif 1 can steadily receive the multicast data sent to multicast group 225.1.1.1.

```
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] igmp static-group 225.1.1.1
```

3. Verify the configuration.

# Run the **display igmp interface** command to view the configuration and running status of IGMP on the interfaces of each S-switch. Take the display on vlanif 1 of S-switch-B as an example.

```
<S-switch-B> display igmp interface vlanif 1
Interface information
vlanif1(10.110.2.1):
  IGMP is enabled
  Current IGMP version is 2
  IGMP group policy: none
  Value of query interval for IGMP(in seconds): 60
  Value of other querier timeout for IGMP(in seconds): 0
  Value of maximum query response time for IGMP(in seconds): 10
  Querier for IGMP: 10.110.2.1 (this router)
  Total 1 IGMP Group reported
```

# Run the **display pim routing-table** command on S-switch-A to check whether vlanif 1 is added to multicast group 225.1.1.1 statically. If (\*, 225.1.1.1) entry is generated on S-switch-A, the downstream interface is vlanif 1, and the protocol type is set to static, it indicates that vlanif 1 is successfully added to multicast group 225.1.1.1.

```
<S-switch-A> display igmp routing-table
Total 1 (*, G) entry; 0 (S, G) entry
(*, 225.1.1.1)
  RP: 192.168.4.1
  Protocol: pim-sm, Flag: WC
  UpTime: 00:12:17
  Upstream interface: vlanif 2
    Upstream neighbor: 192.168.1.1
    RPF prime neighbor: 192.168.1.1
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif1
      Protocol: static, UpTime: 00:12:17, Expires: -
```

## Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
 multicast routing-enable
#
interface vlanif1
undo shutdown
ip address 10.110.1.1 255.255.255.0
pim sm
igmp enable
igmp static-group 225.1.1.1
#
interface vlanif 2
undo shutdown
link-protocol ppp
ip address 192.168.1.1 255.255.255.0
pim sm
#
ospf 1
 area 0.0.0.0
```

```

        network 10.110.1.0 0.0.0.255
        network 192.168.1.0 0.0.0.255
#
return

```

- Configuration file of S-switch-B

```

#
sysname S-switch-B
#
multicast routing-enable
#
interface vlanif1
undo shutdown
ip address 10.110.2.1 255.255.255.0
pim sm
igmp enable
#
interface vlanif 2
undo shutdown
link-protocol ppp
ip address 192.168.2.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 10.110.2.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
return

```

- Configuration file of S-switch-C

```

#
sysname S-switch-C
#
multicast routing-enable
#
interface vlanif1
undo shutdown
ip address 10.110.2.2 255.255.255.0
pim sm
igmp enable
#
interface vlanif 2
link-protocol ppp
ip address 192.168.3.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 10.110.2.0 0.0.0.255
network 192.168.3.0 0.0.0.255
#
return

```

## 7.7.2 Example for Configuring SSM Mapping

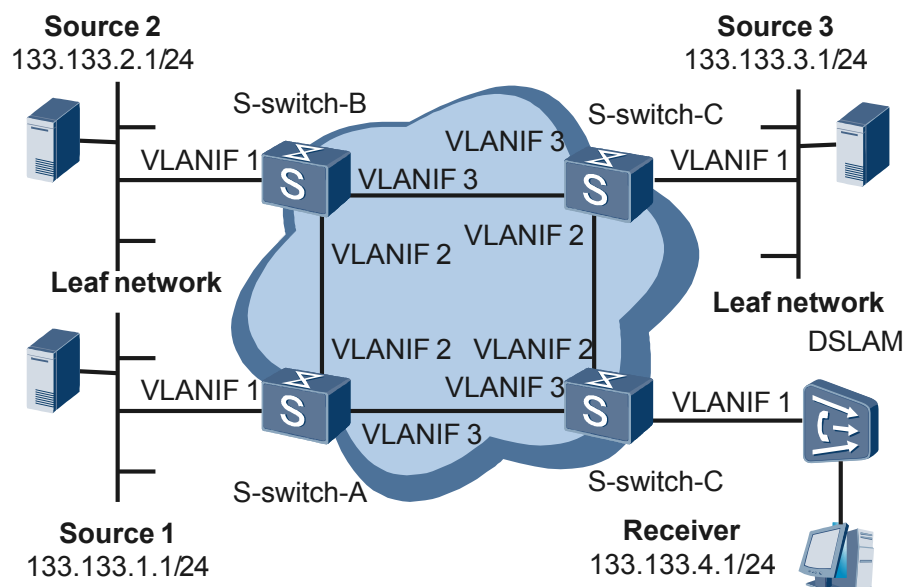
### Networking Requirements

In the multicast network shown in [Figure 7-2](#), PIM-SM is run in the network, and the ASM and SSM models are used to provide multicast services. The interface connected to the receiver runs IGMPv3. The IGMP version on the receiver is IGMPv2 and cannot be upgraded to IGMPv3.

The SSM group address range in the network is 232.1.1.0/24. S1, S2, and S3 send multicast data to the multicast groups in this range. It is required that the receiver receive the multicast data only from S1 and S3.

Solution: Configure SSM mapping on S-switch-D.

**Figure 7-2** SSM mapping network



S-switch	Interface	IP address	S-switch	Interface	IP address
S-switch-A	vlanif 1	133.133.1.2/24	S-switch-C	vlanif 1	133.133.3.2/24
	vlanif 2	192.168.1.1/24		vlanif 2	192.168.3.1/24
	vlanif 3	192.168.4.2/24		vlanif 3	192.168.2.2/24
S-switch-B	vlanif 1	133.133.2.2/24	S-switch-D	vlanif 1	133.133.4.2/24
	vlanif 2	192.168.1.2/24		vlanif 2	192.168.3.2/24
	vlanif 3	192.168.2.1/24		vlanif 3	192.168.4.1/24

## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable SSM Mapping on the multicast S-switch interface connected to hosts.
2. Configure the SSM group address range on all the multicast S-switches in the PIM-SM domain.
3. Configure the static SSM mapping rules on the S-switches that are enabled with SSM Mapping.

## Data Preparation

To complete this configuration, you need the following data:

- SSM group address range
- IP addresses of S1 and S3

## Configuration Procedure

### NOTE

Only the commands related to SSM mapping configuration are mentioned here.

1. Configure an IP address for each interface and a unicast routing protocol on each S-switch. The configuration details are not mentioned here.
2. Enable IGMP and SSM mapping on the interface connected to hosts.

```
[S-switch-D] multicast routing-enable
[S-switch-D] interface vlanif 1
[S-switch-D-Vlanif1] igmp enable
[S-switch-D-Vlanif1] igmp version 3
[S-switch-D-Vlanif1] igmp ssm-mapping enable
[S-switch-D-Vlanif1] quit
```

3. Configure the SSM group address range.

# Configure the SSM group address range to 232.1.1.0/24 on all S-switches. The configurations on S-switch-B, S-switch-C, and S-switch-D are similar to those on S-switch-A, and the detailed configurations are not mentioned here.

```
[S-switch-A] acl number 2000
[S-switch-A-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[S-switch-A-acl-basic-2000] quit
[S-switch-A] pim
[S-switch-A-pim] ssm-policy 2000
```

4. Configure the static SSM mapping rules on the S-switch connected to hosts.

# Map the multicast groups within the 232.1.1.0/24 range to S1 and S3.

```
[S-switch-D] igmp
[S-switch-D-igmp] ssm-mapping 232.1.1.0 24 133.133.1.1
[S-switch-D-igmp] ssm-mapping 232.1.1.0 24 133.133.3.1
```

# View SSM mapping of the source/group-specific address on the S-switch.

```
<S-switch-D> display igmp ssm-mapping group
IGMP SSM-Mapping conversion table
Total 2 entries   Total 2 entries matched
00001. (133.133.1.1, 232.1.1.0)
00002. (133.133.3.1, 232.1.1.0)
```

5. Verify the configuration.

# Configure the receiver to join group 232.1.1.1.

# Run the **display igmp group ssm-mapping** command to check information about a specified source/group address. The information about the specified source or group address on S-switch-D is displayed as follows:

```
<S-switch-D> display igmp group ssm-mapping
IGMP SSM mapping interface group report information
vlanif1 (133.133.4.2):
  Total 1 IGMP SSM-Mapping Group reported
    Group Address   Last Reporter   Uptime         Expires
    232.1.1.1       133.133.4.1     00:01:44       00:00:26
<S-switch-D> display igmp group ssm-mapping verbose
Interface group report information
vlanif1 (133.133.4.2):
  Total entry on this interface: 1
  Total 1 IGMP SSM-Mapping Group reported
    Group: 232.1.1.1
      Uptime: 00:01:52
      Expires: 00:00:18
      Last reporter: 133.133.4.1
      Last-member-query-counter: 0
      Last-member-query-timer-expiry: off
      Group mode: exclude
      Version1-host-present-timer-expiry: off
      Version2-host-present-timer-expiry: 00:00:17
```

# Run the **display pim routing-table** command to view the PIM-SM routing table on a S-switch. The PIM-SM routing table on S-switch-D is as follows:

```
<S-switch-D> display pim routing-table
Total 0 (*, G) entry; 2 (S, G) entries
(133.133.1.1, 232.1.1.1)
  RP: 192.168.3.2
  Protocol: pim-sm, Flag:
  UpTime: 00:11:25
  Upstream interface: vlanif3
    Upstream neighbor: 192.168.4.2
    RPF prime neighbor: 192.168.4.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif1
      Protocol: igmp, UpTime: 00:11:25, Expires:-
(133.133.3.1, 232.1.1.1)
  RP: 192.168.3.2
  Protocol: pim-sm, Flag:
  UpTime: 00:11:25
  Upstream interface: vlanif2
    Upstream neighbor: 192.168.3.1
    RPF prime neighbor: 192.168.3.1
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif1
      Protocol: igmp, UpTime: 00:11:25, Expires:-
```

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
multicast routing-enable
#
acl number 2000
  rule 5 permit source 232.1.1.0 0.0.0.255
#
interface vlanif1
undo shutdown
ip address 133.133.1.2 255.255.255.0
pim sm
#
interface vlanif2
undo shutdown
ip address 192.168.1.1 255.255.255.0
pim sm
#
interface vlanif3
undo shutdown
ip address 192.168.4.2 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
  network 133.133.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
  ssm-policy 2000
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
```

```
#
multicast routing-enable
#
acl number 2000
rule 5 permit source 232.1.1.0 0.0.0.255
#
interface vlanif1
undo shutdown
ip address 133.133.2.2 255.255.255.0
pim sm
#
interface vlanif2
undo shutdown
ip address 192.168.1.2 255.255.255.0
pim sm
#
interface vlanif3
undo shutdown
ip address 192.168.2.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 133.133.2.0 0.0.0.255
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
pim
ssm-policy 2000
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
multicast routing-enable
#
acl number 2000
rule 5 permit source 232.1.1.0 0.0.0.255
#
interface vlanif1
undo shutdown
ip address 133.133.3.2 255.255.255.0
pim sm
#
interface vlanif2
undo shutdown
ip address 192.168.3.1 255.255.255.0
pim sm
#
interface vlanif3
undo shutdown
ip address 192.168.2.2 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 133.133.3.0 0.0.0.255
network 192.168.3.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
pim
ssm-policy 2000
#
return
```

- Configuration file of S-switch-D

```
#
multicast routing-enable
```

```
#
interface vlanif1
undo shutdown
ip address 133.133.4.2 255.255.255.0
pim sm
  igmp enable
  igmp version 3
  igmp ssm-mapping enable
#
interface vlanif2
undo shutdown
ip address 192.168.3.2 255.255.255.0
pim sm
#
interface vlanif3
undo shutdown
ip address 192.168.4.1 255.255.255.0
pim sm
#
pim
  c-bsr vlanif 3
  c-rp vlanif 3
  ssm-policy 2000
#
acl number 2000
  rule 5 permit source 232.1.1.0 0.0.0.255
#
igmp
  ssm-mapping 232.1.1.0 255.255.255.0 133.133.1.1
  ssm-mapping 232.1.1.0 255.255.255.0 133.133.3.1
#
return
```



# 8 IPv4 Multicast Routing Management

---

## About This Chapter

This chapter describes the basic principles of IPv4 multicast forwarding, configuration methods of forwarding policies, and maintenance of commands, and provides configuration examples.

### [8.1 Introduction](#)

This section describes the principle and basic concepts of multicast routing, multicast forwarding, and RPF.

### [8.2 Configuring a Static Multicast Route](#)

This section describes how to configure static multicast routes.

### [8.3 Configuring a Multicast Routing Policy](#)

This section describes how to configure a multicast routing policy.

### [8.4 Configuring the Multicast Forwarding Scope](#)

This section describes how to configure the multicast forwarding range.

### [8.5 Configuring Control Parameters of the Multicast Forwarding Table](#)

This section describes how to configure control parameters of the multicast forwarding table.

### [8.6 Maintaining the Multicast Policy](#)

This section describes how to clear the statistics of multicast routing and forwarding, and debug multicast routing and forwarding.

### [8.7 Configuration Examples](#)

This section provides several configuration examples of IPv4 multicast routing management.

## 8.1 Introduction

This section describes the principle and basic concepts of multicast routing, multicast forwarding, and RPF.

### 8.1.1 Overview of IPv4 Multicast Routing Management

#### 8.1.2 IPv4 Multicast Routing Management Features Supported by the S-switch

### 8.1.1 Overview of IPv4 Multicast Routing Management

In the S-switch, multicast routing and forwarding consist of the following three aspects:

- Each multicast routing protocol has its routing table, such as PIM routing table.
- The multicast routing information of each multicast routing protocol forms a general multicast routing table.

The multicast routing table resides in the multicast route management module. It is composed of (S, G) entries. (S, G) indicates that S sends multicast data to G. If the multicast route management module supports multiple multicast protocols, the routing table contains multicast routes that are generated by the protocols. The routing entries are copied to the forwarding table.

- The multicast forwarding table controls the forwarding of multicast data packets.  
The multicast forwarding table guides the forwarding of multicast data packets. It remains consistent with the multicast routing table.

To ensure that multicast data is transmitted along the correct path, multicast routing protocols use the Reverse Path Forwarding (RPF) to create multicast routing entries.

The system performs RPF check based on the following types of routes:

- Unicast routes  
The unicast routing table collects the shortest paths to each destination.
- MBGP routes  
The MBGP routing table provides multicast routing information.
- Static multicast routes  
The static multicast routing table provides RPF routing information that is specified through static configuration.

### 8.1.2 IPv4 Multicast Routing Management Features Supported by the S-switch

#### Static Multicast Route

The static multicast route is an important factor of RPF check. By configuring the static multicast route, users can specify the RPF interface and RPF neighbor for a specific source of packets on the current S-switch.

The static multicast route cannot be used to forward data. It only affects RPF check, and is also called static RPF route.

The static multicast route is valid only on the configured multicast S-switches, and cannot be advertised or imported to other S-switches.

## Multicast Routing Policy

If multiple unicast routes with the same cost exist when a multicast S-switch selects an upstream interface, users can use one of following methods to configure the S-switch to select the RPF route:

- By default, the S-switch chooses the route with the largest next-hop address.
- According to the longest match, the S-switch selects the route longest matching the address of the source of the packet.
- Load balancing is configured among equal-cost routes. Performing load balancing of multicast traffic according to the source, group, or source/group can optimize network traffic when multiple multicast data flows exist.

## Controlling the Multicast Forwarding Range

In a network, the multicast information to which each multicast group corresponds is transmitted in a certain range. Users can define the multicast forwarding range by using the following methods:

- Configuring a multicast forwarding boundary on an interface to form a closed multicast forwarding area.
- Setting the forwarding TTL threshold on an interface to limit the distance to which a packet is forwarded.

## Controlling a Multicast Forwarding Table

When planning a specific network according to network services, the Internet Service Provider (ISP) can perform the following configurations:

- Limiting the number of entries in the multicast forwarding table  
Each S-switch maintains a forwarding entry for each received multicast packet. Too many multicast forwarding entries, however, use up the memory of a S-switch. Users can define the maximum number of entries in the multicast forwarding table of a S-switch. Limiting the number of entries according to the actual networking and service performance can avoid S-switch faults caused by excessive entries.
- Limiting the number of downstream nodes of each forwarding entry  
S-switch replicate a multicast packet for each downstream node, and then send it out. Each downstream node forms a branch of an MDT. The number of downstream nodes determines the maximum scale of the MDT and the multicast service range. Users can define the number of downstream nodes of a single forwarding entry. Limiting the number of downstream nodes according to the actual networking and service performance can reduce the processing pressure of a S-switch and control the multicast service range.

## Testing Multicast Routing

When a fault occurs on a multicast network, you can run the **ping multicast** and **mtrace** commands to test the connectivity of the network.

The **ping multicast** command is used to check whether a group is reachable and to implement the following functions:

- Pinging a reserved group address  
This is used to check whether a member of a group exists in the directly connected network segment, and is not exclusive for multicast networks. You can ping devices that use multicast addresses.
- Pinging a common group address  
This function is applied as follows:
  - To generate multicast traffic and trigger the creation of multicast routing entries: Based on multicast routing information, you can check whether a protocol runs normally, determine whether the network can carry multicast services, or test the forwarding performance.
  - To check the members of related groups in the network: Based on the ICMP-Echo-Reply messages received from destination hosts, the S-switch on which the command is used checks the members of the groups in the network, and calculates response time and the TTL from the S-switch to members. You can run the command repeatedly in a certain interval to calculate the network delay and route flapping.

The **mtrace** command can be used to trace the following paths and output the hop information:

- RPF path from a source to a querier
- Multicast path from a source to a querier
- RPF path from a source to a destination host
- Multicast path from a source to a destination host

## 8.2 Configuring a Static Multicast Route

This section describes how to configure static multicast routes.

### [8.2.1 Establishing the Configuration Task](#)

### [8.2.2 Configuring a Static Multicast Route](#)

### [8.2.3 Checking the Configuration](#)

## 8.2.1 Establishing the Configuration Task

### Applicable Environment

Static multicast route has the following functions:

- Changing RPF route  
If the topology of multicast is the same as that of unicast, the transmission path of multicast data is the same as that of unicast data. Users can change the RPF route by configuring a static multicast route. Thus a transmission path of the multicast data, which is different from the transmission path of unicast data, is established.
- Connecting RPF route  
In the network segment where unicast routes are blocked, when multicast static routes are not configured, packets cannot be forwarded because there is no RPF route. You can configure multicast static routes. Therefore, the system can generate RPF routes, complete RPF check, create routing entries, and guide the forwarding of packets.

## Pre-configuration Tasks

Before configuring a static multicast route, complete the following tasks:

- Configuring a unicast routing protocol
- Configuring basic multicast functions

## Data Preparation

To configure a static multicast route, you need the following data.

No.	Data
1	Multicast source address, mask or mask length
2	Unicast routing protocol
3	Filtering policy and its preference

## 8.2.2 Configuring a Static Multicast Route

### Context



#### CAUTION

When configuring a static multicast route, configure the outgoing interface through the command if the next hop is in the point-to-point format. If the next hop is not in the point-to-point format, you must use the next hop.

Do as follows on the multicast S-switch:

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
ip rpf-route-static source-address { mask | mask-length } [ protocol [ process-id ] ] [ route-policy policy-name ] { rpf-nbr | interface-type interface-number } [ preference preference ] [ order order-num ]
```

A static multicast route is configured.

The parameters of the command are explained as follows:

- *source-address { mask | mask-length }*: specifies a source address and mask.

- *protocol* [*process-id*]: specifies that the matching route must be present in the specified unicast routing protocol. *protocol* specifies a unicast routing protocol. *process-id* specifies the ID of a process.
- **route-policy** *policy-name*: specifies the matching rule of the static multicast route.
- *rpf-nbr*: specifies the next hop address that acts as the IP address of the RPF neighbor.
- *interface-type interface-number*: specifies the type and the number of the outgoing interface. The outgoing interface acts as the RPF interface.
- **preference** *preference*: specifies the preference of the route. The greater the preference value is, the lower the preference is.
- **order** *order-num*: specifies the configuration order of routes on the same network segment.

----End

## 8.2.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the static multicast routing table.	<b>display multicast routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ]   <b>incoming-interface</b> { <i>interface-type interface-number</i>   <b>register</b> }   <b>outgoing-interface</b> { { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type interface-number</i>   <b>register</b> } } ] *
Check RPF routing information of a specified multicast source.	<b>display multicast rpf-info</b> <i>source-address</i> [ <i>group-address</i> ]

## 8.3 Configuring a Multicast Routing Policy

This section describes how to configure a multicast routing policy.

### 8.3.1 Establishing the Configuration Task

### 8.3.2 Configuring Longest Match of Multicast Routes

### 8.3.3 Configuring Load Balancing of Multicast Routes

### 8.3.4 Checking the Configuration

## 8.3.1 Establishing the Configuration Task

### Applicable Environment

If multiple equal-cost unicast routes exist when a multicast S-switch select an upstream interface, you can configure the S-switch to the RPF S-switch by using one of the following methods:

- By default, the S-switch chooses the route with the largest next-hop address.

- According to the longest match rules, you can configure the S-switch to select the route with the destination address that longest matches the address of the source of the packet.
- You can configure load balancing among these routes. Load balancing based on multicast sources, groups, or source/groups for multicast traffic can optimize network traffic formed by multicast data flows.

## Pre-configuration Tasks

Before configuring the multicast routing policy, complete the following tasks:

- Configuring a unicast routing protocol
- Configuring basic multicast functions

## Data Preparation

To configure the multicast routing policy, you need the following data.

No.	Data
1	Multicast source address, group address, and mask or mask length
2	Matching policy, sequence, and precedence

## 8.3.2 Configuring Longest Match of Multicast Routes

### Context

By default, routes are selected in the order of routing entries.

Do as follows on the multicast S-switch:

### Procedure

Public network instance:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
multicast longest-match
```

Routes are selected according to the longest match.

----End

## 8.3.3 Configuring Load Balancing of Multicast Routes

### Context

By default, load balancing is not performed.

Do as follows on the multicast S-switch:

## Procedure

Public network instance:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
multicast load-splitting { source | group | source-group }
```

The parameters of the command are explained as follows:

- **group**: indicates that load balancing is performed based on a multicast group.
- **source**: indicates that load balancing is performed based on a multicast source.
- **source-group**: indicates that load balancing is performed based on a multicast group and multicast source.

----End

## 8.3.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the multicast routing table.	<b>display multicast routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ]   <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> }   <b>outgoing-interface</b> { { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type</i> <i>interface-number</i>   <b>register</b> } } ] *

## 8.4 Configuring the Multicast Forwarding Scope

This section describes how to configure the multicast forwarding range.

[8.4.1 Establish the Configuration Task](#)

[8.4.2 Configuring the Multicast Forwarding Boundary](#)

[8.4.3 Configuring the TTL Threshold of Multicast Forwarding](#)

[8.4.4 Checking the Configuration](#)

### 8.4.1 Establish the Configuration Task

## Applicable Environment

The multicast information each multicast group corresponds to is transmitted in a certain range. Multicast information to which each multicast group corresponds is forwarded in a certain scope. Users can define the multicast forwarding scope by using the following methods:

- Configuring the multicast forwarding boundary to form a close multicast forwarding area. The interface configured with a forwarding boundary of a multicast group cannot send or receive packets of the multicast group.
- Configuring the TTL threshold of multicast forwarding on an interface to limit the forwarding distance of multicast packets. The interface forwards only the packet whose TTL value is not smaller than the threshold. If the TTL value of a packet is smaller than the threshold, the packet is discarded.

In the task of configuring multicast forwarding range, Configuring Multicast Forwarding Boundary and Configuring TTL Threshold of Multicast Forwarding are parallel. Users can select the configuration as required.

## Pre-configuration Tasks

Before configuring the multicast forwarding scope, complete the following tasks:

- Configuring a unicast routing protocol
- Configuring basic multicast functions

## Data Preparation

To configure the multicast forwarding scope, you need the following data.

No.	Data
1	Multicast source address, multicast group address, and mask or mask length
2	Matching policy, route order, and route preference of the multicast routes

## 8.4.2 Configuring the Multicast Forwarding Boundary

### Context

By default, no multicast forwarding boundary is configured on the interface.

Do as follows on the multicast S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
multicast boundary group-address { mask | mask-length }
```

The multicast forwarding boundary is configured.

----End

## 8.4.3 Configuring the TTL Threshold of Multicast Forwarding

### Context

By default, the forwarding TTL threshold is 1.

Do as follows on the multicast S-switch:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
multicast minimum-ttl ttl-value
```

The multicast forwarding TTL threshold is configured.

----End

## 8.4.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the multicast routing table.	<b>display multicast routing-table</b> [ group-address [ mask { group-mask   group-mask-length } ]   source-address [ mask { source-mask   source-mask-length } ]   <b>incoming-interface</b> { interface-type interface-number   <b>register</b> }   <b>outgoing-interface</b> { { <b>include</b>   <b>exclude</b>   <b>match</b> } { interface-type interface-number   <b>register</b> } } ] *
Check information about the multicast boundary of an interface.	<b>display multicast boundary</b> [ group-address [ mask   mask-length ] ] [ <b>interface</b> interface-type interface-number ]
Check the forwarding TTL threshold on an interface.	<b>display multicast minimum-ttl</b> [ interface-type interface-number ]

## 8.5 Configuring Control Parameters of the Multicast Forwarding Table

This section describes how to configure control parameters of the multicast forwarding table.

### [8.5.1 Establishing the Configuration Task](#)

### [8.5.2 Setting the Maximum Number of Entries in Multicast Forwarding Table](#)

### [8.5.3 Setting the Maximum Number of Downstream Nodes of a Multicast Forwarding Entry](#)

### [8.5.4 Checking the Configuration](#)

## 8.5.1 Establishing the Configuration Task

### Applicable Environment

To plan a network according to the services, the ISP needs to perform the following configuration policies:

- Limiting the number of entries in the multicast forwarding table  
Each S-switch maintains a routing entry for each received multicast packet. Too many entries, however, may exhaust the memory of the S-switch. In this case, you can define the maximum number of multicast routing entries. Limiting the number of the entries can avoid faults in the S-switch.
- Limiting the number of downstream nodes of a single entry  
S-switches copy a multicast packet for each downstream node, and the downstream node sends the copy out. Each downstream node forms a branch of the multicast distribution tree. The number of the downstream nodes determines the maximum scale of the multicast distribution tree and the multicast service scope. Users can define the number of the downstream nodes of a single forwarding entry. Limiting the number of downstream nodes according to the actual networking and the services can reduce the pressure of S-switches and control the multicast service scope.

### Pre-configuration Tasks

Before configuring control parameters of the multicast forwarding table, complete the following tasks:

- Configuring a unicast routing protocol
- Configuring basic multicast functions

### Data Preparation

To configure control parameters of the multicast forwarding table, you need the following data.

No.	Data
1	Multicast source address, group address, and mask or mask length

No.	Data
2	Matching policy, S-switch sequence, and route preference of the multicast routes
3	Maximum number of entries in the multicast forwarding table
4	Maximum number of downstream nodes of each entry in the multicast forwarding table

## 8.5.2 Setting the Maximum Number of Entries in Multicast Forwarding Table

### Context

By default, the maximum number supported by the system is used.

Do as follows on the multicast S-switch:

### Procedure

Public network instance:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
multicast forwarding-table route-limit limit
```

The maximum number of entries in the multicast forwarding table is configured.

By default, the maximum value is adopted.

----End

## 8.5.3 Setting the Maximum Number of Downstream Nodes of a Multicast Forwarding Entry

### Context



#### CAUTION

This configuration becomes valid only after the **reset multicast forwarding-table** command is used. Multicast services are interrupted after you run the **reset multicast forwarding-table** command. So, confirm the action before you use the command.

---

Do as follows on the multicast S-switch:

## Procedure

Public network instance:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
mcast forwarding-table downstream-limit limit
```

The maximum number of downstream nodes of a forwarding entry in the multicast forwarding table is configured.

The maximum number is valid when it is smaller than the default value.

By default, the maximum number supported by the system is used.

----End

## 8.5.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the multicast forwarding table.	<b>display mcast routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ]   <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> }   <b>outgoing-interface</b> { { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type</i> <i>interface-number</i>   <b>register</b> } } ] *

## 8.6 Maintaining the Multicast Policy

This section describes how to clear the statistics of multicast routing and forwarding, and debug multicast routing and forwarding.

### 8.6.1 Clearing Multicast Routing and Forwarding Entries

#### 8.6.2 Monitoring the Status of Multicast Routing and Forwarding

#### 8.6.3 Debugging Multicast Routing and Forwarding

### 8.6.1 Clearing Multicast Routing and Forwarding Entries



#### CAUTION

The **reset** command clears the entries in the multicast forwarding table or the multicast routing table.

To clear the entries in the multicast forwarding table and routing table, run the following **reset** commands in the user view.

Action	Command
Clear the forwarding entries in the multicast forwarding table.	<b>reset multicast forwarding-table</b> { <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ]   <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> }   <b>slot</b> <i>slot-number</i> } *
Clear the routing entries in the multicast routing table.	<b>reset multicast routing-table</b> { <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ]   <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> } } *

## 8.6.2 Monitoring the Status of Multicast Routing and Forwarding

During routine maintenance, run the following commands in any view to know the running status of multicast routing and forwarding.

Action	Command
Check the multicast boundary configured on an interface.	<b>display multicast boundary</b> [ <i>group-address</i> [ <i>mask</i>   <i>mask-length</i> ] ] [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]
Check the multicast forwarding table.	<b>reset multicast forwarding-table</b> { <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ]   <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> }   <b>slot</b> <i>slot-number</i> } *
Check the minimum TTL value when a multicast data packet is forwarded by an interface.	<b>display multicast minimum-ttl</b> [ <i>interface-type</i> <i>interface-number</i> ]
Check the multicast routing table.	<b>display multicast routing-table</b> [ <i>group-address</i> [ <b>mask</b> { <i>group-mask</i>   <i>group-mask-length</i> } ]   <i>source-address</i> [ <b>mask</b> { <i>source-mask</i>   <i>source-mask-length</i> } ]   <b>incoming-interface</b> { <i>interface-type</i> <i>interface-number</i>   <b>register</b> }   <b>outgoing-interface</b> { { <b>include</b>   <b>exclude</b>   <b>match</b> } { <i>interface-type</i> <i>interface-number</i>   <b>register</b> } } ] *
Check the static multicast routing table.	<b>display multicast routing-table static</b> [ <b>config</b> ] [ <i>source-address</i> { <i>mask-length</i>   <i>mask</i> } ]
Check the RPF routing information.	<b>display multicast rpf-info</b> <i>source-address</i> [ <i>group-address</i> ]

## 8.6.3 Debugging Multicast Routing and Forwarding



### CAUTION

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

When a fault occurs when multicast is enabled, run the following **debugging** commands in the user view to debug multicast routes and to locate the fault.

Action	Command
Debug multicast forwarding.	<b>debugging mfib all</b> <b>debugging mfib</b> { <b>no-cache</b>   <b>packet</b>   <b>register</b>   <b>route</b>   <b>sync</b>   <b>upcall</b>   <b>wrong-iif</b> } [ <i>advanced-acl-number</i> ] [ <i>slot slot-number</i> ]
Debug multicast routing management.	<b>debugging mrm</b> { <b>all</b>   <b>event</b>   <b>packet</b> [ <i>advanced-acl-number</i> ]   <b>route</b> [ <i>advanced-acl-number</i> ] }

## 8.7 Configuration Examples

This section provides several configuration examples of IPv4 multicast routing management.

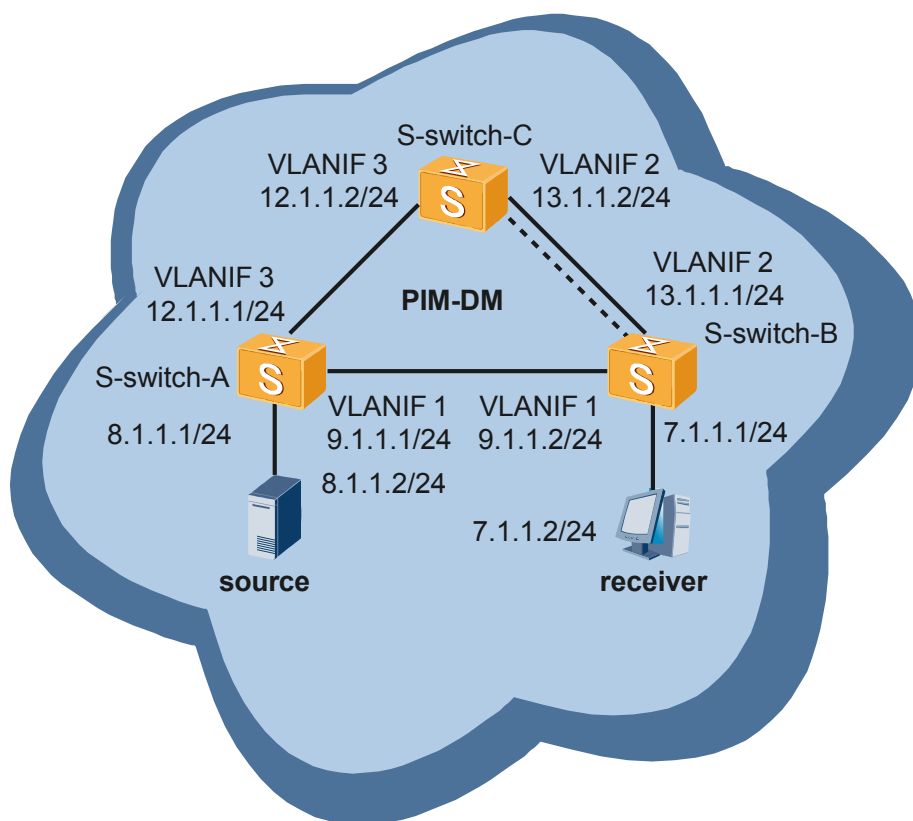
### [8.7.1 Example for Changing Static Multicast Routes to RPF Routes](#)

### [8.7.2 Example for Connecting the RPF Route Through a Static Multicast Route](#)

## 8.7.1 Example for Changing Static Multicast Routes to RPF Routes

### Networking Requirements

As shown in [Figure 8-1](#), the network runs PIM-DM, all S-switches support multicast, and the receiver can receive information from the multicast source. S-switch-A, S-switch-B, and S-switch-C run OSPF. It is required to configure a static multicast route to distinguish the multicast path from the source to the receiver from the unicast path from the source to the receiver.

**Figure 8-1** Networking diagram for changing static multicast routes to RPF routes

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address and enable OSPF on each interface.
2. Enable multicast on each S-switch, PIM-DM on each interface, and IGMP on the interface connected to hosts.
3. Configure static multicast RPF routes on S-switch-, and specify S-switchC as the RPF neighbor to the source.

## Data Preparation

To complete the configuration, you need the following data:

- IP address of the source
- vlanif 2 through which S-switch-B connects to S-switch-C

## Configuration Procedure

### NOTE

In the configuration example, only the commands related to static multicast route configuration are listed.

1. Configure an IP address and a unicast routing protocol on each S-switch.  
# As shown in [Figure 8-1](#), configure IP addresses and masks on the interfaces of each S-switch. OSPF is run on S-switch-A, S-switch-B, and S-switch-C, and the three S-switches

are able to update routes among them through the unicast routing protocol. The configuration procedure is not mentioned here.

## 2. Enable multicast on each S-switch and PIM-DM on each interface

# Enable multicast on each S-switch, PIM-DM on each interface, and IGMP on the interface connected to hosts. The configurations on other S-switches are similar to that of S-switch-B, and are not mentioned here.

```
[S-switch-B] multicast routing-enable
[S-switch-B] interface vlanif 1
[S-switch-B-Vlanif1] pim dm
[S-switch-B-Vlanif1] quit
[S-switch-B] interface vlanif 2
[S-switch-B-Vlanif2] pim dm
[S-switch-B-Vlanif2] quit
[S-switch-B] interface vlanif 3
[S-switch-B-Vlanif3] pim dm
[S-switch-B-Vlanif3] igmp enable
[S-switch-B-Vlanif3] quit
```

# Run the **display multicast rpf-info** command on S-switch-B to view the RPF information of the source. You can find that the RPF route is a unicast route, and the RPF neighbor is S-switch-A. The display is as follows:

```
<S-switch-B> display multicast rpf-info 8.1.1.2
RPF information about source 8.1.1.2:
  RPF interface: vlanif 1, RPF neighbor: 9.1.1.1
  Referenced route/mask: 8.1.1.0/24
  Referenced route type: unicast
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

## 3. Configure a static multicast route

# Configure a static multicast RPF route on S-switch-B and configure S-switch-C as the RPF neighbor to the source.

```
<S-switch-B> system-view
[S-switch-B] ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
```

## 4. Verify the configuration

# Run the **display multicast rpf-info** command on S-switch-B to view the RPF information of the source. The RPF route and the RPF neighbor are updated according to the static multicast route. The display of RPF is as follows:

```
<S-switch-B> display multicast rpf-info 8.1.1.2
RPF information about source 8.1.1.2:
  RPF interface: vlanif 2, RPF neighbor: 13.1.1.2
  Referenced route/mask: 8.1.1.0/24
  Referenced route type: mstatic
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

# Configuration Files

## Configuration file of S-switch-B

```
#
 sysname S-switch-B
#
 multicast routing-enable
#
interface vlanif/1
 undo shutdown
 link-protocol ppp
 ip address 9.1.1.2 255.255.255.0
 pim dm
#
```

```

interface vlanif/2
undo shutdown
link-protocol ppp
ip address 13.1.1.1 255.255.255.0
pim dm
#
interface vlanif3
undo shutdown
ip address 7.1.1.1 255.255.255.0
pim dm
igmp enable
#
ospf 1
area 0.0.0.0
network 7.1.1.0 0.0.0.255
network 9.1.1.0 0.0.0.255
network 13.1.1.0 0.0.0.255
#
ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
#
return

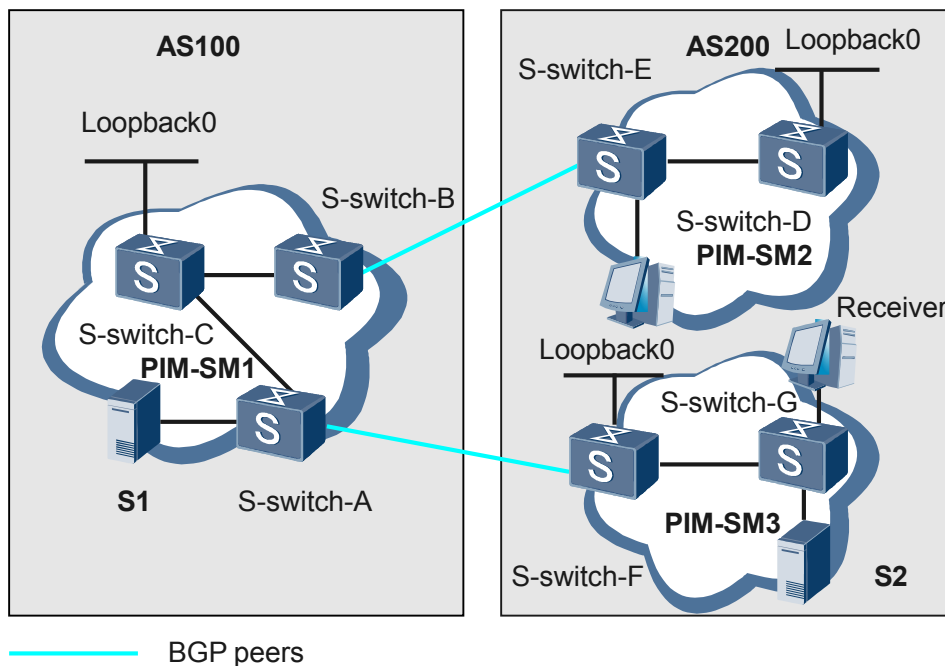
```

## 8.7.2 Example for Connecting the RPF Route Through a Static Multicast Route

### Networking Requirements

As shown in [Figure 8-2](#), the network runs PIM-DM, all S-switches support multicast, and receiver can receive information from the multicast source Source1. S-switch-B and S-switch-C run OSPF. There is no unicast route between S-switch-A and S-switch-B. It is required to use a multicast static route to enable the receiver to receive information sent by Source2.

**Figure 8-2** Networking diagram for connecting the RPF route through static multicast routes



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address and OSPF on each interface.
2. Enable multicast on each S-switch, PIM-DM on each interface, and IGMP on the interface connected to hosts.
3. Configure a static multicast RPF route between S-switch-B and S-switch-C.

## Data Preparation

To complete the configuration, you need the following data:

- IP address of Source 2.
- RPF interface through which S-switch-B connects to Source2 is vlanif 3, and the RPF neighbor is S-switch-A.
- RPF interface through which S-switch-C connects to Source2 is vlanif 1, and the RPF neighbor is S-switch-B.

## Configuration Procedure

### NOTE

In the configuration example, only the commands related to static multicast route configuration are listed.

1. Configure an IP address and a unicast routing protocol on each S-switch.  
# As shown in [Figure 8-2](#), configure IP addresses and masks of the interfaces on each S-switch. S-switch-B and S-switch-C belong to the same OSPF area, and the two S-switches are able to update routes among them through the unicast routing protocol. The configuration procedure is not mentioned here.
2. Enable multicast on each S-switch and PIM-DM on each interface  
# Enable multicast on each S-switch, enable PIM-DM on each interface, and enable IGMP on the interface connected to hosts.

```
[S-switch-A] multicast routing-enable
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] pim dm
[S-switch-A-Vlanif1] quit
[S-switch-A] interface vlanif 3
[S-switch-A-Vlanif3] pim dm
[S-switch-B] multicast routing-enable
[S-switch-B] interface vlanif 1
[S-switch-B-Vlanif1] pim dm
[S-switch-B-Vlanif1] quit
[S-switch-B] interface vlanif 2
[S-switch-B-Vlanif2] pim dm
[S-switch-B-Vlanif2] quit
[S-switch-B] interface vlanif 3
[S-switch-B-Vlanif3] pim dm
[S-switch-B-Vlanif3] quit
[S-switch-C] multicast routing-enable
[S-switch-C] interface vlanif 1
[S-switch-C-Vlanif1] pim dm
[S-switch-C-Vlanif1] quit
[S-switch-C] interface vlanif 2
[S-switch-C-Vlanif2] pim dm
[S-switch-C-Vlanif2] igmp enable
[S-switch-C-Vlanif2] quit
```

# Source 1 (10.1.3.2/24) and Source 2 (10.1.5.2/24) send multicast data to the multicast group G (225.1.1.1). The receiver joins G. The receiver can then receive the multicast data sent by Source 1, but cannot receive the multicast data sent by Source 2.

# Run the **display multicast rpf-info 10.1.5.2** command on S-switch-B and S-switch-C. If there is no display, it indicates that S-switch-B and S-switch-C have no RPF route to Source 2.

### 3. Configure a static multicast route

# Configure a static multicast RPF route on S-switch-B and configure S-switch-A as the RPF neighbor to Source 2.

```
[S-switch-B] ip rpf-route-static 10.1.5.0 255.255.255.0 10.1.4.2
```

# Configure a static multicast RPF route on S-switch-C, and configure S-switch-B as the RPF neighbor to Source 2.

```
[S-switch-C] ip rpf-route-static 10.1.5.0 255.255.255.0 10.1.2.2
```

### 4. Verify the configuration

# Run the **display multicast rpf-info 10.1.5.2** command on S-switch-B and S-switch-C to view the RPF information of Source 2. The display of RPF is as follows:

```
<S-switch-B> display multicast rpf-info 10.1.5.2
RPF information about: 10.1.5.2
  RPF interface: vlanif3, RPF neighbor: 10.1.4.2
  Referenced route/mask: 10.1.5.0/24
  Referenced route type: mstatic
  Route selecting rule: preference-preferred
  Load splitting rule: disable
<S-switch-C> display multicast rpf-info 10.1.5.2
RPF information about source 10.1.5.2:
  RPF interface: vlanif1, RPF neighbor: 10.1.2.2
  Referenced route/mask: 10.1.5.0/24
  Referenced route type: mstatic
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

# Run the **display pim routing-table** command to view the routing table. S-switch-C has the multicast entry of Source 2. The receiver can receive the multicast data from Source 2.

```
<S-switch-C> display pim routing-table
Total 1 (*, G) entry; 2 (S, G) entry
(*, 225.1.1.1)
  Protocol: pim-dm, Flag: WC
  UpTime: 03:54:19
  Upstream interface: NULL
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2
      Protocol: pim-dm, UpTime: 01:38:19, Expires: never
(10.1.3.2, 225.1.1.1)
  Protocol: pim-dm, Flag: ACT
  UpTime: 00:00:44
  Upstream interface: vlanif1
    Upstream neighbor: 10.1.2.2
    RPF prime neighbor: 10.1.2.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif2
      Protocol: pim-dm, UpTime: 00:00:44, Expires: never
(10.1.5.2, 225.1.1.1)
  Protocol: pim-dm, Flag: ACT
  UpTime: 00:00:44
  Upstream interface: vlanif1
    Upstream neighbor: 10.1.2.2
```

```
RPF prime neighbor: 10.1.2.2
Downstream interface(s) information:
Total number of downstreams: 1
  1: vlanif2
    Protocol: pim-dm, UpTime: 00:00:44, Expires: never
```

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
multicast routing-enable
#
interface vlanif1
undo shutdown
ip address 10.1.5.1 255.255.255.0
pim dm
#
interface vlanif3
undo shutdown
ip address 10.1.4.2 255.255.255.0
pim dm
#
ospf 1
area 0.0.0.0
 network 10.1.5.0 0.0.0.255
 network 10.1.4.0 0.0.0.255
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
multicast routing-enable
#
interface vlanif1
undo shutdown
ip address 10.1.2.2 255.255.255.0
pim dm
#
interface vlanif2
undo shutdown
ip address 10.1.3.1 255.255.255.0
pim dm
#
interface vlanif3
undo shutdown
ip address 10.1.4.1 255.255.255.0
pim dm
#
ospf 1
area 0.0.0.0
 network 10.1.2.0 0.0.0.255
 network 10.1.3.0 0.0.0.255
#
ip rpf-route-static 10.1.5.0 24 10.1.4.2
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
multicast routing-enable
#
interface vlanif1
```

```
undo shutdown
ip address 10.1.2.1 255.255.255.0
pim dm
#
interface vlanif2
undo shutdown
ip address 10.1.1.1 255.255.255.0
igmp enable
pim dm
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.1.2.0 0.0.0.255
#
ip rpf-route-static 10.1.5.0 24 10.1.2.2
#
return
```

# 9 MSDP Configuration

---

## About This Chapter

This chapter describes the MSDP fundamentals and configuration steps, and maintenance for MSDP functions, along with typical examples.

### [9.1 Introduction](#)

This section describes basic MSDP functions and MSDP features supported by the S-switch.

### [9.2 Configuring PIM-SM Inter-domain Multicast](#)

This section describes how to configure PIM-SM inter-domain MSDP peers in an AS.

### [9.3 Configuring an Anycast RP in a PIM-SM Domain](#)

This section describes how to configure an anycast RP.

### [9.4 Managing MSDP Peer Connections](#)

This section describes how to manage MSDP peers connections.

### [9.5 Configuring SA Cache](#)

This section describes how to configure SA Cache.

### [9.6 Configuring an SA Request](#)

This section describes how to configure an SA request.

### [9.7 Transmitting Burst Multicast Data Between Domains](#)

This section describes how to transmit burst multicast data between domains.

### [9.8 Configuring the Filtering Rules for SA Messages](#)

This section describes how to configure the filtering rules for SA messages.

### [9.9 Maintaining MSDP](#)

This section describes how to clear MSDP statistics, reset connections between MSDP peers, and debug MSDP.

### [9.10 Configuration Examples](#)

This section provides several configuration examples of MSDP.

## 9.1 Introduction

This section describes basic MSDP functions and MSDP features supported by the S-switch.

### 9.1.1 MSDP Overview

#### 9.1.2 MSDP Features Supported by the S-switch

### 9.1.1 MSDP Overview

In the general PIM-SM mode, a multicast source registers only with the local rendezvous point (RP). The information on the inter-domain multicast sources is isolated. The RP knows only the source in its domain, establishes a multicast distribution tree (MDT) in its domain, and distributes the data sent by the source to the local users.

A type of mechanism is required to enable the local RP to share the information on the multicast sources of other domains. By means of the mechanism, the local RP can send Join messages to the multicast sources of other domains and establish MDTs. Multicast packets can thus be transmitted across domains.

The Multicast Source Discovery Protocol (MSDP) is an inter-area multicast solution based on multiple interconnected PIM-SM domains, and can solve the preceding problem.

MSDP achieves this objective by setting up the MSDP peer relationship between RPs of different domains. MSDP peers share the information on multicast sources by sending Source Active (SA) messages. They transmit the (S, G) information from the RP that the source S registers with to other RPs connected to members of G.

MSDP peers are connected through the TCP connection. MSDP peers perform the RPF check on received SA messages.

#### NOTE

MSDP is applicable only to PIM-SM domains, and useful only for the Any-Source Multicast (ASM) mode.

### 9.1.2 MSDP Features Supported by the S-switch

#### PIM-SM Inter-Domain Multicast

When a multicast network is divided into multiple PIM-SM domains, MSDP is used to connect RPs in each domain to share the multicast source information. In this manner, hosts in a domain can receive multicast data sent by multicast sources in other domains.

You can configure intra-AS MSDP peers, inter-AS MSDP peers, and static RPF peers.

#### PIM-SM Intra-domain Anycast RP

After an anycast RP is applied to a PIM-SM domain, the multicast source registers with the nearest RP and receivers send Join messages to the nearest RP. This reduces the burden of a single RP, implements RP backup, and optimizes the forwarding path.

You can use a loopback interface as a C-RP or a static RP and specify the logical RP address for an SA message.

## Configuring Control Parameters for Maintaining MSDP Peer Connections

In the S-switch, you can set up and tear down an MSDP session, and configure the period for retrying to send TCP connection requests to the remote MSDP peers.

### Configuring SA Cache

By default, SA Cache is enabled on S-switches. Therefore, S-switches can locally store the (S, G) information carried in SA messages. When required to receive the multicast data, the S-switches can obtain the (S, G) information from the SA Cache.

You can set the maximum number of cached (S, G) entries, which can effectively prevent the Denial of Service (DoS) attack.

You can disable SA Cache on a S-switch. After the SA Cache on a S-switch is disabled, the S-switch does not locally store the (S, G) information carried in SA messages. When the S-switch needs to receive multicast data, it needs to wait for the SA message to be sent by its MSDP peer in the next period. This causes a delay for receivers to obtain multicast source information.

### Controlling SA Requests

Certain S-switches cannot be enabled with SA Cache or the capacity of SA Cache on these S-switches is too small. When these S-switches need to receive multicast data, they cannot immediately obtain the valid (S, G) information but need to wait for the SA message to be sent by their MSDP peers in the next period.

If SA Cache is enabled on the remote MSDP peer and the capacity of the SA Cache is large, you can configure "sending SA request messages" on the local S-switch to reduce the period during which receivers obtain multicast source information.

At the same time, you can also configure the filtering rules for receiving SA request messages on the remote MSDP peers.

### Transmitting Burst Multicast Data

When the interval for a certain multicast source to send multicast data is longer than the timeout period of an (S, G) entry, the source DR can only encapsulate burst multicast data in Register messages and send them to the source RP. The source RP uses SA messages to transmit (S, G) information to the remote RP. The remote RP then sends an (S, G) Join message towards the multicast source to create an SPT. Because of the timeout of the (S, G) entry, the remote user cannot receive the multicast data sent by S.

The S-switch supports the transmission of burst multicast data. You can enable the function of encapsulating a multicast data packet in an SA message on the source RP. The source RP can then encapsulate multicast data in an SA message and send the message out. After receiving the SA message, the remote RP decapsulates the message, and then forwards multicast data to hosts in the domain along the RPT.

Setting the TTL threshold can limit the transmission scope of a multicast data packet contained in an SA message. After receiving an SA message containing a multicast data packet, an MSDP peer checks the TTL value in the IP header of the multicast packet. If the TTL value is smaller than the threshold, the MSDP peer does not forward the SA message to the specific remote peers. If the TTL value is greater than the threshold, the MSDP peer reduces the TTL value in the IP header of the multicast packet by 1, and then encapsulates the multicast packet in an SA message and sends the message out.

## Rules for Creating, Receiving, and Forwarding SA Messages

By default, MSDP S-switches receive all SA messages that pass the RPF check and forward them to all MSDP peers.

To control the transmission of SA messages between MSDP peers, you can configure filtering rules by using the following methods:

- Setting rules for filtering SA messages based on multicast sources on the source RP  
The source RP filters active multicast sources that register with the local S-switch, and then determines whether to send (S, G) entries based on the rules.
- Setting rules for filtering SA messages received from remote MSDP peers  
When an SA message sent by a remote MSDP peer reaches the local S-switch, the S-switch determines whether to receive the message based on the rules.
- Setting rules for filtering SA messages forwarded to remote MSDP peers  
Before forwarding an SA message to a remote MSDP peer, the local S-switch determines whether to forward it based on the rules.

## Multi-Instance MSDP

MSDP peer relationships can be set up between interfaces on multicast S-switches that belong to the same instance (including the public instance).

Multicast S-switches on which multi-instance is applied maintain a set of MSDP mechanisms for each instance, including SA Cache, peer connection, timer, sending cache, and the cache area of PIM interaction. Multicast S-switches also guarantee the information separation among different instances; therefore, only MSDP and PIM-SM that belong to the same instance can interact.

## 9.2 Configuring PIM-SM Inter-domain Multicast

This section describes how to configure PIM-SM inter-domain MSDP peers in an AS.

### [9.2.1 Establishing the Configuration Task](#)

### [9.2.2 Configuring Intra-AS MSDP Peers](#)

### [9.2.3 Configuring Static RPF Peers](#)

### [9.2.4 Checking the Configuration](#)

## 9.2.1 Establishing the Configuration Task

### Applicable Environment

When a large multicast network is divided into multiple PIM-SM domains, MSDP is used to connect RPs of various domains to share the source information. In this manner, hosts in a domain can receive multicast data sent by multicast sources in other domains.

To ensure that all RPs in the network can share the source information, reduce the scale of an MSDP connected graph. It is recommended to configure MSDP peer relationships between all RPs, including static RPs and C-RPs, in the network.

To ensure that SA messages transmitted between MSDP peers are not interrupted by RPF rules and to reduce redundant traffic, the following solutions are recommended:

- Configuring all MSDP peers in an AS to join the same mesh group
- Using the same interface address to set up MBGP peer relationships between inter-AS MSDP peers or specifying inter-AS MSDP peers as RPF peers of each other



**NOTE**

Both BGP and MBGP can be used to set up inter-AS EBGP peer relationships. MBGP is recommended because MBGP does not affect the unicast topology of a network.

## Pre-configuration Tasks

Before configuring PIM-SM inter-domain multicast, complete the following tasks:

- Configuring a unicast routing protocol to enable interworking at the network layer
- Enabling IP multicast
- Configuring a PIM-SM domain to implement intra-domain multicast

## Data Preparation

To configure PIM-SM inter-domain multicast, you need the following data.

No.	Data
1	Address of a remote MSDP peer
2	Type and number of the local interface connected to MSDP peers
3	Description of an MSDP peer
4	Name of a mesh group

## 9.2.2 Configuring Intra-AS MSDP Peers

### Context

Do as follows on the RPs of all PIM-SM domains that belong to the same AS:

### Procedure

**Step 1** Run:

```
system-view
```

The system is displayed.

**Step 2** Run:

```
msdp
```

MSDP is enabled in the public network instance and the MSDP view is displayed.

**Step 3** Run:

```
peer peer-address connect-interface interface-type interface-number
```

An MSDP peer connection is configured

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *interface-type interface-number*: specifies the local interface connected to the remote MSDP peer.

**Step 4** (Optional) Run:

```
peer peer-address description text
```

The description of a remote MSDP peer is added.

This configuration helps to differentiate remote MSDP peers and manage the connections with the remote MSDP peers.

The parameters of the command are explained as follows:

- *peer-address* specifies the address of a remote MSDP peer.
- *text*: specifies the description text. The text is a string of 80 characters.

**Step 5** Run:

```
peer peer-address mesh-group name
```

A remote MSDP peer is configured to join a mesh group.

That is, the remote MSDP peer is acknowledged as a member of the mesh group.

The parameters of this command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *name*: specifies the name of a mesh group. The members of the same mesh group use the same mesh group name.

Note the following:

- MSDP peer connections must be set up between all members of the same mesh group.
- All members of the mesh group must acknowledge each other as a member of the group.
- An MSDP peer can belong to only one mesh group. If an MSDP peer is configured to join different mesh groups for multiple times, only the latest configuration is valid.

----End

## 9.2.3 Configuring Static RPF Peers

### Context

Do as follows on two RPs of different ASs:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
msdp
```

MSDP is enabled in the public network instance, and the MSDP view is displayed.

**Step 3** Run:

```
peer peer-address connect-interface interface-type interface-number
```

An MSDP peer connection is configured.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *interface-type interface-number*: specifies the local interface connected to the remote MSDP peer.

**Step 4** (Optional) Run:

```
peer peer-address description text
```

The description of a remote MSDP peer is added.

The configuration helps to distinguish remote MSDP peers and manage the connections with the remote MSDP peers.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *text*: specifies the description text. The text is a string of up to 80 characters.

**Step 5** Run:

```
static-rpf-peer peer-address
```

A remote MSDP peer is statically specified as an RPF peer.

*peer-address* specifies the address of a remote MSDP peer.

----End

## 9.2.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the brief information on the MSDP peer status.	<b>display msdp brief</b> [ <b>state</b> { <b>connect</b>   <b>down</b>   <b>listen</b>   <b>shutdown</b>   <b>up</b> } ]
Check the detailed information on the MSDP peer status.	<b>display msdp peer-status</b> [ <i>peer-address</i> ]

Run the **display msdp brief** command. If the brief information about the statuses of all remote peers that establish MSDP peer relationships with the local host can be viewed, it means that the configuration succeeds. For example:

```
<Quidway> display msdp brief
Configured  Up      Listen    Connect    Shutdown    Down
2           2           0         0          0           0

Peer's Address    State    Up/Down time    AS    SA Count    Reset Count
192.168.2.1      UP      01:07:08       200    8           0
192.168.4.2      UP      00:06:39       100   13           0
```

Run the **display msdp peer-status** [*peer-address*] command. If the detailed information about the statuses of the specified remote peers that establish the MSDP peer relationships with the local host can be viewed, it means that the configuration succeeds.

## 9.3 Configuring an Anycast RP in a PIM-SM Domain

This section describes how to configure an anycast RP.

### 9.3.1 Establishing the Configuration Task

#### 9.3.2 Configuring the Interface Address of an RP

#### 9.3.3 Configuring a C-RP

#### 9.3.4 Statically Configuring an RP

#### 9.3.5 Configuring an MSDP Peer

#### 9.3.6 Specifying the Logical RP Address for an SA Message

#### 9.3.7 Checking the Configuration

## 9.3.1 Establishing the Configuration Task

### Applicable Environment

In a traditional PIM-SM domain, each multicast group can be mapped to only one RP. When the network is overloaded or the traffic is too concentrated, many network problems are caused. For example, the pressure of the RP is too heavy, S-switches converge slowly after the RP fails, and the multicast forwarding path is not optimal.

After anycast RPs are applied in a PIM-SM domain, the source registers with the nearest RP and hosts send Join messages to the nearest RP. That is, the load of a single RP is abated, the RP backup is implemented, and the forwarding path is optimized.

The recommended configuration solutions are as follows:

- Configure loopback interfaces on multiple S-switches in the PIM-SM domain respectively, assign the same IP address to the loopback interfaces, and advertise the IP address by using unicast routes.
- Configure the loopback interfaces on the S-switches as C-RPs or configure the address of the loopback interface as a static RP on all S-switches in the PIM-SM domain.
- Set up the MSDP peer relationship between the S-switches. If the number of S-switches is greater than three, it is recommended to set up the MSDP peer relationship between the S-switches and configure them to join the same mesh group.
- Specify the logical RP address to transmit SA messages between the MSDP peers.

## Pre-configuration Tasks

Before configuring an anycast RP in a PIM-SM domain, complete the following tasks:

- Configuring a unicast routing protocol to implement interconnection at the network layer
- Enabling IP multicast
- Configuring a PIM-SM domain without any RP

## Data Preparation

To configure an anycast RP in a PIM-SM domain, you need the following data.

No.	Data
1	RP address
2	Interface and address of the local MSDP peer
3	Interface and address of the remote MSDP peer
4	Description of an MSDP peer

### 9.3.2 Configuring the Interface Address of an RP

#### Context

Use a unicast routing protocol in the current network to advertise the address of the newly configured RP interface. Ensure that all S-switches in the network have a route to the RP.

In the PIM-SM domain, do as follows on multiple S-switches on which the anycast RP is to be configured:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface loopback interface-number
```

The loopback interface view is displayed.

Multiple RPs can use the same IP address in a network. The RPs, therefore, are configured on the same loopback interface.

**Step 3** Run:

```
ip address ip-address 32
```

The address of the loopback interface is configured.

The parameters of the command are explained as follows:

- *ip-address*: specifies the address of an RP. The RPs configured on multiple devices uses the same IP address.
- *32*: specifies the address mask of the loopback interface.

**Step 4** Run:

```
pim sm
```

PIM-SM is enabled for the RP interface.

----End

## 9.3.3 Configuring a C-RP

### Context

**NOTE**

- If the PIM-SM network uses a static RP, the configuration is not necessary.
- If the PIM-SM network uses a BSR-RP, the configuration is mandatory. Before configuring a C-RP, configure a BSR and BSP boundary. The BSR address cannot be the same as the C-RP address.

Do as follows on multiple S-switches on which an anycast RP is to be configured in the PIM-SM domain:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
pim
```

The PIM view is displayed.

**Step 3** Run:

```
c-rp loopback interface-number
```

An interface is specified as RP.

----End

## 9.3.4 Statically Configuring an RP

### Context

**NOTE**

- When the PIM-SM network uses a BSR-RP, the configuration is not necessary.
- When the PIM-SM network uses a static RP, the configuration is mandatory.

Do as follows on all S-switches in the PIM-SM domain:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`pim`  
The PIM view is displayed.
- Step 3** Run:  
`static-rp rp-address`  
The RP address is configured.  
*rp-address* specifies the IP address of the static RP.  
----End

## 9.3.5 Configuring an MSDP Peer

### Context

Do as follows on multiple S-switches on which an anycast RP is to be created:



#### NOTE

If the number of S-switches configured with the RPs that have the same IP address exceeds two, ensure the interconnection between the S-switches that set up MSDP peer relationship.

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`msdp`  
MSDP is enabled in the public network instance, and the MSDP view is displayed.
- Step 3** Run:  
`peer peer-address connect-interface interface-type interface-number`  
An MSDP peer connection is created.  
The parameters of the command are explained as follows:
- *peer-address*: specifies the address of a remote MSDP peer. The address cannot be the same as that of the C-RP.
  - *interface-type interface-number*: specifies the local interface. The interface type and the interface number cannot be the same as that of the C-RP interface.
- Step 4** (Optional) Run:  
`peer peer-address description text`

The description of the MSDP peer is added.

This configuration helps to differentiate remote MSDP peers and manage the connection with the remote MSDP peers.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *text*: specifies the description text. The text is a string of 80 characters.

**Step 5** (Optional) Run:

```
peer peer-address mesh-group name
```

A remote MSDP peer is configured to join a mesh group.

That is, the remote MSDP peer is acknowledged as a member of the mesh group.

If only two S-switches are configured with the anycast-RP, this configuration is not necessary.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *name*: specifies the name of a mesh group. The members of the same mesh group use the same mesh group name.

Note the following:

- MSDP peer connections must be set up between all members of the mesh group.
- All members of the mesh group must acknowledge each other as the member of the mesh group.
- An MSDP peer belongs to only one mesh group. If an MSDP peer is configured to join different mesh groups for many times, only the last configuration is valid.

----End

## 9.3.6 Specifying the Logical RP Address for an SA Message

### Context

After receiving an SA message, an MSDP peer performs the RPF check on the message. If the remote RP address carried in the SA message is the same as the local RP address, the SA message is discarded.

Do as follows on the S-switches on which the anycast RP is to be configured:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
msdp
```

The MSDP view is displayed.

### Step 3 Run:

```
originating-rp interface-type interface-number
```

The logical RP interface is configured. The logical RP interface cannot be the same as the actual RP interface. It is recommended to configure the logical interface as the MSDP peer interface.

After the **originating-rp** command is used, the logical RP address carried in the SA message sent by the S-switch replaces the RP address in the IP header of the SA message, and the SA message can pass the RPF check after reaching the remote S-switch.

----End

## 9.3.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the brief information of the MSDP peer status.	<b>display msdp brief</b>
Check information about the RP corresponding to the PIM routing table.	<b>display pim routing-table</b>

Run the **display msdp brief** command. If the brief information about the remote MSDP peer status is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display msdp brief
Configured  Up      Listen      Connect      Shutdown      Down
1           1           0           0           0           0

Peer's Address      State      Up/Down time      AS      SA Count      Reset Count
2.2.2.2             UP        00:10:17         ?       0           0
```

Run the **display pim routing-table** command. If the RP information corresponding to the routing table is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(10.11.1.2, 225.1.1.1)
  RP: 7.7.7.7 (local)
  Protocol: pim-sm, Flag: SPT ACT
  UpTime: 00:01:57
  Upstream interface: GigabitEthernet0/0/2
    Upstream neighbor: 10.3.1.2
    RPF prime neighbor: 10.3.1.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: GigabitEthernet0/0/3
      Protocol: pim-sm, UpTime: - , Expires: -
```

## 9.4 Managing MSDP Peer Connections

This section describes how to manage MSDP peers connections.

### 9.4.1 Establishing the Configuration Task

[9.4.2 Controlling the Sessions Between MSDP Peers](#)[9.4.3 Adjusting the interval for Retrying Setting up an MSDP Peer Connection](#)[9.4.4 Checking the Configuration](#)

## 9.4.1 Establishing the Configuration Task

### Applicable Environment

MSDP peers are connected by the TCP connection (the port number is 639). Users can close or reestablish a TCP connection, and flexibly control the sessions set up between MSDP peers.

When a new MSDP peer is created, or when a closed MSDP peer connection is restarted, or when a faulty MSDP peer tries recovering, the TCP connection needs to be immediately set up between MSDP peers. Users can flexibly adjust the interval for retrying setting up an MSDP peer connection.

### Pre-configuration Tasks

Before managing MSDP peer connections, complete the following tasks:

- Configuring a unicast routing protocol to implement interconnection at the network layer
- Enabling IP multicast
- Configuring a PIM-SM domain to implement intra-domain multicast
- [9.2 Configuring PIM-SM Inter-domain Multicast](#) or [9.3 Configuring an Anycast RP in a PIM-SM Domain](#)

### Data Preparation

To manage MSDP peer connections, you need the following data.

No.	Data
1	Address of a remote MSDP peer
2	Interface type and interface number of the local S-switch

## 9.4.2 Controlling the Sessions Between MSDP Peers

### Context

Do as follows on the S-switch on which the MSDP peer is created:

### Procedure

- Step 1** Run:
- ```
system-view
```

The system view is displayed.

**Step 2** Run:

**msdp**

The MSDP view is displayed.

**Step 3** Run:

**shutdown** *peer-address*

A session with the remote MSDP peer is closed.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- After the session with the remote MSDP peer is closed, the TCP connection is closed, the peers no longer transmit SA messages, and the peers do not re-try setting up the connection. The configuration, however, is saved.
- You can run the **undo shutdown** *peer-address* command to open the session with the remote MSDP peer, and reestablish the TCP connection.

----End

### 9.4.3 Adjusting the interval for Retrying Setting up an MSDP Peer Connection

#### Context

Do as follows on the S-switch on which the MSDP peer is created:

#### Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**msdp**

The MSDP view is displayed.

**Step 3** Run:

**timer retry** *interval*

The period for retrying sending the TCP connection request to the remote MSDP peer is set

----End

### 9.4.4 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                  | Command                                                  |
|---------------------------------------------------------|----------------------------------------------------------|
| Check the brief information of the MSDP peer status.    | <b>display msdp brief</b>                                |
| Check the detailed information of the MSDP peer status. | <b>display msdp [peer-status [ <i>peer-address</i> ]</b> |

Run the **display msdp brief** command. If brief information about the status of the connection with the remote MSDP peer is viewed, it means that the configuration succeeds. For example:

```
<Quidway> display msdp brief
Configured   Up        Listen      Connect     Shutdown    Down
2            2          0           0           0           0

Peer's Address   State   Up/Down time   AS    SA Count   Reset Count
192.168.2.1      UP      01:07:08      200    8          0
192.168.4.2      UP      00:06:39      100   13          0
```

Run the **display msdp peer-status [ *peer-address* ]** command. If the detailed information about the status of specified remote MSDP peers that establish MSDP peer relationships with the local host is viewed, it means that the configuration succeeds.

## 9.5 Configuring SA Cache

This section describes how to configure SA Cache.

### 9.5.1 Establishing the Configuration Task

#### 9.5.2 Configuring the Maximum Number of (S, G) Entries in the Cache

#### 9.5.3 Disabling the SA Cache Function

#### 9.5.4 Checking the Configuration

## 9.5.1 Establishing the Configuration Task

### Applicable Environment

By default, SA Cache is enabled on S-switches on which MSDP peers are configured. The S-switches can locally store the (S, G) information carried in SA messages. When the S-switches need to receive (S, G) information, the S-switches can obtain the (S, G) information from the SA Cache.

Setting the maximum number of (S, G) entries can prevent the Denial of Service (DoS) attack.

Users can disable the SA Cache of a S-switch. After the SA Cache of a S-switch is disabled, the S-switch does not locally store the (S, G) information carried in SA messages. When a S-switch wants to receive (S, G) data, it needs to wait for the SA message to be sent by its MSDP peer in the next period. This delays receivers from obtaining multicast data.

### Pre-configuration Tasks

Before configuring SA Cache, complete the following tasks:

- Configuring a unicast routing protocol to implement interconnection at the network layer
- Enabling IP multicast
- Configuring a PIM-SM domain to implement intra-domain multicast
- [9.2 Configuring PIM-SM Inter-domain Multicast](#) or [9.3 Configuring an Anycast RP in a PIM-SM Domain](#)

## Data Preparation

To configure SA Cache, you need the following data.

| No. | Data                                             |
|-----|--------------------------------------------------|
| 1   | Maximum number of (S, G) entries in the SA Cache |

## 9.5.2 Configuring the Maximum Number of (S, G) Entries in the Cache

### Context

Do as follows on the S-switch on which the MSDP peer is configured:

#### NOTE

If the configuration is not done, default values are used.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
msdp
```

The MSDP view is displayed.

#### Step 3 Run:

```
peer peer-address SA Cache-maximum sa-limit
```

The maximum number of (S, G) entries is set.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *sa-limit*: specifies the maximum number of cached (S, G) entries. The redundant entries are discarded. The value that is smaller than the value defined by the cache is valid.

----End

## 9.5.3 Disabling the SA Cache Function

## Context

Do as follows on the S-switch on which the MSDP peer is configured:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
msdp
```

The MSDP view is displayed.

### Step 3 Run:

```
undo cache-sa-enable
```

The SA Cache function is disabled.

### NOTE

To reenale SA Cache, run the **cache-sa-enable** command in the MSDP view.

----End

## 9.5.4 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                                             | Command                                                                                            |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Check (S, G) entries in the SA Cache of the public network instance.               | <b>display msdp sa-cache</b> [ <i>group-address</i>   <i>source-address</i>   <i>as-number</i> ] * |
| Check the number of (S, G) entries in the SA Cache of the public network instance. | <b>display msdp sa-count</b> [ <i>as-number</i> ]                                                  |

## 9.6 Configuring an SA Request

This section describes how to configure an SA request.

### [9.6.1 Establishing the Configuration Task](#)

### [9.6.2 Configuring "Sending SA Request Messages" on the Local Router](#)

### [9.6.3 Configuring the Filtering Rules for Receiving SA Request Messages](#)

### [9.6.4 Checking the Configuration](#)

## 9.6.1 Establishing the Configuration Task

## Applicable Environment

Certain S-switches cannot be enabled with SA Cache or the capacity of SA Cache on these S-switches is too small. When these S-switches need to receive multicast data, they cannot immediately obtain the valid (S, G) information and need to wait for the SA message sent by their MSDP peers in the next period.

If SA Cache is enabled on the remote MSDP peer and the capacity of the SA Cache is large, configuring "sending SA Request message" on the local S-switch can shorten the period during which receivers obtain multicast source information.

- When the local S-switch wants to receive (S, G) information, it sends an SA Request message to a specified remote MSDP peer.
- On receiving the SA Request message, the MSDP peer responds to the SA Request message with the required (S, G) information. If the "filtering rule of SA Request message" is configured on the remote MSDP peer, it checks the SA Request messages received from a specified peers and determines whether to respond according to the checking results.

## Pre-configuration Tasks

Before configuring an SA request, complete the following tasks:

- Configuring a unicast routing protocol to implement interconnection at the network layer
- Enabling IP multicast
- Configuring a PIM-SM domain to implement intra-domain multicast
- [9.2 Configuring PIM-SM Inter-domain Multicast](#) or [9.3 Configuring an Anycast RP in a PIM-SM Domain](#)

## Data Preparation

To configure an SA request, you need the following data.

| No. | Data                                             |
|-----|--------------------------------------------------|
| 1   | Address of a remote MSDP peer                    |
| 2   | Filtering list for receiving SA request messages |

## 9.6.2 Configuring "Sending SA Request Messages" on the Local Router

### Context

Do as follows on the local S-switch:

### Procedure

- Step 1** Run:
- ```
system-view
```

The system view is displayed.

**Step 2** Run:

```
msdp
```

The MSDP view is displayed.

**Step 3** Run:

```
peer peer-address request-sa-enable
```

Sending SA Request message is configured.

*peer-address* specifies the address of a remote MSDP peer. When the local S-switch receives a new Join message from a group, it sends an SA Request message only to *peer-address*.

----End

## 9.6.3 Configuring the Filtering Rules for Receiving SA Request Messages

### Context

Do as follows on the remote MSDP peer specified by using the **peer peer-address request-sa-enable** command. If the configuration is not done, once an SA message reaches, the S-switch immediately responds to it with an SA message containing the required (S, G) information.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
msdp
```

The MSDP view is displayed.

**Step 3** Run:

```
peer peer-address sa-request-policy [ acl basic-acl-number ]
```

The filtering rules for receiving SA Request messages are set.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of an MSDP peer that sends the SA message.
- **acl basic-acl-number**: specifies the filtering policy. If the ACL is not specified, all SA messages sent by a peer are ignored. If the ACL is specified, only the SA messages that match the ACL are received and other SA messages are discarded.

----End

## 9.6.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check detailed information about the MSDP peer status.	<b>display msdp peer-status</b> [ <i>peer-address</i> ]
Check the SA Cache of the public network instance.	<b>display msdp sa-cache</b> [ <i>group-address</i>   <i>source-address</i>   <i>as-number</i> ] *

Run the **display msdp peer-status** [ *peer-address* ] command, and you can view the SA-Requests field and check whether the configuration is valid. For example:

```
<Quidway> display msdp peer-status
MSDP Peer 172.40.41.1, AS ?
Description:
Information about connection status:
  State: Up
  Up/down time: 00:26:41
  Resets: 0
  Connection interface: Ethernet2/0/14 (172.40.41.2)
  Number of sent/received messages: 27/28
  Number of discarded output messages: 0
  Elapsed time since last connection or counters clear: 00:26:56
Information about (Source, Group)-based SA filtering policy:
  Import policy: none
  Export policy: none
Information about SA-Requests:
  Policy to accept SA-Request messages: 2000
  Sending SA-Requests status: enable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA Cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 16/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
```

## 9.7 Transmitting Burst Multicast Data Between Domains

This section describes how to transmit burst multicast data between domains.

### 9.7.1 Establishing the Configuration Task

#### 9.7.2 Encapsulating a Multicast Data Packet in an SA message

#### 9.7.3 (Optional) Setting the TTL Threshold for Forwarding an SA Message Containing a Multicast Data Packet

#### 9.7.4 Checking the Configuration

## 9.7.1 Establishing the Configuration Task

### Applicable Environment

The time during which certain multicast sources send multicast data is long, and is longer than the timeout of an (S, G) entry. In this case, the source DR encapsulates multicast data packets

in Register messages one by one, and sends the messages to the source RP. The source RP then uses SA messages to forward (S, G) entries to the remote RP.

The remote RP then sends a Join message to the source DR. An SPT is thus set up. Because of the timeout of the (S, G) entry, remote users cannot receive multicast data sent by S.

After the function of encapsulating a multicast packet in an SA message is enabled on the source RP, the source RP encapsulates multicast data in SA messages and sends them out. After receiving an SA message, a remote RP decapsulates the message and forwards the multicast data to users in the domain along the RPT.

Setting the TTL threshold can limit the transmission scope of a multicast packet contained in an SA message. After receiving an SA message containing a multicast packet, an MSDP peer checks the TTL value in the IP header of the multicast packet. If the TTL value is smaller than or equal to the threshold, the MSDP peer does not forward the SA message to a specific remote peers. If the TTL value is greater than the threshold, the MSDP peer reduces the TTL value in the IP header of the multicast packet by 1, and then encapsulates the multicast packet in an SA message and sends it out.

## Pre-configuration Tasks

Before transmitting burst multicast data between domains, complete the following tasks:

- Configuring a unicast routing protocol to implement interconnection at the network layer
- Enabling IP multicast
- Configuring a PIM-SM domain to implement intra-domain multicast
- [9.2 Configuring PIM-SM Inter-domain Multicast](#) or [9.3 Configuring an Anycast RP in a PIM-SM Domain](#)

## Data Preparation

To transmit burst multicast data between domains, you need the following data.

No.	Data
1	TTL threshold for forwarding an SA message containing a multicast data packet
2	Address of a remote MSDP peer

## 9.7.2 Encapsulating a Multicast Data Packet in an SA message

### Context

Do as follows on the source RP configured with an MSDP peer:

### Procedure

- Step 1** Run:
- ```
system-view
```

The system view is displayed.

**Step 2** Run:

**msdp**

The MSDP view is displayed.

**Step 3** Run:

**encap-data-enable**

A multicast data packet is encapsulated in an SA message.

By default, the SA message contains only (S, G) information, and does not contain a multicast data packet.

----End

### 9.7.3 (Optional) Setting the TTL Threshold for Forwarding an SA Message Containing a Multicast Data Packet

#### Context

Do as follows on the S-switch configured with an MSDP peer:

 **NOTE**

If the configuration is not done, default values are used.

#### Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**msdp**

The MSDP view is displayed.

**Step 3** Run:

**peer** *peer-address* **minimum-ttl** *tth*

The TTL threshold of a multicast data packet is set.

After receiving an SA message containing a multicast data packet, an MSDP peer forwards the SA message to a specified remote MSDP peers only when the TTL value of the multicast packet is greater than the threshold.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- *tth*: specifies the value of the TTL threshold. By default, the value is 0.

----End

### 9.7.4 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                 | Command                                                                                            |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Check SA Cache of the public network instance.         | <b>display msdp sa-cache</b> [ <i>group-address</i>   <i>source-address</i>   <i>as-number</i> ] * |
| Check detailed information about the MSDP peer status. | <b>display msdp peer-status</b> [ <i>peer-address</i> ]                                            |

Run the **display msdp peer-status** [ *peer-address* ] command, and you can view the minimum TTL for forwarding an SA messages containing a data packet and check whether the configuration is valid. For example:

```
<Quidway> display msdp peer-status
MSDP Peer 172.40.41.1, AS ?
Description:
Information about connection status:
  State: Up
  Up/down time: 00:26:41
  Resets: 0
  Connection interface: Ethernet0/0/14 (172.40.41.2)
  Number of sent/received messages: 27/28
  Number of discarded output messages: 0
  Elapsed time since last connection or counters clear: 00:26:56
Information about (Source, Group)-based SA filtering policy:
  Import policy: none
  Export policy: none
Information about SA-Requests:
  Policy to accept SA-Request messages: 2000
  Sending SA-Requests status: enable
Minimum TTL to forward SA with encapsulated data: 10
SAs learned from this peer: 0, SA Cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 16/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
```

Run the **display msdp sa-cache** command to check the information about (S, G) entries in SA Cache.

- If *group-address* is specified, the (S, G) entry corresponding to a specified group is displayed.
- If *source-address* is specified, the (S, G) entry corresponding to a specified source is displayed.
- If *as-number* is specified, the (S, G) entry of a specified AS that the S belongs to is displayed.
- If none of the preceding parameters is specified, all (S, G) entries in the SA Cache are displayed.

```
<Quidway> display msdp sa-cache
MSDP Total Source-Active Cache - 5 entries
MSDP matched 5 entries
(Source, Group)          Origin RP      Pro   AS   Uptime  Expires
(10.10.1.2, 225.1.1.1)   10.10.10.10   BGP   100  00:00:10 00:05:50
(10.10.1.3, 225.1.1.1)   10.10.10.10   BGP   100  00:00:11 00:05:49
(10.10.1.2, 225.1.1.2)   10.10.10.10   BGP   100  00:00:11 00:05:49
(10.10.2.1, 225.1.1.2)   10.10.10.10   BGP   100  00:00:11 00:05:49
(10.10.1.2, 225.1.2.2)   10.10.10.10   BGP   100  00:00:11 00:05:49
```

## 9.8 Configuring the Filtering Rules for SA Messages

This section describes how to configure the filtering rules for SA messages.

### [9.8.1 Establishing the Configuration Task](#)

### [9.8.2 Setting Rules for Creating an SA Message](#)

### [9.8.3 Setting Rules for Receiving an SA Message](#)

### [9.8.4 Setting Rules for Forwarding an SA Message](#)

### [9.8.5 Checking the Configuration](#)

## 9.8.1 Establishing the Configuration Task

### Applicable Environment

By default, MSDP S-switches receive all SA messages that pass the RPF check and forward them to all MSDP peers. To control of the transmission of SA messages among MSDP peers, users can configure various filtering rules by using the following methods:

- Setting the rules for filtering the multicast source of an SA message on the source RP. The source RP filters active multicast sources that register with the local S-switch, and determines the (S, G) entries to be sent according to the rules.
- Setting the rules for filtering an SA message received from a remote MSDP peer. When an SA message sent by a remote MSDP peer reaches a S-switch, the S-switch determines whether to receive the message based on the rules.
- Setting the rules for filtering an SA message forwarded to a remote MSDP peer. Before forwarding the SA message to the remote MSDP peer, the S-switch determines whether to forward it based on the rules.

### Pre-configuration Tasks

Before configuring the filtering rules for SA messages, complete the following tasks:

- Configuring a unicast routing protocol to implement interconnection at the network layer
- Enabling IP multicast
- Configuring a PIM-SM domain to implement intra-domain multicast
- [9.2 Configuring PIM-SM Inter-domain Multicast](#) or [9.3 Configuring an Anycast RP in a PIM-SM Domain](#)

### Data Preparation

To configure the filtering rules for SA messages, you need the following data.

| No. | Data                                     |
|-----|------------------------------------------|
| 1   | Filtering list for creating SA messages  |
| 2   | Filtering list for receiving SA messages |

| No. | Data                                      |
|-----|-------------------------------------------|
| 3   | Filtering list for forwarding SA messages |
| 4   | Address of a remote MSDP peer             |

## 9.8.2 Setting Rules for Creating an SA Message

### Context

Do as follows on the source RP configured with an MSDP peer:



#### NOTE

If the configuration is not done, an SA message created by the source RP contains the information of all local active sources.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
msdp
```

The MSDP view is displayed.

#### Step 3 Run:

```
import-source [ acl acl-number ]
```

The rules for filtering the multicast source of an SA message are set.

The parameters of the command are explained as follows:

- **acl acl-number**: specifies the filtering list based on multicast sources. The SA message created by an MSDP peer contains the local source information that match the filtering rules. The MSDP peer can thus control the local (S, G) information.
- If the **import-source** command with **acl** is used, the SA message does not advertise any information about the local active source.

----End

## 9.8.3 Setting Rules for Receiving an SA Message

### Context

Do as follows on the S-switch configured with MSDP:



#### NOTE

If the configuration is not done, the S-switch receives all SA messages that pass the RPF check.

## Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**msdp**

The MSDP view is displayed.

**Step 3** Run:

**peer peer-address sa-policy import [ acl advanced-acl-number ]**

The rules for filtering an SA message received from a remote MSDP peer are set.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- **acl advanced-acl-number**: specifies the advanced filtering list. Only the (S, G) information that passes the filtering of the ACL is received. The (S, G) information is contained in an SA message sent by the peer specified by *peer-address*.
- If the **peer peer-address sa-policy import** command without **acl** is used, the S-switch does not receive any (S, G) information from the peer specified by *peer-address*.

----End

## 9.8.4 Setting Rules for Forwarding an SA Message

### Context

Do as follows on the S-switch enabled with MSDP:

 **NOTE**

If the configuration is not done, the S-switch forwards all SA messages that pass the RPF check.

## Procedure

**Step 1** Run:

**system-view**

The system view is displayed.

**Step 2** Run:

**msdp**

The MSDP view is displayed.

**Step 3** Run:

**peer peer-address sa-policy export [ acl advanced-acl-number ]**

The rules for filtering an SA message forwarded to a remote MSDP peer is set.

The parameters of the command are explained as follows:

- *peer-address*: specifies the address of a remote MSDP peer.
- **acl** *advanced-acl-number*: specifies the advanced filtering list. Only the (S, G) information that matches the ACL rule is forwarded to the peer specified by *peer-address*.
- If the **peer** *peer-address* **sa-policy export** command without **acl** is used, the S-switch does not forward any (S, G) information to the peer specified by *peer-address*.

----End

## 9.8.5 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                 | Command                                                                                            |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Check SA Cache of the public network instance.         | <b>display msdp sa-cache</b> [ <i>group-address</i>   <i>source-address</i>   <i>as-number</i> ] * |
| Check detailed information about the MSDP peer status. | <b>display msdp peer-status</b> [ <i>peer-address</i> ]                                            |

Run the **display msdp peer-status** [ *peer-address* ] command, and you can view information about the (Source, Group)-based SA filtering policy field and check whether the configuration is valid. For example:

```
<Quidway> display msdp peer-status
MSDP Peer 172.40.41.1, AS ?
Description:
Information about connection status:
  State: Up
  Up/down time: 00:26:41
  Resets: 0
  Connection interface: Ethernet0/0/14 (172.40.41.2)
  Number of sent/received messages: 27/28
  Number of discarded output messages: 0
  Elapsed time since last connection or counters clear: 00:26:56
Information about (Source, Group)-based SA filtering policy:
  Import policy: 3000
  Export policy: 3002
Information about SA-Requests:
  Policy to accept SA-Request messages: 2000
  Sending SA-Requests status: enable
Minimum TTL to forward SA with encapsulated data: 10
SAs learned from this peer: 0, SA Cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 16/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
```

Run the **display msdp sa-cache** command to check the information about (S, G) entries in SA Cache.

- If *group-address* is specified, the (S, G) entry corresponding to a specified group is displayed.

- If *source-address* is specified, the (S, G) entry corresponding to a specified source is displayed.
- If *as-number* is specified, the (S, G) of a specified AS that the S belongs to is displayed.
- If none of the preceding parameters is specified, all (S, G) entries in the SA Cache are displayed.

```
<Quidway> display msdp sa-cache
MSDP Total Source-Active Cache - 5 entries
MSDP matched 5 entries
(Source, Group)          Origin RP      Pro   AS    Uptime  Expires
(10.10.1.2, 225.1.1.1)   10.10.10.10 BGP   100   00:00:10 00:05:50
(10.10.1.3, 225.1.1.1)   10.10.10.10 BGP   100   00:00:11 00:05:49
(10.10.1.2, 225.1.1.2)   10.10.10.10 BGP   100   00:00:11 00:05:49
(10.10.2.1, 225.1.1.2)   10.10.10.10 BGP   100   00:00:11 00:05:49
(10.10.1.2, 225.1.2.2)   10.10.10.10 BGP   100   00:00:11 00:05:49
```

## 9.9 Maintaining MSDP

This section describes how to clear MSDP statistics, reset connections between MSDP peers, and debug MSDP.

### 9.9.1 Clearing Statistics of MSDP Peers

#### 9.9.2 Clearing (S, G) Information in SA Cache

#### 9.9.3 Monitoring the Running Status of MSDP

#### 9.9.4 Debugging MSDP

### 9.9.1 Clearing Statistics of MSDP Peers



#### CAUTION

The statistics of MSDP peers cannot be restored after you clear it. So, confirm the action before you use the command.

To clear the statistics of MSDP peers, run the following commands in the user view.

| Action                                                                                             | Command                                              |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Clear the TCP connection with a specified MSDP peer and all statistics of the specified MSDP peer. | <b>reset msdp peer</b> [ <i>peer-address</i> ]       |
| Clear the statistics of an MSDP peer or multiple MSDP peers of the public network instance.        | <b>reset msdp statistics</b> [ <i>peer-address</i> ] |

### 9.9.2 Clearing (S, G) Information in SA Cache

**CAUTION**

The (S, G) information in SA Cache cannot be restored after you clear it. So, confirm the action before you use the command.

To clear the (S, G) information in SA Cache, run the following commands in the user view.

| Action                              | Command                                             |
|-------------------------------------|-----------------------------------------------------|
| Clear the entries in MSDP SA Cache. | <b>reset msdp sa-cache</b> [ <i>group-address</i> ] |

## 9.9.3 Monitoring the Running Status of MSDP

During routine maintenance, run the following commands in any view to know the running status of MSDP.

| Action                                                                                      | Command                                                                                                                   |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Check brief information about the MSDP peer status.                                         | <b>display msdp brief</b> [ <b>state</b> { <b>connect</b>   <b>down</b>   <b>listen</b>   <b>shutdown</b>   <b>up</b> } ] |
| Check detailed information about the status of an MSDP peer of the public network instance. | <b>display msdp peer-status</b> [ <i>peer-address</i> ]                                                                   |
| Check the (S, G) information in SA Cache.                                                   | <b>display msdp sa-cache</b> [ <i>group-address</i>   <i>source-address</i>   <i>as-number</i> ] *                        |
| Check the number of (S, G) entries in MSDP Cache.                                           | <b>display msdp sa-count</b> [ <i>as-number</i> ]                                                                         |

## 9.9.4 Debugging MSDP

**CAUTION**

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

When a fault occurs, run the following **debugging** commands in the user view to debug MSDP and locate the fault.

| Action      | Command                   |
|-------------|---------------------------|
| Debug MSDP. | <b>debugging msdp all</b> |

| Action                                                      | Command                             |
|-------------------------------------------------------------|-------------------------------------|
| Debug the retrying of TCP connections set up by MSDP peers. | <b>debugging msdp connect</b>       |
| Debug MSDP events.                                          | <b>debugging msdp event</b>         |
| Debug MSDP packets.                                         | <b>debugging msdp packet</b>        |
| Debug active MSDP sources.                                  | <b>debugging msdp source-active</b> |

## 9.10 Configuration Examples

This section provides several configuration examples of MSDP.

[9.10.1 Example for Configuring PIM-SM Inter-Domain Multicast](#)

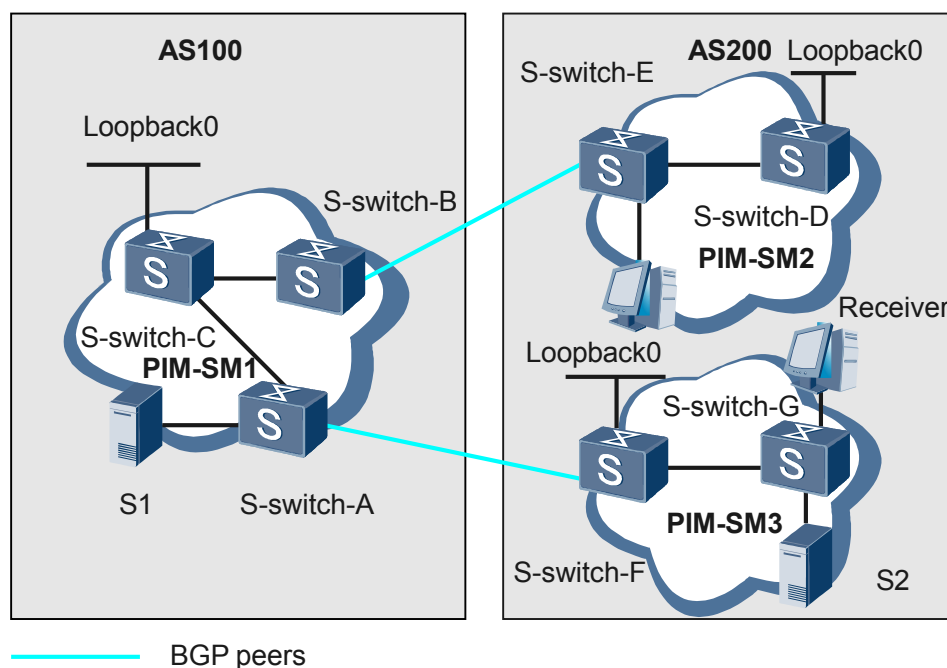
[9.10.2 Example for Configuring Inter-AS Multicast by Using Static RPF Peers](#)

[9.10.3 Example for Configuring an Anycast RP](#)

### 9.10.1 Example for Configuring PIM-SM Inter-Domain Multicast

#### Networking Requirements

As shown in [Figure 9-1](#), there are two ASs in the network. Each AS contains one or more PIM-SM domains. The receivers in PIM-SM2 domain are required to receive multicast data sent by S3 in PIM-SM3 domain and multicast data sent by S1 in PIM-SM1 domain.

**Figure 9-1** Networking diagram of configuring PIM-SM inter-domain multicast

| S-switch   | Interface | IP Address     | S-switch   | Interface | IP Address     |
|------------|-----------|----------------|------------|-----------|----------------|
| S-switch-A | vlanif 1  | 10.110.1.1/24  | S-switch-D | vlanif 1  | 10.110.2.1/24  |
|            | vlanif 2  | 192.168.1.1/24 |            | vlanif 2  | 192.168.3.2/24 |
| S-switch-B | vlanif 1  | 192.168.2.1/24 | S-switch-E | vlanif 2  | 192.168.5.1/24 |
|            | vlanif 2  | 192.168.1.2/24 |            | vlanif 3  | 192.168.4.2/24 |
| S-switch-C | vlanif 1  | 192.168.2.2/24 | S-switch-F | vlanif 1  | 10.110.3.1/24  |
|            | vlanif 2  | 192.168.3.1/24 |            | vlanif 2  | 192.168.5.2/24 |
|            | vlanif 3  | 192.168.4.1/24 |            |           |                |

## Configuration Roadmap

Solution: configure MSDP peer relationships between RPs of each PIM-SM domain. The configuration roadmap is as follows:

1. Configure IP addresses of interfaces on each S-switch, and configure OSPF in the ASs to ensure that unicast routes are reachable in the ASs.
2. Configure EBGP peers between ASs and configure BGP and OSPF to import routes to each other to ensure that unicast routes are reachable.
3. Enable multicast and PIM-SM on each interface, configure the boundary of a domain, and enable IGMP on the interface connected to hosts.
4. Configure a C-BSR and a C-RP. Configure the RPs of PIM-SM1 and PIM-SM2 on ASBRs.
5. Establish the MSDP peer relationship between RPs of each domain. MSDP peers and EBGP peers between ASs use the same interface address. According to RPF rules, S-switches receive SA messages forwarded by the next hop of the route to the source RP.

## Data Preparation

To complete this configuration, you need the following data:

- Address of multicast group G: 225.1.1.1/24.
- The AS number of S-switch-A and S-switch-B is 100. Router ID of S-switch-B is 1.1.1.1.
- The AS number of S-switch-C and S-switch-D is 200. Router ID of S-switch-C is 2.2.2.2.
- The AS number of S-switch-E and S-switch-F is 200.

## Configuration Procedure

### NOTE

In the example, only the commands related to MSDP configuration are mentioned.

1. Configure an IP address and a unicast routing protocol on each S-switch.  
# Configure an IP address and mask on each interface as shown in [Figure 9-1](#). Configure OSPF in the AS. Ensure that the communication between S-switches is normal at the network layer. Ensure dynamic routing updates between S-switches with the help of the unicast routing protocol. The procedures are not mentioned here.
2. Configure BGP between ASs and configure BGP and OSPF to import routes each other.

# Configure EBGP on S-switch-B and import OSPF routes.

```
[S-switch-B] bgp 100
[S-switch-B-bgp] router-id 1.1.1.1
[S-switch-B-bgp] peer 192.168.2.2 as-number 200
[S-switch-B-bgp] import-route ospf 1
[S-switch-B-bgp] quit
```

# Configure EBGP on S-switch-C, and then import OSPF routes.

```
[S-switch-C] bgp 200
[S-switch-C-bgp] router-id 2.2.2.2
[S-switch-C-bgp] peer 192.168.2.1 as-number 100
[S-switch-C-bgp] import-route ospf 1
[S-switch-C-bgp] quit
```

# Import BGP routes to OSPF on S-switch-B. The configuration of S-switch-C is similar to that of S-switch-B, and is not mentioned here.

```
[S-switch-B] ospf 1
[S-switch-B-ospf-1] import-route bgp
[S-switch-B-ospf-1] quit
```

3. Enable multicast on each S-switch and enable PIM-SM on each interface, configure the boundary of a domain and enable IGMP on the interface connected to hosts.

# Enable multicast on S-switchB, and enable PIM-SM on each interface. The configurations of other S-switches are similar to that of S-switch-B, and are not mentioned here.

```
[S-switch-B] multicast routing-enable
[S-switch-B] interface vlanif 2
[S-switch-B-Vlanif2] pim sm
[S-switch-B-Vlanif2] quit
[S-switch-B] interface vlanif 1
[S-switch-B-Vlanif1] pim sm
```

# Configure the BSR boundary on vlanif 1 of S-switch-B.

```
[S-switch-B-Vlanif1] pim bsr-boundary
[S-switch-B-Vlanif1] quit
```

Configure the domain boundary on vlanif 1 and vlanif 3 of S-switch-C and the BSR service boundary on vlanif 3 of S-switch-E. The configurations of S-switch-S-switch-E are similar to that of S-switch-B, and are not mentioned here.

# Enable IGMP on interface through which S-switch-D is connected to the leaf network.

```
[S-switch-D] interface vlanif 1
[S-switch-D-Vlanif1] igmp enable
```

## 4. Configure a C-BSR and a C-RP.

# Configure Loopback 0 interfaces and C-BSRs and C-RPs on S-switch-B. The configurations of S-switch-C and S-switch-E are similar to those of S-switch-B, and are not mentioned here.

```
[S-switch-B] interface loopback 0
[S-switch-B-LoopBack0] ip address 1.1.1.1 255.255.255.255
[S-switch-B-LoopBack0] pim sm
[S-switch-B-LoopBack0] quit
[S-switch-B] pim
[S-switch-B-pim] c-bsr loopback 0
[S-switch-B-pim] c-rp loopback 0
[S-switch-B-pim] quit
```

## 5. Configure MSDP peers.

# Configure MSDP peers on S-switch-B.

```
[S-switch-B] msdp
[S-switch-B-msdp] peer 192.168.2.2 connect-interface vlanif 1
[S-switch-B-msdp] quit
```

# Configure MSDP peers on S-switch-C.

```
[S-switch-C] msdp
[S-switch-C-msdp] peer 192.168.2.1 connect-interface vlanif 1
[S-switch-C-msdp] peer 192.168.4.2 connect-interface vlanif 3
[S-switch-C-msdp] quit
```

# Configure MSDP peers on S-switch-E.

```
[S-switch-E] msdp
[S-switch-E-msdp] peer 192.168.4.1 connect-interface vlanif 3
[S-switch-E-msdp] quit
```

## 6. Verify the configuration.

# Run the **display bgp peer** command. You can view BGP peer relationships between S-switches. For example, the BGP peer relationship between S-switch-B and S-switch-C is as follows:

```
<S-switch-B> display bgp peer
BGP local S-switch ID : 1.1.1.1
Local AS number : 100
Total number of peers : 1
Peers in established state : 1
Peer      V    AS    MsgRcvd   MsgSent   OutQ   Up/Down   State
PrefRcv
192.168.2.2  4    200    24        21        0      00:13:09   Established
6
<S-switch-C> display bgp peer
BGP local Router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 1
Peers in established state : 1
Peer      V    AS    MsgRcvd   MsgSent   OutQ   Up/Down   State
PrefRcv
192.168.2.1  4    100    18        16        0      00:12:04   Established
1
```

# Run the **display bgp routing-table** command. You can view the BGP routing table on a S-switch. For example, the BGP routing table on S-switch-C is as follows:

```
<S-switch-C> display bgp routing-table
Total Number of Routes: 5
BGP Local Router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
```

# Run the **display mdp brief** command. You can view MSDP peer relationships between S-switches. The brief information about MSDP peer relationships between S-switch-B, S-switch-C, and S-switch-E is as follows:

```
<S-switch-B> display mdp brief
```

```

Configured  Up          Listen    Connect    Shutdown    Down
1           1           0         0          0           0

Peer's Address    State    Up/Down time    AS    SA Count    Reset Count
192.168.2.2      UP      00:12:27       200   13          0

<S-switch-C> display msdp brief
Configured  Up          Listen    Connect    Shutdown    Down
2           2           0         0          0           0

Peer's Address    State    Up/Down time    AS    SA Count    Reset Count
192.168.2.1      UP      01:07:08       100   8           0
192.168.4.2      UP      00:06:39       200   13          0

```

<S-switch-E> **display msdp brief**

```

Configured  Up          Listen    Connect    Shutdown    Down
1           1           0         0          0           0
Peer's Address    State    Up/Down time    AS    SA Count    Reset Count
192.168.4.1      UP      00:15:32       200   8           0

```

# Run the **display msdp peer-status** command. You can view the detailed information about the MSDP peers. The detailed information about MSDP peers on S-switch-B is as follows:

<S-switch-B> **display msdp peer-status**

```

MSDP Peer 192.168.2.2, AS 200
Description:
Information about connection status:
  State: Up
  Up/down time: 00:15:47
  Resets: 0
  Connection interface: vlanif 1 (192.168.2.1)
  Number of sent/received messages: 16/16
  Number of discarded output messages: 0
  Elapsed time since last connection or counters clear: 00:17:51
Information about (Source, Group)-based SA filtering policy:
  Import policy: none
  Export policy: none
Information about SA-Requests:
  Policy to accept SA-Request messages: none
  Sending SA-Requests status: disable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA Cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 0/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0

```

# Run the **display pim routing-table** command. You can view the PIM routing table on a S-switch. When S1 (10.110.1.2/24) in PIM-SM1 domain and S3 (10.110.3.2/24) in PIM-SM3 domain send multicast data to G (225.1.1.1/24), Receiver (10.110.2.2/24) in PIM-SM2 domain can receive the multicast data. The information about the PIM routing tables on S-switch-B and S-switch-C is as follows:

<S-switch-B> **display pim routing-table**

```

Total 0 (*, G) entry; 1 (S, G) entry

(10.110.1.2, 225.1.1.1)
  RP: 1.1.1.1(local)
  Protocol: pim-sm, Flag: SPT EXT ACT
  UpTime: 00:00:42
  Upstream interface: vlanif 2
    Upstream neighbor: 192.168.1.1
    RPF neighbor: 192.168.1.1
  Downstream interface(s) information:

```

```

Total number of downstreams: 1
  1: vlanif 1
    Protocol: pim-sm, UpTime: 00:00:42, Expires:-

<S-switch-C> display pim routing-table
Total 1 (*, G) entry; 2 (S, G) entries

(*, 225.1.1.1)
  RP: 2.2.2.2(local)
  Protocol: pim-sm, Flag: WC RPT
  UpTime: 00:13:46
  Upstream interface: NULL,
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
    Total number of downstreams: 1
      1: vlanif 2,
        Protocol: pim-sm, UpTime: 00:13:46, Expires:-
(10.110.1.2, 225.1.1.1)
  RP: 2.2.2.2
  Protocol: pim-sm, Flag: SPT MSDP ACT
  UpTime: 00:00:42
  Upstream interface: vlanif 1
    Upstream neighbor: 192.168.2.1
    RPF neighbor: 192.168.2.1
  Downstream interface(s) information:
    Total number of downstreams: 1
      1: vlanif 2
        Protocol: pim-sm, UpTime: 00:00:42, Expires:-
(10.110.3.2, 225.1.1.1)
  RP: 2.2.2.2
  Protocol: pim-sm, Flag: SPT MSDP ACT
  UpTime: 00:00:42
  Upstream interface: vlanif 3
    Upstream neighbor: 192.168.4.2
    RPF neighbor: 192.168.4.2
  Downstream interface(s) information:
    Total number of downstreams: 1
      1: vlanif 2
        Protocol: pim-sm, UpTime: 00:00:42, Expires:-

```

## Configuration Files

- Configuration file of S-switch-B

```

#
sysname S-switch-B
#
multicast routing-enable
#
interface vlanif 2
undo shutdown
link-protocol ppp
ip address 192.168.1.2 255.255.255.0
pim sm
#
interface vlanif 1
undo shutdown
link-protocol ppp
ip address 192.168.2.1 255.255.255.0
pim sm
pim bsr-boundary
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
pim sm
#
bgp 100
router-id 1.1.1.1
peer 192.168.2.2 as-number 200

```

```
import-route ospf 1
#
ospf 1
import-route bgp
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
#
pim
c-bsr LoopBack0
c-rp LoopBack0
#
msdp
peer 192.168.2.2 connect-interface vlanif 1
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
multicast routing-enable
#
interface vlanif 1
undo shutdown
link-protocol ppp
ip address 192.168.2.2 255.255.255.0
pim sm
pim bsr-boundary
#
interface vlanif 2
undo shutdown
link-protocol ppp
ip address 192.168.3.1 255.255.255.0
pim sm
#
interface vlanif 3
undo shutdown
link-protocol ppp
ip address 192.168.4.1 255.255.255.0
pim sm
pim bsr-boundary
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
pim sm
#
bgp 200
router-id 2.2.2.2
peer 192.168.2.1 as-number 100
import-route ospf 1
#
ospf 1
import-route bgp
area 0.0.0.0
network 192.168.3.0 0.0.0.255
network 192.168.4.0 0.0.0.255
network 2.2.2.2 0.0.0.0
#
pim
c-bsr LoopBack0
c-rp LoopBack0
#
msdp
peer 192.168.2.1 connect-interface vlanif 1
peer 192.168.4.2 connect-interface vlanif 3
#
return
```

- Configuration file of S-switch-E

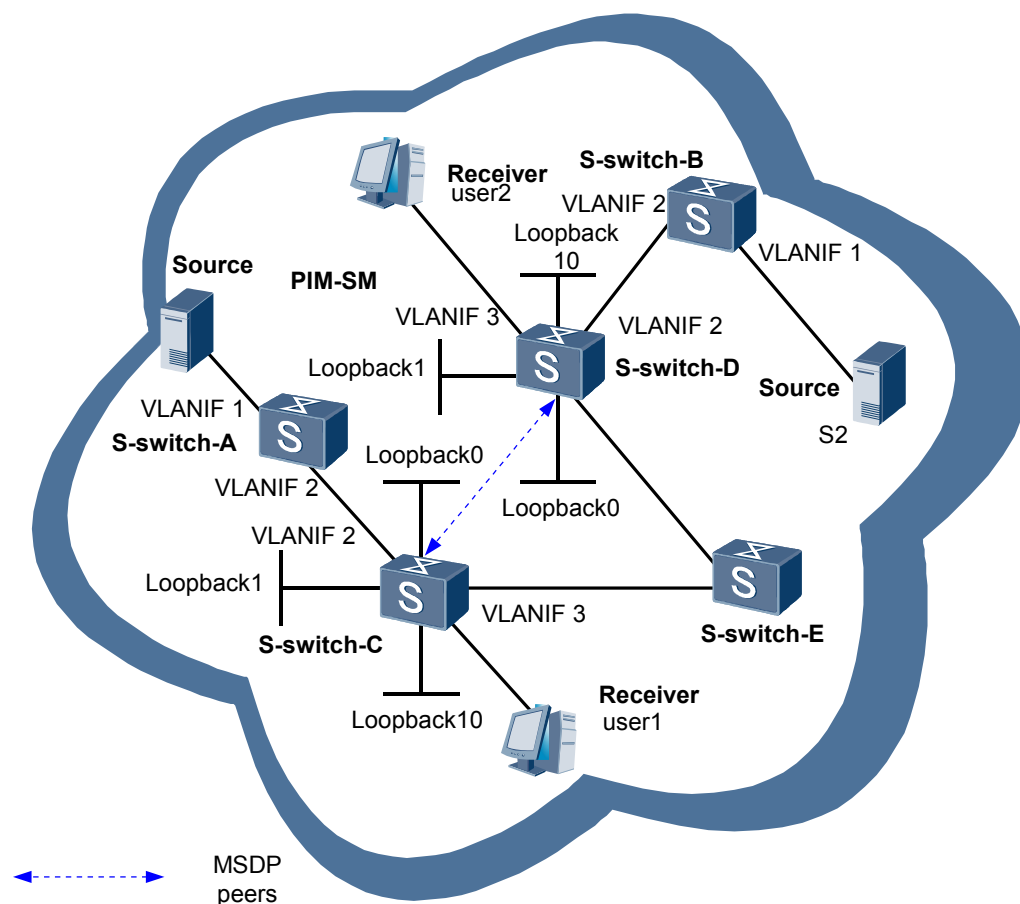
```
#
 sysname S-switch-E
#
 multicast routing-enable
#
interface vlanif 2
 undo shutdown
 link-protocol ppp
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
interface vlanif 3
 undo shutdown
 link-protocol ppp
 ip address 192.168.4.2 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.4.1 connect-interface vlanif 3
#
return
```

## 9.10.2 Example for Configuring Inter-AS Multicast by Using Static RPF Peers

### Networking Requirements

As shown in [Figure 9-2](#), there are two ASs in the network. Each AS contains one or more PIM-SM domains; and each PIM-SM domain has 0 or 1 multicast source or receiver. MSDP peer relationships are required to be set up between PIM-SM domains to share the information about multicast sources.

**Figure 9-2** Networking diagram of configuring inter-AS multicast by using static RPF peers



| S-switch   | Interface  | IP Address     | S-switch   | Interface  | IP Address     |
|------------|------------|----------------|------------|------------|----------------|
| S-switch-A | vlanif 1   | 192.168.5.2/24 | S-switch-D | vlanif 1   | 192.168.3.2/24 |
| S-switch-B | vlanif 2   | 192.168.2.2/24 |            | Loopback 0 | 2.2.2.2/32     |
| S-switch-C | vlanif 1   | 192.168.1.1/24 | S-switch-E | vlanif 2   | 192.168.2.1/24 |
|            | vlanif 2   | 192.168.4.1/24 | S-switch-F | vlanif 1   | 192.168.5.1/24 |
|            | Loopback 0 | 1.1.1.1/32     |            | Loopback 0 | 3.3.3.3/32     |

## Configuration Roadmap

Solution: set up an MSDP peer on RP in each PIM-SM domain. Set up static RPF peer among MSDP peers. Thus the transmission of source information across sources is implemented without changing unicast topology. The steps are as follows:

1. Configure an IP address for each interface, configure OSPF in the ASs, configure EBGp between ASs, and configure BGP and OSPF to import routes into each other.
2. Enable multicast on each S-switch and PIM-SM on each interface, enable IGMP on the interface connected to hosts, and configure the positions of Loopback 0 interfaces, the C-BSR, and the C-RP. The Loopback 0 interfaces on S-switch-C, S-switch-D, and S-switch-F act as C-BSRs and C-RPs of their PIM-SM domains.
3. Set up MSDP peer relationships between RPs in each domain, and the MSDP peer relationship between S-switch-C and S-switch-D and between S-switch-C and S-switch-F.
4. Specify a static RPF peer for an MSDP peer. The static RPF peers of S-switch-C are S-switch-D and S-switch-F. S-switch-D and S-switch-F has only one static RPF peer, that is,

S-switch-C. According to RPF rules, S-switch-s receive SA messages from static RPF peers.

## Data Preparation

To complete this configuration, you need the following data:

- The AS number of S-switch-A, S-switch-B and S-switch-C is 100. The router IDs of the three S-switches are 1.1.1.3, 1.1.1.2 and 1.1.1.1 respectively.
- The AS number of S-switch-D and S-switch-E is 200. The router IDs of the two S-switches are 2.2.2.2 and 2.2.2.1 respectively.
- The AS number of S-switch-F and S-switch-G is 200. The router ID of S-switch-F is 3.3.3.3.
- The name of policy adopted by S-switch-C in filtering the SA message from S-switch-D and S-switch-F is list-df.
- The name of policy adopted by S-switch-D and S-switch-F in filtering the SA message from S-switch-C is list-c.

## Configuration Procedure

### NOTE

In the example, only the commands related to the configuration of static RPF peers are mentioned.

1. Configure an IP address for each interface and a unicast routing protocol.

# As shown in [Figure 9-2](#), configure an IP address and mask for each interface. Configure OSPF in the AS. Configure EBGP between S-switch-A and S-switch-F, S-switch-B, and S-switch-E. Configure BGP and OSPF to import routes into each other. Ensure the normal communication between S-switches on the network layer. Ensure dynamic routing updates between S-switches through the unicast routing protocol. The procedures are not mentioned here.

2. Enable multicast on each S-switch and PIM-SM on each interface.

# Enable multicast on each S-switch and enable PIM-SM on each interface. The configurations of the other S-switches are similar to that of S-switch-C, and are not mentioned here.

```
[S-switch-C] multicast routing-enable
[S-switch-C] interface vlanif 1
[S-switch-C-Vlanif1] pim sm
[S-switch-C-Vlanif1] quit
[S-switch-C] interface vlanif 2
[S-switch-C-Vlanif2] pim sm
[S-switch-C-Vlanif2] quit
```

# Configure the BSR boundary on POS 0/0/1 of S-switch-A, POS 0/0/2 of S-switch-B, POS 0/0/2 of S-switch-E and POS 0/0/1 of S-switch-F. The configurations of S-switch-B, S-switch-E, and S-switch-F are similar to that of S-switch-A, and are not mentioned here.

```
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] pim bsr-boundary
[S-switch-A-Vlanif1] quit
```

3. Configure the Loopback 0 interface, C-BSR, and C-RP.

# Configure Loopback 0 interfaces and positions of the C-BSR and C-RP on S-switch-C, S-switch-D, and S-switch-F. The configurations of S-switch-D and S-switch-F are similar to that of S-switch-C, and are not mentioned here.

```
[S-switch-C] interface loopback 0
[S-switch-C-LoopBack0] ip address 1.1.1.1 255.255.255.255
[S-switch-C-LoopBack0] pim sm
```

```
[S-switch-C-LoopBack0] quit
[S-switch-C] pim
[S-switch-C-pim] c-bsr loopback 0
[S-switch-C-pim] c-rp loopback 0
[S-switch-C-pim] quit
```

4. Configure static RPF peers.

# Configure S-switch-D and S-switch-F as static RPF peers of S-switch-C.

```
[S-switch-C] ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 16 less-equal 32
[S-switch-C] msdp
[S-switch-C-msdp] peer 192.168.3.2 connect-interface vlanif 1
[S-switch-C-msdp] peer 192.168.5.1 connect-interface vlanif 2
[S-switch-C-msdp] static-rpf-peer 192.168.3.2 rp-policy list-df
[S-switch-C-msdp] static-rpf-peer 192.168.5.1 rp-policy list-df
[S-switch-C-msdp] quit
```

# Configure S-switch-C as the static RPF peer of S-switch-D and S-switch-F. The configurations of S-switch-F are similar to that of S-switch-D, and are not mentioned here.

```
[S-switch-D] ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16 less-equal 32
[S-switch-D] msdp
[S-switch-D-msdp] peer 192.168.1.1 connect-interface vlanif 1
[S-switch-D-msdp] static-rpf-peer 192.168.1.1 rp-policy list-c
```

5. Verify the configuration.

# Run the **display bgp peer** command. You can view the BGP peer relationship between S-switches. If there is no output information on S-switch-C, it indicates that the BGP peer relationship is not set up between S-switch-C and S-switch-D, and between S-switch-C and S-switch-F.

# Run the **display msdp brief** command. You can view the MSDP peer relationship between S-switches. When S1 in PIM-SM1 domain sends a multicast packet, the receivers in PIM-SM2 and PIM-SM3 domains can receive it. For example, information about MSDP peers on S-switch-C, S-switch-D, and S-switch-F is as follows:

```
<S-switch-C> display msdp brief
Configured Up Listen Connect Shutdown Down
2 2 0 0 0 0
Peer's Address State Up/Down time AS SA Count Reset Count
192.168.3.2 UP 01:07:08 ? 8 0
192.168.5.1 UP 00:16:39 ? 13 0
<S-switch-D> display msdp brief
Configured Up Listen Connect Shutdown Down
1 1 0 0 0 0
Peer's Address State Up/Down time AS SA Count Reset Count
192.168.1.1 UP 01:07:09 ? 8 0
<S-switch-F> display msdp brief
Configured Up Listen Connect Shutdown Down
1 1 0 0 0 0
Peer's Address State Up/Down time AS SA Count Reset Count
192.168.4.1 UP 00:16:40 ? 13 0
```

## Configuration Files

Configuration file of S-switch-C is as follows:

```
#
sysname S-switch-C
#
multicast routing-enable
#
interface vlanif 1
undo shutdown
link-protocol ppp
ip address 192.168.1.1 255.255.255.0
```

```
pim sm
#
interface vlanif 2
undo shutdown
link-protocol ppp
ip address 192.168.4.1 255.255.255.0
pim sm
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.4.0 0.0.0.255
network 1.1.1.1 0.0.0.0
#
pim
c-bsr LoopBack0
c-rp LoopBack0
#
ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 16 less-equal 32
#
msdp
peer 192.168.3.2 connect-interface vlanif 1
peer 192.168.5.1 connect-interface vlanif 2
static-rpf-peer 192.168.3.2 rp-policy list-df
static-rpf-peer 192.168.5.1 rp-policy list-df
#
return
```

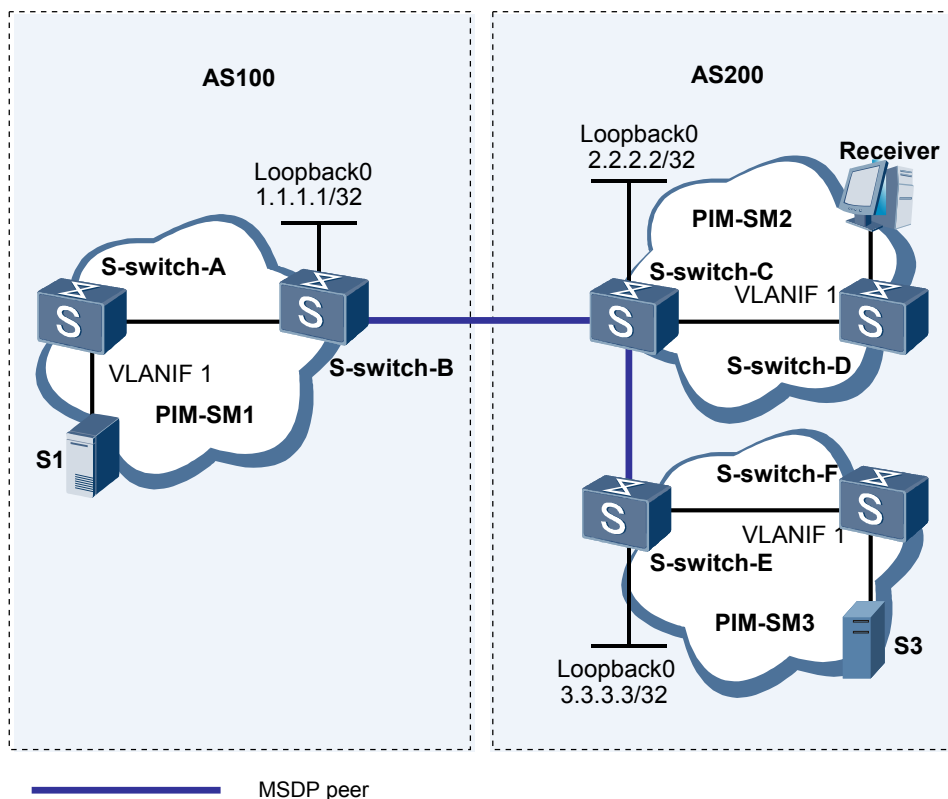
The configuration files of S-switch-D and S-switch-F are similar to the files mentioned previously, and are not mentioned here.

### 9.10.3 Example for Configuring an Anycast RP

#### Networking Requirements

As shown in [Figure 9-3](#), the PIM-SM domain has multiple multicast sources and receivers. It is required to set up MSDP peers in the PIM-SM domain to implement RP load balancing.

**Figure 9-3** Networking diagram of configuring anycast RP



| S-switch   | Interface   | IP Address     | S-switch   | Interface   | IP Address     |
|------------|-------------|----------------|------------|-------------|----------------|
| S-switch-A | vlanif 1    | 10.110.5.1/24  | S-switch-D | vlanif 1    | 192.168.3.1/24 |
|            | vlanif 2    | 10.110.1.2/24  |            | vlanif 2    | 10.110.2.1/24  |
| S-switch-B | vlanif 1    | 10.110.6.1/24  | S-switch-E | vlanif 1    | 192.168.3.2/24 |
|            | vlanif 2    | 10.110.2.2/24  |            | vlanif 2    | 192.168.1.2/24 |
| S-switch-C | vlanif 1    | 192.168.1.1/24 | S-switch-F | vlanif 1    | 192.168.3.2/24 |
|            | vlanif 2    | 10.110.1.1/24  |            | vlanif 2    | 192.168.1.2/24 |
|            | vlanif 3    | 10.110.4.1/24  |            | vlanif 3    | 10.110.3.1/24  |
|            | Loopback 0  | 1.1.1.1/32     |            | Loopback 0  | 2.2.2.2/32     |
|            | Loopback 1  | 3.3.3.3/32     |            | Loopback 1  | 4.4.4.4/32     |
|            | Loopback 10 | 10.1.1.1/32    |            | Loopback 10 | 10.1.1.1/32    |

## Configuration Roadmap

**Solution:** Configure an anycast RP. The receiver sends a Join message to the RP closest to the topology. The source sends a Register message to the RP closest to the topology. The steps are as follows:

1. Configure an IP address for each interface and configure OSPF in the PIM-SM area.
2. Enable multicast on each S-switch and PIM-SM on each interface and enable IGMP on the interface connected to hosts.
3. Configure the same loopback interface address for S-switch-C and S-switch-D. Configure the C-BSR on Loopback 1 interfaces and the C-RP on Loopback 10 interfaces.
4. Configure MSDP peers on Loopback 0 interfaces of S-switch-C and S-switch-D. According to RPF rules, S-switches receive SA messages from the source RP.

## Data Preparation

To complete this configuration, you need the following data:

- Address of group G is 225.1.1.1/24.
- Router ID of S-switch-C is 1.1.1.1.
- Router ID of S-switch-D is 2.2.2.2.

## Configuration Procedure

### NOTE

In the example, only the commands related to the configuration of an anycast RP are mentioned.

1. Configure an IP address on each interface and a unicast routing protocol.  
#Configure an IP address and mask to each interface according to [Figure 9-3](#). Configure OSPF. Ensure the communication between S-switches on the network layer. Ensure dynamic routing updates between S-switches by means of the unicast routing protocol. The procedures are not mentioned here.

2. Enable multicast on each S-switch and configure PIM-SM on each interface.  
# Enable multicast on each S-switch, and enable PIM-SM on each interface. Enable IGMP on the interface connected to hosts. The configurations of other S-switches are similar to that of S-switch-C, and are not mentioned here.

```
[S-switch-C] multicast routing-enable
[S-switch-C] interface vlanif 3
[S-switch-C-Vlanif3] igmp enable
[S-switch-C-Vlanif3] pim sm
[S-switch-C-Vlanif3] quit
[S-switch-C] interface vlanif 2
[S-switch-C-Vlanif2] pim sm
[S-switch-C-Vlanif2] quit
[S-switch-C] interface vlanif 1
[S-switch-C-Vlanif1] pim sm
[S-switch-C-Vlanif1] quit
```

3. Configure Loopback 1 and Loopback 10 interfaces, and the C-BSR and C-RP.  
# Configure the address of Loopback 1 interface and the address of Loopback 10 interface on S-switch C and S-switch-D respectively. Configure the C-BSP on Loopback 1 and the C-RP on Loopback 10. The configurations of S-switch-D are similar to that of S-switch-C, and are not mentioned here.

```
[S-switch-C] interface loopback 1
[S-switch-C-LoopBack1] ip address 3.3.3.3 255.255.255.255
[S-switch-C-LoopBack1] pim sm
[S-switch-C-LoopBack1] quit
[S-switch-C] interface loopback 10
[S-switch-C-LoopBack10] ip address 10.1.1.1 255.255.255.255
[S-switch-C-LoopBack10] pim sm
[S-switch-C-LoopBack10] quit
[S-switch-C] pim
[S-switch-C-pim] c-bsr loopback 1
[S-switch-C-pim] c-rp loopback 10
[S-switch-C-pim] quit
```

4. Verify the configuration.  
# Run the **display msdp brief** command. You can view the MSDP peer relationships between S-switches. The MSDP peer relationship between S-switch-C and S-switch-D is as follows:

```
[S-switch-C] display msdp brief
Configured  Up      Listen      Connect     Shutdown    Down
```

| 1              | 1     | 0            | 0  | 0        | 0           |
|----------------|-------|--------------|----|----------|-------------|
| Peer's Address | State | Up/Down time | AS | SA Count | Reset Count |
| 2.2.2.2        | Up    | 00:10:17     | ?  | 0        | 0           |

| 1              | 1     | 0            | 0  | 0        | 0           |
|----------------|-------|--------------|----|----------|-------------|
| Peer's Address | State | Up/Down time | AS | SA Count | Reset Count |
| 1.1.1.1        | Up    | 00:10:18     | ?  | 0        | 0           |

# Run the **display pim routing-table** command. You can view PIM routes on a S-switch. In the PIM-SM domain, S1 (10.110.5.100/24) sends multicast information to G (225.1.1.1). User 1 that joins G receives the multicast data sent to G. Comparing with the display of PIM routes on S-switch-C and S-switch-D, you can find that the valid RP is S-switch-C. That is, S1 registers with S-switch-C, and User 1 sends Join messages to S-switch-C.

```
<S-switch-C> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry
(*, 225.1.1.1)
  RP: 10.1.1.1 (local)
  Protocol: pim-sm, Flag: WC
  UpTime: 00:28:49
  Upstream interface: Register
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif1
      Protocol: static, UpTime: 00:28:49, Expires: -
(10.110.5.1, 225.1.1.1)
  RP: 10.1.1.1 (local)
  Protocol: pim-sm, Flag: SPT 2MSDP ACT
  UpTime: 00:02:26
  Upstream interface: Gigabitvlanif 0
    Upstream neighbor: 10.110.1.2
    RPF prime neighbor: 10.110.1.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif1
      Protocol: pim-sm, UpTime: 00:02:26, Expires: -
<S-switch-D> display pim routing-table
```

There is no display.

# User 1 leaves G, and S1 stops sending multicast data to G. You can run the **reset multicast routing-table all** and **reset multicast forwarding-table all** commands to clear the multicast routing entries and multicast forwarding entries on S-switch-C.

# User 2 joins G, and S2 (10.110.6.100/24) sends multicast data to G. Comparing with the display of PIM routes on S-switch-C and S-switch-D, you can find that the valid RP is S-switch-D. That is, S2 registers with S-switch-D, and User 2 sends Join messages to S-switch-D.

```
<S-switch-C> reset multicast routing-table all
<S-switch-C> reset multicast forwarding-table all
```

There is no display.

```
<S-switch-D> display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry
(*, 225.1.1.1)
  RP: 10.1.1.1 (local)
  Protocol: pim-sm, Flag: WC RPT
  UpTime: 00:07:23
  Upstream interface: NULL,
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif3,
      Protocol: pim-sm, UpTime: 00:07:23, Expires:-
```

```

(10.110.6.100, 225.1.1.1)
  RP: 10.1.1.1 (local)
  Protocol: pim-sm, Flag: SPT 2MSDP ACT
  UpTime: 00:10:20
  Upstream interface: vlanif2
    Upstream neighbor: 10.110.2.2
    RPF prime neighbor: 10.110.2.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: vlanif3
      Protocol: pim-sm, UpTime: 00:10:22, Expires: -

```

## Configuration Files

Configuration file of S-switch-C is as follows.

```

#
 sysname S-switch-C
#
 multicast routing-enable
#
interface vlanif3
 undo shutdown
 ip address 10.110.4.1 255.255.255.0
 igmp enable
 pim sm
#
interface vlanif2
 undo shutdown
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
interface vlanif 1
 undo shutdown
 link-protocol ppp
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
interface LoopBack10
 ip address 10.1.1.1 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 10.110.4.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
pim
 c-bsr LoopBack1
 c-rp LoopBack10
#
msdp
 originating-rp LoopBack0
 peer 2.2.2.2 connect-interface LoopBack0
#
return

```

The configuration of S-switch-D is similar to that of S-switch-C, and is not mentioned here.