CHAPTER 43

Configuring IP Multicast Routing

This chapter describes how to configure IP multicast routing on the Cisco ME 3400E Ethernet Access switch. IP multicasting is a more efficient way to use network resources, especially for bandwidth-intensive services such as audio and video. IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP *multicast group address.*

Any host, regardless of whether it is a member of a group, can sent to a group. However, only the members of a group receive the message.

To use this feature, the switch must be running the metro IP access image.

Note For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*

This chapter consists of these sections:

For information on configuring the Multicast Source Discovery Protocol (MSDP), see Chapter 44, "Configuring MSDP."

Understanding Cisco's Implementation of IP Multicast Routing

- Internet Group Management Protocol (IGMP) is used among hosts on a LAN and the routers (and multilayer switches) on that LAN to track the multicast groups of which hosts are members.

  Protocol-Independent Multicast (PIM) protocol is used among routers and multilayer switches to track which multicast packets to forward to each other and to their directly connected LANs.

According to IPv4 multicast standards, the MAC destination multicast address begins with 0100:5e and is appended by the last 23 bits of the IP address. On the Cisco ME switch, if the multicast packet does not match the switch multicast address, the packets are treated in this way:

If the packet has a multicast IP address and a unicast MAC address, the packet is forwarded in software. This can occur because some protocols on legacy devices use unicast MAC addresses with multicast IP addresses.

If the packet has a multicast IP address and an unmatched multicast MAC address, the packet is dropped.

This section contains this information:

Understanding IGMP, page 43-2

Understanding PIM, page 43-3

Understanding IGMP

operating. This protocol defines the querier and host roles:

- A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver that sends report messages (in response to query messages) to inform a querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use IGMP messages to join and leave multicast groups.

Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time. How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it can be very short-lived. Membership in a group can constantly change. A group that has members can have no activity.

IP multicast traffic uses group addresses, which are class D addresses. The high-order bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 through 239.255.255.255. Multicast addresses in the range 224.0.0.0 to 24.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are sent using these IP multicast group addresses:

IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).

IGMP group-specific queries are destined to the group IP address for which the switch is querying.

IGMP group membership reports are destined to the group IP address for which the switch is reporting.

IGMP Version 2 (IGMPv2) leave messages are destined to the address 224.0.0.2 (all-multicast-routers on a subnet). In some old host IP stacks, leave messages might be destined to the group IP address rather than to the all-routers address.

IGMP Version 1

IGMP Version 2

Understanding PIM

protocol-independent

Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification

Protocol Independent Multicast (PIM): Motivation and Architecture

Protocol Independent Multicast (PIM), Dense Mode Protocol Specification

Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification

draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2

draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode

Bootstrap Router, page 43-6

Multicast Forwarding and Reverse Path Check, page 43-7

PIMv2 includes these improvements over PIMv1:

A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This single RP compares to multiple active RPs for the same group in PIMv1.

A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism that enables routers and multilayer switches to dynamically learn the group-to-RP mappings.

- Sparse mode and dense mode are properties of a group, as opposed to an interface. We strongly recommend sparse-dense mode, as opposed to either sparse mode or dense mode only.
- PIM join and prune messages have more flexible encoding for multiple address families.
- A more flexible hello packet format replaces the query packet to encode current and future capability options.
- Register messages to an RP specify whether they are sent by a border router or a designated router.
- PIM packets are no longer inside IGMP packets; they are standalone packets.

PIM Modes

PIM DM

PIM SM

[DR]) to complete the shared tree path from the source to the receiver. When using a shared tree, sources must send their traffic to the RP so that the traffic reaches all receivers.

Prune messages are sent up the distribution tree to prune multicast group traffic. This action permits branches of the shared tree or SPT that were created with explicit join messages to be torn down when they are no longer needed.

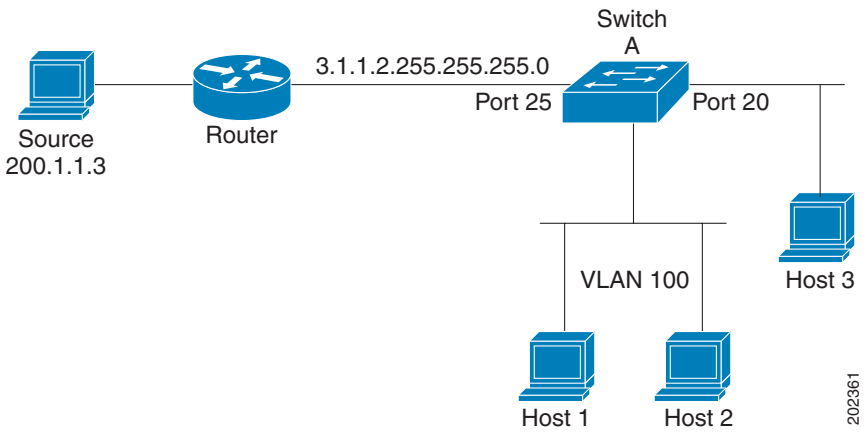
traffic between distribution routers. You also need to configure a routed uplink port on the switch. The switch uplink port cannot be used with SVIs. If you need PIM for an SVI uplink port, you should upgrade to the IP services feature set.

You must also configure EIGRP stub routing when configuring PIM stub routing on the switch. For more information, see the "Configuring EIGRP Stub Routing" section on page 36-40.

The redundant PIM stub router topology is not supported. The redundant topology exists when there is more than one PIM router forwarding multicast traffic to a single access domain. PIM messages are blocked, and the PIM assert and designated router election mechanisms are not supported on the PIM passive interfaces. Only the nonredundant access router topology is supported by the PIM stub feature. By using a nonredundant topology, the PIM passive interface assumes that it is the only interface and designated router on that access domain.

In Figure 43-1, Switch A routed uplink port 25 is connected to the router and PIM stub routing is enabled on the VLAN 100 interfaces and on Host 3. This configuration allows the directly connected hosts to receive traffic from multicast source 200.1.1.3. See the "Configuring PIM Stub Routing" section on page 43-12 for more information.

Figure 43-1 PIM Stub Router Configuration



IGMP Helper

igmp helper help-address

Auto-RP

Bootstrap Router

Multicast Forwarding and Reverse Path Check

1.

2.

3.

Figure 43-2 RPF Check

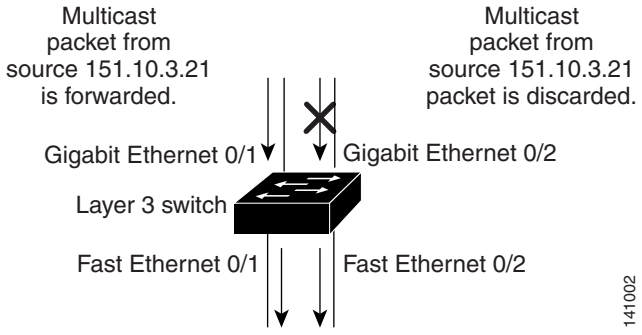


Table 43-1 Routing Table Example for an RPF Check

Network	Port
151.10.0.0/16	Gigabit Ethernet 0/1
198.14.32.0/32	Fast Ethernet 0/1
204.1.16.0/24	Fast Ethernet 0/2

(*,G) joins (which are shared-tree states) are sent toward the RP.

Dense-mode PIM uses only source trees and use RPF as previously described.

Default Multicast Routing Configuration

Default Multicast Routing Configuration

Feature	Default Setting

Default Multicast Routing Configuration (continued)

Multicast Routing Configuration Guidelines

-
-

PIMv1 and PIMv2 Interoperability

-
-

Auto-RP and BSR Configuration Guidelines

-
-
-
-
-
-

Configuring Basic Multicast Routing

Note

Note

Beginning in privileged EXEC mode, follow these steps to enable IP multicasting, to configure a PIM version, and to configure a PIM mode. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	
	ip multicast-routing distributed	
	interface	**no switchport** **interface vlan**
Step 4	**no shutdown**	
Step 5	**1 | 2**	
Step 6	{ | | }	Enable a PIM mode on the interface. By default, no mode is configured. The keywords have these meanings: —Enables dense mode of operation. —Enables sparse mode of operation. If you configure sparse-mode, you must also configure an RP. For more information, see the "Configuring a Rendezvous Point" section on page 43-22. —Causes the interface to be treated in the mode in which the group belongs. Sparse-dense-mode is the recommended setting.
Step 7		Return to privileged EXEC mode.
Step 8		
Step 9	**copy running-config startup-config**	

no ip multicast-routing distributed
no ip pim version
no ip pim

Configuring PIM Stub Routing

PIM Stub Routing Configuration Guidelines

-
-
-
-

Enabling PIM Stub Routing

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		

spare-dense-mode enabled.

```
Switch(config)# ip multicast-routing distributed
                interface GigabitEthernet0/25
Switch(config-if)# no switchport
                   ip address 3.1.1.2 255.255.255.0
                   ip pim sparse-dense-mode
                   exit
                interface vlan100
                   ip pim passive
                   exit
                interface GigabitEthernet0/20
                   ip pim passive
                   exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/20
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

```
Switch# show
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet0/20 v2/P 0 30 1 10.1.1.1
```

Configuring Source-Specific Multicast

SSM Components Overview

-
-

How SSM Differs from Internet Standard Multicast

SSM IP Address Range

SSM Operations

-
-
-

IGMPv3 Host Signalling

Configuration Guidelines

Legacy Applications Within the SSM Range Restrictions

Address Management Restrictions

IGMP Snooping and CGMP Limitations

State Maintenance Limitations

Configuring SSM

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4	ip igmp version 3	

Monitoring SSM

Command	Purpose
show ip igmp groups detail	
show ip mroute	

Configuring Source Specific Multicast Mapping

-
-
-
-

Configuration Guidelines and Restrictions

-
-
-
-

SSM Mapping Overview

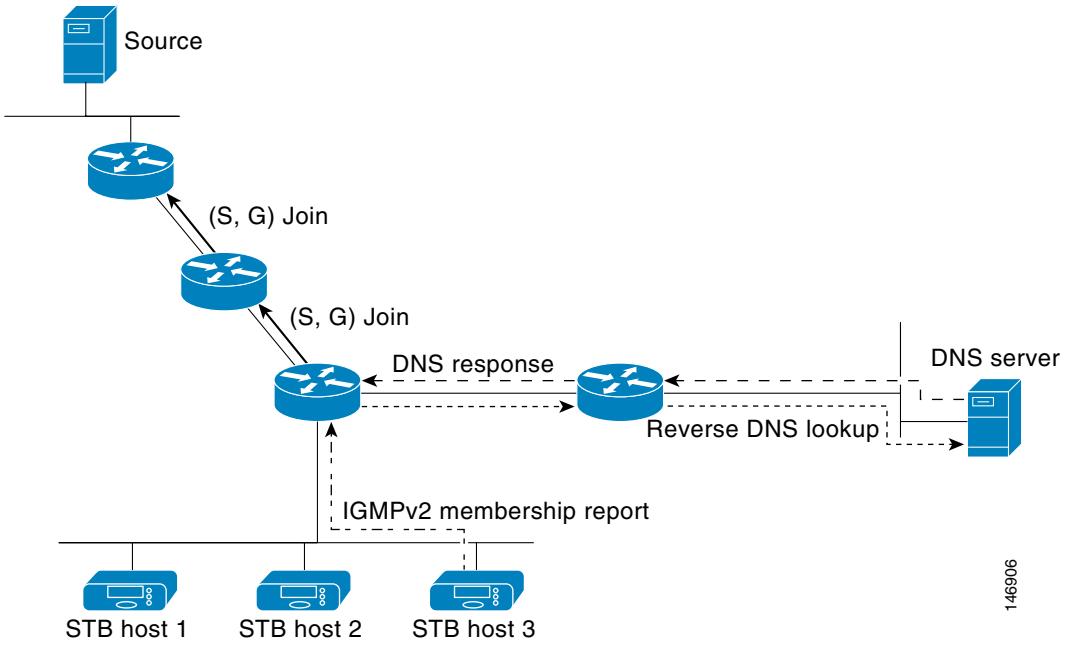
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

With static SSM mapping, you can configure the last hop router to use a static map to determine the sources that are sending to groups. Static SSM mapping requires that you configure ACLs to define group ranges. Then you can map the groups permitted by those ACLs to sources by using the global configuration command.

You can configure static SSM mapping in smaller networks when a DNS is not needed or to locally override DNS mappings. When configured, static SSM mappings take precedence over DNS mappings.

DNS-Based SSM Mapping

DNS-Based SSM-Mapping




```
G4.G3.G2.G1 [multicast-domain] [timeout       source-address-1
         source-address-2
         source-address-n
```

Configuring Static SSM Mapping

	Command	Purpose
Step 1		
Step 2		**Note** mapping.
Step 3	**no ip igmp ssm-map query dns**	**ip igmp ssm-map**
	ip igmp ssm-map static	**ip igmp ssm-map static**
	end	
	show running-config	
	copy running-config startup-config	

Configuring DNS-Based SSM Mapping

configure terminal	
ip igmp ssm-map enable	

	Command	Purpose
Step 3		Note
Step 4		
Step 5		
Step 6		
Step 7		
Step 8		
Step 9		

Configuring Static Traffic Forwarding with SSM Mapping

	Command	Purpose
Step 1		
Step 2	*type number*	
	group-address	

Command	Purpose

html#wp1047772

Configuring a Rendezvous Point

-
-
-

Manually Assigning an RP to Multicast Groups

source-wildcard	*access-list-number* *source* *source-wildcard*

```
ip pim rp-address 147.106.6.22 1
```

Preventing Join Messages to False RPs, page 43-26 (optional)

Filtering Incoming RP Announcement Messages, page 43-27 (optional)

For overview information, see the "Auto-RP" section on page 43-6.

Setting up Auto-RP in a New Internetwork

Adding Auto-RP to an Existing Sparse-Mode Cloud

	Command	Purpose
Step 1		
Step 2		
Step 3		• • • •
Step 4		• • • •

	Command	Purpose
Step 5		
Step 6		
Step 7		
Step 8		

Preventing Join Messages to False RPs

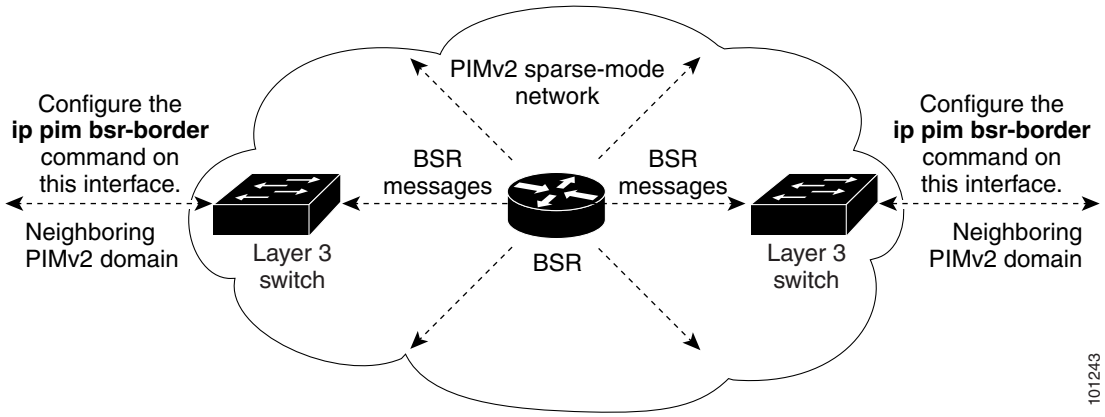
```
access-list 1 permit 224.0.1.39
access-list 1 permit 224.0.1.40
```

Filtering Incoming RP Announcement Messages

	Command	Purpose
Step 1		
Step 2		
Step 3		• • • • • •
Step 4		
Step 5		
Step 6		

```
ip pim rp-announce-filter rp-list 10 group-list 20
access-list 10 permit host 172.16.5.1
access-list 10 permit host 172.16.2.1
access-list 20 deny 239.0.0.0 0.0.255.255
access-list 20 permit 224.0.0.0 15.255.255.255
```


Constraining PIMv2 BSR Messages



hash-mask-length priority	*interface-id,* *hash-mask-length* *priority*

```
ip address 172.21.24.18 255.255.255.0
ip pim sparse-dense-mode
ip pim bsr-candidate gigabitethernet0/2 30 10
```


	Command	Purpose
Step 5		
Step 6		

```
ip pim rp-candidate gigabitethernet0/2 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
```

Using Auto-RP and a BSR

-
-

	Command	Purpose
Step 1		• • •
Step 2		

Monitoring the RP Mapping Information

-
-
-

Troubleshooting PIMv1 and PIMv2 Interoperability Problems

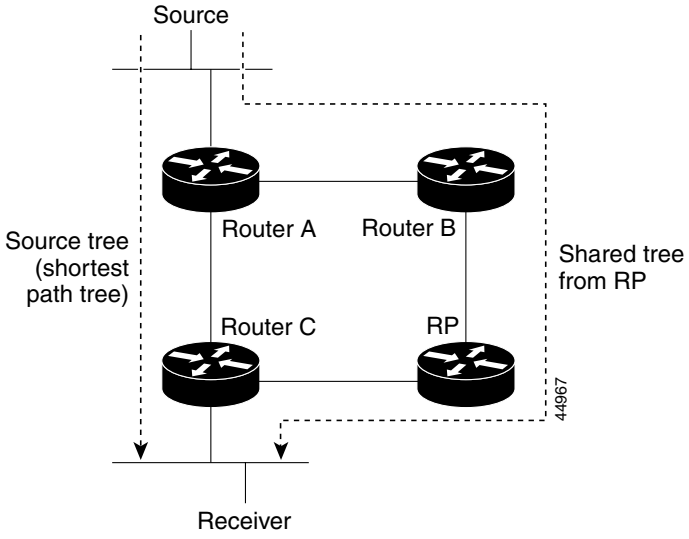
1.
2.

Configuring Advanced PIM Features

-
-
-

Understanding PIM Shared Tree and Source Tree

Figure 43-5 Shared Tree and Source Tree (Shortest-Path Tree)



1.
2.
3.
4.
5.
6.
7.
8.

Delaying the Use of PIM Shortest-Path Tree

	Command	Purpose
Step 1		
Step 2		• • • •
Step 3		• Note • •

	Command	Purpose
Step 4		
Step 5		
Step 6		

Modifying the PIM Router-Query Message Interval

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		

Configuring Optional IGMP Features

-
-
-

-
-
-
-
-

Default IGMP Configuration

Default IGMP Configuration

Feature	Default Setting

Configuring the Switch as a Member of a Group

Caution

	Command	Purpose
Step 1		
Step 2		
Step 3		

ip igmp join-group

```
ip igmp join-group 255.2.2.2
```

exit	

	Command	Purpose
Step 6		• • • •
Step 7		
Step 8		
Step 9		

no ip igmp access-group

Changing the IGMP Version

	Command	Purpose
Step 1		
Step 2		
Step 3		

	Command	Purpose
Step 4		Note
Step 5		
Step 6		
Step 7		

Modifying the IGMP Host-Query Message Interval

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		

Changing the IGMP Query Timeout for IGMPv2

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		

Changing the Maximum Query Response Time for IGMPv2

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		

	Command	Purpose
Step 5		
Step 6	*interface-id*	
Step 7		

Configuring the Switch as a Statically Connected Member

-
-

L

	Command	Purpose
Step 1		
Step 2	*interface-id*	
Step 3		
Step 4	*group-address*	
Step 5		
Step 6	*interface-id*	
Step 7		

group-address

Configuring Optional Multicast Routing Features

-
-

Configuring sdr Listener Support

Enabling sdr Listener Support

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		

Limiting How Long an sdr Cache Entry Exists

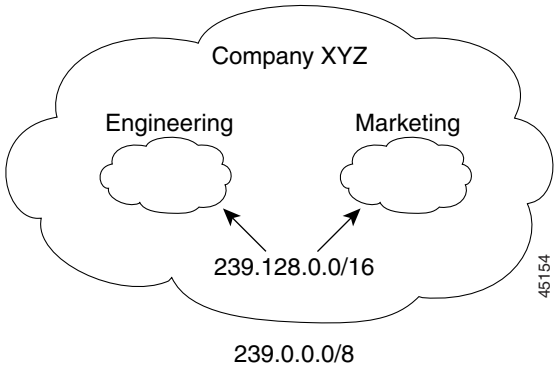
	Command	Purpose
Step 1		Enter global configuration mode.
Step 2		Limit how long an sdr cache entry stays active in the cache. By default, entries are never deleted from the cache. For , the range is 1 to 4294967295.
Step 3		Return to privileged EXEC mode.
Step 4		Verify your entries.
Step 5		(Optional) Save your entries in the configuration file.

Configuring an IP Multicast Boundary

Note

shows that Company XYZ has an administratively-scoped boundary set for the multicast address range 239.0.0.0/8 on all routed interfaces at the perimeter of its network. This boundary prevents any multicast traffic in the range 239.0.0.0 through 239.255.255.255 from entering or leaving the network. Similarly, the engineering and marketing departments have an administratively-scoped boundary of 239.128.0.0/16 around the perimeter of their networks. This boundary prevents multicast traffic in the range of 239.128.0.0 through 239.128.255.255 from entering or leaving their respective networks.

Figure 43-6 Administratively-Scoped Boundaries



	Command	Purpose
Step 7		
Step 8		

Clearing Caches, Tables, and Databases

Commands for Clearing Caches, Tables, and Databases

Command	Purpose
*	
clear ip pim auto-rp	
clear ip sdr “ ”	

Displaying System and Network Statistics

Note

Table 43-7 Commands for Displaying System and Network Statistics

show ip mpacket **detail**	
show ip mroute **summary count active**	
show ip pim interface count	
show ip pim neighbor	
show ip pim rp	
show ip rpf	
show ip sdr “ ” detail	

Table 43-8 Commands for Monitoring IP Multicast Routing
