CHAPTER 22

Configuring PIM Snooping

This chapter describes how to configure protocol independent multicast (PIM) snooping on the ME3600X/ME3800X switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Master Command List*, Release 15.2(2)S

This chapter consists of these sections:

Understanding How PIM Snooping Works

In networks where a Layer 2 switch interconnects several routers, such as an Internet exchange point (IXP), the switch floods IP multicast packets on all multicast router ports by default, even if there are no multicast receivers downstream. With PIM snooping enabled, the switch restricts multicast packets for each IP multicast group to only those multicast router ports that have downstream receivers joined to that group. When you enable PIM snooping, the switch learns which multicast router ports need to receive the multicast traffic within a specific VLAN by listening to the PIM hello messages, PIM join and prune messages, and bidirectional PIM designated forwarder-election messages.

Note To use PIM snooping, you must enable IGMP snooping on the switch. IGMP snooping restricts multicast traffic that exits through the LAN ports to which hosts are connected. IGMP snooping does not restrict traffic that exits through the LAN ports to which one or more multicast routers are connected.

The following illustrations show the flow of traffic and flooding that results in networks without PIM snooping enabled and the flow of traffic and traffic restriction when PIM snooping is enabled.

Figure 22-1 shows the flow of a PIM join message without PIM snooping enabled. In the figure, the switches flood the PIM join message intended for Router B to all connected routers.

Figure 22-1 PIM Join Message Flow without PIM Snooping

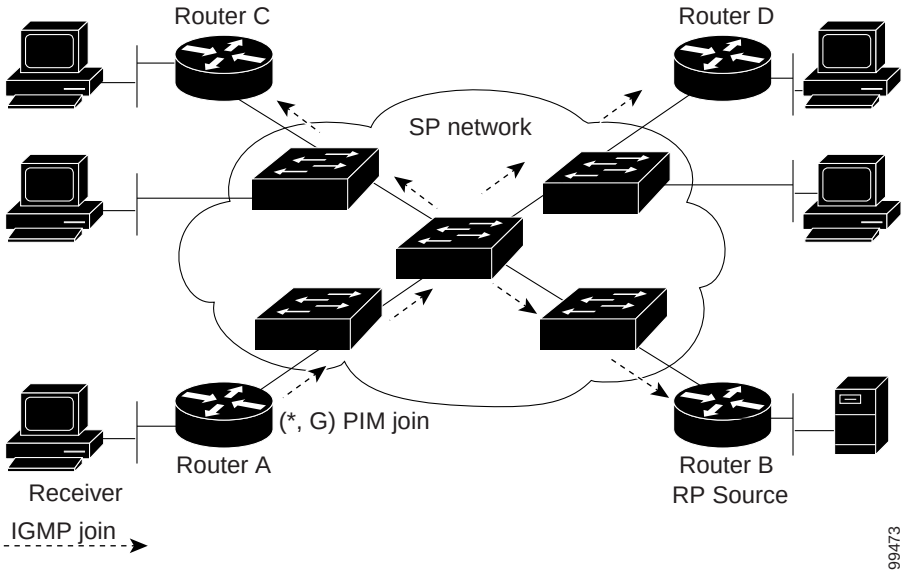


Figure 22-2 shows the flow of a PIM join message with PIM snooping enabled. In the figure, the switches restrict the PIM join message and forward it only to the router that needs to receive it (Router B).

Figure 22-2 PIM Join Message Flow with PIM Snooping

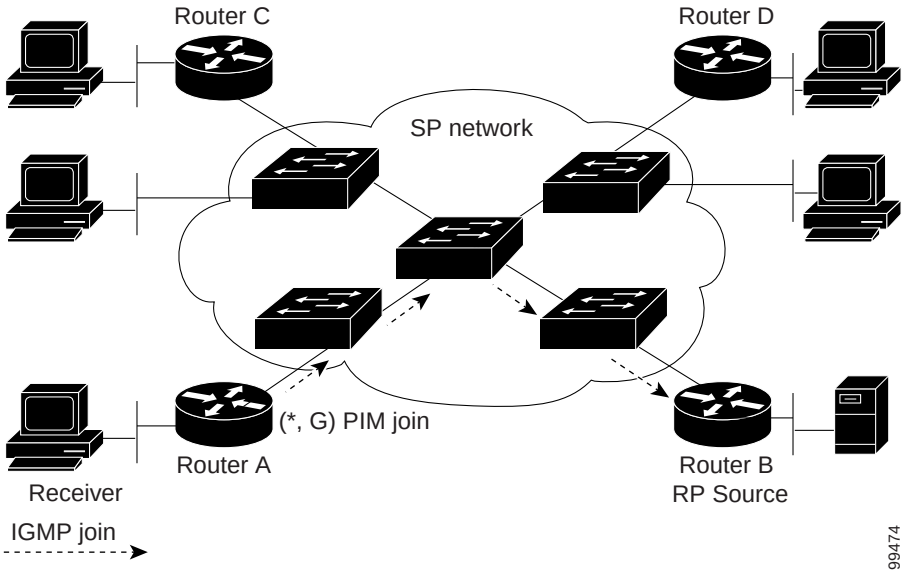


Figure 22-3 shows the flow of data traffic without PIM snooping enabled. In the figure, the switches flood the data traffic intended for Router A to all connected routers.

Figure 22-3 Data Traffic Flow without PIM Snooping

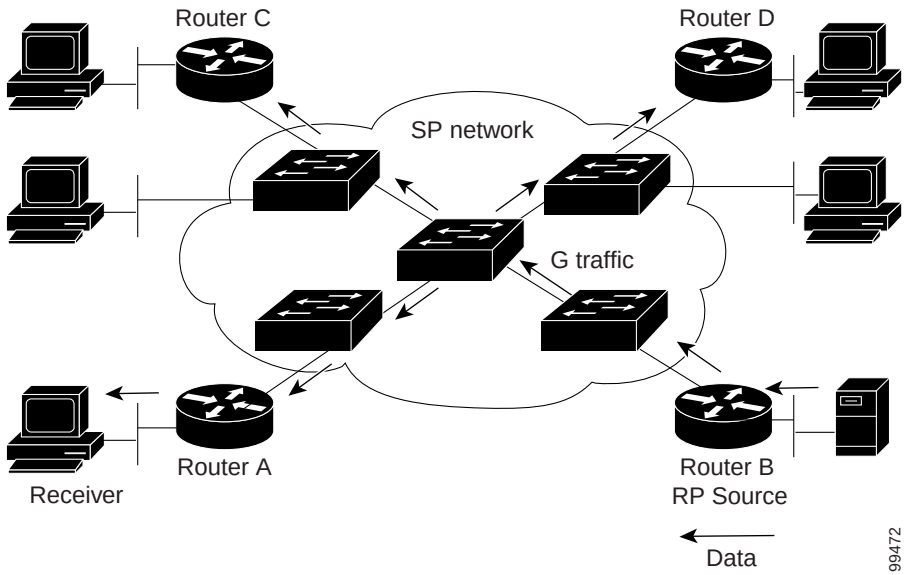
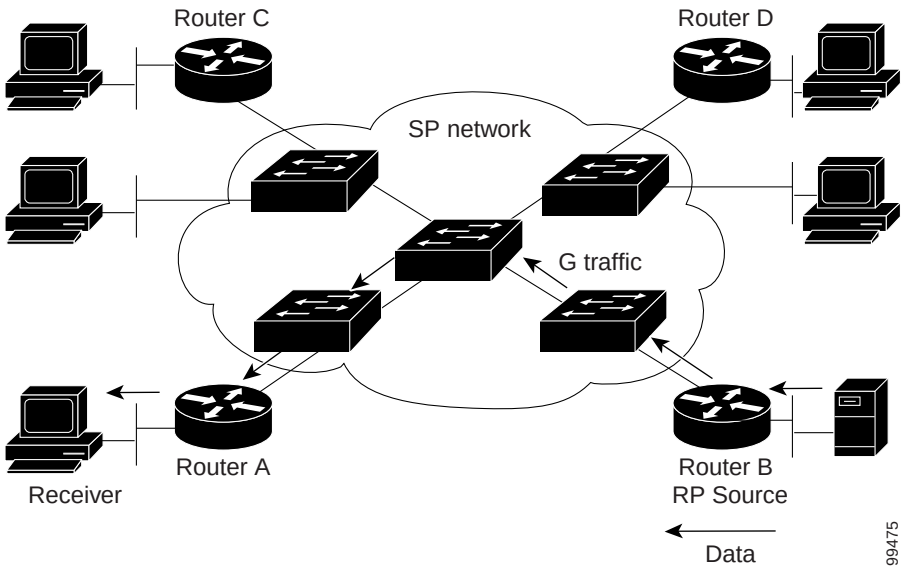


Figure 22-4 shows the flow of data traffic with PIM snooping enabled. In the figure, the switches forward the data traffic only to the router that needs to receive it (Router A).

Figure 22-4 Data Traffic Flow with PIM Snooping



Default PIM Snooping Configuration

PIM snooping is disabled by default.

PIM Snooping Configuration Guidelines and Restrictions

When configuring PIM snooping, follow these guidelines and restrictions:

- To enable PIM snooping IGMP snooping must always be enabled.
- When you use the PIM-sparse mode (PIM-SM) feature, downstream routers only see traffic if they previously indicated interest through a PIM join or prune message. An upstream router only sees traffic if it was used as an upstream router during the PIM join or prune process.
- Join or prune messages are not flooded on all router ports but are sent only to the port corresponding to the upstream router mentioned in the payload of the join or prune message.
- Bidirectional mode is not supported for PIM snooping.
- Dense group mode traffic is seen as unknown traffic and is dropped.
- The AUTO-RP groups (224.0.1.39 and 224.0.1.40) are always flooded.
- PIM snooping and IGMP snooping can be enabled at the same time in a VLAN. Either RGMP or PIM snooping can be enabled in a VLAN but not both.
- Any non-PIMv2 multicast router will receive all traffic.
- You can enable or disable PIM snooping on a per-VLAN basis.
- All mroute and router information is timed out based on the hold-time indicated in the PIM hello and join/prune control packets. All mroute state and neighbor information is maintained per VLAN.

Configuring PIM Snooping

These sections describe how to configure PIM snooping:

- Enabling PIM Snooping Globally, page 22-4
- Enabling PIM Snooping in a VLAN, page 22-5
- Disabling PIM Snooping Designated-Router Flooding, page 22-6

Enabling PIM Snooping Globally

To enable PIM snooping globally, perform this task:

	Command	Purpose
Step 1	**ip pim snooping**	Enables PIM snooping.
	no ip pim snooping	Disables PIM snooping.
Step 2	**end**	Exits configuration mode.
Step 3	**show ip pim snooping**	Verifies the configuration.

This example shows how to enable PIM snooping globally and verify the configuration:

```
Switch(config)# ip pim snooping
Switch(config)# end
Switch# show ip pim snooping
Global runtime mode: Enabled
Global admin mode  : Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 10
Switch#
```

Note You do not need to configure an IP address or IP PIM in order to run PIM snooping.

Enabling PIM Snooping in a VLAN

To enable PIM snooping in a VLAN, perform this task:

	Command	Purpose
Step 1	**interface vlan** *vlan_ID*	Selects a VLAN interface.
Step 2	**ip pim snooping**	Enables PIM snooping.
	no ip pim snooping	Disables PIM snooping.
Step 3	**end**	Exits configuration mode.
Step 4	**show ip pim snooping**	Verifies the configuration.

This example shows how to enable PIM snooping on VLAN 10 and verify the configuration:

```
Switch# interface vlan 10
Switch(config-if)# ip pim snooping
Switch(config-if)# end
Switch# show ip pim snooping vlan 10
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
Switch#
```

Disabling PIM Snooping Designated-Router Flooding

By default, switches that have PIM snooping enabled will flood multicast traffic to the designated router (DR). This method of operation can send unnecessary multicast packets to the designated router. The network must carry the unnecessary traffic, and the designated router must process and drop the unnecessary traffic.

To reduce the traffic sent over the network to the designated router, disable designated-router flooding. With designated-router flooding disabled, PIM snooping only passes to the designated-router traffic that is in multicast groups for which PIM snooping receives an explicit join from the link towards the designated router.

To disable PIM snooping designated-router flooding, perform this task:

	Command	Purpose
Step 1	**no ip pim snooping dr-flood**	Disables PIM snooping designated-router flooding.
Step 2	**end**	Exits configuration mode.
Step 3	**show running-config | include dr-flood**	Verifies the configuration.

This example shows how to disable PIM snooping designated-router flooding:

```
Switch(config)# no ip pim snooping dr-flood
Switch(config)# end
```