Configuring PIM Snooping

Restrictions for PIM Snooping

- This feature is not supported on the C9500-12Q, C9500-16X, C9500-24Q, and C9500-40X models of the Cisco Catalyst 9500 Series Switches.
- PIM snooping is supported only on IPv4 mroutes.
- When PIM snooping is enabled and IGMP snooping is disabled in the VLAN, multicast packets are not bridged to the local receivers, within the VLAN, even after the local receivers send IGMP join request messages.
- Directly connected sources are supported for bidirectional PIM groups. Traffic from directly connected sources is forwarded to the designated router and the designated forwarder for a VLAN. In some cases, a nondesignated router can receive a downstream (S, G) join message. For source-only networks, the initial unknown traffic is flooded only to the designated routers and designated forwarders.
- All (S,G) mroutes are processed as (*,G) mroutes by the router.
- Non-PIMv2 multicast routers will not receive traffic if PIM snooping is enabled.

Information About PIM Snooping

About PIM Snooping

Note PIM snooping is disabled by default

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 We recommend that you use PIM snooping along with IGMP snooping on the switch. IGMP snooping restricts the multicast traffic that exits through the LAN ports to which the hosts are connected. However, 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 1: PIM Join Message Flow without PIM Snooping

The following figure shows the flow of a PIM join message without PIM snooping enabled. In the figure, the switches flood the PIM join message, which is intended for Router B, to all the connected routers.

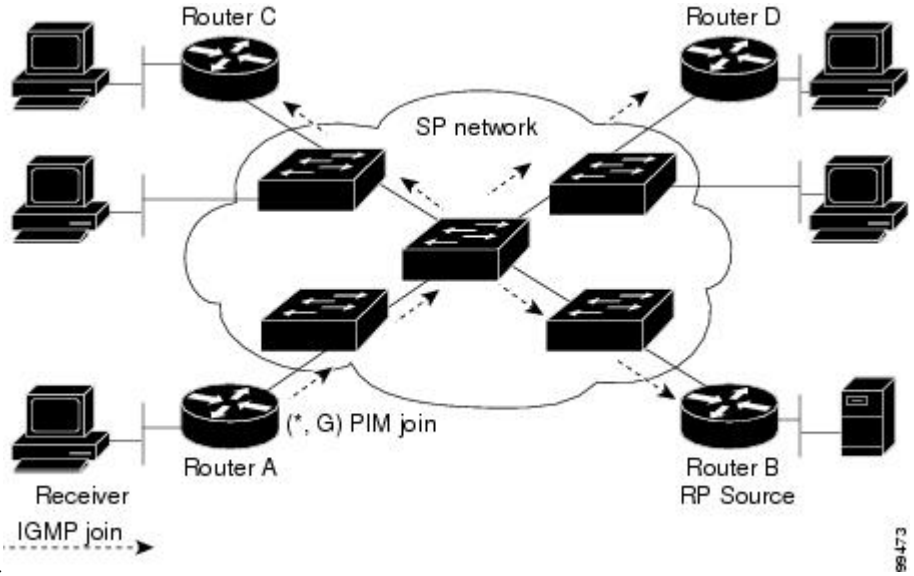


Figure 2: PIM Join Message Flow with PIM Snooping

The following figure 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).

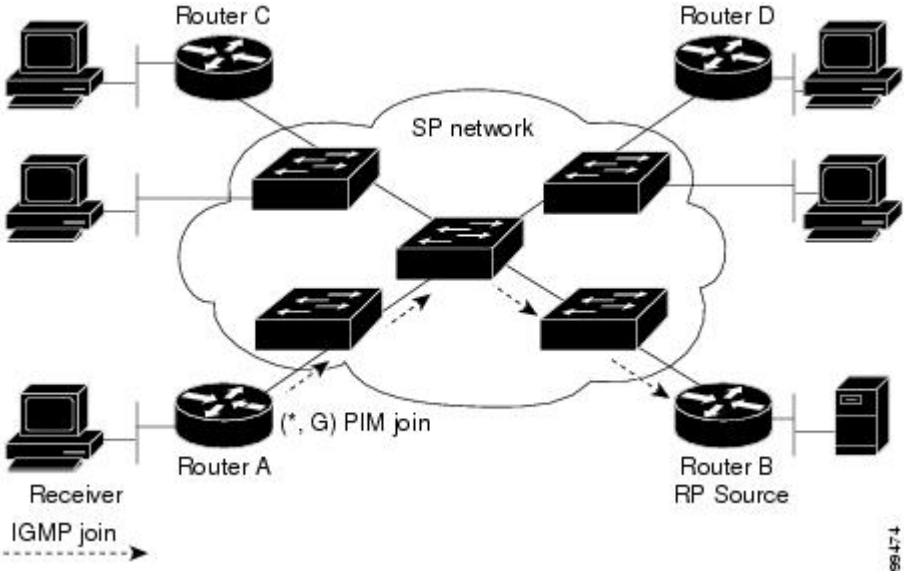


Figure 3: Data Traffic Flow without PIM Snooping

The following figure 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 the connected routers.

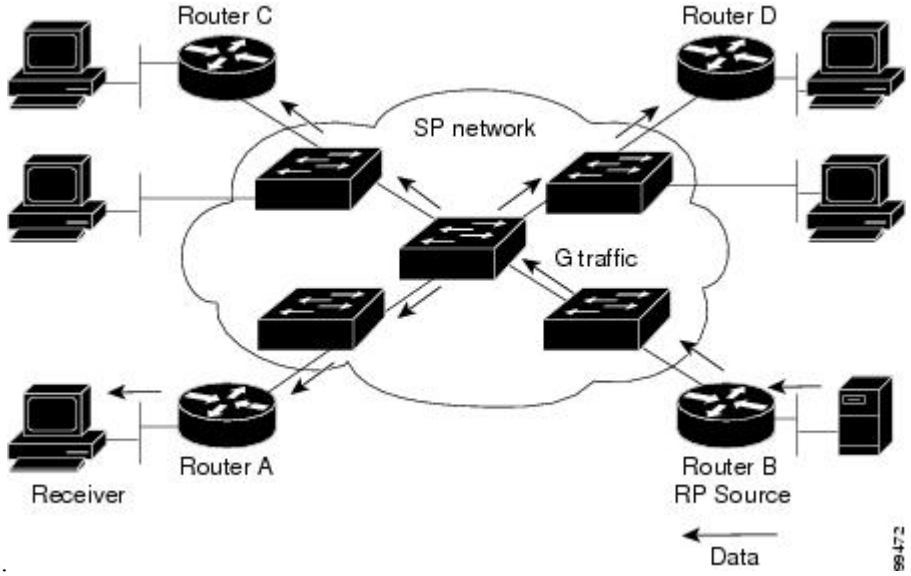
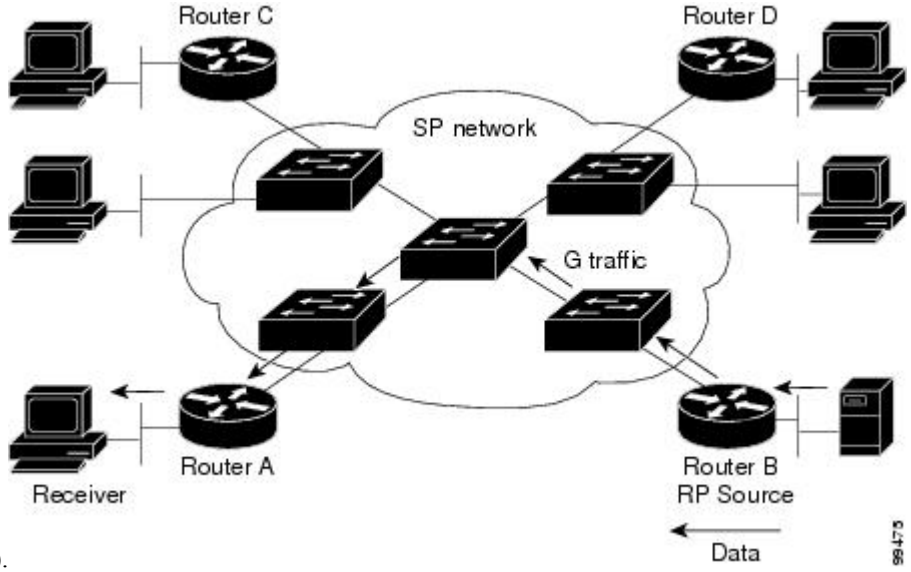


Figure 4: Data Traffic Flow with PIM Snooping

The following figure 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).



PIM Snooping on VLAN

The following characteristics are applicable if PIM Snooping is enabled on a VLAN:

- PIM snooping can be enabled or disabled on a per-VLAN basis.
- The switch snoops on designated forwarder election messages and maintains a list of all the designated forwarder routers for various RPs for a VLAN. All the traffic is sent to all the designated forwarders, which ensures that the bidirectional functionality works properly.
- AUTO-RP groups (224.0.1.39 and 224.0.1.40) are always flooded on all the PIM router ports on all the PIM snooping-enabled VLANs.
- All mroute state and neighbor information is maintained per VLAN.
- Join or prune messages are not flooded on all the router ports, but are sent only to the port corresponding to the upstream router mentioned in the payload of the join or prune message.
- When enabling the PIM sparse mode (PIM-SM) feature, downstream routers can view traffic only if the routers have previously indicated interest through a PIM join or prune message. An upstream router can only view traffic if used as an upstream router during the PIM join or prune process.
- All mroute and router information is timed out based on the hold-time indicated in the PIM hello and join or prune message.

How to Configure PIM Snooping

Enabling PIM Snooping Globally

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

To enable PIM snooping globally, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip pim snooping**
4. **end**
5. **show ip pim snooping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip pim snooping** **Example:** `Router(config)# ip pim snooping`	Enables PIM snooping.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip pim snooping** **Example:** `Router# show ip pim snooping`	Verifies your entries.

Enabling PIM Snooping in a VLAN

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip pim snooping vlan** *vlan_ID*
4. **end**
5. **show ip pim snooping vlan** *vlan_ID*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip pim snooping vlan** *vlan_ID* **Example:** `Router(config)# ip pim snooping vlan 10`	Enables PIM snooping.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip pim snooping vlan** *vlan_ID* **Example:** `Router# show ip pim snooping vlan 10`	Verifies your entries.

Disabling PIM Snooping-Designated Router Flooding

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

To reduce the traffic sent over the network to the designated router, disable designated router flooding. When designated router flooding is disabled, PIM snooping ensures that the designated router receives only the multicast traffic for which it has sent explicit join message.

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

Before you begin

- Do not disable designated router flooding on switches in a Layer 2 broadcast domain that supports multicast sources.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip pim snooping dr-flood**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ip pim snooping dr-flood** **Example:** `Router(config)# no ip pim snooping dr-flood`	Disables PIM snooping-designated router flooding.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Monitoring PIM Snooping Information

Use the privileged EXEC commands in the following table to monitor your PIM snooping configurations.

Table 1: Commands to Monitor PIM Snooping

Command	Purpose
show ip pim snooping detail	Displays the operational state information.
show ip pim snooping vlan *vlan_ID* **detail**	Displays the operational state information of a VLAN.
show ip pim snooping mroute	Displays information about the mroute database.
show ip pim snooping vlan *vlan_ID* **mroute**	Displays information about the mroute of a VLAN.
show ip pim snooping neighbor	Displays information about the neighbor database.
show ip pim snooping vlan *vlan_ID* **neighbor**	Displays information about a VLAN's neighbor.
show ip pim snooping statistics	Displays information about VLAN statistics.

Configuration Examples for PIM

Example: Enabling PIM Snooping Globally

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

```
Router(config)#ip pim snooping
Router(config)#end
Router#show ip pim snooping
Global runtime mode: Enabled
Global admin mode : Enabled
DR Flooding status : Disabled
SGR-Prune Suppression: Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 1001
Router#
```

Example: Enabling PIM Snooping in a VLAN

The following example shows how to enable PIM snooping on VLAN 1001 and verify the configuration:

```
Router(config)#ip pim snooping vlan 1001
Router(config)#end
Router#show ip pim snooping vlan 1001
4 neighbors (0 DR priority incapable, 4 Bi-dir incapable)
5000 mroutes, 0 mac entries
DR is 10.10.10.4
RP DF Set:
QinQ snooping : Disabled
Router#
```

Example: Disabling PIM Snooping-Designated Router Flooding

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

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

Additional References for PIM

Related Documents

Related Topic	Document Title
Complete syntax and usage information about the commands used in this chapter.	See the "IP Multicast Routing Commands" section of the *Command Reference (Catalyst 9500 Series Switches)*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by these features, and support for existing MIBs has not been modified by these features.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for PIM Snooping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for PIM Snooping

Feature Name	Releases	Feature Information
PIM Snooping	Cisco IOS XE Fuji 16.8.1a	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.