Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.x

First Published: 2013-11-20

Last Modified: 2014-11-10

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface includes the following sections:

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which you supply the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments that are separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments that are separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Convention	Description
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string includes the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information that you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation for Cisco Nexus 9000 Series Switches

The entire Cisco Nexus 9000 Series switch documentation set is available at the following URL:

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

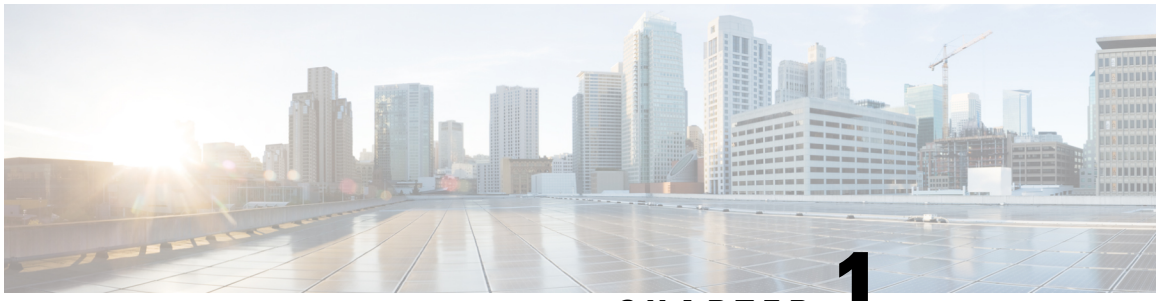
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Preface



CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.x*.

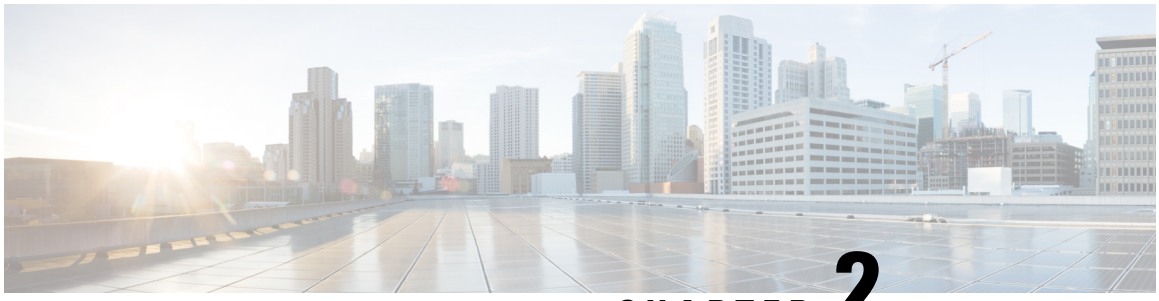
New and Changed Information

This table summarizes the new and changed features for the *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.x* and tells you where they are documented.

Table 1: New and Changed Features for Cisco NX-OS Release 6.x

Feature	Description	Changed in Release	Where Documented
PIM	Added the ability to delay participation in the designated router election, upon bootup or following an IP address or interface state change.	6.1(2)I3(2)	Configuring PIM, on page 27
IGMP snooping	Added the ability to filter IGMP snooping reports.	6.1(2)I2(2)	Configuring IGMP Snooping, on page 71
IGMP	Added support for Layer 2 switching.	6.1(2)I2(1)	Configuring IGMP, on page 13
IGMP snooping	Introduced this feature.	6.1(2)I2(1)	Configuring IGMP Snooping, on page 71
PIM	Added vPC support for PIM ASM.	6.1(2)I2(1)	Configuring PIM, on page 27

New and Changed Information



CHAPTER 2

Overview

This chapter describes the multicast features of Cisco NX-OS.

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

About Multicast

IP multicast is a method of forwarding the same set of IP packets to a number of hosts within a network. You can use multicast in IPv4 networks to provide efficient delivery of data to multiple destinations.

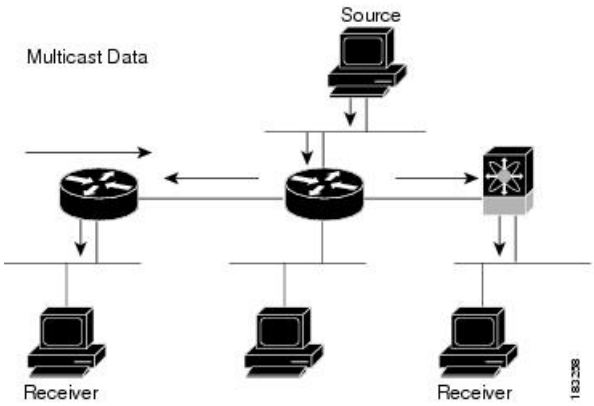
Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel. The Internet Assigned Number Authority (IANA) has assigned 224.0.0.0 through 239.255.255.255 as IPv4 multicast addresses. For more information, see http://www.iana.org/assignments/multicast-addresses.

Note For a complete list of RFCs related to multicast, see the *IETF RFCs for IP Multicast* chapter.

The routers in the network listen for receivers to advertise their interest in receiving multicast data from selected groups. The routers then replicate and forward the data from sources to the interested receivers. Multicast data for a group is transmitted only to those LAN segments with receivers that requested it.

This figure shows one source transmitting multicast data that is delivered to two receivers. In the figure, because the center host is on a LAN segment where no receiver requested multicast data, no data is delivered to that receiver.

Figure 1: Multicast Traffic from One Source to Two Receivers



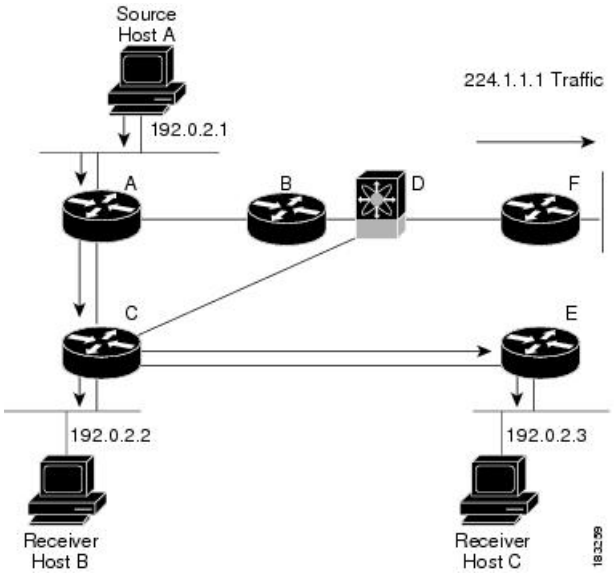
Multicast Distribution Trees

A multicast distribution tree represents the path that multicast data takes between the routers that connect sources and receivers. The multicast software builds different types of trees to support different multicast methods.

Source Trees

A source tree represents the shortest path that the multicast traffic takes through the network from the sources that transmit to a particular multicast group to receivers that requested traffic from that same group. Because of the shortest path characteristic of a source tree, this tree is often referred to as a shortest path tree (SPT). This figure shows a source tree for group 224.1.1.1 that begins at host A and connects to hosts B and C.

Figure 2: Source Tree

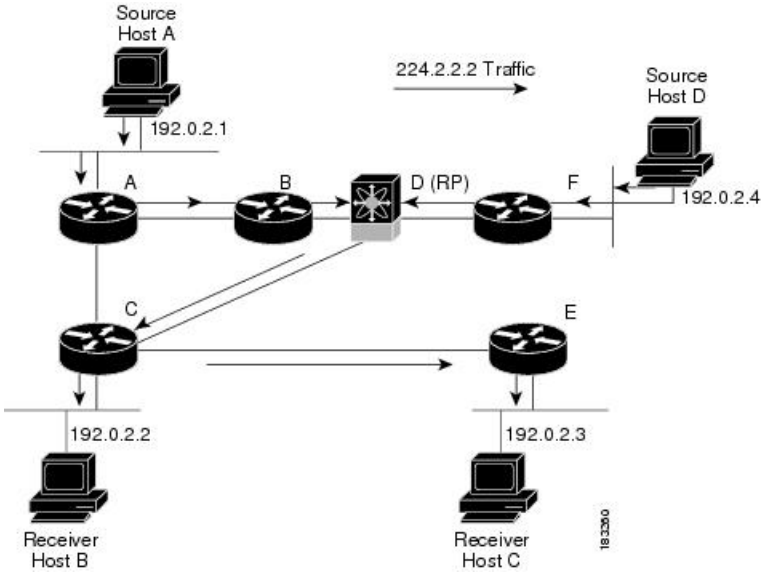


The notation (S, G) represents the multicast traffic from source S on group G. The SPT in this figure is written (192.0.2.1, 224.1.1.1). Multiple sources can be transmitting on the same group.

Shared Trees

A shared tree represents the shared distribution path that the multicast traffic takes through the network from a shared root or rendezvous point (RP) to each receiver. (The RP creates an SPT to each source.) A shared tree is also called an RP tree (RPT). This figure shows a shared tree for group 224.2.2.2 with the RP at router D. Source hosts A and D send their data to router D, the RP, which then forwards the traffic to receiver hosts B and C.

Figure 3: Shared Tree



The notation (*, G) represents the multicast traffic from any source on group G. The shared tree in this figure is written (*, 224.2.2.2).

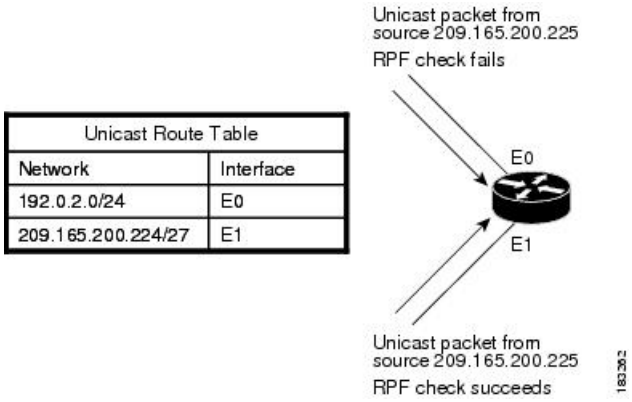
Multicast Forwarding

Because multicast traffic is destined for an arbitrary group of hosts, the router uses reverse path forwarding (RPF) to route data to active receivers for the group. When receivers join a group, a path is formed toward the RP (ASM mode). The path from a source to a receiver flows in the reverse direction from the path that was created when the receiver joined the group.

For each incoming multicast packet, the router performs an RPF check. If the packet arrives on the interface leading to the source, the packet is forwarded out each interface in the outgoing interface (OIF) list for the group. Otherwise, the router drops the packet.

This figure shows an example of RPF checks on packets coming in from different interfaces. The packet that arrives on E0 fails the RPF check because the unicast route table lists the source of the network on interface E1. The packet that arrives on E1 passes the RPF check because the unicast route table lists the source of that network on interface E1.

Figure 4: RPF Check Example



Cisco NX-OS PIM

Cisco NX-OS supports multicasting with Protocol Independent Multicast (PIM) sparse mode. PIM is IP routing protocol independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table. In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it. PIM dense mode is not supported by Cisco NX-OS.

Note In this publication, the term "PIM" is used for PIM sparse mode version 2.

To access multicast commands, you must enable the PIM feature. Multicast is enabled only after you enable PIM on an interface of each router in a domain. You can configure PIM for an IPv4 network. By default, IGMP is running on the system.

PIM, which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees, on which packets from multiple sources are forwarded, as well as source distribution trees, on which packets from a single source are forwarded.

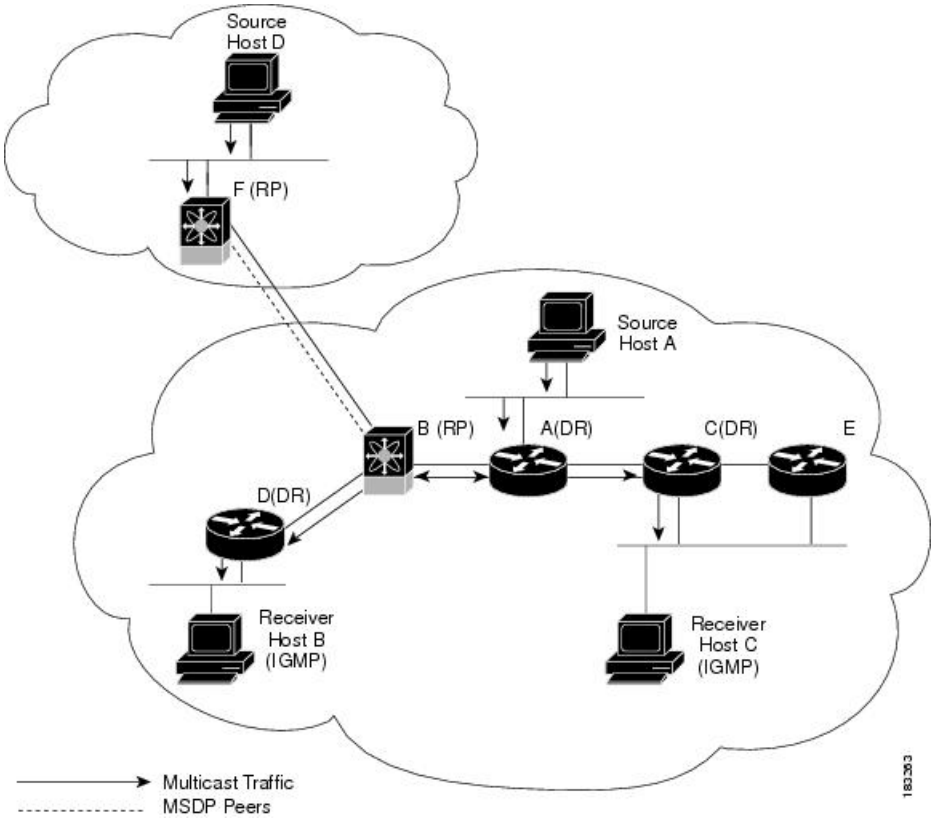
The distribution trees change automatically to reflect the topology changes due to link or router failures. PIM dynamically tracks both multicast-capable sources and receivers.

The router uses the unicast routing table and RPF routes for multicast to create multicast routing information.

Note In this publication, "PIM for IPv4" refers to the Cisco NX-OS implementation of PIM sparse mode.

This figure shows two PIM domains in an IPv4 network.

Figure 5: PIM Domains in an IPv4 Network



- The lines with arrows show the path of the multicast data through the network. The multicast data originates from the sources at hosts A and D.
- The dashed line connects routers B and F, which are Multicast Source Discovery Protocol (MSDP) peers. MSDP supports the discovery of multicast sources in other PIM domains.
- Hosts B and C receive multicast data by using Internet Group Management Protocol (IGMP) to advertise requests to join a multicast group.
- Routers A, C, and D are designated routers (DRs). When more than one router is connected to a LAN segment, such as C and E, the PIM software chooses one router to be the DR so that only one router is responsible for putting multicast data on the segment.

Router B is the rendezvous point (RP) for one PIM domain, and router F is the RP for the other PIM domain. The RP provides a common point for connecting sources and receivers within a PIM domain.

PIM supports these multicast modes for connecting sources and receivers:

- Any source multicast (ASM)

You can also define RPF routes for multicast.

ASM

Any Source Multicast (ASM) is a PIM tree building mode that uses shared trees to discover new sources and receivers as well as source trees to form shortest paths from receivers to sources. The shared tree uses a network

node as the root, called the rendezvous point (RP). The source tree is rooted at first-hop routers, directly attached to each source that is an active sender. The ASM mode requires an RP for a group range. An RP can be configured statically or learned dynamically by the Auto-RP or BSR group-to-RP discovery protocols. If an RP is learned, the group operates in ASM mode.

The ASM mode is the default mode when you configure RPs.

RPF Routes for Multicast

You can configure static multicast RPF routes to override what the unicast routing table uses. This feature is used when the multicast topology is different than the unicast topology.

IGMP

By default, the Internet Group Management Protocol (IGMP) for PIM is running on the system.

IGMP is used by hosts that want to receive multicast data to request membership in multicast groups. Once the group membership is established, multicast data for the group is directed to the LAN segment of the requesting host.

You can configure IGMPv2 or IGMPv3 on an interface. By default, the software enables IGMPv2.

IGMP Snooping

IGMP snooping is a feature that limits multicast traffic on VLANs to the subset of ports that have known receivers. By examining (snooping) IGMP membership report messages from interested hosts, multicast traffic is sent only to VLAN ports that interested hosts reside on. By default, IGMP snooping is running on the system.

Interdomain Multicast

Cisco NX-OS provides several methods that allow multicast traffic to flow between PIM domains.

MSDP

Multicast Source Discovery Protocol (MSDP) is a multicast routing protocol that is used with PIM to support the discovery of multicast sources in different PIM domains.

Note Cisco NX-OS supports the PIM Anycast-RP, which does not require MSDP configuration.

MBGP

Multiprotocol BGP (MBGP) defines extensions to BGP4 that enable routers to carry multicast routing information. PIM can use this multicast information to reach sources in external BGP autonomous systems.

MRIB

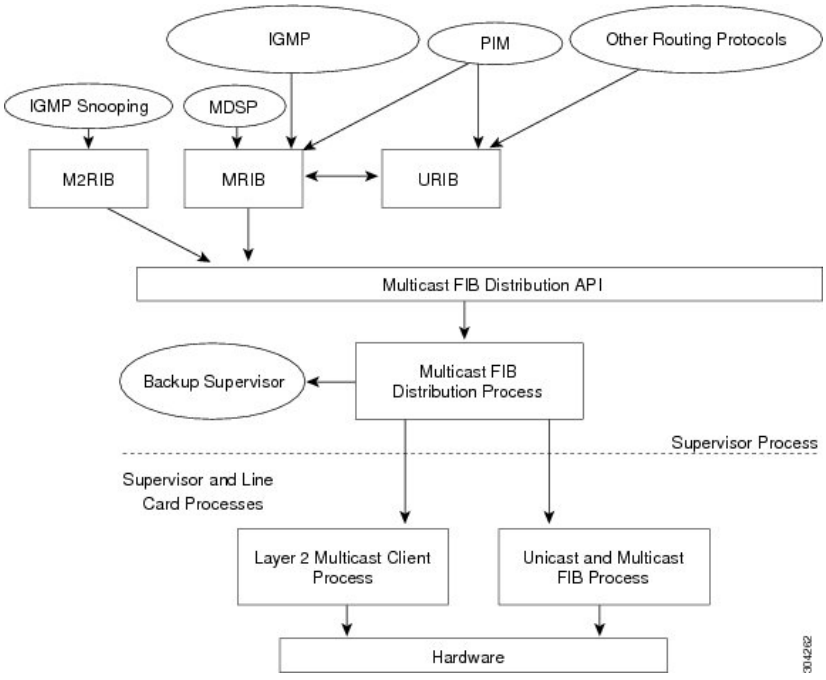
The Cisco NX-OS IPv4 Multicast Routing Information Base (MRIB) is a repository for route information that is generated by multicast protocols such as PIM and IGMP. The MRIB does not affect the route information itself. The MRIB maintains independent route information for each virtual routing and forwarding (VRF) instance.

The major components of the Cisco NX-OS multicast software architecture are as follows:

- The Multicast FIB (MFIB) Distribution (MFDM) API defines an interface between the multicast Layer 2 and Layer 3 control plane modules, including the MRIB, and the platform forwarding plane. The control plane modules send the Layer 3 route update using the MFDM API.
- The multicast FIB distribution process distributes the multicast update messages to all the relevant modules and the standby supervisor. It runs only on the supervisor.
- The Layer 2 multicast client process sets up the Layer 2 multicast hardware forwarding path. It runs on both the supervisor and the modules.
- The unicast and multicast FIB process manages the Layer 3 hardware forwarding path. It runs on both the supervisor and the modules.

  The following figure shows the Cisco NX-OS multicast software architecture.

Figure 6: Cisco NX-OS Multicast Software Architecture



Virtual Port Channels and Multicast

A virtual port channel (vPC) allows a single device to use a port channel across two upstream switches. When you configure a vPC, the following multicast features might be affected:

- PIM—

- IGMP snooping—You should configure the vPC peers identically.

It is recommended to configure a snooping querier on a L2 device with lower IP address to force the L2 device as the querier. This will be useful in handling the scenario where multi chassis EtherChannel trunk (MCT) is down.

Guidelines and Limitations for Multicast

- Layer 3 Ethernet port-channel subinterfaces are not supported with multicast routing.
- Layer 2 IPv6 multicast packets will be flooded on the incoming VLAN.
- Traffic storm control is not supported for unknown multicast traffic.
- IPv6 multicast is not supported on Cisco Nexus 9500 R Series line cards.

High-Availability Requirements for Multicast

After a multicast routing protocol is restarted, its state is recovered from the MRIB process. When a supervisor switchover occurs, the MRIB recovers its state from the hardware, and the multicast protocols recover their state from periodic message activity. For more information about high availability, see the *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*.

Virtual Device Contexts

Cisco NX-OS can segment operating system and hardware resources into virtual device contexts (VDCs) that emulate virtual devices. The Cisco Nexus 9000 Series switches currently do not support multiple VDCs. All switch resources are managed in the default VDC.

Troubleshooting Inconsistency Between SW and HW Multicast Routes

Symptom

This section provides symptoms, possible causes, and recommended actions for when *, G, or S,G entries that are seen in the MRIB with active flow, but are not programmed in MFIB.

Possible Cause

The issue can be seen when numerous active flows are received beyond the hardware capacity. This causes some of the entries not to be programmed in hardware while there is no free hardware index.

If the number of active flows are significantly reduced to free up the hardware resource, inconsistency may be seen between MRIB and MFIB for flows that were previously affected when the hardware table was full until the entry, times out, repopulates, and triggers programming.

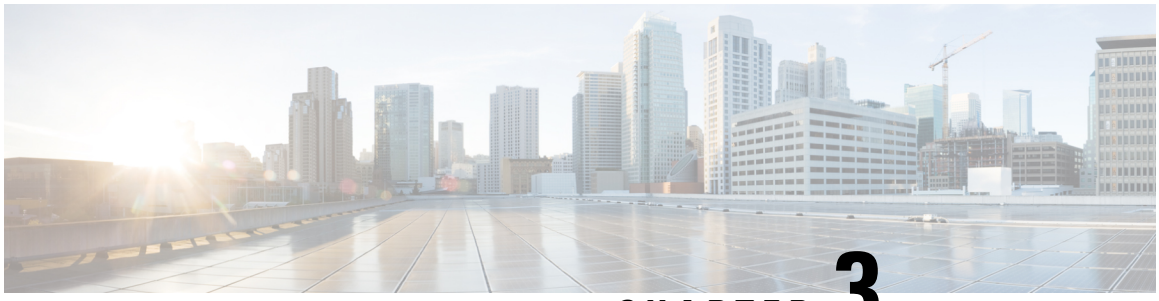
There is currently no mechanism to walk the MRIB table and reprogram missing entries in HW after hardware resource is freed.

Corrective Action

To ensure reprogramming of the entries, use the **clear ip mroute *** command.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml



CHAPTER 3

Configuring IGMP

This chapter describes how to configure the Internet Group Management Protocol (IGMP) on Cisco NX-OS devices for IPv4 networks.

About IGMP

IGMP is an IPv4 protocol that a host uses to request multicast data for a particular group. Using the information obtained through IGMP, the software maintains a list of multicast group or channel memberships on a per-interface basis. The systems that receive these IGMP packets send multicast data that they receive for requested groups or channels out the network segment of the known receivers.

By default, the IGMP process is running. You cannot enable IGMP manually on an interface. IGMP is automatically enabled when you perform one of the following configuration tasks on an interface:

- Enable PIM
- Statically bind a local multicast group
- Enable link-local group reports

IGMP Versions

The device supports IGMPv2 and IGMPv3, and IGMPv1 report reception.

By default, the software enables IGMPv2 when it starts the IGMP process. You can enable IGMPv3 on interfaces where you want its capabilities.

IGMPv3 includes the following key changes from IGMPv2:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following features:
  - Host messages that can specify both the group and the source.
  - The multicast state that is maintained for groups and sources, not just for groups as in IGMPv2.
- Hosts no longer perform report suppression, which means that hosts always send IGMP membership reports when an IGMP query message is received.

Note The Cisco Nexus 9000 Series switches do not support SSM until Cisco NX-OS Release 7.0(3)I2(1).

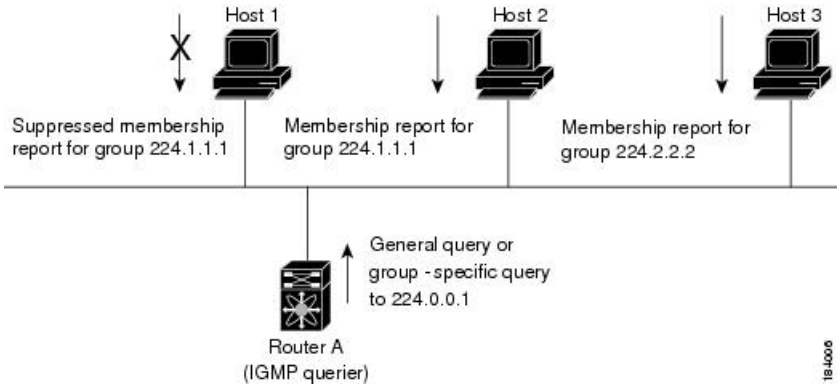
For detailed information about IGMPv2, see RFC 2236.

For detailed information about IGMPv3, see RFC 5790.

IGMP Basics

This figure shows the basic IGMP process of a router that discovers multicast hosts. Hosts 1, 2, and 3 send unsolicited IGMP membership report messages to initiate receiving multicast data for a group or channel.

Figure 7: IGMPv1 and IGMPv2 Query-Response Process



In the figure below, router A, which is the IGMP designated querier on the subnet, sends query messages to the all-hosts multicast group at 224.0.0.1 periodically to discover whether any hosts want to receive multicast data. You can configure the group membership timeout value that the router uses to determine that no members of a group or source exist on the subnet.

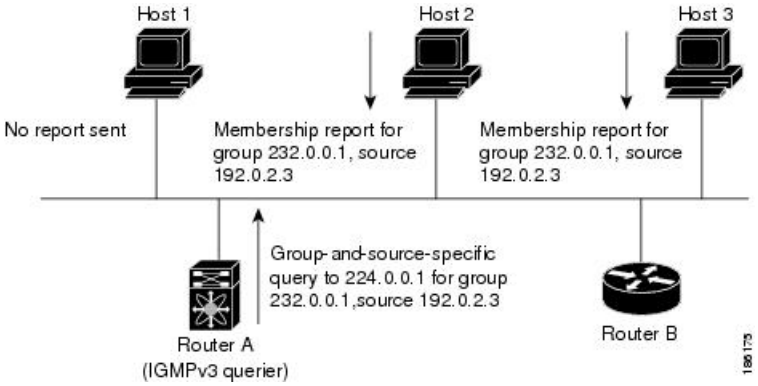
The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.

In this figure, host 1's membership report is suppressed, and host 2 sends its membership report for group 224.1.1.1 first. Host 1 receives the report from host 2. Because only one membership report per group needs to be sent to the router, other hosts suppress their reports to reduce network traffic. Each host waits for a random time interval to avoid sending reports at the same time. You can configure the query maximum response time parameter to control the interval in which hosts randomize their responses.

Note IGMPv1 and IGMPv2 membership report suppression occurs only on hosts that are connected to the same port.

In this figure, router A sends the IGMPv3 group-and-source-specific query to the LAN. Hosts 2 and 3 respond to the query with membership reports that indicate that they want to receive data from the advertised group and source.

Figure 8: IGMPv3 Group-and-Source-Specific Query



Note IGMPv3 hosts do not perform IGMP membership report suppression.

Messages sent by the designated querier have a time-to-live (TTL) value of 1, which means that the messages are not forwarded by the directly connected routers on the subnet. You can configure the frequency and number of query messages sent specifically for IGMP startup, and you can configure a short query interval at startup so that the group state is established as quickly as possible. Although usually unnecessary, you can tune the query interval used after startup to a value that balances the responsiveness to host group membership messages and the traffic created on the network.

Caution Changing the query interval can severely impact multicast forwarding.

When a multicast host leaves a group, a host that runs IGMPv2 or later sends an IGMP leave message. To check if this host is the last host to leave the group, the software sends an IGMP query message and starts a timer that you can configure called the last member query response interval. If no reports are received before the timer expires, the software removes the group state. The router continues to send multicast traffic for a group until its state is removed.

You can configure a robustness value to compensate for packet loss on a congested network. The robustness value is used by the IGMP software to determine the number of times to send messages.

Link local addresses in the range 224.0.0.0/24 are reserved by the Internet Assigned Numbers Authority (IANA). Network protocols on a local network segment use these addresses; routers do not forward these addresses because they have a TTL of 1. By default, the IGMP process sends membership reports only for nonlink local addresses, but you can configure the software to send reports for link local addresses.

Prerequisites for IGMP

IGMP has the following prerequisites:

- You are logged onto the device.
- For global configuration commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

Guidelines and Limitations for IGMP

IGMP has the following guidelines and limitations:

- The IGMP host SG proxy is not supported with vPC.
- Excluding or blocking a list of sources according to IGMPv3 (RFC 5790) is not supported.
- For Cisco Nexus 9200 Series switches, the S, G routes do not expire if IGMP or source traffic originates from the same IP address.
- IGMP is supported on Cisco Nexus 9300-FX platform switches.
- Configuring the route-map in **igmp static-oif** is limited to 255 range. When the route-map is configured with a range larger than /24 such as /8 or /4, the following log will be displayed:

```
2020 May 13 10:10:58 LO5S-NSWDDNGEF01B %IGMP-3-GROUP_RANGE_IGNORE: igmp [29534] Too
many Groups in Group Range 224.4.1.0 - 224.4.13.255
2020 May 13 12:26:13 LO5S-NSWDDNGEF01B %IGMP-3-GROUP_RANGE_IGNORE: igmp [29534] Too
many Groups in Group Range 224.4.1.0 - 224.4.13.255
2020 May 13 12:47:01 LO5S-NSWDDNGEF01B %IGMP-3-GROUP_RANGE_IGNORE: igmp [29534] Too
many Groups in Group Range 224.4.0.64 - 224.4.3.64
```

  The work around for this limitation is to split the required range to multiple 255 ranges or smaller and use the multiple route-map sequences for each range.

- Configuration of nondefault IGMP related timers can be done on L3 physical interface and SVI, or in VLAN configuration mode if querier IP is configured in VLAN configuration mode. It is not recommended to configure querier IP in VLAN configuration mode if there is PIM enabled SVI for that VLAN.

  When query maximum response time (query-max-response-time) and IGMP query-interval are modified on the L3 physical interface or SVI, IGMP querier, timeout gets adjusted automatically to 2 times query interval plus MRT. To modify further, use **ip igmp querier-timeout** command for L3 physical interface.

  However, for SVI the value must be set according to the value shown in **show ip igmp interface vlan X** command output via **ip igmp snooping querier-timeout** command in VLAN configuration mode for querier election to happen as expected shell current querier become unavailable.

  For L3 physical interface, use **show ip igmp interface <intf>** command . For SVI, use **show ip igmp snooping querier <vlan>** to display relevant igmp snooping querier information. Both configuration commands should show same querier timeout for correct configuration.

  PIM hello interval determines how fast a PIM neighbor determines its peer availability. If the unavailable PIM neighbor happens to also be IGMP querier, new querier election happens at the same time as neighbor

expiry (90 seconds - 3 x 30 seconds PIM hello interval). At the same time though L2 snooping querier timer dictates when new querier election is to happen (default 2 x query interval plus MRT).

Default Settings for IGMP

This table lists the default settings for IGMP parameters.

Table 2: Default IGMP Parameters

Parameters	Default
IGMP version	2
Startup query interval	30 seconds
Startup query count	2
Robustness value	2
Querier timeout	255 seconds
Query timeout	255 seconds
Query max response time	10 seconds
Query interval	125 seconds
Last member query response interval	1 second
Last member query count	2
Group membership timeout	260 seconds
Report link local multicast groups	Disabled
Enforce router alert	Disabled
Immediate leave	Disabled

Configuring IGMP Parameters

You can configure the IGMP global and interface parameters to affect the operation of the IGMP process.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring IGMP Interface Parameters

You can configure the optional IGMP interface parameters described in the table below.

Table 3: IGMP Interface Parameters

Parameter	Description
IGMP version	IGMP version that is enabled on the interface. The IGMP version can be 2 or 3. The default is 2.
Static multicast groups	Multicast groups that are statically bound to the interface. You can configure the groups to join the interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. **Note** Although you can configure the (S, G) state, the source tree is built only if you enable IGMPv3. You can configure a multicast group on all the multicast-capable routers on the network so that pinging the group causes all the routers to respond.
Static multicast groups on OIF	Multicast groups that are statically bound to the output interface. You can configure the groups to join the output interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. **Note** Although you can configure the (S, G) state, the source tree is built only if you enable IGMPv3.
Startup query interval	Startup query interval. By default, this interval is shorter than the query interval so that the software can establish the group state as quickly as possible. Values range from 1 to 18,000 seconds. The default is 31 seconds.
Startup query count	Number of queries sent at startup that are separated by the startup query interval. Values range from 1 to 10. The default is 2.

Parameter	Description
Robustness value	Robustness variable that you can tune to reflect expected packet loss on a congested network. You can increase the robustness variable to increase the number of times that packets are resent. Values range from 1 to 7. The default is 2.
Querier timeout	Number of seconds that the software waits after the previous querier has stopped querying and before it takes over as the querier. Values range from 1 to 65,535 seconds. The default is 255 seconds.
Query max response time	Maximum response time advertised in IGMP queries. You can tune the IGMP messages on the network by setting a larger value so that host responses are spread out over a longer time. This value must be less than the query interval. Values range from 1 to 25 seconds. The default is 10 seconds.
Query interval	Frequency at which the software sends IGMP host query messages. You can tune the number of IGMP messages on the network by setting a larger value so that the software sends IGMP queries less often. Values range from 1 to 18,000 seconds. The default is 125 seconds.
Last member query response interval	Interval in which the software sends a response to an IGMP query after receiving a host leave message from the last known active host on the subnet. If no reports are received in the interval, the group state is deleted. You can use this value to tune how quickly the software stops transmitting on the subnet. The software can detect the loss of the last member of a group or source more quickly when the values are smaller. Values range from 1 to 25 seconds. The default is 1 second.
Last member query count	Number of times that the software sends an IGMP query, separated by the last member query response interval, in response to a host leave message from the last known active host on the subnet. Values range from 1 to 5. The default is 2. Setting this value to 1 means that a missed packet in either direction causes the software to remove the multicast state from the queried group or channel. The software may wait until the next query interval before the group is added again.

Parameter	Description
Group membership timeout	Group membership interval that must pass before the router decides that no members of a group or source exist on the network. Values range from 3 to 65,535 seconds. The default is 260 seconds.
Report link local multicast groups	Option that enables sending reports for groups in 224.0.0.0/24. Link local addresses are used only by protocols on the local network. Reports are always sent for nonlink local groups. The default is disabled.
Report policy	Access policy for IGMP reports that is based on a route-map policy. [1]
Access groups	Option that configures a route-map policy to control the multicast groups that hosts on the subnet serviced by an interface can join. **Note** Only the **match ip multicast group** command is supported in this route map policy. The **match ip address** command for matching an ACL is not supported.
Immediate leave	Option that minimizes the leave latency of IGMPv2 group memberships on a given IGMP interface because the device does not send group-specific queries. When immediate leave is enabled, the device removes the group entry from the multicast routing table immediately upon receiving a leave message for the group. The default is disabled. **Note** Use this command only when there is one receiver behind the interface for a given group.

[1] To configure route-map policies, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface* **Example:**	Enters interface configuration mode.

	Command or Action	Purpose
	`switch(config)# interface ethernet 2/1` `switch(config-if)#`	**Note** Use the commands listed from step-3 to configure the IGMP interface parameters.
Step 3	**ip igmp version** *value* **Example:** `switch(config-if)# ip igmp version 3`	Sets the IGMP version to the value specified. Values can be 2 or 3. The default is 2. The **no** form of the command sets the version to 2.
Step 4	**ip igmp join-group** {**group** [**source** *source*] | **route-map** *policy-name*} **Example:** `switch(config-if)# ip igmp join-group 230.0.0.0`	Configures an interface on the device to join the specified group or channel. The device accepts the multicast packets for CPU consumption only. **Caution** The device CPU must be able to handle the traffic generated by using this command. Because of CPU load constraints, using this command, especially in any form of scale, is not recommended. Consider using the **ip igmp static-oif** command instead.
Step 5	**ip igmp static-oif** {*group* [**source** *source*] | **route-map** *policy-name*} **Example:** `switch(config-if)# ip igmp static-oif 230.0.0.0`	Statically binds a multicast group to the outgoing interface, which is handled by the device hardware. If you specify only the group address, the (*, G) state is created. If you specify the source address, the (S, G) state is created. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. **Note** A source tree is built for the (S, G) state only if you enable IGMPv3.
Step 6	**ip igmp startup-query-interval** *seconds* **Example:** `switch(config-if)# ip igmp startup-query-interval 25`	Sets the query interval used when the software starts up. Values can range from 1 to 18,000 seconds. The default is 31 seconds.
Step 7	**ip igmp startup-query-count** *count* **Example:** `switch(config-if)# ip igmp startup-query-count 3`	Sets the query count used when the software starts up. Values can range from 1 to 10. The default is 2.
Step 8	**ip igmp robustness-variable** *value* **Example:**	Sets the robustness variable. Values can range from 1 to 7. The default is 2.

	Command or Action	Purpose
	`switch(config-if)# ip igmp robustness-variable 3`	
Step 9	**ip igmp querier-timeout** *seconds* **Example:** `switch(config-if)# ip igmp querier-timeout 300`	Sets the querier timeout that the software uses when deciding to take over as the querier. Values can range from 1 to 65,535 seconds. The default is 255 seconds.
Step 10	**ip igmp query-timeout** *seconds* **Example:** `switch(config-if)# ip igmp query-timeout 300`	Sets the query timeout that the software uses when deciding to take over as the querier. Values can range from 1 to 65,535 seconds. The default is 255 seconds. **Note** This command has the same functionality as the **ip igmp querier-timeout** command.
Step 11	**ip igmp query-max-response-time** *seconds* **Example:** `switch(config-if)# ip igmp query-max-response-time 15`	Sets the response time advertised in IGMP queries. Values can range from 1 to 25 seconds. The default is 10 seconds.
Step 12	**ip igmp query-interval** *interval* **Example:** `switch(config-if)# ip igmp query-interval 100`	Sets the frequency at which the software sends IGMP host query messages. Values can range from 1 to 18,000 seconds. The default is 125 seconds.
Step 13	**ip igmp last-member-query-response-time** *seconds* **Example:** `switch(config-if)# ip igmp last-member-query-response-time 3`	Sets the query interval waited after sending membership reports before the software deletes the group state. Values can range from 1 to 25 seconds. The default is 1 second.
Step 14	**ip igmp last-member-query-count** *count* **Example:** `switch(config-if)# ip igmp last-member-query-count 3`	Sets the number of times that the software sends an IGMP query in response to a host leave message. Values can range from 1 to 5. The default is 2.
Step 15	**ip igmp group-timeout** *seconds* **Example:** `switch(config-if)# ip igmp group-timeout 300`	Sets the group membership timeout for IGMPv2. Values can range from 3 to 65,535 seconds. The default is 260 seconds.
Step 16	**ip igmp report-link-local-groups** **Example:** `switch(config-if)# ip igmp report-link-local-groups`	Enables sending reports for groups in 224.0.0.0/24. Reports are always sent for nonlink local groups. By default, reports are not sent for link local groups.

	Command or Action	Purpose
Step 17	**ip igmp report-policy** *policy* **Example:** `switch(config-if)# ip igmp report-policy my_report_policy`	Configures an access policy for IGMP reports that is based on a route-map policy.
Step 18	**ip igmp access-group** *policy* **Example:** `switch(config-if)# ip igmp access-group my_access_policy`	Configures a route-map policy to control the multicast groups that hosts on the subnet serviced by an interface can join. **Note** Only the **match ip multicast group** command is supported in this route map policy. The **match ip address** command for matching an ACL is not supported.
Step 19	**ip igmp immediate-leave** **Example:** `switch(config-if)# ip igmp immediate-leave`	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group. Use this command to minimize the leave latency of IGMPv2 group memberships on a given IGMP interface because the device does not send group-specific queries. The default is disabled. **Note** Use this command only when there is one receiver behind the interface for a given group.
Step 20	(Optional) **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] **Example:** `switch(config)# show ip igmp interface`	Displays IGMP information about the interface.
Step 21	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the Enforce Router Alert Option Check

You can configure the enforce router alert option check for IGMPv2 and IGMPv3 packets.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip igmp enforce-router-alert** **Example:** `switch(config)# ip igmp enforce-router-alert`	Enables or disables the enforce router alert option check for IGMPv2 and IGMPv3 packets. By default, the enforce router alert option check is enabled.
Step 3	(Optional) **show running-configuration igmp** **Example:** `switch(config)# show running-configuration igmp`	Shows the running-configuration information.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Restarting the IGMP Process

You can restart the IGMP process and optionally flush all routes.

Procedure

	Command or Action	Purpose
Step 1	**restart igmp** **Example:** `switch# restart igmp`	Restarts the IGMP process.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**ip igmp flush-routes** **Example:** `switch(config)# ip igmp flush-routes`	Removes routes when the IGMP process is restarted. By default, routes are not flushed.
Step 4	(Optional) **show running-configuration igmp** **Example:**	Shows the running-configuration information.

	Command or Action	Purpose
	`switch(config)# show running-configuration igmp`	
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the IGMP Configuration

To display the IGMP configuration information, perform one of the following tasks:

Command	Description
show ip igmp interface [*interface*] [**vrf** *vrf-name* | **all**] [**brief**]	Displays IGMP information about all interfaces or a selected interface, the default VRF, a selected VRF, or all VRFs. If IGMP is in vPC mode, use this command to display vPC statistics.
show ip igmp groups [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**vrf** *vrf-name* | **all**]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
show ip igmp route [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**vrf** *vrf-name* | **all**]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
show ip igmp local-groups	Displays the IGMP local group membership.
show running-configuration igmp	Displays the IGMP running-configuration information.
show startup-configuration igmp	Displays the IGMP startup-configuration information.

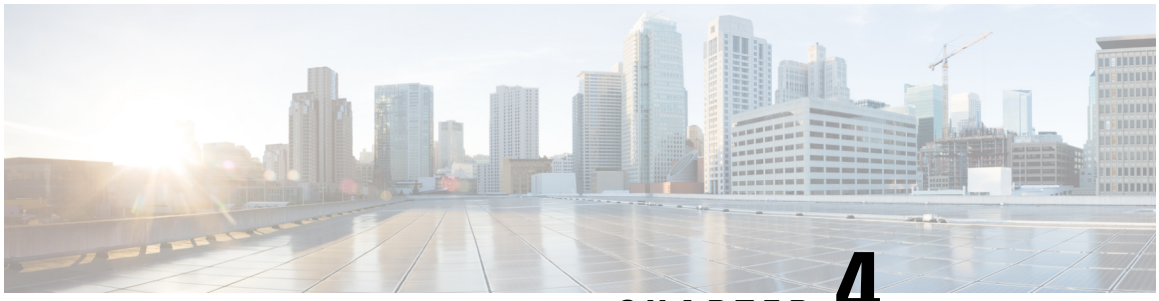
Configuration Examples for IGMP

The following example shows how to configure the IGMP parameters:

```
configure terminal

  interface ethernet 2/1
    ip igmp version 3
    ip igmp join-group 230.0.0.0
    ip igmp startup-query-interval 25
    ip igmp startup-query-count 3
    ip igmp robustness-variable 3
    ip igmp querier-timeout 300
    ip igmp query-timeout 300
    ip igmp query-max-response-time 15
    ip igmp query-interval 100
    ip igmp last-member-query-response-time 3
```

```
ip igmp last-member-query-count 3
ip igmp group-timeout 300
ip igmp report-link-local-groups
ip igmp report-policy my_report_policy
ip igmp access-group my_access_policy
```



CHAPTER 4

Configuring PIM

This chapter describes how to configure the Protocol Independent Multicast (PIM) features on Cisco NX-OS devices in your IPv4 network.

About PIM

PIM, which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees on which packets from multiple sources are forwarded, as well as source distribution trees on which packets from a single source are forwarded.

Cisco NX-OS supports PIM sparse mode for IPv4 networks (PIM). In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it. You can configure PIM to run simultaneously on a router. You can use PIM global parameters to configure rendezvous points (RPs), message packet filtering, and statistics. You can use PIM interface parameters to enable multicast, identify PIM borders, set the PIM hello message interval, and set the designated router (DR) priority.

Note Cisco NX-OS does not support PIM dense mode.

In Cisco NX-OS, multicast is enabled only after you enable the PIM feature on each router and then enable PIM sparse mode on each interface that you want to participate in multicast. You can configure PIM for an IPv4 network . In an IPv4 network, if you have not already enabled IGMP on the router, PIM enables it automatically.

You use the PIM global configuration parameters to configure the range of multicast group addresses to be handled by these distribution modes:

- Any Source Multicast (ASM) provides discovery of multicast sources. It builds a shared tree between sources and receivers of a multicast group and supports switching over to a source tree when a new receiver is added to a group. ASM mode requires that you configure an RP.

For more information about PIM sparse mode and shared distribution trees used by the ASM mode, see RFC 4601.

Hello Messages

The PIM process begins when the router establishes PIM neighbor adjacencies by sending PIM hello messages to the multicast IPv4 address 224.0.0.13. Hello messages are sent periodically at the interval of 30 seconds. When all neighbors have replied, the PIM software chooses the router with the highest priority in each LAN segment as the designated router (DR). The DR priority is based on a DR priority value in the PIM hello message. If the DR priority value is not supplied by all routers, or the priorities match, the highest IP address is used to elect the DR.

The hello message also contains a hold-time value, which is typically 3.5 times the hello interval. If this hold time expires without a subsequent hello message from its neighbor, the device detects a PIM failure on that link.

The configured hold-time changes may not take effect on first two hellos sent after enabling or disabling PIM on an interface. For the first two hellos sent on the interface, thereafter, the configured hold times will be used. This may cause the PIM neighbor to set the incorrect neighbor timeout value for the initial neighbor setup until a hello with the correct hold time is received.

For added security, you can configure an MD5 hash value that the PIM software uses to authenticate PIM hello messages with PIM neighbors.

Join-Prune Messages

When the DR receives an IGMP membership report message from a receiver for a new group or source, the DR creates a tree to connect the receiver to the source by sending a PIM join message out the interface toward the rendezvous point (ASM mode). The rendezvous point (RP) is the root of a shared tree, which is used by all sources and hosts in the PIM domain in the ASM mode.

When the DR determines that the last host has left a group or source, it sends a PIM prune message to remove the path from the distribution tree.

The routers forward the join or prune action hop by hop up the multicast distribution tree to create (join) or tear down (prune) the path.

Note In this publication, the terms “PIM join message” and “PIM prune message” are used to simplify the action taken when referring to the PIM join-prune message with only a join or prune action.

Join-prune messages are sent as quickly as possible by the software. You can filter the join-prune messages by defining a routing policy.

State Refreshes

PIM requires that multicast entries are refreshed within a 3.5-minute timeout interval. The state refresh ensures that traffic is delivered only to active listeners, and it keeps routers from using unnecessary resources.

To maintain the PIM state, the last-hop DR sends join-prune messages once per minute. State creation applies to both (*, G) and (S, G) states as follows:

- (*, G) state creation example—An IGMP (*, G) report triggers the DR to send a (*, G) PIM join message toward the RP.
- (S, G) state creation example—An IGMP (S, G) report triggers the DR to send an (S, G) PIM join message toward the source.

If the state is not refreshed, the PIM software tears down the distribution tree by removing the forwarding paths in the multicast outgoing interface list of the upstream routers.

Rendezvous Points

A rendezvous point (RP) is a router that you select in a multicast network domain that acts as a shared root for a multicast shared tree. You can configure as many RPs as you like, and you can configure them to cover different group ranges.

Static RP

You can statically configure an RP for a multicast group range. You must configure the address of the RP on every router in the domain.

You can define static RPs for the following reasons:

- To configure routers with the Anycast-RP address
- To manually configure an RP on a device

BSRs

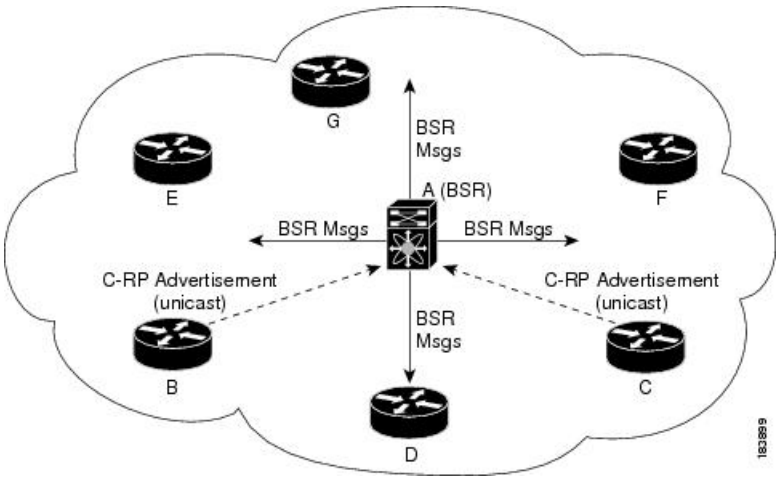
The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs to manage the RPs in the domain. Only one candidate BSR is elected as the BSR for the domain.

BSR is supported on Cisco Nexus 9300-FX, Cisco Nexus 9300-FX2, and Cisco Nexus 9300-FX3S platform switches.

This figure shows the BSR mechanism. Router A, the software-elected BSR, sends BSR messages out all enabled interfaces (shown by the solid lines in the figure). The messages, which contain the RP set, are flooded hop by hop to all routers in the network. Routers B and C are candidate RPs that send their candidate-RP advertisements directly to the elected BSR (shown by the dashed lines in the figure).

The elected BSR receives candidate-RP messages from all the candidate RPs in the domain. The bootstrap message sent by the BSR includes information about all of the candidate RPs. Each router uses a common algorithm to select the same RP address for a given multicast group.

Figure 9: BSR Mechanism



In the RP selection process, the RP address with the best priority is determined by the software. If the priorities match for two or more RP addresses, the software might use the RP hash in the selection process. Only one RP address is assigned to a group.

By default, routers are not enabled to listen or forward BSR messages. You must enable the BSR listening and forwarding feature so that the BSR mechanism can dynamically inform all routers in the PIM domain of the RP set assigned to multicast group ranges.

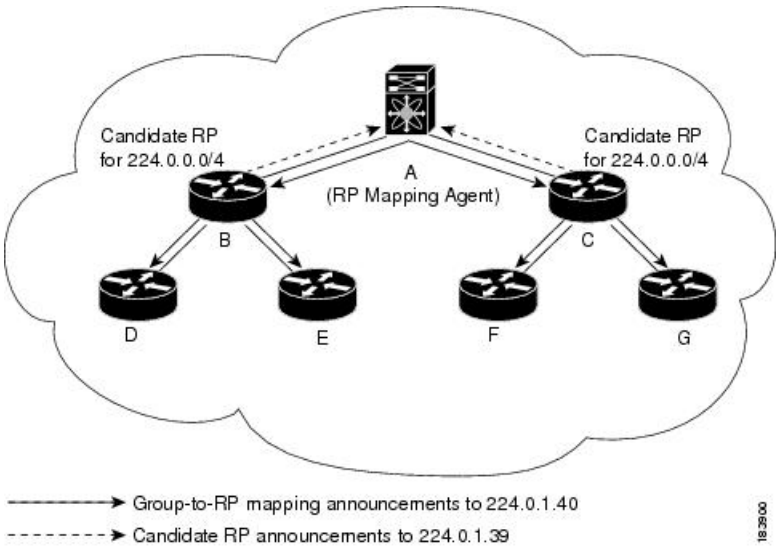
Note The BSR mechanism is a nonproprietary method of defining RPs that can be used with third-party routers.

Auto-RP

Auto-RP is a Cisco protocol that was introduced prior to the Internet standard bootstrap router mechanism. You configure Auto-RP by selecting candidate mapping agents and RPs. Candidate RPs send their supported group range in RP-Announce messages to the Cisco RP-Announce multicast group 224.0.1.39. An Auto-RP mapping agent listens for RP-Announce messages from candidate RPs and forms a Group-to-RP mapping table. The mapping agent multicasts the Group-to-RP mapping table in RP-Discovery messages to the Cisco RP-Discovery multicast group 224.0.1.40.

This figure shows the Auto-RP mechanism. Periodically, the RP mapping agent multicasts the RP information that it receives to the Cisco-RP-Discovery group 224.0.1.40 (shown by the solid lines in the figure).

Figure 10: Auto-RP Mechanism



By default, routers are not enabled to listen or forward Auto-RP messages. You must enable the Auto-RP listening and forwarding feature so that the Auto-RP mechanism can dynamically inform routers in the PIM domain of the group-to-RP mapping.

Caution Do not configure both Auto-RP and BSR protocols in the same network.

Multiple RPs Configured in a PIM Domain

This section describes the election process rules when multiple RPs are configured in a PIM domain.

Anycast-RP

Anycast-RP has two implementations: one uses Multicast Source Discovery Protocol (MSDP) and the other is based on *RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM)*. This section describes how to configure PIM Anycast-RP.

You can use PIM Anycast-RP to assign a group of routers, called the Anycast-RP set, to a single RP address that is configured on multiple routers. The set of routers that you configure as Anycast-RPs is called the Anycast-RP set. This method is the only RP method that supports more than one RP per multicast group, which allows you to load balance across all RPs in the set. The Anycast RP supports all multicast groups.

PIM register messages are sent to the closest RP, and PIM join-prune messages are sent in the direction of the closest RP as determined by the unicast routing protocols. If one of the RPs goes down, unicast routing ensures these messages will be sent in the direction of the next-closest RP.

You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM Bidir RP.

For more information about PIM Anycast-RP, see RFC 4610.

PIM Register Messages

PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The PIM register message has the following functions:

- To notify the RP that a source is actively sending to a multicast group.
- To deliver multicast packets sent by the source to the RP for delivery down the shared tree.

The DR continues to send PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases:

- The RP has no receivers for the multicast group being transmitted.
- The RP has joined the SPT to the source but has not started receiving traffic from the source.

The PIM triggered register is enabled by default.

You can use the **ip pim register-source** command to configure the IP source address of register messages when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation might occur if the source address is filtered so that the packets sent to it are not forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address will fail to reach the DR, resulting in Protocol Independent Multicast sparse mode (PIM-SM) protocol failures.

The following example shows how to configure the IP source address of the register message to the loopback 3 interface of a DR:

```
ip pim register-source loopback 3
```

Note In Cisco NX-OS, PIM register messages are rate limited to avoid overwhelming the RP.

You can filter PIM register messages by defining a routing policy.

Designated Routers

In PIM ASM mode, the software chooses a designated router (DR) from the routers on each network segment. The DR is responsible for forwarding multicast data for specified groups and sources on that segment.

The DR for each LAN segment is determined as described in the Hello messages.

In ASM mode, the DR is responsible for unicasting PIM register packets to the RP. When a DR receives an IGMP membership report from a directly connected receiver, the shortest path is formed to the RP, which may or may not go through the DR. The result is a shared tree that connects all sources transmitting on the same multicast group to all receivers of that group.

ASM Switchover from Shared Tree to Source Tree

Note Cisco NX-OS puts the RPF interface into the OIF-list of the MRIB but not into the OIF-list of the MFIB.

In ASM mode, the DR that is connected to a receiver switches over from the shared tree to the shortest-path tree (SPT) to a source unless you configure the PIM parameter to use shared trees only.

During the switchover, messages on the SPT and shared tree might overlap. These messages are different. The shared tree messages are propagated upstream toward the RP, while SPT messages go toward the source.

For information about SPT switchovers, see the “Last-Hop Switchover to the SPT" section in RFC 4601.

Administratively Scoped IP Multicast

The administratively scoped IP multicast method allows you to set boundaries on the delivery of multicast data. For more information, see RFC 2365.

You can configure an interface as a PIM boundary so that PIM messages are not sent out on that interface.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value.

PIM Graceful Restart

Protocol Independent Multicast (PIM) graceful restart is a multicast high availability (HA) enhancement that improves the convergence of multicast routes (mroutes) after a route processor (RP) switchover. In the event of an RP switchover, the PIM graceful restart feature utilizes the generation ID (GenID) value (defined in RFC 4601) as a mechanism to trigger adjacent PIM neighbors on an interface to send PIM join messages for all (*, G) and (S, G) states that use that interface as a reverse path forwarding (RPF) interface. This mechanism enables PIM neighbors to immediately reestablish those states on the newly active RP.

Generation IDs

A generation ID (GenID) is a randomly generated 32-bit value that is regenerated each time Protocol Independent Multicast (PIM) forwarding is started or restarted on an interface. In order to process the GenID value in PIM hello messages, PIM neighbors must be running Cisco software with an implementation of PIM that is compliant with RFC 4601.

Note PIM neighbors that are not compliant with RFC 4601 and are unable to process GenID differences in PIM hello messages will ignore the GenIDs.

PIM Graceful Restart Operations

This figure illustrates the operations that occur after a route processor (RP) switchover on devices that support the PIM graceful restart feature.

Figure 11: PIM Graceful Restart Operations During an RP Switchover

The PIM graceful restart operations are as follows:

- In steady state, PIM neighbors exchange periodic PIM hello messages.
- An active RP receives PIM joins periodically to refresh multicast route (mroute) states.
- When an active RP fails, the standby RP takes over to become the new active RP.
- The new active RP then modifies the generation ID (GenID) value and sends the new GenID in PIM hello messages to adjacent PIM neighbors.
- Adjacent PIM neighbors that receive PIM hello messages on an interface with a new GenID send PIM graceful restart for all (*, G) and (S, G) mroutes that use that interface as an RPF interface.
- Those mroute states are then immediately reestablished on the newly active RP.

PIM Graceful Restart and Multicast Traffic Flow

Multicast traffic flow on PIM neighbors is not affected if the multicast traffic detects support for PIM graceful restart PIM or PIM hello messages from a node with the failing RP within the default PIM hello hold-time interval. Multicast traffic flow on a failing RP is not affected if it is non-stop forwarding (NSF) capable.

Caution The default PIM hello hold-time interval is 3.5 times the PIM hello period. Multicast high availability (HA) operations might not function as per design if you configure the PIM hello interval with a value lower than the default value of 30 seconds.

High Availability

When a route processor reloads, multicast traffic across VRFs behaves the same as traffic forwarded within the same VRF.

For information about high availability, see the *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*.

Prerequisites for PIM

- You are logged onto the device.
- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

Guidelines and Limitations for PIM

- Configuring a secondary IP address as an RP address is not supported.
- For most Cisco Nexus devices, RPF failure traffic is dropped and sent to the CPU at a very low rate to trigger PIM asserts. For the Cisco Nexus 9000 Series switches, RPF failure traffic is always copied to the CPU in order to learn multicast sources.

- For first-hop source detection in most Cisco Nexus devices, traffic coming from the first hop is detected based on the source subnet check, and multicast packets are copied to the CPU only if the source belongs to the local subnet. The Cisco Nexus 9000 Series switches cannot detect the local source, so multicast packets are sent to the supervisor to learn the local multicast source.
- Cisco NX-OS PIM not interoperate with any version of PIM dense mode or PIM Sparse Mode version 1.
- Cisco Nexus 9300-FX platform switches support PIM and PIM6.
- Cisco Nexus 9000 Series switches support PIM ASM on vPCs.
- PIM bidirectional multicast source VLAN bridging is not supported on FEX ports.
- Multicast heavy template is recommended for optimal bandwidth utilization when using multicast traffic flows.

Guidelines and Limitations for Hello Messages

The following guidelines and limitations apply to Hello Messages:

- Default values for the PIM hello interval are recommended and should not be modified.

Guidelines and Limitations for Rendezvous Points

The following guidelines and limitations apply to Rendezvous Points (RP):

- Configure candidate RP intervals to a minimum of 15 seconds.
- Do not configure both Auto-RP and BSR protocols in the same network.
- PIM6 does not support BSRs and Auto-RP.
- You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM Bidir RP.
- To avoid excessive punts of the RPF failed packets, the Cisco Nexus 9000 Series switches may create S, G entries for active sources in ASM, although there is no rendezvous point (RP) for such group, or in situation when a reverse path forwarding (RPF) fails for the source.

  This behavior does not apply to Nexus 9200, 9300-EX platform switches, and N9K-X9700-EX LC platforms.
- If a device is configured with a BSR policy that should prevent it from being elected as the BSR, the device ignores the policy. This behavior results in the following undesirable conditions:
  - If a device receives a BSM that is permitted by the policy, the device, which incorrectly elected itself as the BSR, drops that BSM so that routers downstream fail to receive it. Downstream devices correctly filter the BSM from the incorrect BSR so that these devices do not receive RP information.
  - A BSM received by a BSR from a different device sends a new BSM but ensures that downstream devices do not receive the correct BSM.

Guidelines and Limitations for Multicast VRF-lite Route Leaking

The following guidelines and limitations apply to multicast VRF-lite route leaking:

Default Settings

This table lists the default settings for PIM parameters.

Table 4: Default PIM Parameters

Parameters	Default
Use shared trees only	Disabled
Flush routes on restart	Disabled
Log neighbor changes	Disabled
Auto-RP message action	Disabled
BSR message action	Disabled
PIM sparse mode	Disabled
Designated router priority	1
Hello authentication mode	Disabled
Domain border	Disabled
RP address policy	No message filtering
PIM register message policy	No message filtering
BSR candidate RP policy	No message filtering
BSR policy	No message filtering
Auto-RP mapping agent policy	No message filtering
Auto-RP RP candidate policy	No message filtering
Join-prune policy	No message filtering
Neighbor adjacency policy	Become adjacent with all PIM neighbors
BFD	Disabled

Configuring PIM

Note Cisco NX-OS supports only PIM sparse mode version 2. In this publication, "PIM" refers to PIM sparse mode version 2.

You can configure separate ranges of addresses in the PIM domain using the multicast distribution modes described in the table below.

Multicast Distribution Mode	Requires RP Configuration	Description
ASM	Yes	Any source multicast
RPF routes for multicast	No	RPF routes for multicast

PIM Configuration Tasks

The following steps configure PIM .

1. Select the range of multicast groups that you want to configure in each multicast distribution mode.
2. Enable PIM .
3. Follow the configuration steps for the multicast distribution modes that you selected in Step 1.
   - For ASM mode, see Configuring ASM.
   - For RPF routes for multicast, see Configuring RPF Routes for Multicast.
4. Configure message filtering.

Note The CLI commands used to configure PIM are as follows:

- Configuration commands begin with **ip pim**.
- Show commands begin with **show ip pim**.

Enabling the PIM Feature

Before you can access the PIM commands, you must enable the PIM feature.

Before you begin

Ensure that you have installed the Enterprise Services license.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature pim** **Example:** `switch(config)# feature pim`	Enables PIM. By default, PIM is disabled.
Step 3	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Shows the running-configuration information for PIM.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring PIM Sparse Mode Parameters

You configure PIM sparse mode on every device interface that you want to participate in a sparse mode domain. You can configure the sparse mode parameters described in the table below.

Table 5: PIM Sparse Mode Parameters

Parameter	Description
Global to the device	
Auto-RP message action	Enables listening for and forwarding of Auto-RP messages. The default is disabled, which means that the router does not listen for or forward Auto-RP messages unless it is configured as a candidate RP or mapping agent.
BSR message action	Enables listening for and forwarding of BSR messages. The default is disabled, which means that the router does not listen for or forward BSR messages unless it is configured as a candidate RP or BSR candidate.
Register rate limit	Configures the IPv4 register rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.

Parameter	Description
Initial holddown period	Configures the IPv4 initial holddown period in seconds. This holddown period is the time it takes for the MRIB to come up initially. If you want faster convergence, enter a lower value. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Per device interface	
PIM sparse mode	Enables PIM on an interface.
Designated router priority	Sets the designated router (DR) priority that is advertised in PIM hello messages on this interface. On a multi-access network with multiple PIM-enabled routers, the router with the highest DR priority is elected as the DR router. If the priorities match, the software elects the DR with the highest IP address. The DR originates PIM register messages for the directly connected multicast sources and sends PIM join messages toward the rendezvous point (RP) for directly connected receivers. Values range from 1 to 4294967295. The default is 1.
Designated router delay	Delays participation in the designated router (DR) election by setting the DR priority that is advertised in PIM hello messages to 0 for a specified period. During this delay, no DR changes occur, and the current switch is given time to learn all of the multicast states on that interface. After the delay period expires, the correct DR priority is sent in the hello packets, which retriggers the DR election. Values range from 3 to 0xffff seconds.
Hello authentication mode	Enables an MD5 hash authentication key, or password, in PIM hello messages on the interface so that directly connected neighbors can authenticate each other. The PIM hello messages are IPsec encoded using the Authentication Header (AH) option. You can enter an unencrypted (cleartext) key or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The authentication key can be up to 16 characters. The default is disabled.

Parameter	Description
Hello interval	Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000. **Note** See the *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide* for the verified range of this parameter and associated PIM neighbor scale.
Domain border	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.
Neighbor policy	Configures which PIM neighbors to become adjacent to based on a prefix-list policy.[2] If the policy name does not exist or no prefix lists are configured in a policy, adjacency is established with all neighbors. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you should configure this feature only if you are an experienced network administrator. **Note** The PIM neighbor policy supports only prefix lists. It does not support ACLs used inside a route map.

[2] To configure prefix-list policies, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Configuring PIM Sparse Mode Parameters

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]} **Example:** `switch(config)# ip pim auto-rp listen`	Enables listening for or forwarding of Auto-RP messages. The default is disabled, which means that the software does not listen for or forward Auto-RP messages.

	Command or Action	Purpose
Step 3	(Optional) **ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} **Example:** `switch(config)# ip pim bsr forward`	Enables listening for or forwarding of BSR messages. The default is disabled, which means that the software does not listen for or forward BSR messages.
Step 4	(Optional) **ip pim register-rate-limit** *rate* **Example:** `switch(config)# ip pim register-rate-limit 1000`	Configures the rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Step 5	(Optional) **ip pim spt-threshold infinity group-list** *route-map-name* **Example:** `switch(config)# ip pim spt-threshold infinity group-list my_route-map-name`	Creates the IPv4 PIM (*, G) state only, for the group prefixes defined in the specified route map. Cisco NX-OS Release 3.1 supports up to 1000 route-map entries, and Cisco NX-OS releases prior to 3.1 support up to 500 route-map entries. **Note** The **ip pim use-shared-tree-only group-list** command performs the same function as the **ip pim spt-threshold infinity group-list** command. You can choose to use either command to implement this step. Both the commands (**ip pim spt-threshold infinity group-list** and **ip pim use-shared-tree-only group-list** has the following limitations: • It is only supported for virtual port channels (vPC) on the Cisco Nexus 9000 Cloud Scale Switches. • It is supported in standalone (non-vPC) Last Hop Router (LHR) configurations.
Step 6	(Optional) [**ip** | **ipv4**] **routing multicast holddown** *holddown-period* **Example:** `switch(config)# ip routing multicast holddown 100`	Configures the initial holddown period in seconds. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Step 7	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Displays PIM running-configuration information.

	Command or Action	Purpose

Step 8	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 9	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 10	(Optional) **ip pim dr-priority** *priority* **Example:** `switch(config-if)# ip pim dr-priority 192`	Sets the designated router (DR) priority that is advertised in PIM hello messages. Values range from 1 to 4294967295. The default is 1.
Step 11	(Optional) **ip pim dr-delay** *delay* **Example:** `switch(config-if)# ip pim dr-delay 3`	Delays participation in the designated router (DR) election by setting the DR priority that is advertised in PIM hello messages to 0 for a specified period. During this delay, no DR changes occur, and the current switch is given time to learn all of the multicast states on that interface. After the delay period expires, the correct DR priority is sent in the hello packets, which retriggers the DR election. Values range from 3 to 0xffff seconds. **Note** This command delays participation in the DR election only upon bootup or following an IP address or interface state change. It is intended for use with multicast-access non-vPC Layer 3 interfaces only.
Step 12	(Optional) **ip pim hello-authentication ah-md5** *auth-key* **Example:** `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	Enables an MD5 hash authentication key in PIM hello messages. You can enter an unencrypted (cleartext) key or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The key can be up to 16 characters. The default is disabled.

	Command or Action	Purpose
Step 13	(Optional) **ip pim hello-interval** *interval* **Example:** `switch(config-if)# ip pim hello-interval 25000`	Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000. **Note** The minimum value is 1 millisecond.
Step 14	(Optional) **ip pim border** **Example:** `switch(config-if)# ip pim border`	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.
Step 15	(Optional) **ip pim neighbor-policy prefix-list** *prefix-list* **Example:** `switch(config-if)# ip pim neighbor-policy prefix-list AllowPrefix`	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. Also configures which PIM neighbors to become adjacent to based on a prefix-list policy with the **ip prefix-list** *prefix-list* command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 16	(Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-if)# show ip pim interface`	Displays PIM interface information.
Step 17	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring ASM

To configure ASM mode, you configure sparse mode and the RP selection method, where you indicate the distribution mode and assign the range of multicast groups.

Configuring Static RPs

You can configure an RP statically by configuring the RP address on every router that will participate in the PIM domain.

Note We recommend that the RP address uses the loopback interface and also the interface with the RP address must have **ip pim sparse-mode** enabled.

You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command or specify a prefix-list method of configuration.

Note Cisco NX-OS always uses the longest-match prefix to find the RP, so the behavior is the same irrespective of the position of the group prefix in the route map or in the prefix list.

The following example configuration produces the same output using Cisco NX-OS (231.1.1.0/24 is always denied irrespective of the sequence number):

```
ip prefix-list plist seq 10 deny 231.1.1.0/24
ip prefix-list plist seq 20 permit 231.1.0.0/16
ip prefix-list plist seq 10 permit 231.1.0.0/16
ip prefix-list plist seq 20 deny 231.1.1.0/24
```

Configuring Static RPs

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **prefix-list** *name* |**override** |**route-map** *policy-name*] [**bidir**] **Example:** `switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9`	Configures a PIM static RP address for a multicast group range. You can specify a prefix-list policy name for the static RP address or a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The mode is ASM. The **override** option causes the RP address to override the dynamically learned RP addresses for specified groups in route-map.

	Command or Action	Purpose
		The example configures PIM ASM mode for the specified group range.
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM RP information, including BSR listen and forward states.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring BSRs

You configure BSRs by selecting candidate BSRs and RPs.

Caution Do not configure both Auto-RP and BSR protocols in the same network.

You can configure a candidate BSR with the arguments described in the table below.

Table 6: Candidate BSR Arguments

Argument	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.
hash-length	Number of high order 1s used to form a mask that is ANDed with group address ranges of candidate RPs to form a hash value. The mask determines the number of consecutive addresses to assign across RPs with the same group range. For PIM, this value ranges from 0 to 32 and has a default of 30.
priority	Priority assigned to this BSR. The software elects the BSR with the highest priority, or if the BSR priorities match, the software elects the BSR with the highest IP address. This value ranges from 0, the lowest priority, to 255 and has a default of 64.

Configuring BSRs Candidate RP Arguments and Keywords

You can configure a candidate RP with the arguments and keywords described in this table.

Table 7: BSR Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP specified in a prefix format.
interval	Number of seconds between sending candidate-RP messages. This value ranges from 1 to 65,535 and has a default of 60 seconds. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
priority	Priority assigned to this RP. The software elects the RP with the highest priority for a range of groups or, if the priorities match, the highest IP address. (The highest priority is the lowest numerical value.) This value ranges from 0, the highest priority, to 255 and has a default of 192. **Note** This priority differs from the BSR BSR-candidate priority, which prefers the highest value between 0 and 255.
route-map *policy-name*	Route-map policy name that defines the group prefixes where this feature is applied.

Tip You should choose the candidate BSRs and candidate RPs that have good connectivity to all parts of the PIM domain.

You can configure the same router to be both a BSR and a candidate RP. In a domain with many routers, you can select multiple candidate BSRs and RPs to automatically fail over to alternates if a BSR or an RP fails.

To configure candidate BSRs and RPs, follow these steps:

1. Configure whether each router in the PIM domain should listen for and forward BSR messages. A router configured as either a candidate RP or a candidate BSR will automatically listen for and forward all bootstrap router protocol messages, unless an interface is configured with the domain border feature.
2. Select the routers to act as candidate BSRs and RPs.
3. Configure each candidate BSR and candidate RP as described in this section.
4. Configure BSR message filtering.

Configuring BSRs

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim bsr** {**forward** [**listen**] | **listen** [**forward**]} **Example:** `switch(config)# ip pim bsr listen forward`	Configures listen and forward. Ensure that you have entered this command in each VRF on the remote PE.
Step 3	**ip pim** [**bsr**] **bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*] **Example:** `switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24`	Configures a candidate bootstrap router (BSR). The source IP address used in a bootstrap message is the IP address of the interface. The hash length ranges from 0 to 32 and has a default of 30. The priority ranges from 0 to 255 and has a default of 64.
Step 4	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 5	(Optional) **ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* **Example:** `switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	Configures a candidate RP for BSR. The priority ranges from 0, the highest priority, to 65,535 and has a default of 192. The interval ranges from 1 to 65,535 seconds and has a default of 60. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.
Step 6	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 7	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Configuring Auto-RP

You can configure Auto-RP by selecting candidate mapping agents and RPs. You can configure the same router to be both a mapping agent and a candidate RP.

Caution Do not configure both Auto-RP and BSR protocols in the same network.

You can configure an Auto-RP mapping agent with the arguments described in this table.

Table 8: Auto-RP Mapping Agent Arguments

Argument	Description
interface	Interface type and number used to derive the IP address of the Auto-RP mapping agent used in bootstrap messages.
scope *ttl*	Time-to-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32.

If you configure multiple Auto-RP mapping agents, only one is elected as the mapping agent for the domain. The elected mapping agent ensures that all candidate RP messages are sent out. All mapping agents receive the candidate RP messages and advertise the same RP cache in their RP-discovery messages.

You can configure a candidate RP with the arguments and keywords described in this table.

Table 9: Auto-RP Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the IP address of the candidate RP used in bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP. It is specified in a prefix format.
scope *ttl*	Time-to-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32.

Argument or Keyword	Description
interval	Number of seconds between sending RP-Announce messages. This value can range from 1 to 65,535 and has a default of 60. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
route-map *policy-name*	Route-map policy name that defines the group prefixes where this feature is applied.

Tip You should choose mapping agents and candidate RPs that have good connectivity to all parts of the PIM domain.

To configure Auto-RP mapping agents and candidate RPs, follow these steps:

1. For each router in the PIM domain, configure whether that router should listen for and forward Auto-RP messages. A router configured as either a candidate RP or an Auto-RP mapping agent will automatically listen for and forward all Auto-RP protocol messages, unless an interface is configured with the domain border feature.
2. Select the routers to act as mapping agents and candidate RPs.
3. Configure each mapping agent and candidate RP as described in this section.
4. Configure Auto-RP message filtering.

Ensure that you have installed the Enterprise Services license and enabled PIM.

Configuring Auto RP (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim** {**send-rp-discovery** | **auto-rp mapping-agent**} *interface* [**scope** *ttl*] **Example:** `switch(config)# ip pim auto-rp mapping-agent ethernet 2/1`	Configures an Auto-RP mapping agent. The source IP address used in Auto-RP Discovery messages is the IP address of the interface. The default scope is 32.

	Command or Action	Purpose
Step 3	**ip pim** {**send-rp-announce** | **auto-rp rp-candidate**} *interface* {**group-list** *ip-prefix* | **prefix-list** *name* | **route-map** *policy-name*} [**scope** *ttl*] **interval** *interval*] [**bidir**] **Example:** `switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	Configures an Auto-RP candidate RP. The default scope is 32. The default interval is 60 seconds. By default, the command creates an ASM candidate RP. Use the **bidir** option to create a Bidir candidate RP. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.
Step 4	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 5	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring a PIM Anycast-RP Set

To configure a PIM Anycast-RP set, follow these steps:

1. Select the routers in the PIM Anycast-RP set.
2. Select an IP address for the PIM Anycast-RP set.
3. Configure each peer RP in the PIM Anycast-RP set as described in this section.

Configuring a PIM Anycast RP Set

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**interface loopback** *number*
	Example:
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		Configures an interface loopback.
		This example configures interface loopback 0.

Step 3	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 192.168.1.1/32`	Configures an IP address for this interface. It should be a unique IP address that helps to identify this router.
Step 4	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode.
Step 5	**ip router** *routing-protocol-configuration* **Example:** `switch(config-if)# ip router ospf 1 area 0.0.0.0`	Enables the interface to be reachable by other routers in the Anycast RP set.

Step 6	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 7	**interface loopback** *number*
	Example:
	`switch(config)# interface loopback 1`
	`switch(config-if)#`
		Configures an interface loopback.
		This example configures interface loopback 1.

Step 8	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 10.1.1.1/32`	Configures an IP address for this interface. It should be a common IP address that acts as the Anycast RP address.
Step 9	**ip router** *routing-protocol-configuration* **Example:** `switch(config-if)# ip router ospf 1 area 0.0.0.0`	Enables the interface to be reachable by other routers in the Anycast RP set.

Step 10	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

	Command or Action	Purpose
Step 11	**ip pim rp-address** *anycast-rp-address* [**group-list** *ip-address*] **Example:** `switch(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4`	Configures the PIM Anycast RP address.
Step 12	**ip pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address* **Example:** `switch(config)# ip pim anycast-rp 10.1.1.1 192.168.1.1`	Configures a PIM Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.
Step 13	Repeat Step 13 using the same Anycast-RP address for each peer router in the RP set (including the local router).	—
Step 14	(Optional) **show ip pim rp** **Example:** `switch(config)# show ip pim rp`	Displays the PIM RP mapping.
Step 15	(Optional) **show ip mroute** *ip-address* **Example:** `switch(config)# show ip mroute 239.1.1.1`	Displays the mroute entries.
Step 16	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 17	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Shared Trees Only for ASM

You can configure shared trees only on the last-hop router for Any Source Multicast (ASM) groups, which means that the router never switches over from the shared tree to the SPT when a receiver joins an active group. You can specify a group range where the use of shared trees is to be enforced with the **match ip multicast** command. This option does not affect the normal operation of the router when a source tree join-prune message is received.

Note The Cisco NX-OS software does not support the shared-tree feature on vPCs. For more information about vPCs, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.

The default is disabled, which means that the software can switch over to source trees.

Note In ASM mode, only the last-hop router switches from the shared tree to the SPT.

Configuring Shared Trees Only for ASM

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim use-shared-tree-only group-list** *policy-name* **Example:** `switch(config)# ip pim use-shared-tree-only group-list my_group_policy`	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy name that lists the groups to use with the **match ip multicast** command. By default, the software triggers a PIM (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state. This command has the following limitations: • It is only supported for virtual port channels (vPC) on the Cisco Nexus 9000 Cloud Scale Switches. • It is supported in standalone (non-vPC) Last Hop Router (LHR) configurations.
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring RPF Routes for Multicast

You can define reverse path forwarding (RPF) routes for multicast when you want multicast data to diverge from the unicast traffic path. You can define RPF routes for multicast on border routers to enable RPF to an external network.

Multicast routes are used not to directly forward traffic but to make RPF checks. RPF routes for multicast cannot be redistributed.

Note IPv6 static multicast routes are not supported.

Note If the **ip multicast multipath s-g-hash** CLI is not configured, the multicast traffic may fail the RFP check.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* | *interface*} [*route-preference*] [**vrf** *vrf-name*] **Example:** `switch(config)# ip mroute 192.0.2.33/1 224.0.0.0/1`	Configures an RPF route for multicast for use in RPF calculations. Route preference values range from 1 to 255. The default preference is 1.
Step 3	(Optional) **show ip static-route** [**multicast**] [**vrf** *vrf-name*] **Example:** `switch(config)# show ip static-route multicast`	Displays configured static routes.
Step 4	(Optional) **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring Multicast Multipath

By default, the RPF interface for multicast is chosen automatically when multiple ECMP paths are available.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip multicast multipath** {**none** | **resilient** | **s-g-hash**} **Example:** `switch(config)# ip multicast multipath none`	Configure multicast multipath using the following options: • **none**—Disables multicast multipath by suppressing hashing across multiple ECMPs in the URIB RPF lookup. With this option, the highest RPF neighbor (next-hop) address is used for the RPF interface. **Note** Use the **ip multicast multipath none** command to completely disable hashing. • **s-g-hash**—Initiates S, G, nexthop hashing (rather than the default of S/RP, G-based hashing) to select the RPF interface. This option configures the hash based on source and group address. This is the default setting. • **resilient**—If the ECMP path list changes and the old RPF information is still part of the ECMP, this option uses the old RPF information instead of performing a rehash and potentially changing the RPF information. The **ip multicast multipath resilient** command is for maintaining resiliency (Stickiness) to the current RPF if there is a path in the route reachability notification from URIB. **Note** The **no ip multicast multipath resilient** command disables the stickiness algorithm. This command is independent of the hashing algorithm.
Step 3	**clear ip mroute** * **Example:** `switch(config)# clear ip mroute *`	Clears multipath routes and activates multicast multipath suppression.

Configuring Route Maps to Control RP Information Distribution

You can configure route maps to help protect against some RP configuration errors and malicious attacks.

By configuring route maps, you can control distribution of RP information that is distributed throughout the network. You specify the BSRs or mapping agents to be listened to on each client router and the list of candidate RPs to be advertised (listened to) on each BSR and mapping agent to ensure that what is advertised is what you expect.

Note Only the **match ipv6 multicast** command has an effect in the route map.

Ensure that you have installed the Enterprise Services license and enabled PIM.

Configuring Route Maps to Control RP Information Distribution (PIM)

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
	Example:
	`switch(config)# route-map ASM_only permit 10`
	`switch(config-route-map)#`
		Enters route-map configuration mode.

Step 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ip-prefix*} {**source** *source-ip-address*} **Example:** `switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM`	Matches the group, RP, and RP type specified. You can specify the RP type (ASM). This configuration method requires the group and RP specified as shown in the example.
Step 4	(Optional) **show route-map** **Example:** `switch(config-route-map)# show route-map`	Displays configured route maps.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-route-map)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Message Filtering

Note Prefix matches in the rp-candidate-policy must be exact relative to what the c-rp is advertising. Subset matches are not possible.

You can configure filtering of the PIM messages described in the table below.

Table 10: PIM Message Filtering

Message Type	Description
Global to the Device	
Log Neighbor changes	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
PIM register policy	Enables PIM register messages to be filtered based on a route-map policy[3] where you can specify group or group and source addresses with the **match ip multicast** command. This policy applies to routers that act as an RP. The default is disabled, which means that the software does not filter PIM register messages.
BSR candidate RP policy	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses with the **match ip multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages.
BSR policy	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.
Auto-RP candidate RP policy	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses with the **match ip multicast** command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages.

Message Type	Description
Auto-RP mapping agent policy	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages. **Note** PIM6 does not support the Auto-RP method.
Per Device Interface	
Join-prune policy	Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the **match ip multicast** command. The default is no filtering of join-prune messages.

[3] For information about configuring route-map policies, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Route maps as a filtering policy can be used (either **permit** or **deny** for each statement) for the following commands:

- The **jp-policy** command can use (S,G), (*,G), or (RP,G).
- The **register-policy** command can use (S,G) or (*,G).
- The **igmp report-policy** command can use (*,G) or (S,G).
- The **state-limit reserver-policy** command can use (*,G) or (S,G).
- The **auto-rp rp-candidate-policy** command can use (RP,G).
- The **bsr rp-candidate-policy** command can use (RP,G).
- The **autorp mapping-agent policy** command can use (S).
- The **bsr bsr-policy** command can use (S).

Route maps as containers can be used for the following commands, where the route-map action (**permit** or **deny**) is ignored:

- The **ip pim rp-address route map** command can use only G.
- The **ip igmp static-oif route map** command can use (S,G), (*,G), (S,G-range), (*,G-range).
- The **ip igmp join-group route map** command can use (S,G), (*,G), (S,G-range, (*, G-range).

Configuring Message Filtering

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **ip pim log-neighbor-changes** **Example:** `switch(config)# ip pim log-neighbor-changes`	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
Step 3	(Optional) **ip pim register-policy** *policy-name* **Example:** `switch(config)# ip pim register-policy my_register_policy`	Enables PIM register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ip multicast** command.
Step 4	(Optional) **ip pim bsr rp-candidate-policy** *policy-name* **Example:** `switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy`	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses with the **match ip multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages.
Step 5	(Optional) **ip pim bsr bsr-policy** *policy-name* **Example:** `switch(config)# ip pim bsr bsr-policy my_bsr_policy`	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.
Step 6	(Optional) **ip pim auto-rp rp-candidate-policy** *policy-name* **Example:** `switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy`	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses with the **match ip multicast** command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages.
Step 7	(Optional) **ip pim auto-rp mapping-agent-policy** *policy-name* **Example:** `switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy`	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages.

	Command or Action	Purpose

Step 8	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

Step 9	(Optional) **ip pim jp-policy** *policy-name* [**in** | **out**] **Example:** `switch(config-if)# ip pim jp-policy my_jp_policy`	Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the **match ip multicast** command. The default is no filtering of join-prune messages.
Step 10	(Optional) **show run pim** **Example:** `switch(config-if)# show run pim`	Displays PIM configuration commands.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Restarting the PIM Processes

When routes are flushed, they are removed from the Multicast Routing Information Base (MRIB) and the Multicast Forwarding Information Base (MFIB).

When you restart PIM, the following tasks are performed:

- The PIM database is deleted.
- The MRIB and MFIB are unaffected and forwarding of traffic continues.
- The multicast route ownership is verified through the MRIB.
- Periodic PIM join and prune messages from neighbors are used to repopulate the database.

Restarting the PIM Process

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose
Step 1	**restart pim** **Example:**	Restarts the PIM process.

	Command or Action	Purpose
	`switch# restart pim`	**Note** Traffic loss might occur during the restart process.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**ip pim flush-routes** **Example:** `switch(config)# ip pim flush-routes`	Removes routes when the PIM process is restarted. By default, routes are not flushed.
Step 4	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Displays the PIM running-configuration information, including the **flush-routes** command.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring BFD for PIM in VRF Mode

Note You can configure Bidirectional Forwarding Detection (BFD) for PIM by either VRF or interface.

Before you begin

Ensure that you have installed the Enterprise Services license, enabled PIM, and enabled BFD.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vrf context** *vrf-name*
	Example:
	`switch# vrf context test`
	`switch(config-vrf)#`
		Enters VRF configuration mode.

	Command or Action	Purpose
Step 3	**ip pim bfd** **Example:** `switch(config-vrf)# ip pim bfd`	Enables BFD on the specified VRF. **Note** You can also enter the **ip pim bfd** command in global configuration mode, which enables BFD on the VRF instance.

Configuring BFD for PIM in Interface Mode

Before you begin

Ensure that you have installed the Enterprise Services license, enabled PIM, and enabled BFD.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface-type*
	Example:
	`switch(config)# interface ethernet 7/40`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	**ip pim bfd instance** **Example:** `switch(config-if)# ip pim bfd instance`	Enables BFD on the specified interfaces. You can enable or disable BFD on PIM interfaces irrespective of whether BFD is enabled on the VRF.
Step 4	(Optional) **show running-configuration pim** **Example:** `switch(config-if)# show running-configuration pim`	Displays the PIM running-configuration information.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the PIM Configuration

To display the PIM configuration information, perform one of the following tasks.

Command	Description
show ip mroute [*ip-address*] [**detail** | **summary**]	Displays the IP multicast routing table. The **detail** option displays detailed route attributes. The **summary** option displays route counts and packet rates.
show ip pim group-range [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays the learned or configured group ranges and modes. For similar information, see the **show ip pim rp** command.
show ip pim interface [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	Displays information by the interface.
show ip pim neighbor [**interface** *interface* | *ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays neighbors by the interface.
show ip pim oif-list *group* [*source*] [**vrf** *vrf-name* | **all**]	Displays all the interfaces in the outgoing interface (OIF) list.
show ip pim route [*source* | *group* [*source*]] [**vrf** *vrf-name* | **all**]	Displays information for each multicast route, including interfaces on which a PIM join for that (S, G) has been received.
show ip pim rp [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays rendezvous points (RPs) known to the software, how they were learned, and their group ranges. For similar information, see the **show ip pim group-range** command.
show ip pim rp-hash *group* [**vrf** *vrf-name* | **all**]	Displays the bootstrap router (BSR) RP hash information.
show running-config pim	Displays the running-configuration information.
show startup-config pim	Displays the startup-configuration information.
show ip pim vrf [*vrf-name* | **all**] [**detail**]	Displays per-VRF information.

Displaying Statistics

You can display and clear PIM statistics by using the commands in this section.

Displaying PIM Statistics

You can display the PIM statistics and memory usage using these commands.

Command	Description
show ip pim policy statistics	Displays policy statistics for register, RP, and join-prune message policies.

Command	Description
show ip pim statistics [**vrf** *vrf-name*]	Displays global statistics.

Clearing PIM Statistics

You can clear the PIM statistics using these commands.

Command	Description
clear ippim interface statistics *interface*	Clears counters for the specified interface.
clear ip pim policy statistics	Clears policy counters for register, RP, and join-prune message policies.
clear ip pim statistics [**vrf** *vrf-name*]	Clears global counters handled by the PIM process.

Configuration Examples for PIM

This section describes how to configure PIM using different data distribution modes and RP selection methods.

BSR Configuration Example

To configure PIM in ASM mode using the BSR mechanism, follow these steps for each router in the PIM domain:

1. Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2. Configure whether that router should listen and forward BSR messages.

```
switch# configure terminal
switch(config)# ip pim bsr forward listen
```

3. Configure the BSR parameters for each router that you want to act as a BSR.

```
switch# configure terminal
switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 30
```

4. Configure the RP parameters for each router that you want to act as a candidate RP.

```
switch# configure terminal
switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
```

5. Configure message filtering.

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

The following example shows how to configure PIM ASM mode using the BSR mechanism and how to configure the BSR and RP on the same router:

```
configure terminal
  interface ethernet 2/1
    ip pim sparse-mode
    exit
  ip pim bsr forward listen
ip pim bsr-candidate ethernet 2/1 hash-len 30
  ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
  ip pim log-neighbor-changes
```

PIM Anycast RP Configuration Example

To configure ASM mode using the PIM Anycast-RP method, follow these steps for each router in the PIM domain:

1. Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2. Configure the RP address that you configure on all routers in the Anycast-RP set.

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.3/32
switch(config-if)# ip pim sparse-mode
```

3. Configure a loopback with an address to use in communication between routers in the Anycast-RP set for each router that you want to be in the Anycast-RP set.

```
switch# configure terminal
switch(config)# interface loopback 1
switch(config-if)# ip address 192.0.2.31/32
switch(config-if)# ip pim sparse-mode
```

4. Configure the Anycast-RP parameters and repeat with the IP address of each Anycast-RP for each router that you want to be in the Anycast-RP set. This example shows two Anycast-RPs.

```
switch# configure terminal
switch(config)# ip pim anycast-rp 192.0.2.3 193.0.2.31
switch(config)# ip pim anycast-rp 192.0.2.3 193.0.2.32
```

5. Configure message filtering.

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

The following example shows how to configure PIM Anycast RP for IPv6:

```
configure terminal
interface loopback 0
ipv6 address 2001:0db8:0:abcd::5/32
ipv6 pim sparse-mode
ipv6 router ospfv3 1 area 0.0.0.0
exit
interface loopback 1
ipv6 address 2001:0db8:0:abcd::1111/32
ipv6 pim sparse-mode
ipv6 router ospfv3 1 area 0.0.0.0
exit
ipv6 pim rp-address 2001:0db8:0:abcd::1111 group-list ff1e:abcd:def1::0/24
ipv6 pim anycast-rp 2001:0db8:0:abcd::5 2001:0db8:0:abcd::1111
```

The following example shows how to configure PIM ASM mode using two Anycast-RPs:

```
configure terminal
interface ethernet 2/1
ip pim sparse-mode
exit
interface loopback 0
ip address 192.0.2.3/32
ip pim sparse-mode
exit
interface loopback 1
ip address 192.0.2.31/32
ip pim sparse-mode
exit
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
ip pim log-neighbor-changes
```

Prefix-Based and Route-Map-Based Configurations

```
ip prefix-list plist11 seq 10 deny 231.129.128.0/17
ip prefix-list plist11 seq 20 deny 231.129.0.0/16
ip prefix-list plist11 seq 30 deny 231.128.0.0/9
ip prefix-list plist11 seq 40 permit 231.0.0.0/8

ip prefix-list plist22 seq 10 deny 231.129.128.0/17
ip prefix-list plist22 seq 20 deny 231.129.0.0/16
ip prefix-list plist22 seq 30 permit 231.128.0.0/9
ip prefix-list plist22 seq 40 deny 231.0.0.0/8

ip prefix-list plist33 seq 10 deny 231.129.128.0/17
ip prefix-list plist33 seq 20 permit 231.129.0.0/16
ip prefix-list plist33 seq 30 deny 231.128.0.0/9
ip prefix-list plist33 seq 40 deny 231.0.0.0/8

ip pim rp-address 172.21.0.11 prefix-list plist11
ip pim rp-address 172.21.0.22 prefix-list plist22
ip pim rp-address 172.21.0.33 prefix-list plist33
route-map rmap11 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap11 deny 20
```

```
 match ip multicast group 231.129.0.0/16
route-map rmap11 deny 30
 match ip multicast group 231.128.0.0/9
route-map rmap11 permit 40
 match ip multicast group 231.0.0.0/8

route-map rmap22 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap22 deny 20
 match ip multicast group 231.129.0.0/16
route-map rmap22 permit 30
 match ip multicast group 231.128.0.0/9
route-map rmap22 deny 40
 match ip multicast group 231.0.0.0/8

route-map rmap33 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap33 permit 20
 match ip multicast group 231.129.0.0/16
route-map rmap33 deny 30
 match ip multicast group 231.128.0.0/9
route-map rmap33 deny 40
 match ip multicast group 231.0.0.0/8

ip pim rp-address 172.21.0.11 route-map rmap11
ip pim rp-address 172.21.0.22 route-map rmap22
ip pim rp-address 172.21.0.33 route-map rmap33
```

Output

```
dc3rtg-d2(config-if)# show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

RP: 172.21.0.11, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap11, group ranges:
      231.0.0.0/8  231.128.0.0/9 (deny)
      231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 172.21.0.22, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap22, group ranges:
      231.0.0.0/8 (deny) 231.128.0.0/9
      231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 172.21.0.33, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap33, group ranges:
      231.0.0.0/8 (deny) 231.128.0.0/9 (deny)
      231.129.0.0/16  231.129.128.0/17 (deny)

dc3rtg-d2(config-if)# show ip mroute
IP Multicast Routing Table for VRF "default"

(*, 231.1.1.1/32), uptime: 00:07:20, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:07:20, igmp

(*, 231.128.1.1/32), uptime: 00:14:27, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
```

```
    loopback1, uptime: 00:14:27, igmp

(*, 231.129.1.1/32), uptime: 00:14:25, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:25, igmp

(*, 231.129.128.1/32), uptime: 00:14:26, igmp pim ip
  Incoming interface: Null, RPF nbr: 10.0.0.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:26, igmp

(*, 232.0.0.0/8), uptime: 1d20h, pim ip
  Incoming interface: Null, RPF nbr: 10.0.0.1
  Outgoing interface list: (count: 0)

dc3rtg-d2(config-if)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
232.0.0.0/8        ASM       -                -
231.0.0.0/8        ASM       172.21.0.11      -
231.128.0.0/9      ASM       172.21.0.22      -
231.129.0.0/16     ASM       172.21.0.33      -
231.129.128.0/17   Unknown   -                -
```

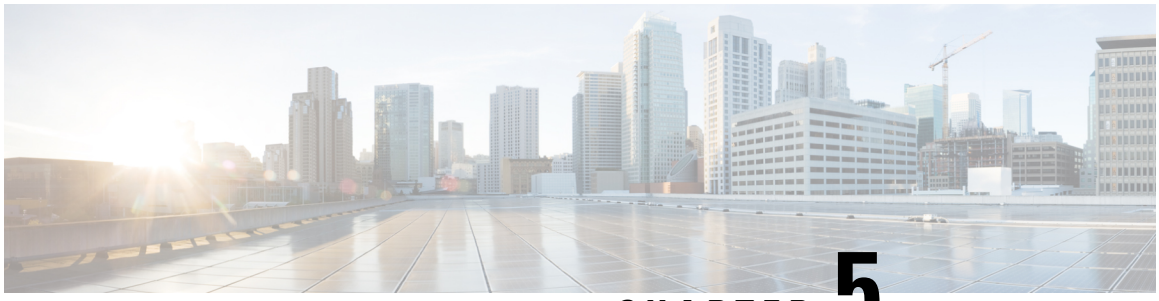
Related Documents

Related Topic	Document Title
Configuring VRFs	*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*

Standards

MIBs

MIBs	MIBs Link
MIBs related to PIM	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



CHAPTER 5

Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on a Cisco NX-OS device.

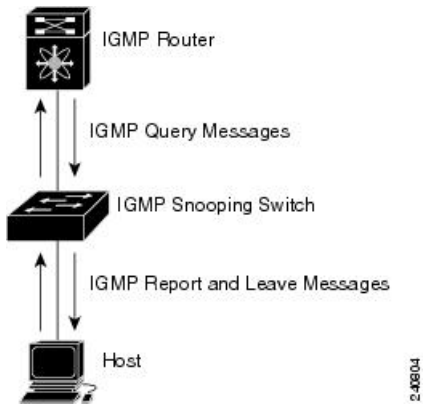
About IGMP Snooping

Note We recommend that you do not disable IGMP snooping on the device. If you disable IGMP snooping, you might see reduced multicast performance because of excessive false flooding within the device.

IGMP snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. IGMP snooping tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the device.

This figure shows an IGMP snooping switch that sits between the host and the IGMP router. The IGMP snooping switch snoops the IGMP membership reports and Leave messages and forwards them only when necessary to the connected IGMP routers.

Figure 12: IGMP Snooping Switch



The IGMP snooping software operates upon IGMPv1, IGMPv2, and IGMPv3 control plane packets where Layer 3 control plane packets are intercepted and influence the Layer 2 forwarding behavior.

The Cisco NX-OS IGMP snooping software has the following proprietary features:

- Source filtering that allows forwarding of multicast packets based on destination and source IP addresses
- Multicast forwarding based on IP addresses rather than the MAC address
- Multicast forwarding alternately based on the MAC address

For more information about IGMP snooping, see RFC 4541.

IGMPv1 and IGMPv2

Both IGMPv1 and IGMPv2 support membership report suppression, which means that if two hosts on the same subnet want to receive multicast data for the same group, the host that receives a member report from the other host suppresses sending its report. Membership report suppression occurs for hosts that share a port.

If no more than one host is attached to each VLAN switch port, you can configure the fast leave feature in IGMPv2. The fast leave feature does not send last member query messages to hosts. As soon as the software receives an IGMP leave message, the software stops forwarding multicast data to that port.

IGMPv1 does not provide an explicit IGMP leave message, so the software must rely on the membership message timeout to indicate that no hosts remain that want to receive multicast data for a particular group.

Note The software ignores the configuration of the last member query interval when you enable the fast leave feature because it does not check for remaining hosts.

IGMPv3

The IGMPv3 snooping implementation on Cisco NX-OS supports full IGMPv3 snooping, which provides constrained flooding based on the (S, G) information in the IGMPv3 reports. This source-based filtering enables the device to constrain multicast traffic to a set of ports based on the source that sends traffic to the multicast group.

By default, the software tracks hosts on each VLAN port. The explicit tracking feature provides a fast leave mechanism. Because every IGMPv3 host sends membership reports, report suppression limits the amount of traffic that the device sends to other multicast-capable routers. When report suppression is enabled, and no IGMPv1 or IGMPv2 hosts requested the same group, the software provides proxy reporting. The proxy feature builds the group state from membership reports from the downstream hosts and generates membership reports in response to queries from upstream queriers.

Even though the IGMPv3 membership reports provide a full accounting of group members on a LAN segment, when the last host leaves, the software sends a membership query. You can configure the parameter last member query interval. If no host responds before the timeout, the software removes the group state.

IGMP Snooping Querier

When PIM is not enabled on an interface because the multicast traffic does not need to be routed, you must configure an IGMP snooping querier to send membership queries. You define the querier in a VLAN that contains multicast sources and receivers but no other active querier.

The querier can be configured to use any IP address in the VLAN.

As a best practice, a unique IP address, one that is not already used by the switch interface or the Hot Standby Router Protocol (HSRP) virtual IP address, should be configured so as to easily reference the querier.

Note The IP address for the querier should not be a broadcast IP address, multicast IP address, or 0 (0.0.0.0).

When an IGMP snooping querier is enabled, it sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

The IGMP snooping querier performs querier election as described in RFC 2236. Querier election occurs in the following configurations:

- When there are multiple switch queriers configured with the same subnet on the same VLAN on different switches.
- When the configured switch querier is in the same subnet as with other Layer 3 SVI queriers.

Virtualization Support

You can define multiple virtual routing and forwarding (VRF) instances for IGMP snooping.

You can use the **show** commands with a VRF argument to provide a context for the information displayed. The default VRF is used if no VRF argument is supplied.

For information about configuring VRFs, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged onto the device.

- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

Guidelines and Limitations for IGMP Snooping

IGMP snooping has the following guidelines and limitations:

- Mrouter/IGMP querier is not supported on the FEX HIF ports.
- IGMP snooping is not supported with PVLAN.
- Cisco Nexus 9000 Series switches support IGMP snooping for IPv4 but do not support MLD snooping for IPv6.
- Layer 3 IPv6 multicast routing is not supported.
- Layer 2 IPv6 multicast packets will be flooded on the incoming VLAN.
- Cisco Nexus 9000 Series switches support IGMP snooping with vPCs.
- You must enable the **ip igmp snooping group-timeout** command when you use the **ip igmp snooping proxy general-queries** command. We recommend that you set it to "never". Otherwise, you might experience multicast packet loss.
- All external multicast router ports (either statically configured or dynamically learned) use the global ltl index. As a result, traffic in VLAN X goes out on the multicast router ports in both VLAN X and VLAN Y, in case both multicast router ports (Layer 2 trunks) carry both VLAN X and VLAN Y.

Default Settings

Parameters	Default
IGMP snooping	Enabled
Explicit tracking	Enabled
Fast leave	Disabled
Last member query interval	1 second
Snooping querier	Disabled
Report suppression	Enabled
Link-local groups suppression	Enabled
Optimise-multicast-flood	Disabled
IGMPv3 report suppression for the entire device	Disabled
IGMPv3 report suppression per VLAN	Enabled

Configuring IGMP Snooping Parameters

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Note You must enable IGMP snooping globally before any other commands take effect.

Configuring Global IGMP Snooping Parameters

To affect the operation of the IGMP snooping process globally, you can configure various optional IGMP snooping parameters.

Notes for IGMP Snooping Parameters

- IGMP Snooping Proxy parameter

  To decrease the burden placed on the snooping switch during each IGMP general query (GQ) interval, the Cisco NX-OS software provides a way to decouple the periodic general query behavior of the IGMP snooping switch from the query interval configured on the multicast routers.

  You can configure the device to consume IGMP general queries from the multicast router, rather than flooding the general queries to all the switchports. When the device receives a general query, it produces proxy reports for all currently active groups and distributes the proxy reports over the period specified by the MRT that is specified in the router query. At the same time, independent of the periodic general query activity of the multicast router, the device sends an IGMP general query on each port in the VLAN in a round-robin fashion. It cycles through all the interfaces in the VLAN at the rate given by the following formula.

  Rate = {number of interfaces in VLAN} * {configured MRT} * {number of VLANs}

  When queries are run in this mode, the default MRT value is 5,000 milliseconds (5 seconds). For a device that has 500 switchports in a VLAN, it would take 2,500 seconds (40 minutes) to cycle through all the interfaces in the system. This is also true when the device itself is the querier.

  This behavior ensures that only one host responds to a general query at a given time, and it keeps the simultaneous reporting rate below the packet-per-second IGMP capability of the device (approximately 3,000 to 4,000 pps).

  Note When you use this option, you must change the **ip igmp snooping group-timeout** parameter to a high value or to never time out.

  The **ip igmp snooping proxy general-queries** [**mrt**] command causes the snooping function to proxy reply to general queries from the multicast router while also sending round-robin general queries on each switchport with the specified MRT value. (The default MRT value is 5 seconds.)

- IGMP Snooping Group-timeout parameter

Configuring the group-timeout parameter disables the behavior of an expiring membership based on three missed general queries. Group membership remains on a given switchport until the device receives an explicit IGMP leave on that port.

The **ip igmp snooping group-timeout** {*timeout* | **never**} command modifies or disables the behavior of an expiring IGMP snooping group membership after three missed general queries.

Procedure

Step 1 **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 Use the following commands to configure global IGMP snooping parameters.

Option	Description
ip igmp snooping `switch(config)# ip igmp snooping`	Enables IGMP snooping for the device. The default is enabled. **Note** If the global setting is disabled with the **no** form of this command, IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. If you disable IGMP snooping, Layer 2 multicast frames flood to all modules.
ip igmp snooping event-history `switch(config)# ip igmp snooping event-history`	Configures the size of the event history buffer. The default is small.
ip igmp snooping group-timeout {*minutes* | **never**} `switch(config)# ip igmp snooping group-timeout never`	Configures the group membership timeout value for all VLANs on the device.
ip igmp snooping link-local-groups-suppression `switch(config)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression for the entire device. The default is enabled.
ip igmp snooping proxy general-inquiries [**mrt** *seconds*]	Configures the IGMP snooping proxy for the device. The default is 5 seconds.

Option	Description
`switch(config)# ip igmp snooping proxy general-inquiries`	
ip igmp snooping v3-report-suppression `switch(config)# ip igmp snooping v3-report-suppression`	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as-is to multicast-capable routers. The default is enabled.
ip igmp snooping report-suppression `switch(config)# ip igmp snooping report-suppression`	Configures IGMPv3 report suppression and proxy reporting. The default is disabled.

Step 3 **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

(Optional) Copies the running configuration to the startup configuration.

Configuring IGMP Snooping Parameters per VLAN

To affect the operation of the IGMP snooping process per VLAN, you can configure various optional IGMP snooping parameters.

Note You configure the IGMP snooping parameters that you want by using this configuration mode; however, the configurations apply only after you specifically create the specified VLAN. See the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide* for information on creating VLANs.

Procedure

Step 1 **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **ip igmp snooping**

Example:

```
switch(config)# ip igmp snooping
```

Enables IGMP snooping. The default is enabled.

Note If the global setting is disabled with the **no** form of this command, IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. If you disable IGMP snooping, Layer 2 multicast frames flood to all modules.

Step 3 **vlan configuration** *vlan-id*

Example:

```
switch(config)# vlan configuration 2
switch(config-vlan-config)#
```

Configures the IGMP snooping parameters you want for the VLAN. These configurations do not apply until you create the specified VLAN.

Step 4 Use the following commands to configure IGMP snooping parameters per VLAN.

Option	Description
ip igmp snooping `switch(config-vlan-config)# ip igmp snooping`	Enables IGMP snooping for the current VLAN. The default is enabled.
ip igmp snooping access-group {**prefix-list** | **route-map**} *policy-name* **interface** *interface slot/port* `switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 2/2`	Configures a filter for IGMP snooping reports that is based on a prefix-list or route-map policy. The default is disabled.
ip igmp snooping explicit-tracking `switch(config-vlan-config)# ip igmp snooping explicit-tracking`	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.
ip igmp snooping fast-leave `switch(config-vlan-config)# ip igmp snooping fast-leave`	Supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol. When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port. The default is disabled for all VLANs.
ip igmp snooping group-timeout {*minutes* | **never**}	Configures the group membership timeout for the specified VLANs.

Option	Description
`switch(config-vlan-config)# ip igmp snooping group-timeout never`	
ip igmp snooping last-member-query-interval *seconds* `switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	Removes the group from the associated VLAN port if no hosts respond to an IGMP query message before the last member query interval expires. Values range from 1 to 25 seconds. The default is 1 second.
ip igmp snooping proxy general-queries [**mrt** *seconds*] `switch(config-vlan-config)# ip igmp snooping proxy general-queries`	Configures an IGMP snooping proxy for specified VLANs. The default is 5 seconds.
ip igmp snooping querier *ip-address* `switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106`	Configures a snooping querier when you do not enable PIM because multicast traffic does not need to be routed. The IP address is used as the source in messages.
ip igmp snooping querier-timeout *seconds* `switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	Configures a snooping querier timeout value for IGMPv2 when you do not enable PIM because multicast traffic does not need to be routed. The default is 255 seconds.
ip igmp snooping query-interval *seconds* `switch(config-vlan-config)# ip igmp snooping query-interval 120`	Configures a snooping query interval when you do not enable PIM because multicast traffic does not need to be routed. The default value is 125 seconds.
ip igmp snooping query-max-response-time *seconds* `switch(config-vlan-config)# ip igmp snooping query-max-response-time 12`	Configures a snooping MRT for query messages when you do not enable PIM because multicast traffic does not need to be routed. The default value is 10 seconds.
ip igmp snooping report-policy {**prefix-list** | **route-map**} *policy-name* **interface** *interface slot/port* `switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 2/4`	Configures a filter for IGMP snooping reports that is based on a prefix-list or route-map policy. The default is disabled.

Option	Description
ip igmp snooping startup-query-count *value* `switch(config-vlan-config)# ip igmp snooping startup-query-count 5`	Configures snooping for a number of queries sent at startup when you do not enable PIM because multicast traffic does not need to be routed.
ip igmp snooping startup-query-interval *seconds* `switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000`	Configures a snooping query interval at startup when you do not enable PIM because multicast traffic does not need to be routed.
ip igmp snooping robustness-variable *value* `switch(config-vlan-config)# ip igmp snooping robustness-variable 5`	Configures the robustness value for the specified VLANs. The default value is 2.
ip igmp snooping report-suppression `switch(config-vlan-config)# ip igmp snooping report-suppression`	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as-is to multicast-capable routers. The default is enabled.
ip igmp snooping mrouter interface *interface* `switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1`	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as **ethernet** *slot*/*port*.
ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface* `switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	Configures the Layer 2 port of a VLAN as a static member of a multicast group. You can specify the interface by the type and the number, such as **ethernet** *slot*/*port*.
ip igmp snooping link-local-groups-suppression `switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression for the specified VLANs. The default is enabled.
ip igmp snooping v3-report-suppression	Configures IGMPv3 report suppression and proxy reporting for the specified VLANs. The default is enabled per VLAN.

Option	Description
`switch(config-vlan-config)# ip igmp snooping v3-report-suppression`	
ip igmp snooping version *value* `switch(config-vlan-config)# ip igmp snooping version 2`	Configures the IGMP version number for the specified VLANs.

Step 5 **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

(Optional) Copies the running configuration to the startup configuration.

Verifying the IGMP Snooping Configuration

Command	Description
show ip igmp snooping [**vlan** *vlan-id*]	Displays the IGMP snooping configuration by VLAN.
show ip igmp snooping groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*] [**detail**]	Displays IGMP snooping information about groups by VLAN.
show ip igmp snooping querier [**vlan** *vlan-id*]	Displays IGMP snooping queriers by VLAN.
show ip igmp snooping mroute [**vlan** *vlan-id*]	Displays multicast router ports by VLAN.
show ip igmp snooping explicit-tracking [**vlan** *vlan-id*] [**detail**]	Displays IGMP snooping explicit tracking information by VLAN.

Displaying IGMP Snooping Statistics

You can display the IGMP snooping statistics using these commands.

Command	Description
show ip igmp snooping statistics vlan	Displays IGMP snooping statistics. You can see the virtual port channel (vPC) statistics in this output.
show ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan** *vlan*]	Displays detailed statistics per VLAN when IGMP snooping filters are configured.

Clearing IGMP Snooping Statistics

You can clear the IGMP snooping statistics using these commands.

Command	Description
clear ip igmp snooping statistics vlan	Clears the IGMP snooping statistics.
clear ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan** *vlan*]	Clears the IGMP snooping filter statistics.

Configuration Examples for IGMP Snooping

Note The configurations in this section apply only after you create the specified VLAN. See the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide* for information on creating VLANs.

The following example shows how to configure the IGMP snooping parameters:

```
config t
  ip igmp snooping
  vlan configuration 2
    ip igmp snooping
    ip igmp snooping explicit-tracking
    ip igmp snooping fast-leave
    ip igmp snooping last-member-query-interval 3
    ip igmp snooping querier 172.20.52.106
    ip igmp snooping report-suppression
    ip igmp snooping mrouter interface ethernet 2/1
    ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
    ip igmp snooping link-local-groups-suppression
    ip igmp snooping v3-report-suppression
```

The following example shows how to configure prefix lists and use them to filter IGMP snooping reports:

```
ip prefix-list plist seq 5 permit 224.1.1.1/32
ip prefix-list plist seq 10 permit 224.1.1.2/32
ip prefix-list plist seq 15 deny 224.1.1.3/32
ip prefix-list plist seq 20 deny 225.0.0.0/8 eq 32

vlan configuration 2
  ip igmp snooping report-policy prefix-list plist interface Ethernet 2/2
  ip igmp snooping report-policy prefix-list plist interface Ethernet 2/3
```

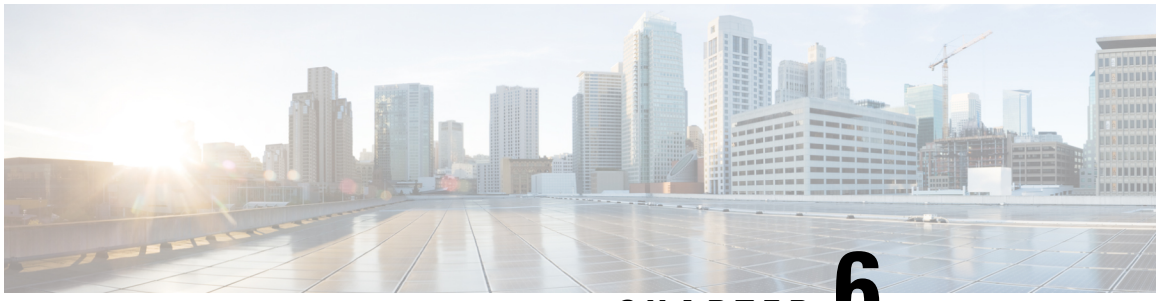
In the above example, the prefix-list permits 224.1.1.1 and 224.1.1.2 but rejects 224.1.1.3 and all the groups in the 225.0.0.0/8 range. The prefix-list is an implicit "deny" if there is no match. If you wish to permit everything else, add **ip prefix-list plist seq 30 permit 224.0.0.0/4 eq 32**.

The following example shows how to configure route maps and use them to filter IGMP snooping reports:

```
route-map rmap permit 10
  match ip multicast group 224.1.1.1/32
route-map rmap permit 20
  match ip multicast group 224.1.1.2/32
route-map rmap deny 30
  match ip multicast group 224.1.1.3/32
route-map rmap deny 40
  match ip multicast group 225.0.0.0/8

vlan configuration 2
  ip igmp snooping report-policy route-map rmap interface Ethernet 2/4
  ip igmp snooping report-policy route-map rmap interface Ethernet 2/5
```

In the above example, the route-map permits 224.1.1.1 and 224.1.1.2 but rejects 224.1.1.3 and all the groups in the 225.0.0.0/8 range. The route-map is an implicit "deny" if there is no match. If you wish to permit everything else, add **route-map rmap permit 50 match ip multicast group 224.0.0.0/4**.



CHAPTER 6

Configuring MSDP

This chapter describes how to configure Multicast Source Discovery Protocol (MSDP) on a Cisco NX-OS device.

About MSDP

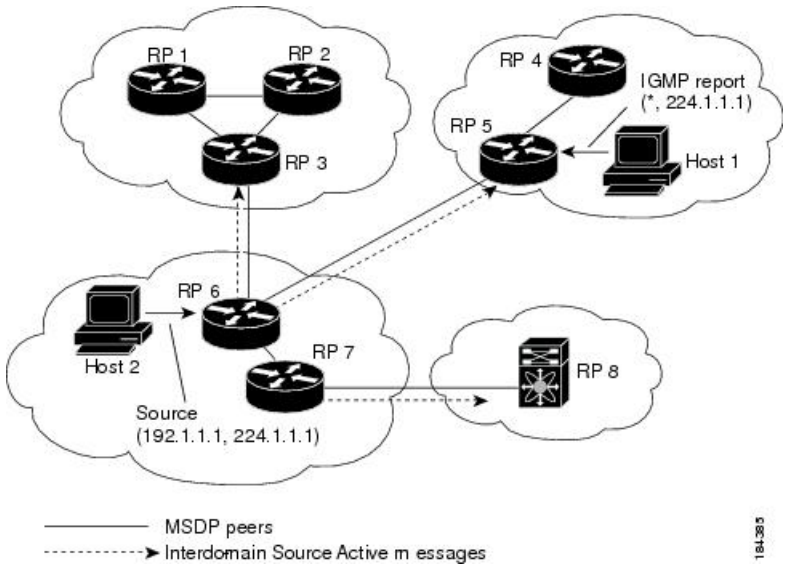
You can use the Multicast Source Discovery Protocol (MSDP) to exchange multicast source information between multiple Border Gateway Protocol (BGP) enabled Protocol Independent Multicast (PIM) sparse-mode domains. In addition, MSDP can be used to create an Anycast-RP configuration to provide RP redundancy and load sharing. For information about BGP, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

MSDP is supported on all Cisco Nexus 9000 series switches.

When a receiver joins a group that is transmitted by a source in another domain, the rendezvous point (RP) sends PIM join messages in the direction of the source to build a shortest path tree. The designated router (DR) sends packets on the sourcetree within the source domain, which can travel through the RP in the source domain and along the branches of the sourcetree to other domains. In domains where there are receivers, RPs in those domains can be on the sourcetree. The peering relationship is conducted over a TCP connection.

The following figure shows four PIM domains. The connected RPs (routers) are called MSDP peers because they are exchanging active source information with each other. Each MSDP peer advertises its own set of multicast source information to the other peers. Source Host 2 sends the multicast data to group 224.1.1.1. On RP 6, the MSDP process learns about the source through PIM register messages and generates Source-Active (SA) messages to its MSDP peers that contain information about the sources in its domain. When RP 3 and RP 5 receive the SA messages, they forward them to their MSDP peers. When RP 5 receives the request from Host 1 for the multicast data on group 224.1.1.1, it builds a shortest path tree to the source by sending a PIM join message in the direction of Host 2 at 192.1.1.1.

Figure 13: MSDP Peering Between RPs in Different PIM Domains



When you configure MSDP peering between each RP, you create a full mesh. Full MSDP meshing is typically done within an autonomous system, as shown between RPs 1, 2, and 3, but not across autonomous systems. You use BGP to do a loop suppression and MSDP peer-RPF to suppress looping SA messages.

Note You do not need to configure BGP in order to use Anycast-RP (a set of RPs that can perform load balancing and failover) within a PIM domain.

Note You can use PIM Anycast (RFC 4610) to provide the Anycast-RP function instead of MSDP.

For detailed information about MSDP, see RFC 3618.

SA Messages and Caching

MSDP peers exchange Source-Active (SA) messages to propagate information about active sources. SA messages contain the following information:

- Source address of the data source
- Group address that the data source uses
- IP address of the RP or the configured originator ID

When a PIM register message advertises a new source, the MSDP process reencapsulates the message in an SA message that is immediately forwarded to all MSDP peers.

The SA cache holds the information for all sources learned through SA messages. Caching reduces the join latency for new receivers of a group because the information for all known groups can be found in the cache. You can limit the number of cached source entries by configuring the SA limit peer parameter. You can limit

the number of cached source entries for a specific group prefix by configuring the group limit global parameter. The SA cache is enabled by default and cannot be disabled.

The MSDP software sends SA messages for each group in the SA cache every 60 seconds or at the configured SA interval global parameter. An entry in the SA cache is removed if an SA message for that source and group is not received within the SA interval plus 3 seconds.

MSDP Peer-RPF Forwarding

MSDP peers forward the SA messages that they receive away from the originating RP. This action is called peer-RPF flooding. The router examines the BGP or MBGP routing table to determine which peer is the next hop in the direction of the originating RP of the SA message. This peer is called a reverse path forwarding (RPF) peer.

If the MSDP peer receives the same SA message from a non-RPF peer in the direction of the originating RP, it drops the message. Otherwise, it forwards the message to all its MSDP peers.

MSDP Mesh Groups

You can use MSDP mesh groups to reduce the number of SA messages that are generated by peer-RPF flooding. By configuring a peering relationship between all the routers in a mesh and then configuring a mesh group of these routers, the SA messages that originate at a peer are sent by that peer to all other peers. SA messages received by peers in the mesh are not forwarded.

A router can participate in multiple mesh groups. By default, no mesh groups are configured.

Prerequisites for MSDP

MSDP has the following prerequisites:

- You are logged onto the device.
- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.
- You configured PIM for the networks where you want to configure MSDP.

Default Settings

This table lists the default settings for MSDP parameters.

Table 11: Default MSDP Parameters

Parameters	Default
Description	Peer has no description
Administrative shutdown	Peer is enabled when it is defined
MD5 password	No MD5 password is enabled

Parameters	Default
SA policy IN	All SA messages are received
SA policy OUT	All registered sources are sent in SA messages
SA limit	No limit is defined
Originator interface name	RP address of the local system
Group limit	No group limit is defined
SA interval	60 seconds

Configuring MSDP

You can establish MSDP peering by configuring the MSDP peers within each PIM domain as follows:

1. Select the routers to act as MSDP peers.
2. Enable the MSDP feature.
3. Configure the MSDP peers for each router identified in Step 1.
4. Configure the optional MSDP peer parameters for each MSDP peer.
5. Configure the optional global parameters for each MSDP peer.
6. Configure the optional mesh groups for each MSDP peer.

Note The MSDP commands that you enter before you enable MSDP are cached and then run when MSDP is enabled. Use the **ip msdp peer** or **ip msdp originator-id** command to enable MSDP.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Enabling the MSDP Feature

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**feature msdp** **Example:** `switch# feature msdp`	Enables the MSDP feature so that you can enter MSDP commands. By default, the MSDP feature is disabled.
Step 3	(Optional) **show running-configuration msdp** **Example:** `switch# show running-configuration msdp`	Shows the running-configuration information for MSDP.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring MSDP Peers

You can configure an MSDP peer when you configure a peering relationship with each MSDP peer that resides either within the current PIM domain or in another PIM domain. MSDP is enabled on the router when you configure the first MSDP peering relationship.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM and MSDP.

Ensure that you configured PIM in the domains of the routers that you will configure as MSDP peers.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip msdp peer** *peer-ip-address* **connect-source** *interface* [**remote-as** *as-number*] **Example:** `switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 2/1 remote-as 8`	Configures an MSDP peer with the specified peer IP address. The software uses the source IP address of the interface for the TCP connection with the peer. The interface can take the form of *type slot/port*. If the AS number is the same as the local AS, then the peer is within the PIM domain; otherwise, this peer is external to the PIM domain. By default, MSDP peering is disabled. **Note** MSDP peering is enabled when you use this command.

	Command or Action	Purpose
Step 3	Repeat Step 2 for each MSDP peering relationship by changing the peer IP address, the interface, and the AS number as appropriate.	—
Step 4	(Optional) **show ip msdp summary** [**vrf** [*vrf-name* | **all**]] **Example:** `switch# show ip msdp summary`	Displays a summary of MDSP peers.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring MSDP Peer Parameters

You can configure the optional MSDP peer parameters described in this table. You configure these parameters in global configuration mode for each peer based on its IP address.

Table 12: MSDP Peer Parameters

Parameter	Description
Description	Description string for the peer. By default, the peer has no description.
Administrative shutdown	Method to shut down the MSDP peer. The configuration settings are not affected by this command. You can use this parameter to allow configuration of multiple parameters to occur before making the peer active. The TCP connection with other peers is terminated by the shutdown. By default, a peer is enabled when it is defined.
MD5 password	MD5-shared password key used for authenticating the peer. By default, no MD5 password is enabled.
SA policy IN	Route-map policy for incoming SA messages. By default, all SA messages are received. **Note** To configure route-map policies, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.
SA policy OUT	Route-map policy for outgoing SA messages. By default, all registered sources are sent in SA messages. **Note** To configure route-map policies, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Parameter	Description
SA limit	Number of (S, G) entries accepted from the peer and stored in the SA cache. By default, there is no limit.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM and MSDP.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.
		Note Use the commands listed from step-2 to configure the MSDP peer parameters.

Step 2	**ip msdp description** *peer-ip-address description* **Example:** `switch(config)# ip msdp description 192.168.1.10 peer in Engineering network`	Sets a description string for the peer. By default, the peer has no description.
Step 3	**ip msdp shutdown** *peer-ip-address* **Example:** `switch(config)# ip msdp shutdown 192.168.1.10`	Shuts down the peer. By default, the peer is enabled when it is defined.
Step 4	**ip msdp password** *peer-ip-address password* **Example:** `switch(config)# ip msdp password 192.168.1.10 my_md5_password`	Enables an MD5 password for the peer. By default, no MD5 password is enabled.
Step 5	**ip msdp sa-policy** *peer-ip-address policy-name* **in** **Example:** `switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in`	Enables a route-map policy for incoming SA messages. By default, all SA messages are received.
Step 6	**ip msdp sa-policy** *peer-ip-address policy-name* **out** **Example:** `switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out`	Enables a route-map policy for outgoing SA messages. By default, all registered sources are sent in SA messages.

	Command or Action	Purpose
Step 7	**ip msdp sa-limit** *peer-ip-address limit* **Example:** `switch(config)# ip msdp sa-limit 192.168.1.10 5000`	Sets a limit on the number of (S, G) entries accepted from the peer. By default, there is no limit.
Step 8	(Optional) **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | **all**]] **Example:** `switch(config)# show ip msdp peer 192.168.1.10`	Displays detailed MDSP peer information.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring MSDP Global Parameters

You can configure the optional MSDP global parameters described in this table.

Table 13: MSDP Global Parameters

Parameter	Description
Originator interface name	IP address used in the RP field of an SA message entry. When Anycast RPs are used, all RPs use the same IP address. You can use this parameter to define a unique IP address for the RP of each MSDP peer. By default, the software uses the RP address of the local system. **Note** We recommend that you use a loopback interface for the RP address.
Group limit	Maximum number of (S, G) entries that the software creates for the specified prefix. The software ignores groups when the group limit is exceeded and logs a violation. By default, no group limit is defined.
SA interval	Interval at which the software transmits Source-Active (SA) messages. The range is from 60 to 65,535 seconds. The default is 60 seconds.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM and MSDP.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip msdp originator-id** *interface* **Example:** `switch(config)# ip msdp originator-id loopback0`	Sets a description string for the peer. By default, the peer has no description. Sets the IP address used in the RP field of an SA message entry. By default, the software uses the RP address of the local system. **Note** We recommend that you use a loopback interface for the RP address.
Step 3	**ip msdp group-limit** *limit* **source** *source-prefix* **Example:** `switch(config)# ip msdp group-limit 1000 source 192.168.1.0/24`	Maximum number of (S, G) entries that the software creates for the specified prefix. The software ignores groups when the group limit is exceeded and logs a violation. By default, no group limit is defined.
Step 4	**ip msdp sa-interval** *seconds* **Example:** `switch(config)# ip msdp sa-interval 80`	Interval at which the software transmits Source-Active (SA) messages. The range is from 60 to 65,535 seconds. The default is 60 seconds.
Step 5	(Optional) **show ip msdp summary** [**vrf** [*vrf-name* | **all**]] **Example:** `switch(config)# show ip msdp summary`	Displays a summary of the MDSP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring MSDP Mesh Groups

You can configure optional MDSP mesh groups in global configuration mode by specifying each peer in the mesh. You can configure multiple mesh groups on the same router and multiple peers per mesh group.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM and MSDP.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip msdp mesh-group** *peer-ip-addr mesh-name* **Example:** `switch(config)# ip msdp mesh-group 192.168.1.10 my_mesh_1`	Configures an MSDP mesh with the peer IP address specified. You can configure multiple meshes on the same router and multiple peers per mesh group. By default, no mesh groups are configured.
Step 3	Repeat Step 2 for each MSDP peer in the mesh by changing the peer IP address.	—
Step 4	(Optional) **show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name* | **all**]] **Example:** `switch# show ip msdp mesh-group`	Displays information about the MDSP mesh group configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Restarting the MSDP Process

Before you begin

You can restart the MSDP process and optionally flush all routes.

Procedure

	Command or Action	Purpose
Step 1	**restart msdp** **Example:** `switch# restart msdp`	Restarts the MSDP process.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**ip msdp flush-routes** **Example:**	Removes routes when the MSDP process is restarted. By default, routes are not flushed.

	Command or Action	Purpose
	`switch(config)# ip msdp flush-routes`	
Step 4	(Optional) **show running-configuration | include flush-routes** **Example:** `switch(config)# show running-configuration | include flush-routes`	Displays flush-routes configuration lines in the running configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the MSDP Configuration

To display the MSDP configuration information, perform one of the following tasks.

Command	Description
show ip msdp count [*as-number*] [**vrf** [*vrf-name* | **all**]]	Displays MSDP (S, G) entry and group counts by the autonomous system (AS) number.
show ip msdp mesh-group [*mesh-group*] [**vrf** [*vrf-name* | **all**]]	Displays the MSDP mesh group configuration.
show ip msdp peer [*peer-address*] [**vrf** [*vrf-name* | **all**]]	Displays MSDP information for the MSDP peer.
show ip msdp rpf [*rp-address*] [**vrf** [*vrf-name* | **all**]]	Displays the next-hop AS on the BGP path to an RP address.
show ip msdp sources [**vrf** [*vrf-name* | **all**]]	Displays the MSDP-learned sources and violations of configured group limits.
show ip msdp summary [**vrf** [*vrf-name* | **all**]]	Displays a summary of the MSDP peer configuration.

Monitoring MSDP

You can display and clear MSDP statistics by using the features in this section.

Displaying Statistics

You can display MSDP statistics using these commands.

Command	Description
show ip msdp policy statistics sa-policy *peer-address* {**in** | **out**} [**vrf** [*vrf-name* | **all**]]	Displays the MSDP policy statistics for the MSDP peer.
show ip msdp {**sa-cache** | **route**} [*source-address*] [*group-address*] [**vrf** [*vrf-name* | **all**]] [*asn-number*] [**peer** *peer-address*]	Displays the MSDP SA route cache. If you specify the source address, all groups for that source are displayed. If you specify a group address, all sources for that group are displayed.

Clearing Statistics

You can clear the MSDP statistics using these commands.

Command	Description
clear ip msdp peer [*peer-address*] [**vrf** *vrf-name*]	Clears the TCP connection to an MSDP peer.
clear ip msdp policy statistics sa-policy *peer-address* {**in** | **out**} [**vrf** *vrf-name*]	Clears statistics counters for MSDP peer SA policies.
clear ip msdp statistics [*peer-address*] [**vrf** *vrf-name*]	Clears statistics for MSDP peers.
clear ip msdp {**sa-cache** | **route**} [*group-address*] [**vrf** [*vrf-name* | **all**]]	Clears the group entries in the SA cache.

Configuration Examples for MSDP

To configure MSDP peers, some of the optional parameters, and a mesh group, follow these steps for each MSDP peer:

1. Configure the MSDP peering relationship with other routers.

```
switch# configure terminal
switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 1/0 remote-as 8
```

2. Configure the optional peer parameters.

```
switch# configure terminal
switch(config)# ip msdp password 192.168.1.10 my_peer_password_AB
```

3. Configure the optional global parameters.

```
switch# configure terminal
switch(config)# ip msdp sa-interval 80
```

4. Configure the peers in each mesh group.

```
switch# configure terminal
switch(config)# ip msdp mesh-group 192.168.1.10 mesh_group_1
```

The following example shows how to configure a subset of the MSDP peering that is shown below.

RP 3: 192.168.3.10 (AS 7)

```
configure terminal
  ip msdp peer 192.168.1.10 connect-source ethernet 1/1
  ip msdp peer 192.168.2.10 connect-source ethernet 1/2
  ip msdp peer 192.168.6.10 connect-source ethernet 1/3 remote-as
9
  ip msdp password 192.168.6.10 my_peer_password_36
  ip msdp sa-interval 80
  ip msdp mesh-group 192.168.1.10 mesh_group_123
  ip msdp mesh-group 192.168.2.10 mesh_group_123
  ip msdp mesh-group 192.168.3.10 mesh_group_123
```

RP 5: 192.168.5.10 (AS 8)

```
configure terminal
  ip msdp peer 192.168.4.10 connect-source ethernet 1/1
  ip msdp peer 192.168.6.10 connect-source ethernet 1/2 remote-as
9
  ip msdp password 192.168.6.10 my_peer_password_56
  ip msdp sa-interval 80
```

RP 6: 192.168.6.10 (AS 9)

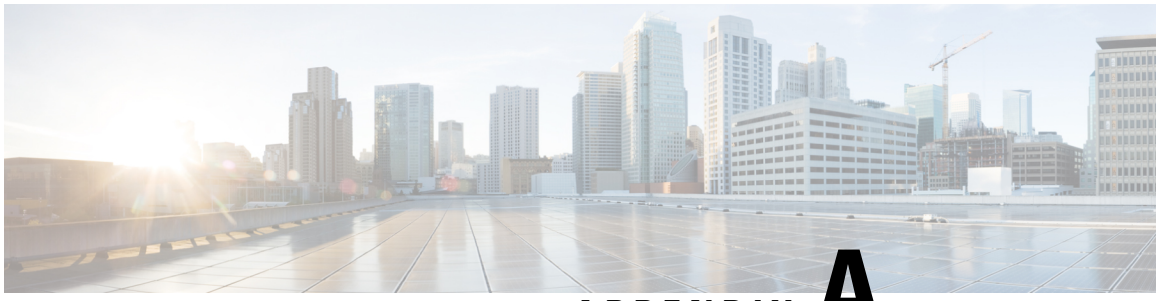
```
configure terminal
  ip msdp peer 192.168.7.10 connect-source ethernet 1/1
  ip msdp peer 192.168.3.10 connect-source ethernet 1/2 remote-as
7
  ip msdp peer 192.168.5.10 connect-source ethernet 1/3 remote-as
8
  ip msdp password 192.168.3.10 my_peer_password_36
  ip msdp password 192.168.5.10 my_peer_password_56
  ip msdp sa-interval 80
```

Related Documents

Related Topic	Document Title
Configuring MBGP	*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
RFC 4624	Multicast Source Discovery Protocol (MSDP) MIB



APPENDIX A

IETF RFCs for IP Multicast

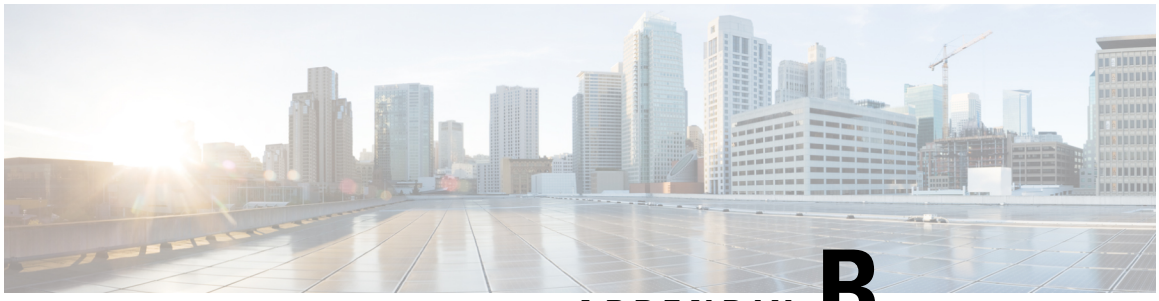
This appendix contains Internet Engineering Task Force (IETF) RFCs related to IP multicast. For information about IETF RFCs, see https://www.ietf.org/search/?query=RFC.

IETF RFCs for IP Multicast

This table lists the RFCs related to IP multicast.

RFCs	Title
RFC 2236	*Internet Group Management Protocol*
RFC 2365	*Administratively Scoped IP Multicast*
RFC 2858	*Multiprotocol Extensions for BGP-4*
RFC 3376	*Internet Group Management Protocol*
RFC 3446	*Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
RFC 3618	*Multicast Source Discovery Protocol (MSDP)*
RFC 4601	*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*
RFC 4610	*Anycast-RP Using Protocol Independent Multicast (PIM)*
RFC 5132	*IP Multicast MIB*

IETF RFCs for IP Multicast



APPENDIX B

Configuration Limits for Cisco NX-OS Multicast

This appendix describes the configuration limits for Cisco NX-OS multicast.

Configuration Limits

The features supported by Cisco NX-OS have maximum configuration limits. Some of the features have configurations that support limits less than the maximum limits.

The configuration limits are documented in the Cisco Nexus 9000 Series NX-OS Verified Scalability Guide.

Configuration Limits for Cisco NX-OS Multicast