Cisco Nexus 3550-T NX-OS Multicast Routing Configuration Guide, Release 10.2(x)

First Published: 2022-09-14

Last Modified: 2023-07-13

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

Trademarks ?

PREFACE

Preface vii

Audience vii

Document Conventions vii

Related Documentation for Cisco Nexus 3550-T Switches viii

Documentation Feedback viii

Communications, Services, and Additional Information viii

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Multicast Configuration Overview 3

Licensing Requirements 3

About Multicast 3

Cisco NX-OS PIM 4

ASM 6

IGMP 6

Guidelines and Limitations for Multicast 6

High-Availability Requirements for Multicast 6

Troubleshooting Inconsistency Between SW and HW Multicast Routes 7

CHAPTER 3

Configuring IGMP 9

About IGMP 9

IGMP Versions 9

IGMP Basics 10

Prerequisites for IGMP 11
Guidelines and Limitations for IGMP 12
Default Settings for IGMP 12
Configuring IGMP Parameters 13
Configuring IGMP Interface Parameters 13
Restarting the IGMP Process 18
Verifying the IGMP Configuration 19
Configuration Examples for IGMP 19

CHAPTER 4 **Configuring IGMP Snooping** 21
About IGMP Snooping 21
IGMPv1 and IGMPv2 22
IGMPv3 22
IGMP Snooping Querier 23
Prerequisites for IGMP Snooping 23
Guidelines and Limitations for IGMP Snooping 24
Default Settings 24
Configuring IGMP Snooping Parameters 25
Configuring Global IGMP Snooping Parameters 25
Configuring IGMP Snooping Parameters per VLAN 28
Verifying the IGMP Snooping Configuration 32
Displaying IGMP Snooping Statistics 32
Clearing IGMP Snooping Statistics 33
Configuration Examples for IGMP Snooping 33

CHAPTER 5 **Configuring PIM** 35
About PIM 35
Hello Messages 36
Join-Prune Messages 36
State Refreshes 37
Rendezvous Points 37
Static RP 37
PIM Register Messages 37
Designated Routers 38

ASM Switchover from Shared Tree to Source Tree 38
Prerequisites for PIM 39
Guidelines and Limitations for PIM 39
Guidelines and Limitations for Hello Messages 40
Guidelines and Limitations for Rendezvous Points 40
Default Settings 40
Configuring PIM 41
PIM Configuration Tasks 42
Enabling the PIM Feature 42
Configuring PIM Sparse Mode Parameters 43
Configuring PIM Sparse Mode Parameters 44
Configuring Layer 3 Multicast Receiver VLAN 46
Configuring ASM 47
Configuring Static RPs 47
Configuring RPF Routes for Multicast 48
Configuring Message Filtering 49
Configuring Message Filtering 49
Restarting the PIM Processes 50
Restarting the PIM Process 51
Verifying the PIM Configuration 51
Displaying Statistics 52
Displaying PIM Statistics 52
Clearing PIM Statistics 52
Related Documents 53
MIBs 53

CHAPTER 6 **Configuring Multicast ACL for RPs for PIM-SM 55**
Introduction 55
Guidelines and Limitations for PIM Allow RP 55
Information about PIM Allow RP 55
Configuring RPs for PIM-SM 56

Preface

This preface includes the following sections:

- Audience, on page vii
- Document Conventions, on page vii
- Related Documentation for Cisco Nexus 3550-T Switches, on page viii
- Documentation Feedback, on page viii
- Communications, Services, and Additional Information, on page viii

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 3550-T Switches

The entire Cisco Nexus 3550-T switch documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-3550-series/series.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.

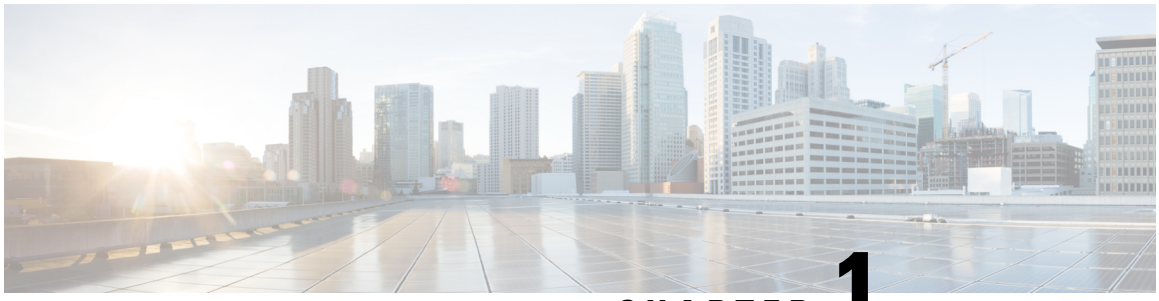
Communications, Services, and Additional Information

- 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 section contains the new and changed information for a release.

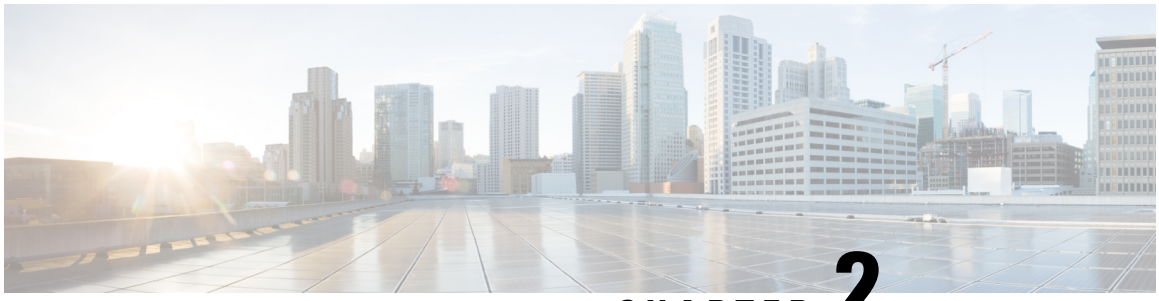
- New and Changed Information, on page 1

New and Changed Information

Table 1: New and Changed Information for Cisco Nexus 3550-T NX-OS Release 10.2(x)

Feature	Description	Changed in Release	Where Documented
Multicast Support Enhancements	Support for single configured PIM-enabled VLAN with Layer 3 egress multicast capability.	10.2(3v)	Configuring Layer 3 Multicast Receiver VLAN, on page 46
Layer 3 Multicast Enhancements	Support for multicast is available on Layer 3 ports or access ports.	10.2(3t)	Guidelines and Limitations for Multicast, on page 6
PIM	• FHR support for PIM-sparse mode. • Support for static RP. • Support for ip pim jp-policy policy-name command.	10.2(3t)	About PIM, on page 35 Guidelines and Limitations for Rendezvous Points, on page 40 Configuring Message Filtering , on page 49
IGMP Snooping	Support for new IGMP query flood parameter.	10.2(3t)	Configuring Global IGMP Snooping Parameters, on page 25
PIM-SM	Support for Multicast ACLs for RP.	10.2(3t)	Information about PIM Allow RP, on page 55

New and Changed Information



CHAPTER 2

Multicast Configuration Overview

- Licensing Requirements, on page 3
- About Multicast, on page 3
- Guidelines and Limitations for Multicast, on page 6
- High-Availability Requirements for Multicast, on page 6
- Troubleshooting Inconsistency Between SW and HW Multicast Routes , on page 7

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.

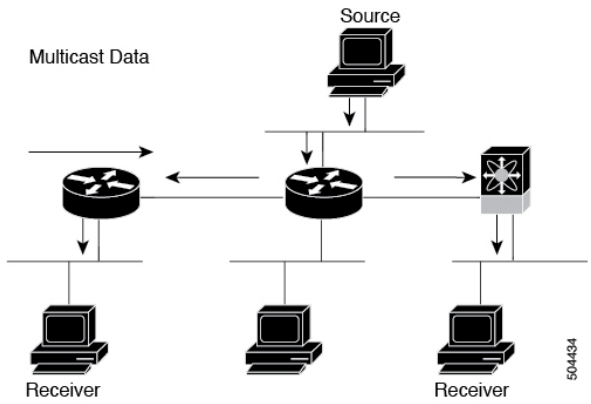
Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel. The Internet Assigned Number Authority (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



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.

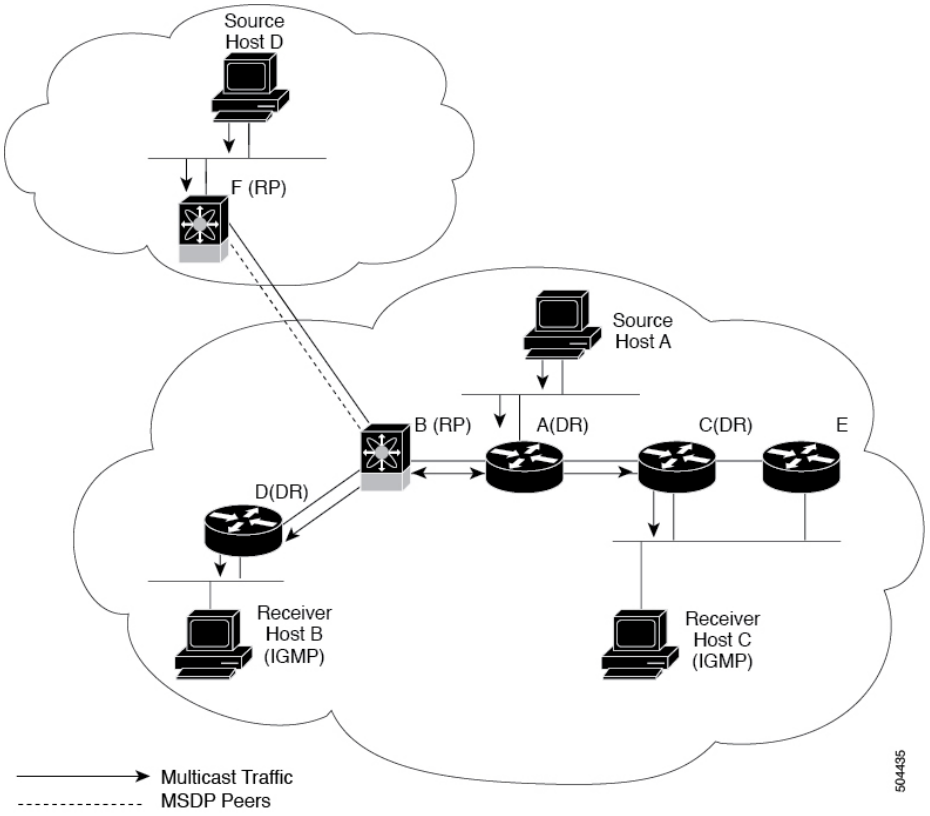
The distribution trees change automatically to reflect the topology changes due to link or router failures. PIM dynamically tracks both multicast-capable sources and receivers.

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 2: PIM Domains in an IPv4 Network



Note Cisco Nexus 3550-T Release 10.2(3t) does not support MSDP.

- 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 only supports Any source multicast (ASM) mode for connecting sources and receivers.

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.

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 on an interface. By default, the software enables IGMPv2.

Note There are limitations to using IGMPv2 on Layer 2 ports. Please see Guidelines and Limitations for IGMP Snooping, on page 24 before using the feature.

Guidelines and Limitations for Multicast

- Layer 3 Ethernet subinterfaces are not supported.
- Layer3 multicast functionality is available only on L3 ports and access ports in Cisco Nexus 3550T.
- Trunk ports on Cisco Nexus 3550T support partial Layer3 multicast capability. Hence, all Layer3 multicast{vrf,S,G} lookup result with trunk egress port can be sent only on a configured layer3-multicast receiver-vlan. If a receiver is learned on a non-configured VLAN, it does not receive the expected multicast traffic. If you have not configured any layer3-multicast receiver-vlan, multicast-receivers learned on the native-vlan of trunk can receive configured traffic.
- Traffic storm control is not supported for unknown multicast traffic.
- Device cannot operate as multicast non-DR for a VLAN segment.
- Cisco Nexus 3550-T series switch does not support AutoRP or BSR configuration.
- Bidirectional mode is not supported on Cisco Nexus® 3550-T platform switches.

High-Availability Requirements for Multicast

After a multicast routing protocol is restarted, its state is recovered from the MRIB process.

Troubleshooting Inconsistency Between SW and HW Multicast Routes

Symptom

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

Possible Cause

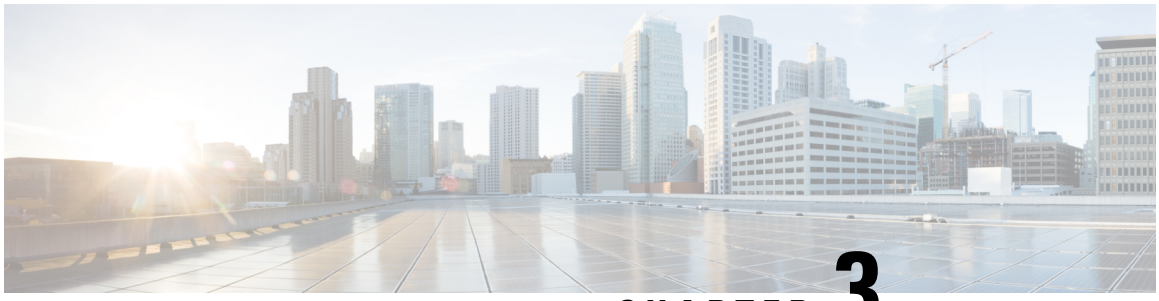
The issue can be seen when numerous active flows are received beyond the hardware capacity. This causes some of the entries not to be programmed in hardware while there is no free hardware index.

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.



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, on page 9
- Prerequisites for IGMP, on page 11
- Guidelines and Limitations for IGMP, on page 12
- Default Settings for IGMP, on page 12
- Configuring IGMP Parameters, on page 13
- Restarting the IGMP Process, on page 18
- Verifying the IGMP Configuration, on page 19
- Configuration Examples for IGMP, on page 19

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

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:

- 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® 3550-T switches does not support SSM.

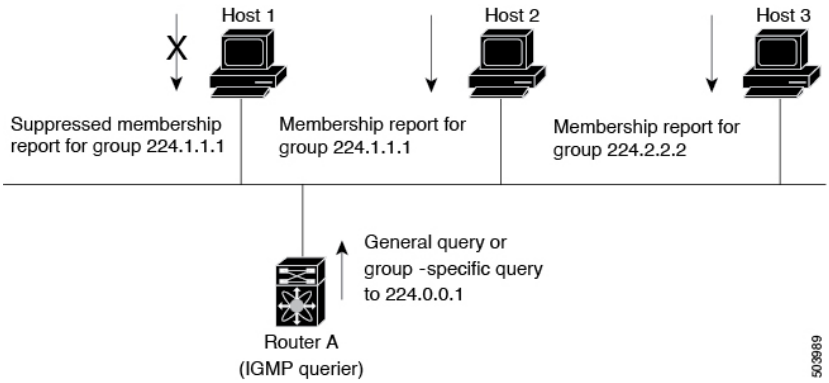
For detailed information about IGMPv2, see RFC 2236.

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 3: 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.

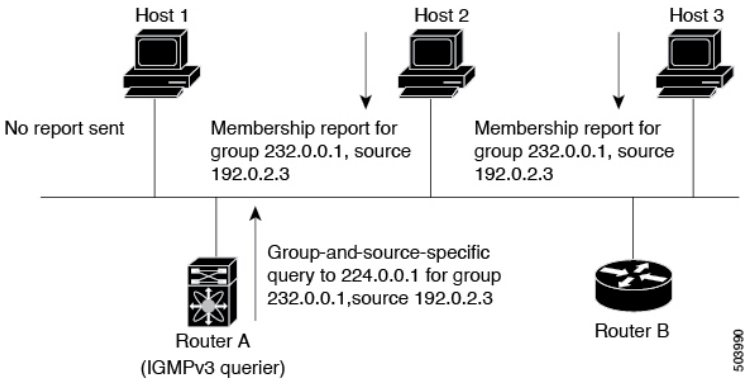
The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes 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 4: 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:

- For having low latency, Cisco Nexus® 3550-T switch only supports {Vlan,MAC} lookup for L2 ports. There is no IP based {VLAN,G} or {VLAN,G,S} lookup.
- Route-Aliasing is expected as routes are installed for optimized {Vlan,MAC} lookup.
- All unknown multicast packet miss are forwarded to OMF ports on the L2 segment. There is a FHR copy to SUP when L3 multicast is enabled on L2 access ports.
- Multi-access Network with Cisco Nexus® 3550-T switch would not work, there cannot be 2 PIM-Routers in same VLan segment if one of the PIM enabled routers is Cisco Nexus® 3550-T switch. Cisco Nexus® 3550-T switch cannot act as non-DR.
- PIM can be enabled on L2 transit node provided the other routers have PIM or IGMP querier configured.
- Owing to {Vlan,Mac} lookup, IGMPv2 reports are flooded to the receivers already attached, this results in report-suppression. It is recommended to have hosts configured as IGMPv3.
- Excluding or blocking a list of sources according to IGMPv3 (RFC 5790) is not supported.

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

Parameters	Default
Report link local multicast groups	Disabled
Enforce router alert	Disabled
Immediate leave	Disabled
IGMP query flood	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 (*, 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 (*, 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 (*, 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 (*, G) state, the source tree is built only if you enable IGMPv3.

Parameter	Description
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.
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.
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.

Parameter	Description
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 3550-T Unicast Routing Configuration* section.

Procedure

	Command or Action	Purpose

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

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

	Command or Action	Purpose
		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. The command works only on PIM enabled Layer 3 or access ports.
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 (*, 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 (*, 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:** `switch(config-if)# ip igmp robustness-variable 3`	Sets the robustness variable. Values can range from 1 to 7. The default is 2.
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:**	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.

	Command or Action	Purpose
	`switch(config-if)# ip igmp query-timeout 300`	**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.
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.

	Command or Action	Purpose
		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) **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:**	Removes routes when the IGMP process is restarted. By default, routes are not flushed.

	Command or Action	Purpose
	`switch(config)# ip igmp flush-routes`	
Step 4	(Optional) **show running-configuration igmp** **Example:** `switch(config)# show running-configuration igmp`	Shows the running-configuration information.
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.
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.

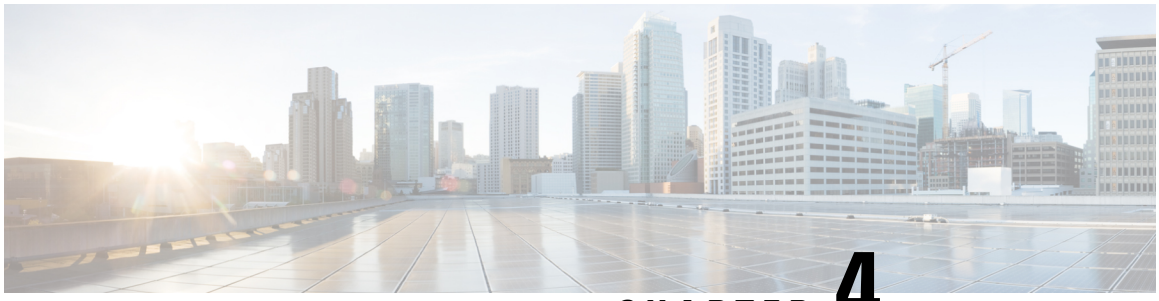
Configuration Examples for IGMP

The following example shows how to configure the IGMP parameters:

```
configure terminal

  interface ethernet 1/1
    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 IGMP Snooping

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

- About IGMP Snooping, on page 21
- Prerequisites for IGMP Snooping, on page 23
- Guidelines and Limitations for IGMP Snooping, on page 24
- Default Settings, on page 24
- Configuring IGMP Snooping Parameters, on page 25
- Verifying the IGMP Snooping Configuration, on page 32
- Displaying IGMP Snooping Statistics, on page 32
- Clearing IGMP Snooping Statistics, on page 33
- Configuration Examples for IGMP Snooping, on page 33

About IGMP Snooping

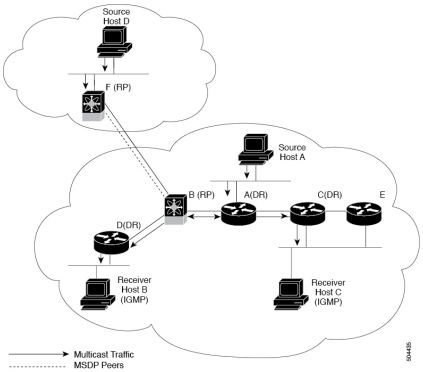
Note We recommend that you do not disable IGMP snooping on the device. If you disable IGMP snooping, you might see reduced multicast performance because of excessive false flooding within the device.

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.

Note Owing to {Vlan,Mac} lookup IGMPv2 reports are flooded/forwarded to the receivers already attached, this results in report-suppression. This is specific to Cisco Nexus 3550-T only.

Figure 5: 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:

- Layer 2 multicast forwarding is only done based on MAC address on the Cisco Nexus 3550-T hardware.
- Optimized Multicast Flooding (OMF) forwards unknown traffic to only routers and performs no data-driven state creation.

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. The source based filtering is not supported for L2 multicast on Cisco NX-OS 3550-T series switches, owing to MAC based multicast forwarding.

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.

Note Owing to cut-through forwarding of L2 multicast based on destination MAC, (S,G) information in the IGMPv3 reports is ignored when PIM is not enabled on VLAN. Cisco Nexus 3550-T series switch does not support PIM on trunk ports.

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.

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:

- Cisco Nexus 3550-T Release 10.2(3t) does not enable PIM on trunk ports
- If there is a host on a network segment sending periodic reports, hosts on other ports suppress IGMPv2 reports resulting in a timeout. If such hosts are presemt, use static configuration of receivers to prevent host timeouts.
- Cisco Nexus® 3550-T 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 are flooded on the incoming VLAN.
- Cisco Nexus® 3550-T switch does not flood/forward unknown L2/L3 multicast packets on incoming VLAN. As a result, multicast packets are not sent to OMF ports (all external multicast router ports, either statically configured or dynamically learned).
- 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.
- Cisco Nexus® 3550-T switch forwards known multicast packets based on Multicast DestMAC of packets on incoming ports where PIM is dis-abled to provide lower latency. Hence, Cisco Nexus® 3550-T switch IGMPv1/v2 incoming reports are forwarded to known multicast receivers.
- Enable the IGMP query flood parameter to send queries one port at a time.

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	Enabled
IGMPv3 report suppression for the entire device	Disabled

Parameters	Default
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.

- IGMP query flood

  On Cisco Nexus 3550-T platform, forwarding of IPv4 multicast packets is based on DMAC which can result in host report suppression for IGMP snooping, as all learned ports for the group receive the IGMPv1 and IGMPv2 reports. Due to report suppression by IGMPv1 and IGMPv2 hosts, the querier times out the host resulting in a drop in multicast traffic to the hosts. To reduce host timeout probability, this configuration enables you to send queries one port at a time

Note

- The changes are applicable only to a Cisco Nexus 3550-T switch acting as a IGMP snooping and querier device.
- Enabling this is required only when PIM is disabled on VLAN.

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.

Option	Description
	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, Cisco Nexus® 3550-Tswitch only disables IGMP snoop packet handling. Hence, even with the **no** form of this command, IGMP packets including multicast packets are not forwarded in hardware.
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*] `switch(config)# ip igmp snooping proxy general-inquiries`	Configures the IGMP snooping proxy for the device. The default is 5 seconds.
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.

Option	Description
[no] ip igmp snooping query flood `switch(config)# ip igmp snooping query flood`	Configure globally to enable feature. Use the **no** form of the command to enable sending queries one port at a time. **Note** Global setting applies only on VLAN where per VLAN setting is also enabled.

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 3550-T 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. **Note** Cisco Nexus 3550-T switches can flood layer 2 multicast packets only to multicast router and IGMP querier ports. This behaviour is not modified with no form of the **ip igmp snooping** command.
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 1/2`	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**} `switch(config-vlan-config)# ip igmp snooping group-timeout never`	Configures the group membership timeout for the specified VLANs.
ip igmp snooping last-member-query-interval *seconds*	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.

Option	Description
`switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	
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 1/4`	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 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.

Option	Description
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 1/1`	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 1/1`	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 `switch(config-vlan-config)# ip igmp snooping v3-report-suppression`	Configures IGMPv3 report suppression and proxy reporting for the specified VLANs. The default is enabled per VLAN.
ip igmp snooping version *value*	Configures the IGMP version number for the specified VLANs.

Option	Description
`switch(config-vlan-config)# ip igmp snooping version 2`	
[no] ip igmp snooping query flood `switch(config-vlan-config)# ip igmp snooping query flood`	Configures per port query feature, default behaviour is to flood the queries on all ports together. Use the **no** form of the command to enable sending queries one port at a time. **Note** This setting is applied only when the feature is enabled globally.

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.

Command	Description
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 3550-T Layer 2 Switching Configuration* section 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 1/1
    ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1
    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 1/2
  ip igmp snooping report-policy prefix-list plist interface Ethernet 1/3
```

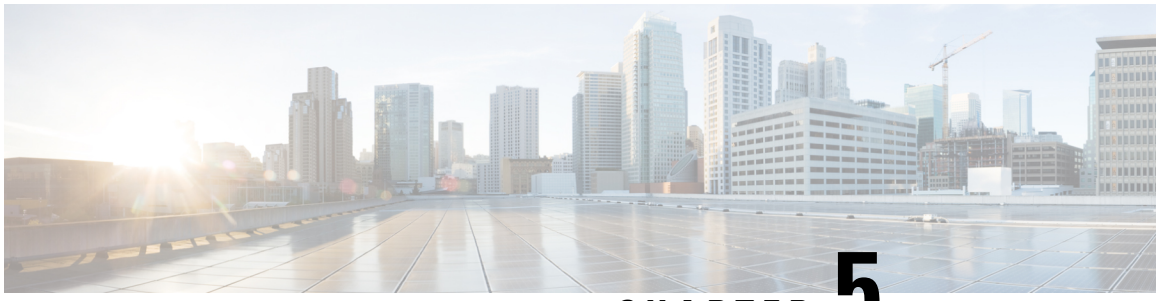
In the above example, the prefix-list permits 224.1.1.1 and 224.1.1.2 but rejects 224.1.1.3 and all the groups in the 225.0.0.0/8 range. The prefix-list is an implicit "deny" if there is no match. If you wish to permit everything else, add **ip prefix-list plist seq 30 permit 224.0.0.0/4 eq 32**.

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 1/4
  ip igmp snooping report-policy route-map rmap interface Ethernet 1/5
```

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 5

Configuring PIM

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

- About PIM, on page 35
- Prerequisites for PIM, on page 39
- Guidelines and Limitations for PIM, on page 39
- Default Settings, on page 40
- Configuring PIM, on page 41
- Verifying the PIM Configuration, on page 51
- Displaying Statistics, on page 52
- Related Documents, on page 53
- MIBs, on page 53

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 3550-T

- Supports FHR for PIM-sparse mode.
- Forms {*,G} only in software.
- 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 (*, G) state as follows:

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

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
- Cisco Nexus® 3550-T only supports and validates Static-RP.

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.

Note PIM Bidir mode is not supported in Cisco Nexus 3550-T Release 10.2(3t).

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.

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

PIM has the following guidelines and limitations:

- Only PIM-ASM mode is supported in the Cisco Nexus® 3550-T switches.
- Cisco Nexus® 3550-T switch does cut-through forwarding; hence there is no MTU- check implemented. Hardware buffering is not designed for jumbo packets and packets beyond regular mtu size 1518 is not supported.
- L3 Multicast has the following scale numbers:
  - L2MCAST - 1536 system-wide shared with MAC tabel - {vlan,MAC}
  - L3MCAST - 6000 system-wide {vrf,G,S} entries in hardware
- Only partial support for L3 Multicast on Trunk Vlan is available.
- Layer 3 Multicast traffic is forwarded only to the learned receiver when layer3-multicast receiver-vlan is configured for receiver vlan on the trunk port. If the multicast receiver is learned on non-configured PIM enabled Vlan, a warning is generated. For example,

  ```
  %USER-4-SYSTEM_MSG: L3-Multicast for {22.102.0.100,227.0.1.1) receiver on Trunk Port
  Ethernet1/11 vlan 1002 not enabled - exusd
  ```

  The above warning level syslog message is not enabled by default. To display and to enable it, configure `logging monitor 4` and/or `logging console 4`.
- When L3 lookup is done; even the L2 domain multicast receivers receive packets with decremented TTL.
- Cisco Nexus® 3550-T platform switches do not support MSDP.
- RPF failure traffic is dropped and sent to the CPU at a very low rate to trigger PIM asserts.
- 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 3550-T switches do not implement source subnet check. All L3 multicast miss traffic is copied to CPU to learn the local multicast source.
- Cisco NX-OS PIM do not interoperate with any version of PIM dense mode or PIM Sparse Mode version 1.
- 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.
- Device cannot operate as multicast non-DR for a VLAN segment.

- Cisco Nexus 3550-T series switch does not support AutoRP or BSR configuration.
- Cisco Nexus 3550-T series switch does not support PIM on VPC VLANs.

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):

- Cisco Nexus 3550-T - 10.2(3t) release can only operate as a static RP.
- To avoid excessive punts of the RPF failed packets, the Cisco Nexus® 3550-T 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.

Default Settings

This table lists the default settings for PIM parameters.

Table 4: Default PIM Parameters

Parameters	Default
Use shared trees only	Disabled **Note** {*,G} support is not available in hardware. Hence, no line-rate forwarding can occur if this parameter is enabled.
Flush routes on restart	Disabled
Log neighbor changes	Disabled
Auto-RP message action	Disabled **Note** Do Not Enable Auto-RP message action since, BSR is not available in Cisco Nexus 3550-T 10.2(3t) release.
BSR message action	Disabled **Note** Do not Enable BSR message action since, BSR is not available in Cisco Nexus 3550-T - 10.2(3t) release.

Parameters	Default
PIM sparse mode	Disabled
Designated router priority	1
Hello authentication mode	Disabled
Domain border	Disabled **Note** Do not Enable since Domain border is not available in Cisco Nexus 3550-T - 10.2(3t) release.
RP address policy	No message filtering
PIM register message policy	No message filtering
BSR candidate RP policy	No message filtering (BSR not supported)
BSR policy	No message filtering (BSR not supported)
Auto-RP mapping agent policy	No message filtering (Auto-RP not supported)
Auto-RP RP candidate policy	No message filtering (Auto-RP not supported)
Join-prune policy	No message filtering
Neighbor adjacency policy	Become adjacent with all PIM neighbors

Configuring PIM

Note

- Cisco NX-OS supports only PIM sparse mode version 2. In this publication, “PIM” refers to PIM sparse mode version 2.
- There are no {*,G} routes installed in hardware. All hardware forwarding of multicast traffic occurs only after the source trees are formed.

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.
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	
Register rate limit	Configures the IPv4 register rate limit in packets per second. The range is from 1 to 65,53 is no limit.
Initial holddown period	Configures the IPv4 initial holddown period in seconds. This holddown period is the time MRIB to come up initially. If you want faster convergence, enter a lower value. The range 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 i multi-access network with multiple PIM-enabled routers, the router with the highest DR pr as the DR router. If the priorities match, the software elects the DR with the highest IP ad originates PIM register messages for the directly connected multicast sources and sends PIM toward the rendezvous point (RP) for directly connected receivers. Values range from 1 to The default is 1.
Designated router delay	Delays participation in the designated router (DR) election by setting the DR priority that PIM hello messages to 0 for a specified period. During this delay, no DR changes occur, a switch is given time to learn all of the multicast states on that interface. After the delay per correct DR priority is sent in the hello packets, which retriggers the DR election. Values r 0xffff seconds.
Hello authentication mode	Enables an MD5 hash authentication key, or password, in PIM hello messages on the inte directly connected neighbors can authenticate each other. The PIM hello messages are IPsec the Authentication Header (AH) option. You can enter an unencrypted (cleartext) key or c 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.
Hello interval	Configures the interval at which hello messages are sent in milliseconds. The range is fro 18724286. The default is 30000. **Note** See the *Cisco Nexus® 3550-T Verified Scalability Guide* for the verified range of and associated PIM neighbor scale.

Parameter	Description
Neighbor policy	Configures which PIM neighbors to become adjacent to based on a prefix-list policy.[2] If the p does not exist or no prefix lists are configured in a policy, adjacency is established with all nei default is to become adjacent with all PIM neighbors. **Note** We recommend that you should configure this feature only if you are an experienc administrator. **Note** The PIM neighbor policy supports only prefix lists. It does not support ACLs use route map.

[2] To configure prefix-list policies, see the *Cisco Nexus® 3550-T Unicast Routing Configuration* section.

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 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 3	(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 4	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Displays PIM running-configuration information.

Step 5	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 6	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.

	Command or Action	Purpose
Step 7	(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 8	(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 Layer 3 interfaces only.
Step 9	(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.
Step 10	(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 11	(Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	Displays PIM interface information.

	Command or Action	Purpose
	Example: `switch(config-if)# show ip pim interface`	
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Layer 3 Multicast Receiver VLAN

Procedure

	Command or Action	Purpose

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

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

Step 3	**switchport** **Example:** `switch(config-if)# switchport`	Enables Layer 2 mode.
Step 4	**switchport mode trunk** **Example:** `switch(config-if)# switchport mode trunk`	Enables Layer 2 Trunk mode.
Step 5	**[no] switchport trunk l3-multicast receiver-vlan** *vlan-id* **Example:** `switch(config-if)# switchport trunk l3-multicast receiver-vlan 5`	Enables receiver vlan on trunk port.
Step 6	(Optional) **show running-config interface ethernet** *slot/port* **Example:** `switch(config-if)# show running-config interface ethernet1/1`	Displays the configured receiver vlan.

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* |**route-map** *policy-name*] **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.

	Command or Action	Purpose
		The mode is ASM. 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.
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 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.

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 192.0.2.0/24 10.0.0.1`	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.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring Message Filtering

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

Table 6: PIM Message Filtering

Message Type	Description
Global to the Device	
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.
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® 3550-T Unicast Routing Configuration* section.

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 (*,G) or (RP,G).
- The **igmp report-policy** command can use (*,G).

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 (*,G) and (*,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	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

Step 4	(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 5	(Optional) **show run pim** **Example:** `switch(config-if)# show run pim`	Displays PIM configuration commands.
Step 6	(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:** `switch# restart pim`	Restarts the PIM process. **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.

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 The **summary** option displays route co packet rates.
show ip pim group-range [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays the learned or configured grou and modes. For similar information, see **ip pim rp** command.

Command	Description
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 in (OIF) list.
show ip pim route [*source* | *group* [*source*]] [**vrf** *vrf-name* | **all**]	Displays information for each multicast rou including interfaces on which a PIM join fo (*, G) has been received.
show ip pim rp [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays rendezvous points (RPs) known t software, how they were learned, and their ranges. For similar information, see the **sho pim group-range** command.
show running-config pim	Displays the running-configuration informa
show startup-config pim	Displays the startup-configuration informa
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.
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 ip pim 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.

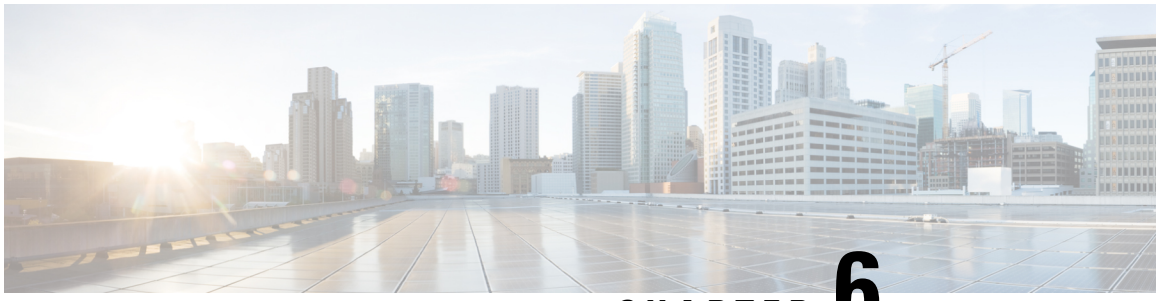
Command	Description
clear ip pim statistics [**vrf** *vrf-name*]	Clears global counters handled by the PIM process.

Related Documents

Related Topic	Document Title
Configuring VRFs	*Cisco Nexus® 3550-T Unicast Routing Configuration* sec

MIBs

MIBs	MIBs Link
MIBs related to PIM	To locate and download supported MIBs, go to the follow 3500-T MIBs



CHAPTER 6

Configuring Multicast ACL for RPs for PIM-SM

This chapter describes how to configure the Protocol Independent Multicast (PIM) and PIM6 features on Cisco NX-OS devices in your IPv4 networks.

- Introduction, on page 55
- Guidelines and Limitations for PIM Allow RP, on page 55
- Information about PIM Allow RP, on page 55
- Configuring RPs for PIM-SM, on page 56

Introduction

This chapter describes how to configure multicast ACL for RP feature in IPv4 networks. This determines RP is used to create state and build shared trees when an incoming (*, G) Join is processed. This allows for creating (*,G) trees determined by the policy for a given multicast group.

Guidelines and Limitations for PIM Allow RP

- A route-map policy for RP should only contain group prefixes to use with the match ip multicast command.

Information about PIM Allow RP

Rendezvous Points

A rendezvous point (RP) is a role that a device performs when operating in Protocol Independent Multicast (PIM) Sparse Mode (SM). An RP is required only in networks running PIM SM. In the PIM-SM model, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data contrasts with PIM Dense Mode (PIM DM). In PIM DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic. An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.

By default, when the first hop device of the receiver learns about the source, it will send a Join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does

not include the RP unless the RP is located within the shortest path between the source and receiver. In most cases, the placement of the RP in the network is not a complex decision.

By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM version 2, the RP performs less processing than in PIM version 1 because sources must only periodically register with the RP to create state.

Configuring RPs for PIM-SM

Before you begin

All access lists should be configured prior to beginning the configuration task. For information about how to configure an access list, see the "Configuring IP ACLs" chapter in the Cisco Nexus 3550 Series NX-OS Security 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:
	`switch(config)# interface gigabitethernet 1/1`
	`switch(config-if)#`
		Selects an interface that is connected to hosts on which PIM can be enabled. **interface** type number.

Step 3	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enable PIM. You must use sparse mode.
Step 4	**no shut** **Example:** `switch(config-if)# no shut`	Enable an interface.
Step 5	**Exit** **Example:** `switch(config-if)# exit`	Return to global configuration mode. Repeat Steps 3 through 5 on every interface that uses IP multicast.
Step 6	**ip pim rp-address** *rp-address*[**group-list***ip-prefix* | **route-map***policy-name*] **Example:** `switch(config)# ip pim rp-address 30.2.2.2 group-list 224.0.0.0/4`	Configures a PIM static RP address for a multicast group range. You can specify a route-map policy name that lists the group prefixes to use with the match ip multicast command. This command can also be used in VRF mode.

	Command or Action	Purpose
Step 7	**end** **Example:** `Switch(config)# end`	Exit configuration mode.
Step 8	(Optional) **show ip pim rp** [**vrf**|*rp-address*] **Example:** `switch# show ip pim rp`	Display the RPs known in the network and shows how the router learned about each RP.
Step 9	(Optional) **show ip mroute** **Example:** `switch# show ip mroute`	Display the contents of the IP mroute table.