Cisco Nexus 3000 Series NX-OS Multicast Routing Configuration Guide, Release 9.2(x)

First Published: 2018-07-18

Last Modified: 2020-09-03

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

CONTENTS

PREFACE

Preface xi
Audience xi
Document Conventions xi
Related Documentation for Cisco Nexus 3000 Series Switches xii
Documentation Feedback xii
Communications, Services, and Additional Information xii

CHAPTER 1

New and Changed Information 1
New and Changed Information 1

CHAPTER 2

Overview 3
Licensing Requirements 3
About Multicast 3
Multicast Distribution Trees 4
Source Trees 4
Shared Trees 5
Multicast Forwarding 6
Cisco NX-OS PIM 6
ASM 8
SSM 8
RPF Routes for Multicast 8
IGMP 8
IGMP Snooping 9
Interdomain Multicast 9
SSM 9

MSDP 9

MRIB 9

General Multicast Restrictions 10

Troubleshooting Inconsistency Between SW and HW Multicast Routes 11

Additional References 11

Related Documents 11

MIBs 12

Technical Assistance 12

CHAPTER 3 **Configuring IGMP** 13

About IGMP 13

IGMP Versions 13

IGMP Basics 14

Virtualization Support 16

Guidelines and Limitations for IGMP 16

Default Settings for IGMP 17

Configuring IGMP Parameters 17

Configuring IGMP Interface Parameters 18

Configuring an IGMP SSM Translation 24

Configuring the Enforce Router Alert Option Check 25

Verifying the IGMP Configuration 26

Configuration Examples for IGMP 26

Where to Go Next 27

Feature History for IGMP 27

CHAPTER 4 **Configuring PIM and PIM6** 29

About PIM and PIM6 30

PIM SSM with vPC 31

Hello Messages 31

Join-Prune Messages 32

State Refreshes 33

Rendezvous Points 33

Static RP 33

BSRs 33

Auto-RP 34

Anycast-RP 35

PIM Register Messages 36

Designated Routers 36

Designated Forwarders 37

Administratively Scoped IP Multicast 37

Virtualization Support 37

Prerequisites for PIM and PIM6 37

Guidelines and Limitations for PIM and PIM6 38

Default Settings 40

Configuring PIM and PIM6 40

Configuring PIM and PIM6 41

Enabling the PIM or PIM6 Feature 42

Configuring PIM or PIM6 Sparse Mode 43

Configuring PIM Sparse Mode Parameters 45

Configuring PIM6 Sparse Mode Parameters 48

Configuring ASM and Bidir 49

Configuring Static RPs (PIM) 49

Configuring Static RPs (PIM6) 50

Configuring BSRs 51

Configuring BSRs (PIM) 53

Configuring Auto-RP 54

Configuring Auto RP 56

Configuring Auto RP (PIM) 56

Configuring a PIM Anycast RP Set (PIM) 57

Configuring a PIM Anycast RP Set (PIM6) 59

Configuring Shared Trees Only for ASM (PIM) 60

Configuring Shared Trees Only for ASM (PIM6) 61

Setting the Maximum Number of Entries in the Multicast Routing Table 62

Preventing Duplicate Packets During an RPT to SPT Switchover 62

Configuring SSM (PIM) 63

Configuring SSM (PIM6) 65

Configuring PIM SSM Over a vPC 66

Configuring RPF Routes for Multicast 67

Disabling Multicast Multipath 68
Configuring Route Maps to Control RP Information Distribution (PIM) 69
Configuring Route Maps to Control RP Information Distribution (PIM6) 70
Configuring Message Filtering 71
Configuring Message Filtering (PIM) 72
Restarting the PIM Process 74
Configuring Message Filtering (PIM6) 75
Verifying the PIM and PIM6 Configuration 76
Configuring Multicast Table Size 77
Configuring the Multicast Entries Using the CLI 77
Displaying the Multicast Entries 77
Configuring the Unicast Entries Using the CLI 77
Displaying the Unicast Entries 78
Displaying Statistics 78
Displaying PIM and PIM6 Statistics 78
Clearing PIM Statistics 78
Configuration Examples for PIM 79
SSM Examples for Configuration 79
Configuration Example for PIM SSM Over vPC 79
Configuration Example for BSR 83
Configuration Example for PIM Anycast-RP 84
Auto-RP Configuration Example 85
Where to Go Next 86
Additional References 86
Related Documents 86
Standards 87
MIBs 87
Feature History for PIM and PIM6 87
CHAPTER 5 Configuring IGMP Snooping 89
About IGMP Snooping 89
IGMPv1 and IGMPv2 90
IGMPv3 90
IGMP Snooping Querier 91

IGMP Filtering on Router Ports 91
IGMP Snooping with VRFs 91
Prerequisites for IGMP Snooping 91
Default Settings 92
Configuring IGMP Snooping Parameters 92
Configuring IGMP Snooping Parameters 94
Verifying the IGMP Snooping Configuration 98
Setting Interval for Multicast Routes 99
Displaying IGMP Snooping Statistics 99
Configuration Examples for IGMP Snooping 100
Where to Go Next 100
Additional References 100
Related Documents 100
Standards 101
Feature History for IGMP Snooping 101

CHAPTER 6 Configuring MSDP 103
About MSDP 103
SA Messages and Caching 104
MSDP Peer-RPF Forwarding 105
MSDP Mesh Groups 105
Virtualization Support 105
Prerequisites for MSDP 105
Default Settings 106
Configuring MSDP 106
Enabling the MSDP Feature 107
Configuring MSDP Peers 107
Configuring MSDP Peer Parameters 108
Configuring MSDP Global Parameters 111
Configuring MSDP Mesh Groups 112
Restarting the MSDP Process 113
Verifying the MSDP Configuration 114
Displaying Statistics 114
Displaying Statistics 114

Clearing Statistics 115
Configuration Examples for MSDP 115
Additional References 117
Related Documents 117
Standards 117
Feature History for IGMP 117

CHAPTER 7 Configuring Multicast VRF-Lite Route Leaking 119
About Multicast VRF-Lite Route Leaking 119
Guidelines and Limitations for VRF-Lite Route Leaking 119
Configuring Multicast VRF-Lite Route Leaking 120
Verifying the Multicast VRF-Lite Route Leaking Configuration 120
Configuration Examples for Multicast VRF-Lite Route Leaking 121
Related Documents 121
Standards 121
Feature History for Multicast VRF-Lite Route Leaking 122

APPENDIX A IETF RFCs for IP Multicast 123
IETF RFCs for IP Multicast 123

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Preface

This preface includes the following sections:

- Audience, on page xi
- Document Conventions, on page xi
- Related Documentation for Cisco Nexus 3000 Series Switches, on page xii
- Documentation Feedback, on page xii
- Communications, Services, and Additional Information, on page xii

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 the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments 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 will include 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 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 3000 Series Switches

The entire Cisco Nexus 3000 Series switch documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html

Documentation Feedback

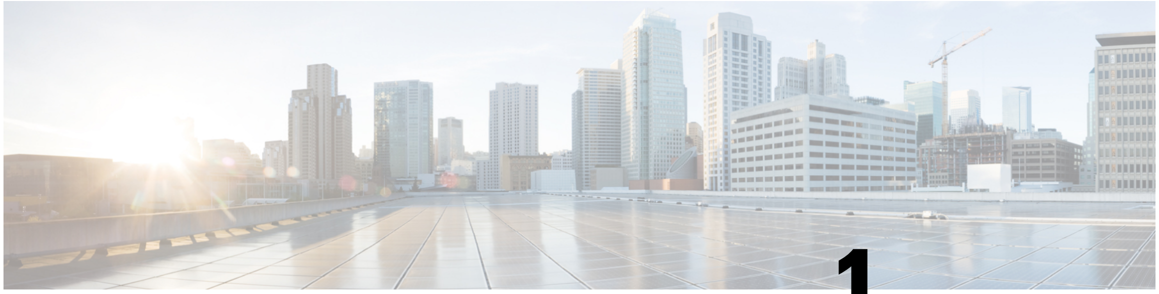
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

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.



CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3000 Series NX-OS Multicast Routing Configuration Guide, Release 9.2(x)*.

- New and Changed Information, on page 1

New and Changed Information

This table summarizes the new and changed features for the Cisco Nexus 3000 Series NX-OS Multicast Routing Configuration Guide, Release 9.2(x) and tells you where they are documented.

Table 1: New and Changed Features for Cisco NX-OS Release 9.2(x)

Feature	Description	Changed in Release	Where Documented
No updates since Cisco NX-OS Release 7.x	First 9.2(x)release	9.2(1)	-
IGMP	Added support for the Cisco Nexus 34180YC platform switch.	9.2.2	Configuring IGMP, on page 13

CHAPTER 2

Overview

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

This chapter includes the following sections:

- Licensing Requirements, on page 3
- About Multicast, on page 3
- General Multicast Restrictions, on page 10
- Troubleshooting Inconsistency Between SW and HW Multicast Routes , on page 11
- Additional References, on page 11

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.

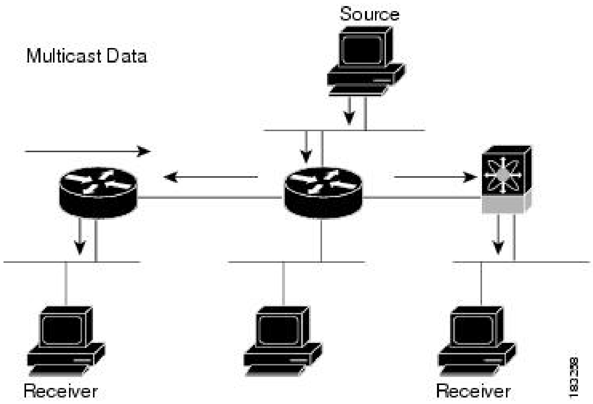
Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel. The Internet Assigned Number Authority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

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.

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

Figure 1: Multicast Traffic from One Source to Two Receivers



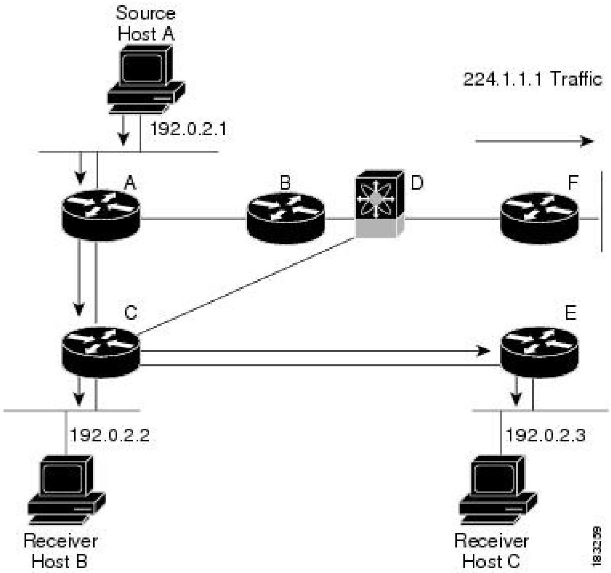
Multicast Distribution Trees

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

Source Trees

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

Figure 2: Source Tree

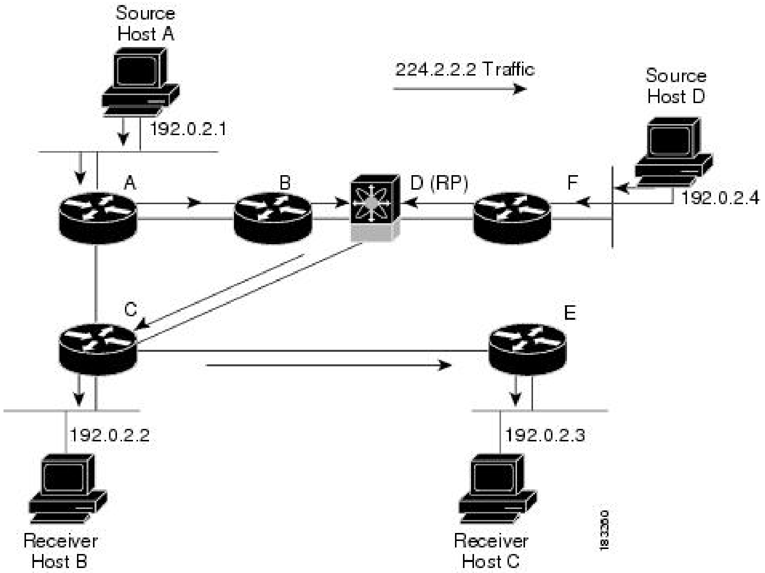


The notation (S, G) represents the multicast traffic from source S on group G. The SPT in this figure is written (192.0.2.1, 224.1.1.1). Multiple sources can be transmitting on the same group.

Shared Trees

A shared tree represents the shared distribution path that the multicast traffic takes through the network from a shared root or rendezvous point (RP) to each receiver. (The RP creates an SPT to each source.) A shared tree is also called an RP tree (RPT). The following figure shows a shared tree for group 224.1.1.1 with the RP at router D. Source hosts A and D send their data to router D, the RP, which then forwards the traffic to receiver hosts B and C.

Figure 3: Shared Tree



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

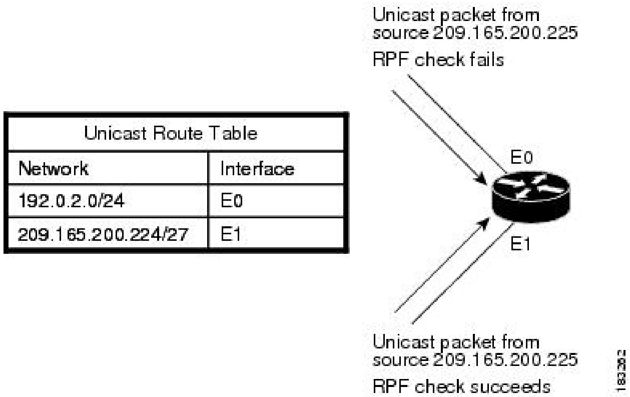
Multicast Forwarding

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

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

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

Figure 4: RPF Check Example



Unicast Route Table

Network	Interface
192.0.2.0/24	E0
209.165.200.224/27	E1

Unicast packet from source 209.165.200.225
RPF check fails
E0
E1
Unicast packet from source 209.165.200.225
RPF check succeeds
183282

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 configure PIM for an IPv4 network. By default, IGMP runs 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.

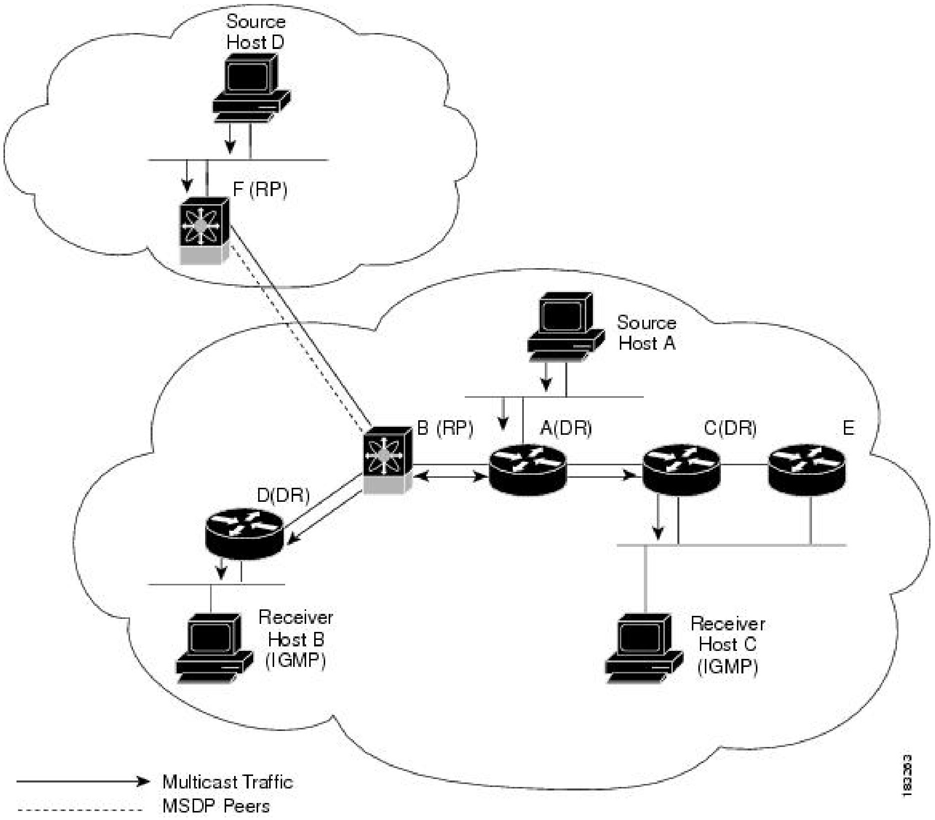
The distribution trees change automatically to reflect the topology changes due to link or router failures. PIM dynamically tracks both multicast-capable sources and receivers.

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

The following figure shows two PIM domains in an IPv4 network.

Note In this publication, “PIM for IPv4” refer to the Cisco NX-OS implementation of PIM sparse mode. A PIM domain can include an IPv4 network.

Figure 5: PIM Domains in an IPv4 Network



- The lines with arrows show the path of the multicast data through the network. The multicast data originates from the sources at hosts A and D.
- The dashed line connects routers B and F, which are Multicast Source Discovery Protocol (MSDP) peers. MSDP supports the discovery of multicast sources in other PIM domains.
- Hosts B and C receive multicast data by using Internet Group Management Protocol (IGMP) to advertise requests to join a multicast group.

- Routers A, C, and D are designated routers (DRs). When more than one router is connected to a LAN segment, such as C and E, the PIM software chooses one router to be the DR so that only one router is responsible for putting multicast data on the segment.

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

PIM supports these multicast modes for connecting sources and receivers:

- Any source multicast (ASM)
- Source-Specific Multicast (SSM)

Cisco NX-OS supports a combination of these modes for different ranges of multicast groups. You can also define RPF routes for multicast.

ASM

Any Source Multicast (ASM) is a PIM tree building mode that uses shared trees to discover new sources and receivers as well as source trees to form shortest paths from receivers to sources. The shared tree uses a network node as the root, called the rendezvous point (RP). The source tree is rooted at first-hop routers, directly attached to each source that is an active sender. The ASM mode requires an RP for a group range. An RP can be configured statically or learned dynamically by the Auto-RP or BSR group-to-RP discovery protocols.

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

For information about configuring ASM, see the Configuring ASM and Bidir section.

SSM

Source-Specific Multicast (SSM) is a PIM mode that builds a source tree that originates at the designated router on the LAN segment that receives a request to join a multicast source. Source trees are built by sending PIM join messages in the direction of the source. The SSM mode does not require you to configure RPs.

The SSM mode allows receivers to connect to sources outside the PIM domain.

For information about configuring SSM, see the Configuring SSM (PIM) section.

RPF Routes for Multicast

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

For information about configuring RPF routes for multicast, see the Configuring RPF Routes for Multicast section.

IGMP

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

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

You can configure IGMPv2 or IGMPv3 on an interface. You will usually configure IGMPv3 to support SSM mode. By default, the software enables IGMPv2.

For information about configuring IGMP, see Configuring IGMP.

IGMP Snooping

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

For information about configuring IGMP snooping, see Configuring IGMP Snooping.

Interdomain Multicast

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

SSM

The PIM software uses SSM to construct a shortest path tree from the designated router for the receiver to a known source IP address, which may be in another PIM domain. The ASM mode cannot access sources from another PIM domain without the use of another protocol.

Once you enable PIM in your networks, you can use SSM to reach any multicast source that has an IP address known to the designated router for the receiver.

For information about configuring SSM, see the Configuring SSM (PIM) section.

MSDP

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

Note Cisco NX-OS supports the PIM Anycast-RP, which does not require MSDP configuration. For information about PIM Anycast-RP, see the Configuring a PIM Anycast RP Set (PIM) section.

For information about MSDP, see Configuring MSDP.

MRIB

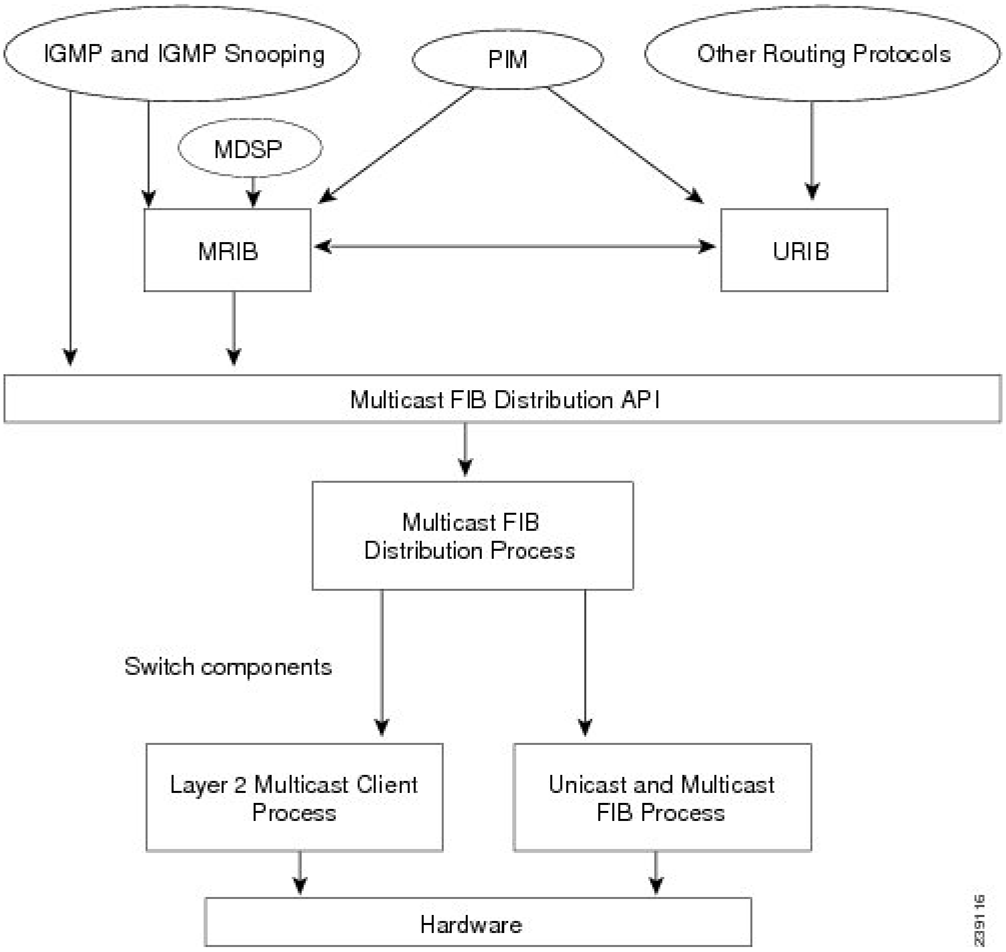
The Cisco NX-OS IPv4 Multicast Routing Information Base (MRIB) is a repository for route information that is generated by multicast protocols such as PIM and IGMP. The MRIB does not affect the route information itself. The MRIB maintains independent route information for each virtual routing and forwarding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

The following figure shows the major components of the Cisco NX-OS multicast software architecture:

- The Multicast FIB (MFIB) Distribution (MFDM) API defines an interface between the multicast Layer 2 and Layer 3 control plane modules, including the MRIB, and the platform forwarding plane. The control plane modules send the Layer 3 route update and Layer 2 lookup information using the MFDM API.
- The multicast FIB distribution process distributes the multicast update messages to the switch.

- The Layer 2 multicast client process sets up the Layer 2 multicast hardware forwarding path.
- The unicast and multicast FIB process manages the Layer 3 hardware forwarding path.

Figure 6: Cisco NX-OS Multicast Software Architecture


IGMP and IGMP Snooping
PIM
Other Routing Protocols
MDSP
MRIB
URIB
Multicast FIB Distribution API
Multicast FIB Distribution Process
Switch components
Layer 2 Multicast Client Process
Unicast and Multicast FIB Process
Hardware
239116

General Multicast Restrictions

The following are the guidelines and limitations for Multicast on Cisco NX-OS:

- Cisco NX-OS does not support Pragmatic General Multicast (PGM).
- Layer 3 Ethernet port-channel subinterfaces are not supported with multicast routing.
- Layer 3 IPv6 multicast routing is not supported.
- Layer 2 IPv6 multicast packets will be flooded on the incoming VLAN.
- The Cisco Nexus 34180YC platform switch does not support IPv6.
- Network Load Balancing (NLB) feature is not supported on the Cisco Nexus 3000 series switches.

Troubleshooting Inconsistency Between SW and HW Multicast Routes

Symptom

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

Possible Cause

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

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

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

Corrective Action

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

Additional References

For additional information related to implementing multicast, see the following sections:

- Related Documents, on page 11
- IETF RFCs for IP Multicast
- Technical Assistance

Related Documents

Related Topic	Document Title
CLI Commands	Nexus 3000 Series NX-OS Multicast Routing Command Reference. .
Configuring VRFs	Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.

MIBs

MIBs	MIBs Link
IP Multicast	To locate and download MIBs, go to the following: MIB Locator.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

CHAPTER 3

Configuring IGMP

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

This chapter includes the following sections:

- About IGMP, on page 13
- Guidelines and Limitations for IGMP, on page 16
- Default Settings for IGMP, on page 17
- Configuring IGMP Parameters, on page 17
- Verifying the IGMP Configuration, on page 26
- Configuration Examples for IGMP, on page 26
- Where to Go Next, on page 27
- Feature History for IGMP, on page 27

About IGMP

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

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

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

IGMP Versions

The switch supports IGMPv2 and IGMPv3, as well as IGMPv1 report reception.

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

IGMPv3 includes the following key changes from IGMPv2:

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

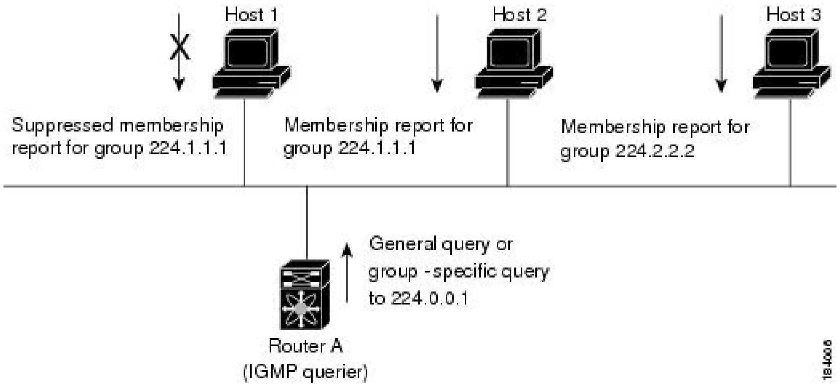
For detailed information about IGMPv2, see RFC 2236.

For detailed information about IGMPv3, see RFC 3376.

IGMP Basics

The basic IGMP process of a router that discovers multicast hosts is shown in this figure. Hosts 1, 2, and 3 send unsolicited IGMP membership report messages to initiate receiving multicast data for a group or channel.

Figure 7: IGMPv1 and IGMPv2 Query-Response Process


Host 1
Host 2
Host 3
Suppressed membership report for group 224.1.1.1
Membership report for group 224.1.1.1
Membership report for group 224.2.2.2
General query or group -specific query to 224.0.0.1
Router A (IGMP querier)
184006

In the figure **IGMPv1 and IGMPv2 Query-Response Process**, 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. For more information about configuring the IGMP parameters, see the Configuring IGMP Interface Parameters section.

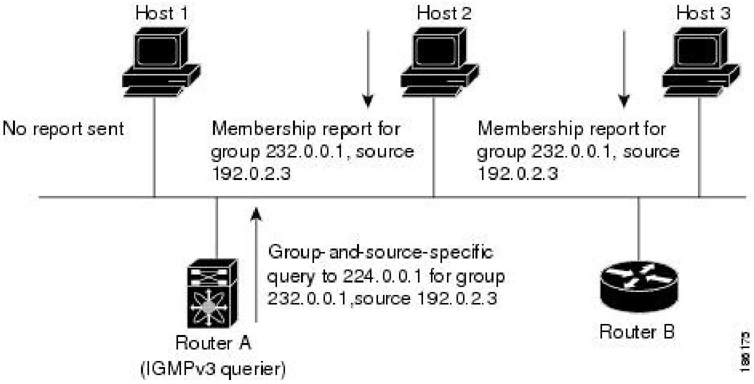
The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes 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 the following 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. This IGMPv3 feature supports SSM. For information about configuring SSM translation to support SSM for IGMPv1 and IGMPv2 hosts, see the Configuring an IGMP SSM Translation, on page 24 section.

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


Host 1
Host 2
Host 3
No report sent
Membership report for group 232.0.0.1, source 192.0.2.3
Membership report for group 232.0.0.1, source 192.0.2.3
Group-and-source-specific query to 224.0.0.1 for group 232.0.0.1,source 192.0.2.3
Router A
(IGMPv3 querier)
Router B
185173

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.

For more information about configuring the IGMP parameters, see the Configuring IGMP Interface Parameters section.

Virtualization Support

Cisco NX-OS supports virtual routing and forwarding (VRF). You can define multiple VRF instances. A VRF configured with IGMP supports the following IGMP features:

- IGMP is enabled or disabled on per interface
- IGMPv1, IGMPv2, and IGMPv3 provide router-side support
- IGMPv2 and IGMPv3 provide host-side support
- Supports configuration of IGMP querier parameters
- IGMP reporting is supported for link local multicast groups
- IGMP SSM-translation supports mapping of IGMPv2 groups to a set of sources
- Supports multicast trace-route (Mtrace) server functionality to process Mtrace requests

For information about configuring VRFs, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.

Guidelines and Limitations for IGMP

IGMP has the following guidelines and limitations:

- Excluding or blocking a list of sources according to IGMPv3 (RFC 3376) is not supported.
- All external multicast router ports (either statically configured or dynamically learned) use the global LTL index. As a result, traffic in VLAN X goes out on the multicast router ports in both VLAN X and VLAN Y, in case both multicast router ports (Layer 2 trunks) carry both VLAN X and VLAN Y.
- On Cisco Nexus 3000 Series switches, you must carve the switch RACL TCAM regions in order to make IGMP and PIM work on Layer 3 interfaces. Some system default Multicast ACLs that are installed in the RACL regions are required for IGMP and PIM to work on Layer 3 interfaces.
- Starting with Release 7.0(3)I2(1), when you configure an interface in the VRF, configure the PIM, send the IGMP joins and verify the CLI command **show ip fib mroute**, an error message is displayed as follows: **ERROR: Invalid Table-id**.

  The default table is not created until there are joins in the interface under the default VRF. Therefore, an error is displayed while attempting to display the default table. When a group is learned in the default table, the default table is created and the error message is not displayed anymore.

  The CLI command **show ip fib mroute** is not supported on the Cisco Nexus 34180YC platform switch.
- In Cisco NX-OS releases older than Cisco NX-OS Release 6.0(2)U1(1), you can use the **ip igmp join-group** command to bind a Nexus 3000 Series switch to a multicast group. The switch generates an Internet Group Management Protocol (IGMP)-join for the specified group, and any multicast packets

destined to the group are sent to the CPU. If there are receivers connected to the Nexus 3000 Series switch, which request for the group, then a copy of the packet is also sent to the receiver.

- In Cisco NX-OS Release 6.0(2)U1(1) and higher releases, you cannot use the **ip igmp join-group** command to program any Outgoing Interface Lists (OILs). Even if there are receivers that request for the stream, no packets are sent to them. To bind a Nexus 3000 Series switch to a multicast group, use the **ip igmp static-oif** command instead of the **ip igmp join-group** command.
- Ingress RACL for L3 multicast data traffic, is not supported on the Cisco Nexus 34180YC platform switch.

Default Settings for IGMP

This table lists the default settings for IGMP parameters.

Table 2: Default IGMP Parameters

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

Configuring IGMP Parameters

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

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

Configuring IGMP Interface Parameters

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

Table 3: IGMP Interface Parameters

Parameter	Description
IGMP version	IGMP version that is enabled on the interface. The IGMP version can be 2 or 3. The default is 2.
Static multicast groups	Multicast groups that are statically bound to the interface. You can configure the groups to join the interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. **Note** Although you can configure the (S, G) state, the source tree is built only if you enable IGMPv3. For information about SSM translation, see the Configuring an IGMP SSM Translation section. You can configure a multicast group on all the multicast-capable routers on the network so that pinging the group causes all the routers to respond.
Static multicast groups on OIF	Multicast groups that are statically bound to the output interface. You can configure the groups to join the output interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. **Note** Although you can configure the (S, G) state, the source tree is built only if you enable IGMPv3. For information about SSM translation, see the Configuring an IGMP SSM Translation section.

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.

Parameter	Description
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.
Report policy	Access policy for IGMP reports that is based on a route-map policy. **Tip** To configure route-map policies, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.
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.
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.
global-leave-ignore-gss-mrt	Beginning with Cisco NX-OS Release 5.0(3)U1(2), you can use the configured Maximum Response Time (MRT) value in group-specific queries against a lower MRT value in response to IGMP global leave messages (IGMP leave reports to group 0.0.0.0).

Procedure

	Command or Action	Purpose

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

Step 2	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the interface type and number, such as **ethernet** *slot/port.*.

Step 3	**no switchport**
	Example:
	`switch(config-if)# no switchport`
	`switch(config-if)#`	

Step 4	**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 5	**ip igmp join-group** {**group** [**source** *source*] | **route-map** *policy-name*}
	Example:
	`switch(config-if)# ip igmp join-group 230.0.0.0`
		Configures an interface on the device to join the specified group or channel. The device accepts the multicast packets for CPU consumption only.
		Caution The device CPU must be able to handle the traffic generated by using this command. Because of CPU load constraints, using this command, especially in any form of scale, is not recommended. Consider using the **ip igmp static-oif** command instead.

Step 6	**ip igmp static-oif** {*group* [**source** *source*] | **route-map** *policy-name*}
	Example:
	`switch(config-if)# ip igmp static-oif 230.0.0.0`
		Statically binds a multicast group to the outgoing interface, which is handled by the device hardware. If you specify only the group address, the (*, G) state is created. If you specify the source address, the (S, G) state is created. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command.
		Note A source tree is built for the (S, G) state only if you enable IGMPv3.

	Command or Action	Purpose
Step 7	**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 8	**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 9	**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 10	**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 11	**ip igmp query-timeout** *seconds* **Example:** `switch(config-if)# ip igmp query-timeout 300`	Sets the query timeout that the software uses when deciding to take over as the querier. Values can range from 1 to 65,535 seconds. The default is 255 seconds. **Note** This command has the same functionality as the **ip igmp querier-timeout** command.
Step 12	**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 13	**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 14	**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 15	**ip igmp last-member-query-count** *count* **Example:**	Sets the number of times that the software sends an IGMP query in response to a host

	Command or Action	Purpose
	`switch(config-if)# ip igmp last-member-query-count 3`	leave message. Values can range from 1 to 5. The default is 2.
Step 16	**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 17	**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 18	**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 19	**ip igmp access-group** *policy* **Example:** `switch(config-if)# ip igmp access-group my_access_policy`	Configures a route-map policy to control the multicast groups that hosts on the subnet serviced by an interface can join. **Note** Only the **match ip multicast group** command is supported in this route map policy. The **match ip address** command for matching an ACL is not supported.
Step 20	**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 21	**ip igmp global-leave-ignore-gss-mrt** **Example:** `switch(config-if)# ip igmp global-leave-ignore-gss-mrt`	Enables the switch to use the general Maximum Response Time (MRT) in response to an IGMP global leave message for general queries.
Step 22	(Optional) **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] **Example:**	Displays IGMP information about the interface.

	Command or Action	Purpose
	`switch(config)# show ip igmp interface`	
Step 23	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. Saves the configuration changes

Configuring an IGMP SSM Translation

You can configure an SSM translation to provide SSM support when the router receives IGMPv1 or IGMPv2 membership reports. Only IGMPv3 provides the capability to specify group and source addresses in membership reports. By default, the group prefix range is 232.0.0.0/8. To modify the PIM SSM range, see the Configuring SSM (PIM) section.

This table lists the example SSM translations.

Table 4: Example SSM Translations

Group Prefix	Source Address
232.0.0.0/8	10.1.1.1
232.0.0.0/8	10.2.2.2
232.1.0.0/16	10.3.3.3
232.1.1.0/24	10.4.4.4

This table shows the resulting MRIB routes that the IGMP process creates when it applies an SSM translation to the IGMP membership report. If more than one translation applies, the router creates the (S, G) state for each translation.

Table 5: Example Result of Applying SSM Translations

IGMPv2 Membership Report	Resulting MRIB Route
232.1.1.1	(10.4.4.4, 232.1.1.1)
232.2.2.2	(10.1.1.1, 232.2.2.2) (10.2.2.2, 232.2.2.2)

Note This feature is similar to SSM mapping found in some Cisco IOS software.

Procedure

	Command or Action	Purpose

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

Step 2	**ip igmp ssm-translate** *group-prefix source-addr* **Example:** `switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1`	Configures the translation of IGMPv1 or IGMPv2 membership reports by the IGMP process to create the (S,G) state as if the router had received an IGMPv3 membership report.
Step 3	(Optional) **show running-configuration igmp** **Example:** `switch(config)# show running-configuration igmp`	Shows the running-configuration information, including **ssm-translate** command lines.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring the Enforce Router Alert Option Check

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

Procedure

	Command or Action	Purpose

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

Step 2	(Optional) **[no] ip igmp enforce-router-alert** **Example:** `switch(config-if)# ip igmp enforce-router-alert`	Enables or Disables the enforce router alert option check for IGMPv2 and IGMPv3 packets. By default, the enforce router alert option check is enabled.
Step 3	(Optional) **show running-configuration igmp** **Example:** `switch(config)# show running-configuration igmp`	Shows the running-configuration information, including the **enforce-router-alert** command line.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Verifying the IGMP Configuration

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

Command	Purpose
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 *group*|*interface*] [**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*group* | *interface* **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.

For detailed information about the fields in the output from these commands, see the Cisco Nexus 3000 Series Command Reference.

Configuration Examples for IGMP

The following example shows how to configure the IGMP parameters:

```
switch# configure terminal
switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip igmp version 3
switch(config-if)# ip igmp join-group 230.0.0.0
switch(config-if)# ip igmp startup-query-interval 25
switch(config-if)# ip igmp startup-query-count 3
switch(config-if)# ip igmp robustness-variable 3
switch(config-if)# ip igmp querier-timeout 300
switch(config-if)# ip igmp query-timeout 300
switch(config-if)# ip igmp query-max-response-time 15
switch(config-if)# ip igmp query-interval 100
switch(config-if)# ip igmp last-member-query-response-time 3
switch(config-if)# ip igmp last-member-query-count 3
switch(config-if)# ip igmp group-timeout 300
switch(config-if)# ip igmp report-link-local-groups
switch(config-if)# ip igmp report-policy my_report_policy
switch(config-if)# ip igmp access-group my_access_policy
switch(config-if)# ip igmp immediate-leave
switch(config-if)# ip igmp global-leave-ignore-gss-mrt
```

This example shows how to configure a route map that accepts all multicast reports (joins):

```
switch(config)# route-map foo
switch(config-route-map)# exit
switch(config)# interface vlan 10
switch(config-if)# no switchport
switch(config-if)# ip pim sparse-mode
switch(config-if)# ip igmp report-policy foo
```

This example shows how to configure a route map that denies all multicast reports (joins):

```
switch(config)# route-map foo deny 10
switch(config-route-map)# exit
switch(config)# interface vlan 5
switch(config-if)# ip pim sparse-mode
switch(config-if)# ip igmp report-policy foo
```

Where to Go Next

You can enable the following features that work with PIM and IGMP:

- Configuring IGMP Snooping
- Configuring MSDP

Feature History for IGMP

This Table lists the release history for this feature.

Table 6: Feature History for IGMP

Feature Name	Releases	Feature Information
IGMP	5.0(3)U1(1)	This feature was introduced.
IGMP	9.2.2	Added support for the Cisco Nexus 34180YC platform switch.

CHAPTER 4

Configuring PIM and PIM6

This chapter describes how to configure the Protocol Independent Multicast (PIM) and PIM6 features on Cisco NX-OS switches in your IPv4 and IPv6 networks.

This chapter includes the following sections:

- About PIM and PIM6, on page 30
- Prerequisites for PIM and PIM6, on page 37
- Guidelines and Limitations for PIM and PIM6, on page 38
- Default Settings, on page 40
- Configuring PIM and PIM6, on page 40
- Configuring PIM or PIM6 Sparse Mode, on page 43
- Configuring ASM and Bidir, on page 49
- **Setting the Maximum Number of Entries in the Multicast Routing Table**, on page 62
- Preventing Duplicate Packets During an RPT to SPT Switchover, on page 62
- Configuring SSM (PIM), on page 63
- Configuring SSM (PIM6), on page 65
- Configuring PIM SSM Over a vPC, on page 66
- Configuring RPF Routes for Multicast, on page 67
- Configuring Route Maps to Control RP Information Distribution (PIM), on page 69
- Configuring Route Maps to Control RP Information Distribution (PIM6), on page 70
- Configuring Message Filtering, on page 71
- Verifying the PIM and PIM6 Configuration, on page 76
- Configuring Multicast Table Size, on page 77
- Configuration Examples for PIM, on page 79
- Where to Go Next, on page 86
- Additional References, on page 86
- Related Documents, on page 86
- Standards, on page 87
- MIBs, on page 87
- Feature History for PIM and PIM6, on page 87

About PIM and PIM6

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. For more information about multicast, see the About Multicast section.

Cisco NX-OS supports PIM sparse mode for IPv4 networks (PIM) and for IPv6 networks (PIM6). In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it. You can configure PIM and PIM6 to run simultaneously on a router. You can use PIM and PIM6 global parameters to configure rendezvous points (RPs), message packet filtering, and statistics. You can use PIM and PIM6 interface parameters to enable multicast, identify PIM borders, set the PIM hello message interval, and set the designated router (DR) priority. For more information, see the Configuring PIM or PIM6 Sparse Mode section.

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

In Cisco NX-OS, multicast is enabled only after you enable the PIM and PIM6 features on each router and then enable PIM or PIM6 sparse mode on each interface that you want to participate in multicast. You can configure PIM for an IPv4 network and PIM6 for an IPv6 network. In an IPv4 network, if you have not already enabled IGMP on the router, PIM enables it automatically. In an IPv6 network, MLD is enabled by default. For information about configuring IGMP, see Configuring IGMP.

You use the PIM and PIM6 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.
- Source-Specific Multicast (SSM) builds a source tree originating at the designated router on the LAN segment that receives a request to join a multicast source. SSM mode does not require you to configure RPs. Source discovery must be accomplished through other means.
- Bidirectional shared trees (Bidir) build a shared tree between sources and receivers of a multicast group but do not support switching over to a source tree when a new receiver is added to a group. Bidir mode requires that you configure an RP. Bidir forwarding does not require source discovery because only the shared tree is used.

Note Cisco Nexus 3000 Series switches do not support PIM6 Bidir.

You can combine the modes to cover different ranges of group addresses. For more information, see the Configuring PIM and PIM6 section.

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

For more information about PIM SSM mode, see RFC 3569.

For more information about PIM Bidir mode, see draft-ietf-pim-bidir-09.txt

Note Multicast equal-cost multipathing (ECMP) is on by default in the Cisco NX-OS for the Cisco Nexus 3000 Series switches; you cannot turn ECMP off. If multiple paths exist for a prefix, PIM selects the path with the lowest administrative distance in the routing table.Cisco NX-OS supports up to 16 paths to a destination.

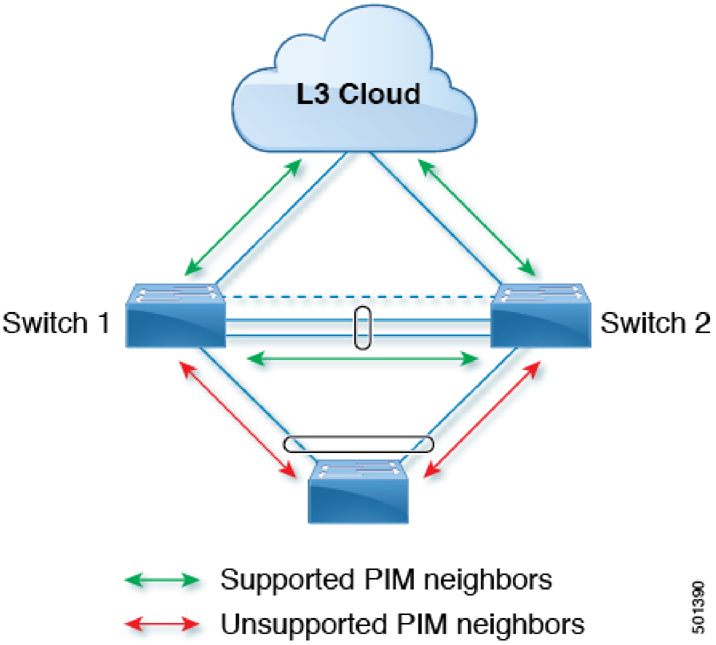
PIM SSM with vPC

Beginning with Cisco NX-OS Release 7.0(3)I4(1), you can enable PIM SSM on Cisco Nexus 3000 Series switches with an upstream Layer 3 cloud along with the vPC feature.

A PIM adjacency between a Switched Virtual Interface (SVI) on a vPC VLAN (a VLAN that is carried on a vPC Peer-Link) and a downstream device is not supported; this configuration can result in dropped multicast packets. If a PIM neighbor relationship is required with a downstream device, a physical Layer 3 interface must be used on the Nexus switches instead of a vPC SVI.

For SVIs on vPC VLANs, only one PIM adjacency is supported, which is with the vPC peer switch. PIM adjacencies over the vPC peer-link with devices other than the vPC peer switch for the vPC-SVI are not supported.

Figure 9: PIM SSM with vPC



Hello Messages

The PIM process begins when the router establishes PIM neighbor adjacencies by sending PIM hello messages to the multicast address 224.0.0.13 or IPv6 address FF02::d. Hello messages are sent periodically at the interval of 30 seconds. When all neighbors have replied, then 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.

Caution If you change the PIM hello interval to a lower value, we recommend that you ensure it is appropriate for your network environment.

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.

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

Note PIM6 does not support MD5 authentication.

Note If PIM is disabled on the switch, the IGMP snooping software processes the PIM hello messages.

For information about configuring hello message authentication, see the Configuring PIM or PIM6 Sparse Mode section.

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 or Bidir mode) or source (SSM 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 or Bidir mode. SSM does not use an RP but builds a shortest path tree (SPT) that is the lowest cost path between the source and the receiver.

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. For information about configuring the join-prune message policy, see the Configuring PIM or PIM6 Sparse Mode section.

You can prebuild the SPT for all known (S,G) in the routing table by triggering PIM joins upstream. To prebuild the SPT for all known (S,G)s in the routing table by triggering PIM joins upstream, even in the absence of any receivers, use the **ip pim pre-build-spt** command. By default, PIM (S,G) joins are triggered upstream only if the OIF-list for the (S,G) is not empty.

State Refreshes

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

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

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

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

Rendezvous Points

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

Static RP

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

You can define static RPs for the following reasons:

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

For information about configuring static RPs, see the Configuring Static RPs (PIM) section.

BSRs

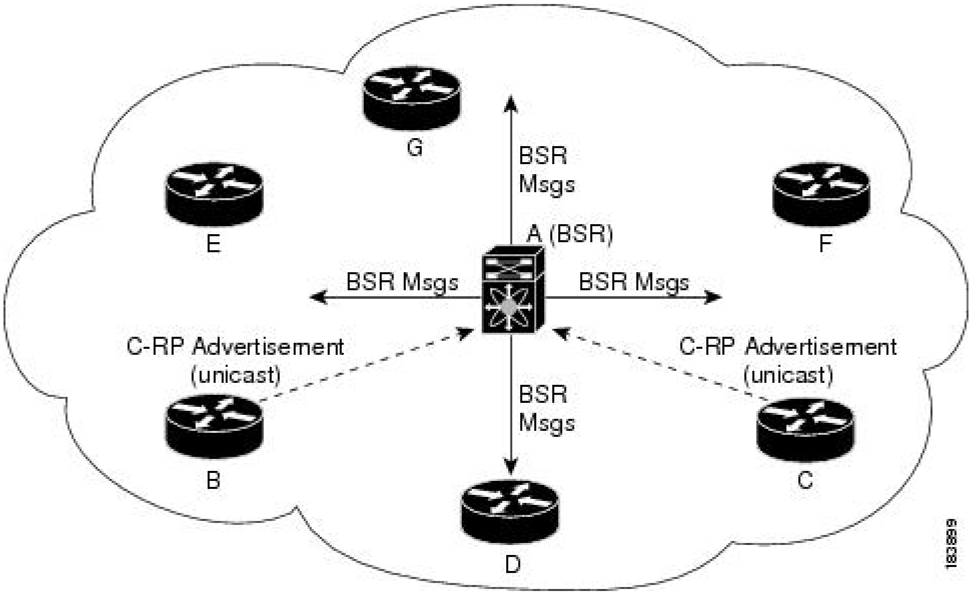
The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs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

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

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

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

Figure 10: BSR Mechanism



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

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

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

Note BSR is not supported for PIM6.

For information about configuring BSRs and candidate RPs, see the Configuring Static RPs (PIM6) section.

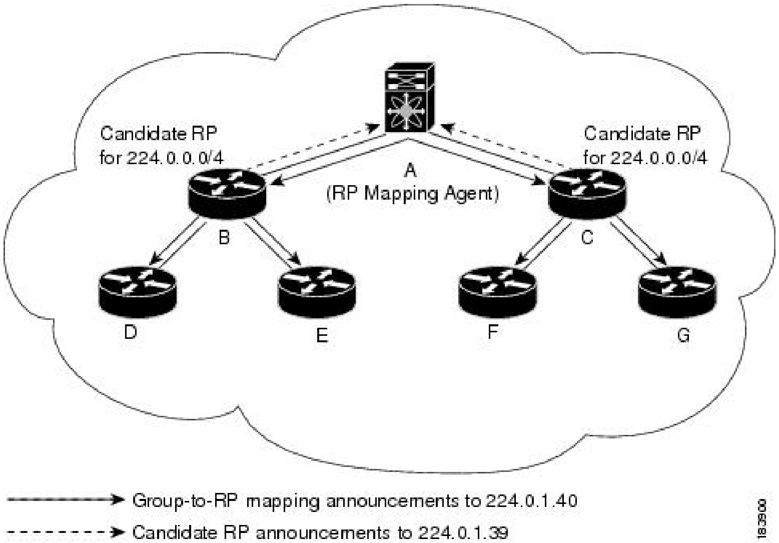
Auto-RP

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

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

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

Figure 11: Auto-RP Mechanism


Candidate RP
for 224.0.0.0/4
A
(RP Mapping Agent)
Candidate RP
for 224.0.0.0/4
B
C
D
E
F
G
Group-to-RP mapping announcements to 224.0.1.40
Candidate RP announcements to 224.0.1.39
183900

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

Note Auto-RP is not supported for PIM6.

For information about configuring Auto-RP, see the Configuring Auto-RP section.

Anycast-RP

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

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

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

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

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

For information about configuring Anycast-RPs, see the Configuring a PIM Anycast RP Set (PIM) section.

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 that are 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.

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 that are sent from the RP to the source address fails 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:

```
switch # configuration terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim register-source ethernet 2/3
switch(config-vrf)#
```

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

You can filter PIM register messages by defining a routing policy. For information about configuring the PIM register message policy, see the Configuring a PIM Anycast RP Set (PIM6) section.

Designated Routers

In PIM ASM and SSM modes, 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 PIM SSM with vPC section.

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.

In SSM mode, the DR triggers (*, G) or (S, G) PIM join messages toward the source. The path from the receiver to the source is determined hop by hop. The source must be known to the receiver or the DR.

For information about configuring the DR priority, see the Configuring PIM or PIM6 Sparse Mode section.

Designated Forwarders

In PIM Bidir mode, the software chooses a designated forwarder (DF) at RP discovery time from the routers on each network segment. The DF is responsible for forwarding multicast data for specified groups on that segment. The DF is elected based on the best metric from the network segment to the RP.

If the router receives a packet on the RPF interface toward the RP, the router forwards the packet out all interfaces in the OIF-list. If a router receives a packet on an interface on which the router is the elected DF for that LAN segment, the packet is forwarded out all interfaces in the OIF-list except the interface that it was received on and also out the RPF interface toward the RP.

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

Administratively Scoped IP Multicast

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

You can configure an interface as a PIM boundary so that PIM messages are not sent out that interface. For information about configuring the domain border parameter, see the Configuring PIM or PIM6 Sparse Mode section.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value. For more information, see the Configuring a PIM Anycast RP Set (PIM6) section.

Virtualization Support

You can define multiple virtual routing and forwarding (VRF) instances. For each VRF, independent multicast system resources are maintained, including the MRIB.

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

For information about configuring VRFs, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.

Prerequisites for PIM and PIM6

PIM and PIM6 have the following prerequisites:

- You are logged on to 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.
- For PIM Bidir, you must configure the ACL TCAM region size using the **hardware access-list tcam region mcast-bidir** command.

  Use the **hardware access-list tcam region ing-sup** command to change the ACL TCAM region size and to configure the size of the ingress supervisor TCAM region.

Note By default the mcast-bidir region size is zero. You need to allocate enough entries to this region in order to support PIM Bidir.

- Make sure that the mask length for Bidir ranges is equal to or greater than 24 bits.

Guidelines and Limitations for PIM and PIM6

PIM and PIM6 have the following guidelines and limitations:

- Configuring a secondary IP address as an RP address is not supported.
- Cisco Nexus 3000 Series switches support PIM SSM mode on vPCs.
- All Cisco Nexus 3000 Series switches support PIM6 ASM and SSM modes.
- The Cisco Nexus 34180YC platform switch does not support PIM6.
- Cisco Nexus 3000 Series switches do not support PIM adjacency with a vPC leg or with a router behind a vPC.
- The PIM process is spawned only when at least one interface is PIM enabled. If no interface is PIM enabled, entering the **show ip pim rp** command sends the following error message: “Process is not running.”
- The loopback interface that is used as a RP in multicast must have the **ip[v6] pim sparse-mode configuration**.
- Cisco NX-OS PIM and PIM6 do not interoperate with any version of PIM dense mode or PIM sparse mode version 1.
- PIM6 is not supported on SVIs and port-channel subinterfaces.
- PIM bidirectional multicast source VLAN bridging is not supported on FEX ports.
- PIM6 Bidirectional is not supported.
- Cisco Nexus 3000 Series switches do not support PIM Bidir on vPCs or PIM6 ASM, SSM, and Bidirectional on vPCs.
- You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM Bidir RP.
- PIM6 does not support BSRs and Auto-RP.

- On Cisco Nexus 3000 Series switches, you must carve the switch RACL TCAM regions in order to make IGMP and PIM work on Layer 3 interfaces. Some system default Multicast ACLs that are installed in the RACL regions are required for IGMP and PIM to work on Layer 3 interfaces.
- Cisco Nexus 3000/3100 vPC secondary does not build the S,G interfaces when there is vPC attached source, vPC attached receiver, PIM-DR is on vPC primary, flow ingresses vPC Primary, and no Remote Peer (RP) is defined for this group.

  The traffic must only need to be interVLAN routed on these vPC peers and the PIM state is not required to be built on any other devices for an RP to not have to be defined.

  For Cisco Nexus 3000 Series devices, this topology cannot be supported because of the hardware limitation. Cisco Nexus 3000 ASIC does not have the capability to detect the RPF fail packets. As a result, the PIM Asserts cannot be generated on VPC when both primary and secondary have the Output Interface List (OIFL) populated. On Cisco Nexus 3000 Series switches, the incoming PIM join on the VPC Switch Virtual Interface (SVI) is ignored.
- Cisco NX-OS 3000 Series switches do not support per **multicast group statistics** command from the **show forward multicast route** command.
- Do not configure both Auto-RP and BSR protocols in the same network.
- Configure candidate RP intervals to a minimum of 15 seconds.
- If a switch is configured with a BSR policy that should prevent it from being elected as the BSR, the switch ignores the policy. This behavior results in the following undesirable conditions:
  - If a switch receives a BSM that is permitted by the policy, the switch, which incorrectly elected itself as the BSR, drops that BSM so that routers downstream fail to receive it. Downstream switches correctly filter the BSM from the incorrect BSR so that they do not receive RP information.
  - A BSM received by a BSR from a different switch sends a new BSM but ensures that downstream switches do not receive the correct BSM.
- You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM Bidir RP.
- PIM is enabled on all interfaces so that it is chosen as the RPF. It is not mandatory to enable the PIM feature for the IGMP host proxy functionality to work.
- In PIM-SM, some duplication or drops of packets are expected behavior when there are changes in the forwarding path. This behavior results in the following undesirable conditions:
  - When switching from receiving on the shared tree to shortest path tree (SPT), there is typically a small window when packets get dropped. The SPT feature may prevent this, but it may cause duplication sometimes.
  - The RP which initially forward packets that it may have received via PIM registers or MSDP will next join the SPT for native forwarding, and there is a small window where the RP may forward the same data packet twice, once as a native packet and once after PIM register or MSDP decap.

  To resolve these issues, ensure that the forwarding path does not change by configuring a long (S,G) expiration time or by using SSM/PIM Bidir.
- PIM must be configured on all L3 interfaces between sources, receivers, and rendezvous points (RPs).

Default Settings

This table lists the default settings for PIM and PIM6 parameters.

Table 7: Default PIM and PIM6 Parameters

Parameters	Default
Use shared trees only	Disabled
Flush routes on restart	Disabled
Log neighbor changes	Disabled
Auto-RP message action	Disabled
BSR message action	Disabled
SSM multicast group range or policy	232.0.0.0/8 for IPv4 and FF3x::/96 for IPv6
PIM sparse mode	Disabled
Designated router priority	0
Hello authentication mode	Disabled
Domain border	Disabled
RP address policy	No message filtering
PIM register message policy	No message filtering
BSR candidate RP policy	No message filtering
BSR policy	No message filtering
Auto-RP mapping agent policy	No message filtering
Auto-RP RP candidate policy	No message filtering
Join-prune policy	No message filtering
Neighbor adjacency policy	Become adjacent with all PIM neighbors

Configuring PIM and PIM6

You can configure both PIM and PIM6 for each interface, depending on whether that interface is running IPv4 or IPv6.

Note Cisco NX-OS supports only PIM Sparse Mode version 2. In this publication, “PIM” refers to PIM Sparse Mode version 2.

You can configure separate ranges of addresses in the PIM or PIM6 domain using the multicast distribution modes that are described in the table below.

Table 8: PIM Multicast Distribution Modes

Multicast Distribution Mode	Requires RP Configuration	Description
ASM	Yes	Any source multicast
Bidir	Yes	Bidirectional shared trees
SSM	No	Single source multicast
RPF routes for multicast	No	RPF routes for multicast

Configuring PIM and PIM6

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.

To configure PIM and PIM6, follow these steps:

Procedure

Step 1 From the multicast distribution modes that are described in Table 3-2, select the range of multicast groups that you want to configure in each mode.

Step 2 Enable the PIM or PIM6 features. See the Enabling the PIM or PIM6 Feature section.

Step 3 Configure PIM Sparse Mode on each interface that you want to participate in a PIM domain. See the Configuring PIM or PIM6 Sparse Mode section.

Step 4 Follow the configuration steps for the multicast distribution modes that you selected in Step 1 as follows:

- For ASM or Bidir mode, see the Configuring ASM and Bidir section.
- For SSM mode, see the Configuring SSM (PIM) section.
- For RPF routes for multicast, see the Configuring RPF Routes for Multicast section.

Step 5 Configure message filtering. See the Configuring Route Maps to Control RP Information Distribution (PIM6) section.

Enabling the PIM or PIM6 Feature

Before you can access the PIM or PIM6 commands, you must enable the PIM or PIM6 feature.

Note Beginning with Cisco NX-OS Release 7.0(3)I5(1), you no longer need to enable at least one interface with IP PIM Sparse Mode in order to enable PIM or PIM6.

Before you begin

Ensure that you have installed the LAN Base Services license.

Procedure

	Command or Action	Purpose

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

Step 2	**feature pim** **Example:** `switch(config)# feature pim`	Enables PIM. By default, PIM is disabled.
Step 3	**feature pim6** **Example:** `switch(config)# feature pim6`	Enables PIM6. By default, PIM6 is disabled.
Step 4	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Shows the running-configuration information for PIM, including the **feature** command.
Step 5	(Optional) **show running-configuration pim6** **Example:** `switch(config)# show running-configuration pim6`	Shows the running-configuration information for PIM6, including the **feature** command.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring PIM or PIM6 Sparse Mode

You configure PIM or PIM6 sparse mode on every switch interface that you want to participate in a sparse mode domain. You can configure the sparse mode parameters that are described in the table below.

Table 9: PIM and PIM6 Sparse Mode Parameters

Parameter	Description
Global to the switch	
Auto-RP message action	Enables listening and forwarding of Auto-RP messages. The default is disabled, which means that the router does not listen or forward Auto-RP messages unless it is configured as a candidate RP or mapping agent. **Note** PIM6 does not support the Auto-RP method.
BSR message action	Enables listening and forwarding of BSR messages. The default is disabled, which means that the router does not listen or forward BSR messages unless it is configured as a candidate RP or BSR candidate. **Note** PIM6 does not support BSR.
Bidirectional RP limit	Configures the number of bidirectional RPs that you can configure for IPv4. The maximum number of bidirectional RPs supported per VRF for PIM cannot exceed 8. Values range from 0 to 8. The default is 6. **Note** PIM6 does not support bidirectional.
Register rate limit	Configures the IPv4 or IPv6 register rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Initial holddown period	Configures the IPv4 or IPv6 initial holddown period in seconds. This holddown period is the time that it takes for the MRIB to come up initially. If you want faster convergence, enter a lower value. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Per switch interface	
PIM sparse mode	Enables PIM or PIM6 on an interface.

Parameter	Description
Designated router priority	Sets the designated router (DR) priority that is advertised in PIM hello messages on this interface. On a multi-access network with multiple PIM-enabled routers, the router with the highest DR priority is elected as the DR router. If the priorities match, the software elects the DR with the highest IP address. The DR originates PIM register messages for the directly connected multicast sources and sends PIM join messages toward the rendezvous point (RP) for directly connected receivers. Values range from 1 to 4294967295. The default is 1.
Hello authentication mode	Enables an MD5 hash authentication key, or password, in PIM hello messages on the interface so that directly connected neighbors can authenticate each other. The PIM hello messages are IPsec encoded using the Authentication Header (AH) option. You can enter an unencrypted (cleartext) key, or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The authentication key can be up to 16 characters. The default is disabled. **Note** PIM6 does not support MD5 authentication.
Hello interval	Configures the interval at which hello messages are sent in milliseconds. The range is from 1 to 4294967295. The default is 30000.
Domain border	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. **Note** PIM6 does not support the Auto-RP method.

Parameter	Description
Neighbor policy	Configures which PIM neighbors to become adjacent to based on a prefix-list policy. To configure prefix-list policies, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide. If the policy name does not exist or no prefix lists are configured in a policy, adjacency is established with all neighbors. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you should configure this feature only if you are an experienced network administrator. **Note** The PIM neighbor policy supports only prefix lists. It does not support ACLs used inside a route map.

For information about configuring multicast route maps, see the Configuring Route Maps to Control RP Information Distribution (PIM) section.

Note To configure the join-prune policy, see the Configuring Route Maps to Control RP Information Distribution (PIM6) section.

Configuring PIM Sparse Mode Parameters

Before you begin

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

Procedure

	Command or Action	Purpose

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

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

Step 3	(Optional) **ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} **Example:**	Enables listening for or forwarding of BSR messages. The default is disabled, which means that the software does not listen for or forward BSR messages.

	Command or Action	Purpose
	`switch(config)# ip pim bsr forward`	
Step 4	(Optional) **ip pim bidir-rp-limit** *limit* **Example:** `switch(config)# ip pim bidir-rp-limit 4`	Specifies the number of Bidir RPs that you can configure for IPv4. The maximum number of Bidir RPs supported per VRF for PIM cannot exceed 8. Values range from 0 to 8. The default value is 6.
Step 5	**ip pim rp** [*ip prefix*] **vrf** *vrf-name*| **all** **Example:** `switch(config)# show ip pim rp`	Displays PIM RP information, including Auto-RP and BSR listen and forward states.
Step 6	(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 7	(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 8	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Displays PIM running-configuration information, including the Bidir RP limit and register rate limit.

Step 9	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the interface type and number, such as **ethernet** *slot/port.*

Step 10	**no switchport** **Example:** `sswitch(config-if)# no switchport`	Configures the interface as a Layer 3 routed interface.
Step 11	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM Sparse Mode on this interface. The default is disabled.
Step 12	(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 13	(Optional) **ip pim hello-authentication ah-md5** *auth-key*	Enables an MD5 hash authentication key in PIM hello messages. You can enter an

	Command or Action	Purpose
	Example: `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	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
Step 14	(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 1 to 4294967295. The default is 30000. **Note** The minimum value is 1 millisecond.
Step 15	(Optional) **ip pim border** **Example:** `switch(config-if)# ip pim border`	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.
Step 16	(Optional) **ip pim neighbor-policy prefix-list** *prefix-list* **Example:** `switch(config-if)# ip pim neighbor-policy prefix-list AllowPrefix`	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. Also configures which PIM neighbors to become adjacent to based on a prefix-list policy with the **ip prefix-list** *prefix-list* command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 17	(Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-if)# show ip pim interface`	Displays PIM interface information.
Step 18	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Configuring PIM6 Sparse Mode Parameters

Before you begin

Ensure that you have installed the LAN Base 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) **ipv6 pim register-rate-limit** *rate* **Example:** `switch(config)# ipv6 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) **ipv6 routing multicast holddown** *holddown-period* **Example:** `switch(config)# ipv6 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 pim6** **Example:** `switch(config)# show running-configuration pim6`	Displays PIM6 running-configuration information, including the register rate limit.

Step 5	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the interface type and number, such as **ethernet** *slot/port.*

Step 6	**ipv6 pim sparse-mode** **Example:** `switch(config-if)# ipv6 pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 7	(Optional) **ipv6 pim dr-priority** *priority* **Example:** `switch(config-if)# ipv6 pim dr-priority 192`	Sets the designated router (DR) priority that is advertised in PIM6 hello messages. Values range from 1 to 4294967295. The default is 1.
Step 8	(Optional) **ipv6 pim hello-interval** *interval* **Example:** `switch(config-if)# ipv6 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.

	Command or Action	Purpose
Step 9	(Optional) **ipv6 pim border** **Example:** `switch(config-if)# ipv6 pim border`	Enables the interface to be on the border of a PIM6 domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.
Step 10	(Optional) **ipv6 pim neighbor-policy prefix-list** *prefix-list* **Example:** `switch(config-if)# ipv6 pim neighbor-policy prefix-list AllowPrefix`	Configures which PIM6 neighbors to become adjacent to based on a prefix-list policy with the **ipv6 prefix-list** *prefix-list* command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM6 neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 11	**show ipv6 pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-if)# show ipv6 pim interface`	Displays PIM6 interface information.
Step 12	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Configuring ASM and Bidir

Any Source Multicast (ASM) and bidirectional shared trees (Bidir) is a multicast distribution mode that requires the use of RPs to act as a shared root between sources and receivers of multicast data.

To configure ASM or Bidir 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 (PIM)

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

You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command.

Note We recommend the following:

- The RP address uses the loopback interface.
- The static route is added toward the source.

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 configuration mode.

Step 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **route-map** *policy-name*] [**bidir**] **Example:** `switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9`	Configures a PIM static RP address for a multicast group range. You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The default mode is ASM unless you specify the bidir keyword. The default group range is 224.0.0.0 through 239.255.255.255. The example configures PIM ASM mode for the specified group range.
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] **Example:** `switch(config)#show ip pim group-range`	Displays PIM modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring Static RPs (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services License and enabled PIM6.

Procedure

	Command or Action	Purpose

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

Step 2	**ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix* | **route-map** *policy-name*] **Example:** `switch(config)#` **`ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/24`**	Configures a PIM6 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. The mode is ASM. The default group range is ff00::0/8. The example configures PIM6 ASM mode for the specified group range.
Step 3	(Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)#` **`show ipv6 pim group-range`**	Displays PIM6 modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)#` **`copy running-config startup-config`**	Saves configuration changes.

Configuring BSRs

You configure BSRs by selecting candidate BSRs and RPs.

Note BSRs and Auto-RP are not supported by PIM6.

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

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

Table 10: Candidate BSR Arguments

Argument	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.

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

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

Table 11: BSR Candidate RP Arguments and Keywords

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

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

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

To configure candidate BSRs and RPs, follow these steps:

1. Configure whether each router in the PIM domain should listen and forward BSR messages. A router configured as either a candidate RP or a candidate BSR will automatically listen to and forward all bootstrap router protocol messages, unless an interface is configured with the domain border feature. For more information, see the Configuring PIM or PIM6 Sparse Mode section.
2. Select the routers to act as candidate BSRs and RPs.
3. Configure each candidate BSR and candidate RP as described in this section.
4. Configure BSR message filtering. See the Configuring Route Maps to Control RP Information Distribution (PIM6) section.

Configuring BSRs (PIM)

Before you begin

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

Procedure

	Command or Action	Purpose

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

Step 2	**ip pim** [**bsr**] **bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*] **Example:** `switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24`	Configures a candidate bootstrap router (BSR). The source IP address used in a bootstrap message is the IP address of the interface. The hash length ranges from 0 to 32 and has a default of 30. The priority ranges from 0 to 255 and has a default of 64. For parameter details, see Table 10.
Step 3	(Optional) **ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* [**bidir**] **Example:** `switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	Configures a candidate RP for BSR. The priority ranges from 0, the highest priority, to 65,535 and has a default of 192. The interval ranges from 1 to 65,535 seconds and has a default of 60. Use the bidir option to create a Bidir candidate RP.

	Command or Action	Purpose
		Note We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.
Step 4	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Auto-RP

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

Note Auto-RP and BSRs are not supported by PIM6.

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

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

Table 12: Auto-RP Mapping Agent Arguments

Argument	Description
interface	Interface type and number used to derive the IP address of the Auto-RP mapping agent used in bootstrap messages.
scope *ttl*	Time-to-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32. **Note** See the border domain feature in the Configuring PIM or PIM6 Sparse Mode section.

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

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

Table 13: Auto-RP Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the IP address of the candidate RP used in bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP. Specified in a prefix format.
scope *ttl*	Time-to-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32. **Note** See the border domain feature in the Configuring PIM or PIM6 Sparse Mode section.
interval	Number of seconds between sending RP-Announce messages. This value can range from 1 to 65,535 and has a default of 60. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
bidir	If not specified, this RP will be in ASM mode. If specified, this RP will be in Bidir mode.

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

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

1. For each router in the PIM domain, configure whether that router should listen and forward Auto-RP messages. A router configured as either a candidate RP or an Auto-RP mapping agent will automatically listen to and forward all Auto-RP protocol messages, unless an interface is configured with the domain border feature. For more information, see the Configuring PIM or PIM6 Sparse Mode section.
2. Select the routers to act as mapping agents and candidate RPs.
3. Configure each mapping agent and candidate RP as described in this section.
4. Configure Auto-RP message filteringConfigure Auto-RP message filtering. See the Configuring Route Maps to Control RP Information Distribution (PIM6) section.

Configuring Auto RP

Before you begin

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

Procedure

	Command or Action	Purpose

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

Step 2	**ip pim** {**send-rp-discovery** | **auto-rp mapping-agent**} *interface* [**scope** *ttl*] **Example:** `switch(config)# ip pim auto-rp mapping-agent ethernet 2/1`	Configures an Auto-RP mapping agent. The source IP address used in Auto-RP Discovery messages is the IP address of the interface. The default scope is 32. For parameter details, see Table 12.
Step 3	**ip pim** {**send-rp-announce** | **auto-rp rp-candidate**} *interface* {**group-list** *ip-prefix* | **prefix-list** *name* | **route-map** *policy-name*} [**scope** *ttl*] **interval** *interval*] **Example:** `switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	Configures an Auto-RP candidate RP. The default scope is 32. The default interval is 60 seconds. By default, the command creates an ASM candidate RP. For parameter details, see Table 13. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.
Step 4	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring Auto RP (PIM)

Before you begin

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

Procedure

	Command or Action	Purpose

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

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

Configuring a PIM Anycast RP Set (PIM)

Before you begin

Ensure that you have installed the LAN Base 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	**interface loopback** *number*
	Example:
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		Configures an interface loopback.
		This example configures interface loopback 0.

Step 3	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 192.168.1.1/32`	Configures an IP address for this interface. This example configures an IP address for the Anycast-RP.
Step 4	**exit** **Example:** `switch(config)# exit`	Returns to configuration mode.
Step 5	**ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address* **Example:** `switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31`	Configures a PIM Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.
Step 6	Repeat Step 5 using the same Anycast-RP address for each peer RP in the Anycast-RP set.	—
Step 7	**ip**[**autoconfig** | *ip-address* [**secondary**]]	Generates a link-local address from the link-local prefix and a modified EUI-64 format Interface Identifier, where the EUI-64 Interface Identifier is created from the relevant HSRP virtual MAC address. Virtual IP address for the virtual router (HSRP group). The IP address must be in the same subnet as the interface IP address. You must configure the virtual IP address for at least one of the routers in the HSRP group. Other routers in the group will pick up this address. The IP address can be an IPv4 address.
Step 8	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.

	Command or Action	Purpose
Step 9	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring a PIM Anycast RP Set (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

Procedure

	Command or Action	Purpose

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

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

Step 3	**ipv6 address** *ipv6-prefix* **Example:** `switch(config-if)# ipv6 address 2001:0db8:0:abcd::5/32`	Configures an IP address for this interface. This example configures an IP address for the Anycast-RP.
Step 4	**ipv6 pim sparse-mode** **Example:** `switch(config-if)# ipv6 pim sparse-mode`	Enable PIM6 sparse mode.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Returns to configuration mode.

Step 6	**ipv6 pim anycast-rp** *anycast-rp-address anycast-rp-peer-address* **Example:** `switch(config)# ipv6 pim anycast-rp 192.0.2.3 192.0.2.31`	Configures a PIM6 Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.

	Command or Action	Purpose
Step 7	Repeat Step 6 using the same Anycast-RP address for each peer RP in the Anycast-RP set	—
Step 8	(Optional) **show ipv6 pim group-range** [*ipv6-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ipv6 pim group-range`	Displays PIM6 modes and group ranges.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring Shared Trees Only for ASM (PIM)

You can configure shared trees only on the last-hop router for Any Source Multicast (ASM) groups, which means that the router never switches over from the shared tree to the SPT when a receiver joins an active group. You can specify a group range where the use of shared trees is to be enforced with the **match ip[v6] multicast** command. This option does not affect the normal operation of the router when a source tree join-prune message is received.

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

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

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 configuration mode.

Step 2	**ip pim use-shared-tree-only group-list** *policy-name* **Example:** `switch(config)# ip pim use-shared-tree-only group-list my_group_policy`	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy name that lists the groups to use with the **match ip multicast** command. By default, the software triggers a PIM (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state.

	Command or Action	Purpose
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Configuring Shared Trees Only for ASM (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

Procedure

	Command or Action	Purpose

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

Step 2	**ipv6 pim use-shared-tree-only group-list** *policy-name* **Example:** `switch(config)# ipv6 pim use-shared-tree-only group-list my_group_policy`	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy name that lists the groups to use with the **match ip multi cast** command. By default, the software triggers a PIM6 (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state.
Step 3	(Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ipv6 pim group-range`	Displays PIM6 modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Setting the Maximum Number of Entries in the Multicast Routing Table

You can set the maximum number of entries in the multicast routing table (MRT)

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

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 configuration mode.

Step 2	**hardware profile multicast max-limit** *max-entries* **Example:** `switch(config)# hardware profile multicast max-limit 3000`	Sets the maximum number of entries in the multicast routing table. The maximum number of entries in the multicast routing table can range from 0 to 8000.
Step 3	(Optional) **show hardware profile status** **Example:** `switch(config)# show hardware profile status`	Displays PIM modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Preventing Duplicate Packets During an RPT to SPT Switchover

Beginning with Cisco NX-OS Release 5.0(3)U1(2), you can prevent duplicate packets in the hardware when the transition from RPT to SPT is in progress.

Note When you use this command to prevent packet duplication during an RPT to SPT switchover, the switch supports source (S, G) route injections at a rate of only 500 routes every two minutes. The multicast routing table must have 500 entries free for source (S, G) routes.

Procedure

	Command or Action	Purpose

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

Step 2	**hardware profile multicast prefer-source-tree eternity limit ?**
	Example:
	`switch(config)# hardware profile multicast prefer-source-tree eternity limit ?`
	`<256-4000> Number of (S,G) for which source tree is preferred`
		Prevents duplicate packets in the hardware when the transition from RPT to SPT is in progress.

Step 3	(Optional) **show hardware profile status** **Example:** `switch(config)# show hardware profile status`	Displays information about the multicast routing table limits.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Configuring SSM (PIM)

Source-Specific Multicast (SSM) is a multicast distribution mode where the software on the DR connected to a receiver that is requesting data for a multicast source builds a shortest path tree (SPT) to that source.

On an IPv4 network, a host can request multicast data for a specific source only if it is running IGMPv3 and the DR for that host is running IGMPv3. You will usually enable IGMPv3 when you configure an interface for PIM in the SSM mode. For hosts running IGMPv1 or IGMPv2, you can configure group to source mapping using SSM translation. For more information, see Configuring IGMP.

You can configure the group range that is used by SSM by specifying values on the command line. By default, the SSM group range for PIM is 232.0.0.0/8.

You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command.

Note If you want to use the default SSM group range, you do not need to configure the SSM group range.

Before you begin

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

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td><b>configure terminal</b>
<b>Example:</b>
<code>switch# configure terminal</code>
<code>switch(config)#</code></td><td>Enters global configuration mode.</td></tr>
<tr><td>Step 2</td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Option</td><td>Description</td></tr>
<tr><td><b>ip pim ssm range</b> {<i>ip-prefix</i> | <b>none</b>} | <b>route-map</b> <i>policy-name</i>}
Example:
<code>switch(config)# <b>ip pim ssm range 239.128.1.0/24</b></code></td><td>Configures up to four group ranges to be treated in SSM mode. You can specify a route-map policy name that lists the group prefixes to use with the <b>match ip multicast</b> command. The default range is 232.0.0.0/8. If the keyword <b>none</b> is specified, all group ranges are removed.</td></tr>
<tr><td><b>no ip pim ssm range</b> {<b>range</b> <i>ip-prefix</i> | <b>none</b>} | <b>route-map</b> <i>policy-name</i>}
Example:
<code>switch(config)# <b>no ip pim ssm range none</b></code></td><td>Removes the specified prefix from the SSM range, or removes the route-map policy. If the keyword <b>none</b> is specified, resets the SSM range to the default of 232.0.0.0/8.</td></tr>
</table>
</td><td></td></tr>
<tr><td>Step 3</td><td>(Optional) <b>show ip pim group-range</b> [<i>ip-prefix</i> | <b>vrf</b> <i>vrf-name</i>]
<b>Example:</b>
<code>switch(config)# <b>show ip pim group-range</b></code></td><td>Displays PIM modes and group ranges.</td></tr>
<tr><td>Step 4</td><td>(Optional) <b>copy running-config startup-config</b>
<b>Example:</b>
<code>switch(config)# <b>copy running-config startup-config</b></code></td><td>Saves configuration changes.</td></tr>
</table>

Configuring SSM (PIM6)

Before you begin

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

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td><b>Step 1</b></td><td><b>configure terminal</b>
<b>Example:</b><pre>switch# configure terminal
switch(config)#</pre></td><td>Enters global configuration mode.</td></tr>
<tr><td><b>Step 2</b></td><td><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Option</td><td>Description</td></tr>
<tr><td><b>ipv6 pim ssm range</b> {<i>ip-prefix</i> | <b>none</b>} | <b>route-map</b> <i>policy-name</i>}
Example:<pre>switch(config)# <b>ipv6 pim ssm range 239.128.1.0/24</b></pre></td><td>The following options are available:<ul><li><b>prefix-list</b>—Specifies a prefix-list policy name for the SSM range.</li><li><b>range</b> —Configures a group range for SSM. The default range is FF3x/96. If the keyword none is specified, all group ranges are removed.</li><li><b>route-map</b> —Specifies a route-map policy name that lists the group prefixes to use with the <b>match ipv6 multicast</b> command.</li></ul></td></tr>
<tr><td><b>no ipv6 pim ssm range</b> {<b>range</b> <i>ipv6-prefix</i> | <b>none</b>} | <b>route-map</b> <i>policy-name</i>}
Example:</td><td>The <b>no</b> option removes the specified prefix from the SSM range or removes the prefix-list or route-map policy. If the keyword <b>none</b> is specified, the <b>no</b> command resets the SSM</td></tr>
</table></td><td></td></tr>
</table>

	Command or Action	Purpose
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>switch(config)# **no ipv6 pim ssm range none**</td><td>range to the default value of FF3x/96.</td></tr></table>	
Step 3	(Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*] **Example:** `switch(config)# show ipv6 pim group-range`	Displays PIM6 modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring PIM SSM Over a vPC

Configuring PIM SSM over a vPC enables support for IGMPv3 joins and PIM S,G joins over vPC peers in the SSM range. This configuration is supported for orphan sources or receivers in the Layer 2 or Layer 3 domain. When you configure PIM SSM over a vPC, no rendezvous point (RP) configuration is required.

(S,G) entries will have the RPF as the interface toward the source, and no *,G states will be maintained in the MRIB.

Before you begin

Ensure that you have the PIM and vPC features enabled.

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 configuration mode.

Step 2	**vrf context** *name*
	Example:
	`switch(config)# vrf context Enterprise`
	`switch(config-vrf)#`
		Creates a new VRF and enters VRF configuration mode. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.

Step 3	(Optional) [**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | **none**} | **route-map** *policy-name*}	The following options are available: • **prefix-list**—Specifies a prefix-list policy name for the SSM range.

	Command or Action	Purpose
	Example: `switch(config-vrf)# ip pim ssm range 234.0.0.0/24`	• **range**—Configures a group range for SSM. The default range is 232.0.0.0/8. If the keyword **none** is specified, all group ranges are removed. • **route-map**—Specifies a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. By default, the SSM range is 232.0.0.0/8. PIM SSM over vPC works as long as S,G joins are received in this range. If you want to override the default with some other range, you must specify that range using this command. The command in the example overrides the default range to 234.0.0.0/24. The *no* option removes the specified prefix from the SSM range or removes the prefix-list or route-map policy. If the keyword none is specified, the **no** command resets the SSM range to the default value of 232.0.0.0/8.
Step 4	(Optional) **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-vrf)# show ip pim group-range`	Displays PIM modes and group ranges.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-vrf)# copy running-config startup-config`	Saves configuration changes.

Configuring RPF Routes for Multicast

You can define 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 reverse path forwarding (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. For more information about multicast forwarding, see the Multicast Forwarding section.

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 configuration mode.

Step 2	**ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* } [*route-preference*] [**vrf** *vrf-name*] **Example:** `switch(config)# ip mroute 192.0.2.33/24 192.0.2.1`	Configures an RPF route for multicast for use in RPF calculations. Route preference values range from 1 to 255. The default preferenceis 1.
Step 3	(Optional) **show ip static-route** [**vrf** *vrf-name*] **Example:** `switch(config)# show ip static-route`	Displays configured static routes.
Step 4	(Optional) **copy running-config startup-config**	Saves configuration changes.

Disabling Multicast Multipath

By default, the RPF interface for multicast is chosen automatically when there are multiple ECMP paths available. Disabling the automatic selection allows you to specify a single RPF interface for multicast.

Procedure

	Command or Action	Purpose

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

Step 2	**ip multicast multipath none** **Example:** `switch(config)# ip multicast multipath none`	Disables multicast multipath. .
Step 3	**clear ip mroute * vrf all**	Clears multipath routes and activates multicast multipath suppression.

Configuring Route Maps to Control RP Information Distribution (PIM)

You can configure route maps to help protect against some RP configuration errors and malicious attacks. You use route maps in commands that are described in the Configuring Route Maps to Control RP Information Distribution (PIM6), on page 70 section.

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

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

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 configuration mode.

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

Step 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*] [**group** *ip-prefix*]} | {**group** *ip-prefix* **rp** *ip-address* [**rp-type** *rp-type*]}
	Example:
	`switch(config)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM`
	`switch(config)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type bidir`
		Matches the group, RP, and RP type specified. You can specify the RP type (ASM or bidir). This configuration method requires the group and RP specified as shown in the examples.

	Command or Action	Purpose
Step 4	(Optional) **show route-map** **Example:** `switch(config-route-map)# show route-map`	Displays configured route maps.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-route-map)# copy running-config startup-config`	Saves configuration changes.

Configuring Route Maps to Control RP Information Distribution (PIM6)

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 configuration mode.

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

Step 3	**match ipv6 multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ipv6-prefix*} | {**group** *ipv6-prefix* **rp** *ip-address* **rp** *rp-type*]}
	Example:
	`switch(config-route-map)# match ipv6 multicast group ff1e:abcd:def1::0/24 rp 2001:0db8:0:abcd::1 rp-type ASM`
		Matches the group, RP, and RP type specified. You can specify the RP type (ASM). This configuration method requires the group and RP specified as shown in the examples.

Step 4	(Optional) **show route-map** **Example:** `switch(config-route-map)# show route-map`	Displays configured route maps.

	Command or Action	Purpose
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-route-map)# copy running-config startup-config`	Saves configuration changes.

Configuring Message Filtering

You can configure filtering of the PIM and PIM6 messages described in the table below.

Table 14: PIM and PIM6 Message Filtering

Message Type	Description
Global to the switch	
Log Neighbor changes	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
PIM register policy	Enables PIM register messages to be filtered based on a route-map policy,where you can specify group or group and source addresses with the **match ip[v6] multicast** command. This policy applies to routers that act as an RP. The default is disabled, which means that the software does not filter PIM register messages.
BSR candidate RP policy	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy, where you can specify the RP and group addresses, and the type ASM or bidir with the **match ip multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages. **Note** PIM6 does not support BSRs.
BSR policy	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy, where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages. **Note** PIM6 does not support BSRs.

Message Type	Description
Auto-RP candidate RP policy	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses, and the type ASM or bidir with the **match ip multicast** command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages. **Note** PIM6 does not support the Auto-RP method.
Auto-RP mapping agent policy	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages. **Note** PIM6 does not support the Auto-RP method.
Per Switch 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**[**v6**] **multicast** command. The default is no filtering of join-prune messages.

For information about configuring multicast route maps, see the Configuring Route Maps to Control RP Information Distribution (PIM) section.

Note For information on about configuring route-map policies, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.

Configuring Message Filtering (PIM)

Before you begin

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

Procedure

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

	Command or Action	Purpose
	switch# **configure terminal** switch(config)#	
Step 2	(Optional) **ip pim log-neighbor-changes** **Example:** switch(config)# ip pim log-neighbor-changes	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
Step 3	(Optional) **ip pim register-policy** *policy-name* **Example:** switch(config)# **ip pim register-policy my_register_policy**	Enables PIM register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ip multicast** command.
Step 4	(Optional) **ip pim bsr rp-candidate-policy** *policy-name* **Example:** switch(config)# **ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy**	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses, and the type ASM or bidir with the *match ip multicast* command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages.
Step 5	(Optional) **ip pim bsr bsr-policy** *policy-name* **Example:** switch(config)# **ip pim bsr bsr-policy my_bsr_policy**	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.
Step 6	(Optional) **ip pim auto-rp rp-candidate-policy** *policy-name* **Example:** switch(config)# **ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy**	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses with the **match ip multicast**command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages.
Step 7	(Optional) **ip pim auto-rp mapping-agent-policy** *policy-name* **Example:** switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages.
Step 8	**interface** *interface* **Example:** switch(config)# **interface ethernet 2/1** switch(config-if)#	Enters interface mode on the specified interface.

	Command or Action	Purpose
Step 9	**no switchport** **Example:** `switch(config-if)# no switchport`	Configures the interface as a Layer 3 routed interface.
Step 10	(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. This command filters messages in both incoming and outgoing directions.
Step 11	(Optional) **show run pim** **Example:** `switch(config-if)# show run pim`	Displays PIM configuration commands.
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

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.

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

	Command or Action	Purpose
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`	Saves configuration changes.

Configuring Message Filtering (PIM6)

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 configuration mode.

Step 2	(Optional) **ipv6 pim log-neighbor-changes** **Example:** `switch(config)# ipv6 pim log-neighbor-changes`	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
Step 3	(Optional) **ipv6 pim register-policy** *policy-name* **Example:** `switch(config)# ipv6 pim register-policy my_register_policy`	Enables PIM6 register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ipv6 multicast** command.

Step 4	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

Step 5	(Optional) **ipv6 pim jp-policy** *policy-name* [**in** | **out**] **Example:** `switch(config-if)# ipv6 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 ipv6 multicast** command. The default is no filtering of join-prune messages.

	Command or Action	Purpose
		This command filters messages in both incoming and outgoing directions.
Step 6	(Optional) **show run pim6** **Example:** `switch(config-if)# show run pim6`	Displays PIM6 configuration commands.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the PIM and PIM6 Configuration

To display the PIM and PIM6 configuration information, perform one of the following tasks.

Command	Description
show ip[**v6**] **mroute**{*source group* | *group* [*source*]}[**vrf** *vrf-name* | **all**	Displays the IP or IPv6 multicast routing table.
show ip[**v6**] **pim group-range** [**vrf** *vrf-name* | **all**]	Displays the learned or configured group ranges and modes. For similar information, see also the show **ip[v6] pim rp** command.
show ip[**v6**] **pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**	Displays information by the interface.
show ip[**v6**] **pim neighbor** [**vrf** *vrf-name* | **all**	Displays neighbors by the interface.
show ip[**v6**] **pim oif-list** *group* [*source*][**vrf** *vrf-name* | **all**	Displays all the interfaces in the OIF-list.
show ip[**v6**] **pim route**{*source group* | **group** [**source**]}[**vrf** *vrf-name* | **all**]	Displays information for each multicast route, including interfaces on which a PIM join for that (S, G) has been received.
show ip[**v6**] **pim rp** [**vrf** *vrf-name* | **all**]	Displays rendezvous points (RPs) known to the software, how they were learned, and their group ranges. For similar information, see also the **show ip[v6] pim group-range** command.
show ip pim rp-hash [**vrf** *vrf-name* | **all**]	Displays the bootstrap router (BSR) RP hash information.
show running-config pim[**6**]	Displays the running-configuration information.
show startup-config pim[**6**]	Displays the startup-configuration information.
show ip[**v6**] **pim vrf** *vrf-name* | **all** [**detail**]	Displays per-VRF information.

For detailed information about the fields in the output from these commands, see the Cisco Nexus 3000 Series Command Reference.

Configuring Multicast Table Size

The multicast entries use the host table in the hardware. The host table is shared between the multicast and the unicast routes. Each multicast entry consists of the source and the group and it takes two entries in the hardware table. Each IPv4 unicast entry takes one entry in the hardware table. Each IPv6 unicast route entry takes two entries in the hardware table.

The hardware table size is 16384. As per the default configuration on Cisco Nexus 3000 Series switches, you can configure 4096 multicast entries and 8192 unicast entries. For unicast entries, you can configure up to 8192 IPv4 or 4096 IPv6 entries in the host table.

As per multicast table size controller feature, you can control the sharing of the hardware host table across the multicast and the unicast routes.

If you do not use multicast entries into your network, you can set the multicast entry limit to 0 and you can use all 16K entries for the unicast entries.

If you are going to use more than 4k multicast entries into your network and fewer unicast entries, you can increase the multicast limit size up to 8000.

Configuring the Multicast Entries Using the CLI

Configure the multicast entries in your network using the CLI command:

```
(config)# hardware profile multicast max-limit ?
<0-8000> Mcast Table Entries

(config)# hardware profile multicast max-limit 6000
Warning!!: The multicast and host (v4 & v6) unicast route limits have been changed.
Any route exceeding the limit may get dropped.
Please reload the switch now for the change to take effect.
(config)#
```

Displaying the Multicast Entries

Display the multicast entries in your network using the CLI command:

```
# sh hardware profile status

slot 1
=======

Total Host Entries = 16384.
Reserved LPM Entries = 1024.
Max Host4/Host6 Limit Entries (shared)= 4384/2192* --> Since we increased multicast entries
 this limit reduced.
Max Mcast Limit Entries = 6000.
```

Configuring the Unicast Entries Using the CLI

Configure the unicast entries in your network using the CLI command:

```
(config)# hardware profile ucast6 max-limit 1000
Warning!!: The host (v4 & v6) unicast route limits have been changed.
Any route exceeding the limit may get dropped.
(config)#
```

Displaying the Unicast Entries

Display the unicast entries in your network using the CLI command:

```
# sh hardware profile status

slot 1
=======
Total Host Entries = 16384.
Reserved LPM Entries = 1024.
Max Host Limit Entries = 2384.
Max Host6 Limit Entries = 1000.
Max Mcast Limit Entries = 6000.
```

Displaying Statistics

You can display and clear PIM and PIM6 statistics by using the commands in this section.

Displaying PIM and PIM6 Statistics

You can display the PIM and PIM6 statistics and memory usage using the commands listed in Table 3-9 . Use the **show ip** form of the command for PIM.

Command	Description
show ip[**v6**] **pim policy statistics**	Displays policy statistics for Register, RP, and join-prune message policies.

For detailed information about the fields in the output from these commands, see the Cisco Nexus 3000 Series Command Reference.

Clearing PIM Statistics

You can clear the PIM and PIM6 statistics using the commands listed in Table. Use the **show ip** form of the command for PIM and the **show ipv6** form of the command for PIM6.

Table 15: PIM Commands to Clear Statistics

Command	Description
clear ip[**v6**] **pim interface statistics** *interface*	Clears counters for the specified interface.
clear ip[**v6**] **pim policy statistics**	Clears policy counters for Register, RP, and join-prune message policies.
clear ip[**v6**] **pim statistics** [**vrf***vrf-name* | **all**]	Clears global counters handled by the PIM process.

Configuration Examples for PIM

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

SSM Examples for Configuration

To configure PIM in SSM mode, follow these steps for each router in the PIM domain:

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

   ```
   switch# configure terminal
   switch(config)# interface ethernet 2/1
   switch(config-if)# no switchport
   switch(config-if)# ip pim sparse-mode
   ```

2. Configure the parameters for IGMP that support SSM. See Configuring IGMP. Usually, you configure IGMPv3 on PIM interfaces to support SSM.

   ```
   switch# configure terminal
   switch(config)# interface ethernet 2/1
   switch(config-if)# no switchport
   switch(config-if)# ip igmp version 3
   ```

3. Configure the SSM range if you do not want to use the default range.

   ```
   switch# configure terminal
   switch(config)# ip pim ssm range 239.128.1.0/24
   ```

4. Configure message filtering.

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

The following example shows how to configure PIM SSM mode:

```
configure terminal
interface ethernet 2/1
no switchport
ip pim sparse-mode
ip igmp version 3
exit
ip pim ssm range 239.128.1.0/24
ip pim log-neighbor-changes
```

Configuration Example for PIM SSM Over vPC

This example shows how to override the default SSM range of 232.0.0.0/8 to 225.1.1.1/32. PIM SSM over vPC will work as long as S,G joins are received in this range.

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim ssm range 225.1.1.1/32
switch(config-vrf)# show ip pim group-range --> Shows the configured SSM group range. Note:
The SSM range is changed to 225.1.1.1/24 in the output.
```

```
PIM Group-Range Configuration for VRF "Enterprise"
Group-range Mode RP-address Shared-tree-only range
225.1.1.1/24 SSM - -

switch1# show vpc (primary vPC) --> Shows vPC-related information. Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id: 10
Peer status: peer adjacency formed ok
vPC keep-alive status: peer is alive
Configuration consistency status: success
Per-vlan consistency status: success
Type-2 consistency status: success
vPC role: primary
Number of vPCs configured: 2
Peer Gateway: Disabled
Dual-active excluded VLANs: -
Graceful Consistency Check: Enabled
Auto-recovery status: Disabled
Delay-restore status: Timer is off.(timeout = 30s)
Delay-restore SVI status: Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po1000 up 101-102

vPC status
----------------------------------------------------------------------
id Port Status Consistency Reason Active vlans
-- ---- ------ ----------- ------ ------------
1 Po1 up success success 102
2 Po2 up success success 101

switch2# show vpc (secondary vPC)
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id: 10
Peer status: peer adjacency formed ok
vPC keep-alive status: peer is alive
Configuration consistency status: success
Per-vlan consistency status: success
Type-2 consistency status: success
vPC role: primary
Number of vPCs configured: 2
Peer Gateway: Disabled
Dual-active excluded VLANs: -
Graceful Consistency Check: Enabled
Auto-recovery status: Disabled
Delay-restore status: Timer is off.(timeout = 30s)
Delay-restore SVI status: Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po1000 up 101-102
vPC status
----------------------------------------------------------------------
id Port Status Consistency Reason Active vlans
-- ---- ------ ----------- ------ ------------
1 Po1 up success success 102
2 Po2 up success success 101
```

```
switch1# show ip igmp snooping group vlan 101 (primary vPC IGMP snooping states) --> Shows
 if S,G v3 joins are received and on which VLAN. The same VLAN should be OIF in the MRIB
output.
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port
Vlan Group Address
101 */*
101 225.1.1.1
100.6.160.20
Ver Type Port list
- R Po1000 Vlan101
v3
D Po2
switch2# show ip igmp snooping group vlan 101 (secondary vPC IGMP snooping states) Type: S
 - Static, D - Dynamic, R - Router port, F - Fabricpath core port
Vlan Group Address
101 */*
101 225.1.1.1
100.6.160.20
Ver Type Port list
- R Po1000 Vlan101
v3
D Po2
switch1# show ip pim route (primary vPC PIM route) --> Shows the route information in the
PIM protocol.
PIM Routing Table for VRF "default" - 3 entries
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:37
Incoming interface: Ethernet1/19, RPF nbr 10.6.159.20
Oif-list: (1) 00000000, timeout-list: (0) 00000000
Immediate-list: (1) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holdtime round-up: 3
(100.6.160.20/32, 225.1.1.1/32), expires 00:01:19
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holdtime round-up: 3
(*, 232.0.0.0/8), expires 00:01:19
Incoming interface: Null0, RPF nbr 0.0.0.0
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holdtime round-up: 3
switch2# show ip pim route (secondary vPC PIM route) PIM Routing Table for VRF "default" -
 3 entries (10.6.159.20/32, 225.1.1.1/32), expires 00:02:51
Incoming interface: Vlan102, RPF nbr 100.6.160.100
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3
(100.6.160.20/32, 225.1.1.1/32), expires 00:02:51
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000

PIM SSM Over vPC Configuration Example
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3
(*, 232.0.0.0/8), expires 00:02:51
Incoming interface: Null0, RPF nbr 0.0.0.0
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3
```

```
switch2# show ip pim route (secondary vPC PIM route) PIM Routing Table for VRF "default" -
 3 entries
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:29
Incoming interface: Vlan102, RPF nbr 100.6.160.100
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3
(100.6.160.20/32, 225.1.1.1/32), expires 00:02:29
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3
(*, 232.0.0.0/8), expires 00:02:29
Incoming interface: Null0, RPF nbr 0.0.0.0
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3

switch1# show ip mroute (primary vPC MRIB route) --> Shows the IP multicast routing table.
IP Multicast Routing Table for VRF "default"
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:16:40, pim ip
Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
Outgoing interface list: (count: 1)
Vlan102, uptime: 03:16:40, pim
(100.6.160.20/32, 225.1.1.1/32), uptime: 03:48:57, igmp ip pim
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 03:48:57, igmp
(*, 232.0.0.0/8), uptime: 6d06h, pim ip
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

switch1# show ip mroute detail (primary vPC MRIB route) --> Shows if the (S,G) entries have
 the RPF as the interface toward the source and no *,G states are maintained for the SSM
group range in the MRIB.
IP Multicast Routing Table for VRF "default"
Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:24:28, pim(1) ip(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
Outgoing interface list: (count: 1)
Vlan102, uptime: 03:24:28, pim
(100.6.160.20/32, 225.1.1.1/32), uptime: 03:56:45, igmp(1) ip(0) pim(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 03:56:45, igmp (vpc-svi)
(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000 bps
```

```
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

switch2# show ip mroute detail (secondary vPC MRIB route) IP Multicast Routing Table for
VRF "default"
Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:26:24, igmp(1) pim(0) ip(0)
Data Created: Yes
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.100
Outgoing interface list: (count: 1)
Ethernet1/17, uptime: 03:26:24, igmp
(100.6.160.20/32, 225.1.1.1/32), uptime: 04:06:32, igmp(1) ip(0) pim(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 04:03:24, igmp (vpc-svi)
(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)
```

Configuration Example for BSR

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

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

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

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

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

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

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

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

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

5. Configure message filtering.

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

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

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

Configuration Example for PIM Anycast-RP

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

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

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

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

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

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

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

4. Configure the RP-address which will be used as Anycast-RP on all routers.

```
switch# configure terminal
switch(config)# ip pim rp-address 192.0.2.3
```

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

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

6. Configure message filtering.

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

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

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

Auto-RP Configuration Example

To configure PIM in Bidir mode using the Auto-RP mechanism, follow these steps for each router in the PIM domain:

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

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

2. Configure whether that router should listen and forward Auto-RP messages.

   ```
   switch# configure terminal
   switch(config)# ip pim auto-rp forward listen
   ```

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

   ```
   switch# configure terminal
   switch(config)# ip pim auto-rp mapping-agent ethernet 2/1
   ```

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

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

5. Configure message filtering.

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

This example shows how to configure PIM Bidir mode using the Auto-RP mechanism and how to configure the mapping agent and RP on the same router:

```
configure terminal
  interface ethernet 2/1
    ip pim sparse-mode
    exit
  ip pim auto-rp listen
  ip pim auto-rp forward
  ip pim auto-rp mapping-agent ethernet 2/1
  ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir
  ip pim log-neighbor-changes
```

Where to Go Next

You can configure the following features that work with PIM:

- Configuring IGMP
- Configuring IGMP Snooping
- Configuring MSDP

Additional References

For additional information related to implementing PIM, see the following sections:

- Related Documents
- Standards
- MIBs
- IETF RFCs for IP Multicast
- Feature History for PIM and PIM6

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3000 Series Command Reference
Configuring VRFs	Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature	

MIBs

MIBs	MIBs Link
IPMCAST-MIB	To locate and download MIBs, go to the following: MIB Locator.

Feature History for PIM and PIM6

Table below lists the release history for this feature.

Table 16: Feature History for PIM

Feature Name	Releases	Feature Information
PIM6	7.0(3)I6(1)	This feature was introduced.
Disabling Multicast Multipath	5.0(3)U4(1)	This feature was introduced.
PIM Register Messages	5.0(3)U4(1)	This feature was introduced.
PIM	5.0(3)U1(1)	This feature was introduced.

CHAPTER 5

Configuring IGMP Snooping

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

This chapter includes the following sections:

- About IGMP Snooping, on page 89
- Prerequisites for IGMP Snooping, on page 91
- Default Settings, on page 92
- Configuring IGMP Snooping Parameters, on page 92
- Verifying the IGMP Snooping Configuration, on page 98
- Setting Interval for Multicast Routes, on page 99
- Displaying IGMP Snooping Statistics, on page 99
- Configuration Examples for IGMP Snooping, on page 100
- Where to Go Next, on page 100
- Additional References, on page 100
- Feature History for IGMP Snooping, on page 101

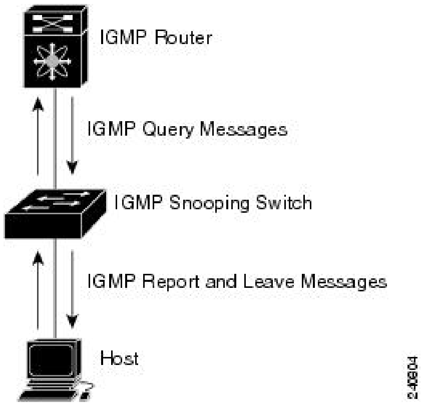
About IGMP Snooping

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 switch.

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 switch.

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

Figure 12: IGMP Snooping Switch



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

For more information about IGMP, see Configuring IGMP.

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

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

For more information about IGMP snooping, see RFC 4541.

IGMPv1 and IGMPv2

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

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

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

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

IGMPv3

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

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

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

IGMP Snooping Querier

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

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.

IGMP Filtering on Router Ports

IGMP filtering allows users to configure a router port on the switch that leads the switch to a Layer 3 multicast switch. The switch stores all manually configured static router ports in its router port list.

When an IGMP packet is received, the switch forwards the traffic through the router port in the VLAN. The switch recognizes a port as a router port through the PIM hello message or the IGMP query received by the switch.

IGMP Snooping with VRFs

You can define multiple virtual routing and forwarding (VRF) instances. An IGMP process supports all VRFs.

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

For information about configuring VRFs, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged onto the switch.
- 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.

Default Settings

Table 17: Default IGMP Snooping Parameters

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
IGMPv3 report suppression for the entire device	Disabled
IGMPv3 report suppression per VLAN	Enabled

Configuring IGMP Snooping Parameters

To affect the operation of the IGMP snooping process, you can configure the optional IGMP snooping parameters described in Table below.

Table 18: IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping on the switch or on a per-VLAN basis. The default is enabled. **Note** If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.
Explicit tracking	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled.
Fast leave	Enables the software to remove the group state when it receives an IGMP Leave report without sending an IGMP query message. This parameter is used for IGMPv2 hosts when no more than one host is present on each VLAN port. The default is disabled.

Parameter	Description
Last member query interval	Sets the interval that the software waits after sending an IGMP query to verify that no hosts that want to receive a particular multicast group remain on a network segment. If no hosts respond before the last member query interval expires, the software removes the group from the associated VLAN port. Values range from 1 to 25 seconds. The default is 1 second.
Proxy leave messages	Changes the destination address of proxy leave messages to the address of the group that is leaving. Normally, IGMP proxy leave messages generated by the IGMP snooping module use the 224.0.0.2 multicast router address when all hosts leave the group. You should implement this configuration if your multicast applications rely on receiving reports and leave messages to start or stop multicast traffic based on the destination address of the packet.
Floods report and leaves	Floods IGMP reports on all active interfaces of the VLAN or only on specific interfaces and leaves. IGMP reports typically are forwarded to multicast router ports as detected by the IGMP snooping module and are not flooded in the VLAN. However, this command forces the switch to send IGMP reports to custom ports belonging to the VLAN in addition to the multicast router ports. You should implement this configuration if your multicast applications require the ability to view IGMP reports in order to transmit traffic.
Snooping querier	Configures a snooping querier on an interface when you do not enable PIM because multicast traffic does not need to be routed.
Report suppression	Limits the membership report traffic sent to multicast-capable routers on the switch or on a per-VLAN basis. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.
Multicast router	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN.
Static group	Configures a Layer 2 port of a VLAN as a static member of a multicast group.
Link-local groups suppression	Configures link-local groups suppression on the switch or on a per-VLAN basis. The default is enabled.

Parameter	Description
IGMPv3 report suppression	Configures IGMPv3 report suppression and proxy reporting on the switch or on a per-VLAN basis. The default is disabled for the entire switch and enabled per VLAN.

Configuring IGMP Snooping Parameters

You can disable IGMP snooping either globally or for a specific VLAN. You cannot disable IGMP snooping on a PIM enabled SVIs. The warning message displayed is:IGMP snooping cannot be disabled on a PIM enabled SVIs. There are one or more vlans with PIM enabled.

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td><b>Step 1</b></td><td><b>configure terminal</b>
<b>Example:</b>
switch# <b>configure terminal</b>
switch(config)#</td><td>Enters configuration mode.</td></tr>
<tr><td><b>Step 2</b></td><td><b>ip igmp snooping</b>
<b>Example:</b>
switch(config)# <b>ip igmp snooping</b></td><td>Enables IGMP snooping. The default is enabled.
<b>Note</b> If the global setting is disabled with the <b>no</b> form of this command, then 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.</td></tr>
<tr><td><b>Step 3</b></td><td><b>vlan</b> <i>vlan-id</i>
<b>Example:</b>
switch(config)# <b>vlan 2</b>
switch(config-vlan)#</td><td>Enters configuration mode.</td></tr>
<tr><td><b>Step 4</b></td><td colspan="2">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Option</td><td>Description</td></tr>
<tr><td><b>ip igmp snooping</b>
Example:
switch(config-vlan-config)# <b>ip igmp snooping</b></td><td>Enables IGMP snooping for the current VLAN. The default is enabled.</td></tr>
<tr><td><b>ip igmp snooping explicit-tracking</b>
Example:</td><td>Tracks IGMPv3 membership reports from individual hosts</td></tr>
</table>
</td></tr>
</table>

Command or Action	Purpose
Option	**Description**
`switch(config-vlan)# **ip igmp snooping explicit-tracking**`	for each port on a per-VLAN basis. The default is enabled on all VLANs.
ip igmp snooping fast-leave Example: `switch(config-vlan)# **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 last-member-query-interval *seconds* Example: `switch(config-vlan)# **ip igmp snooping last-member-query-interval 3**`	Removes the group from the associated VLAN port if no hosts respond to an IGMP query message before the last member query interval expires. Values range from 1 to 25 seconds. The default is 1 second.
[**no**] **ip igmp snooping proxy-leave use-group-address** Example: `switch(config-vlan-config)# **ip igmp snooping proxy-leave use-group-address**`	Changes the destination address of proxy leave messages to the address of the group that is leaving. Normally, IGMP proxy leave messages generated by the IGMP snooping module use the 224.0.0.2 multicast router address when all hosts leave the group. You should implement this configuration if your

Option	Description
	multicast applications rely on receiving reports and leave messages to start or stop multicast traffic based on the destination address of the packet.
[**no**] **ip igmp snooping report-flood**{**all** | **interface ethernet** *slot/port*} Example: `switch(config-vlan-config)# `**`ip igmp snooping report-flood interface ethernet 1/2 ip igmp snooping report-flood interface ethernet 1/3`**	Floods IGMP reports on all active interfaces of the VLAN or only on specific interfaces and leaves. IGMP reports typically are forwarded to multicast router ports as detected by the IGMP snooping module and are not flooded in the VLAN. However, this command forces the switch to send IGMP reports to custom ports belonging to the VLAN in addition to the multicast router ports. You should implement this configuration if your multicast applications require the ability to view IGMP reports in order to transmit traffic.
ip igmp snooping querier *ip-address* Example: `switch(config-vlan)# `**`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 report-suppression	Limits the membership report

	Command or Action	Purpose

Option	Description
Example: `switch(config-vlan)# ip igmp snooping report-suppression`	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. **Note** This command can also be entered in global configuration mode to affect all interfaces.
ip igmp snooping mrouter interface *interface* Example: `switch(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1`	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as **ethernet** *slot/port.*
ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface* Example: `switch(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1`	Configures a 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 Example:	Configures link-local groups suppression. The default is enabled.

	Command or Action	Purpose

Option	Description
switch(config-vlan)# **ip igmp snooping link-local-groups-suppression**	**Note** This command can also be entered in global configuration mode to affect all interfaces
ip igmp snooping v3-report-suppression Example: switch(config-vlan)# **ip igmp snooping v3-report-suppress**	Configures IGMPv3 report suppression and proxy reporting. The default is disabled for the global command for the entire switch and enabled per VLAN. **Note** This command can also be entered in global configuration mode to affect all interfaces.

	Command or Action	Purpose
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config)# **copy running-config startup-config**	Saves configuration changes.

Verifying the IGMP Snooping Configuration

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

Command	Purpose
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.

Command	Purpose
show ip igmp snooping mroute [**vlan** *vlan-id*]	Displays multicast router ports by VLAN.
show ip igmp snooping explicit-tracking [**vlan** *vlan-id*]	Displays IGMP snooping explicit tracking information by VLAN.

For detailed information about the fields in the output from these commands, see the Cisco Nexus 3000 Series Command Reference.

Setting Interval for Multicast Routes

When the Cisco Nexus 3000 Series switch has high multicast route creation or deletion rates (for example, too many IGMP join or leave requests), the switch cannot program the multicast routes into the hardware as fast as the requests are made. To resolve this problem, you can now configure an interval after which multicast routes are programmed into the hardware.

When you have very low multicast route creations or deletions per second, configure a low interval (up to 50 milliseconds). A low interval enables the hardware to be programmed faster than it would be by using the default interval of 1 second.

When you have very high multicast route creations or deletions per second, configure a high interval (up to 2 seconds). A high interval enables the hardware to be programmed over a longer period of time without dropping the requests.

Displaying IGMP Snooping Statistics

Use the **show ip igmp snooping statistics vlan** command to display IGMP snooping statistics.

Use the **clear ip igmp snooping statistics vlan** command to clear IGMP snooping statistics.

Note Starting with Release 7.0(3)I2(1), the output of the CLI command **clear ip igmp snooping** displays extra options, for example, access-group, groups, proxy, and report-policy.

See the following example:

```
switch(config)# clear ip igmp snooping ?
*** No matching command found in current mode, matching in (exec) mode ***
access-group IGMP access-group
event-history Clear event history buffers
explicit-tracking Clear Explicit Host tracking information
groups Clear snooped groups
proxy Clear IGMP snooping proxy
report-policy IGMP Report Policy
statistics Packet/internal counter statistics
```

For detailed information about using these commands, see the Cisco Nexus 3000 Series Command Reference.

Configuration Examples for IGMP Snooping

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

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

Where to Go Next

You can enable the following features that work with PIM:

- Configuring IGMP
- Configuring MSDP

Additional References

For additional information related to implementing IGMP snooping, see the following sections:

- Related Documents
- Standards
- Feature History for IGMP Snooping

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3000 Series Command Reference.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IGMP Snooping

Following table lists the release history for this feature.

Table 19: Feature History for IGMP Snooping

Feature Name	Releases	Feature Information
IGMP Snooping	5.0(3)U1(1)	This feature was introduced.

CHAPTER 6

Configuring MSDP

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

This chapter includes the following sections:

- About MSDP, on page 103
- Prerequisites for MSDP, on page 105
- Default Settings, on page 106
- Configuring MSDP, on page 106
- Verifying the MSDP Configuration, on page 114
- Displaying Statistics, on page 114
- Configuration Examples for MSDP, on page 115
- Additional References, on page 117
- Feature History for IGMP, on page 117

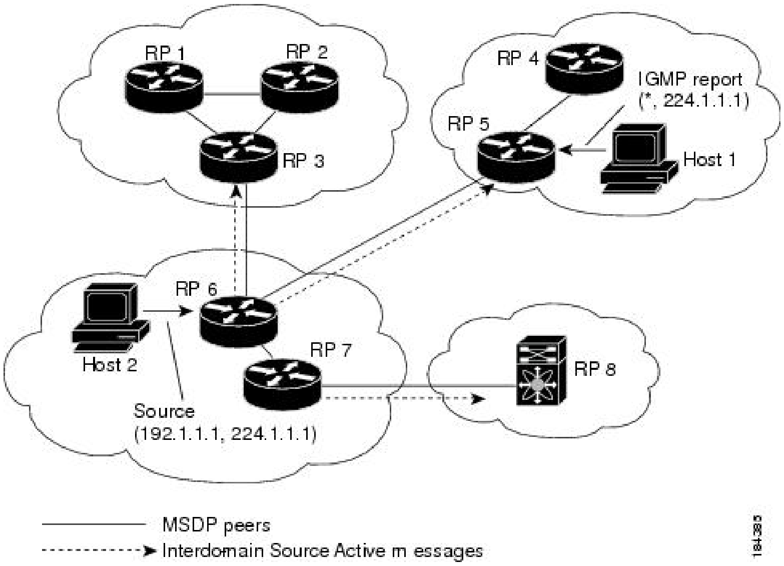
About MSDP

You can use MSDP to exchange multicast source information between multiple BGP-enabled Protocol Independent Multicast (PIM) sparse-mode domains. For information about PIM, see Configuring PIM and PIM6. For information about BGP, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.

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

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

Figure 13: MSDP Peering Between RPs in Different PIM Domains



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

Note You do not need to configure MSDP in order to use Anycast-RP (a set of RPs that can perform load balancing and failover) within a PIM domain. For more information, see the Configuring a PIM Anycast RP Set (PIM) section.

For detailed information about MSDP, see RFC 3618.

SA Messages and Caching

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

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

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

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

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

MSDP Peer-RPF Forwarding

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

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

MSDP Mesh Groups

You can use MSDP mesh groups to reduce the number of SA messages that are generated by peer-RPF flooding. In Figure 5-1, RPs 1, 2, and 3 receive SA messages from RP 6. By configuring a peering relationship between all the routers in a mesh and then configuring a mesh group of these routers, the SA messages that originate at a peer are sent by that peer to all other peers. SA messages received by peers in the mesh are not forwarded. An SA message that originates at RP 3 is forwarded to RP 1 and RP 2, but these RPs do not forward those messages to other RPs in the mesh.

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

Virtualization Support

ou can define multiple virtual routing and forwarding (VRF) instances. The MSDP configuration applies to the selected VRF.

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

For information about configuring VRFs, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.

Prerequisites for MSDP

MSDP has the following prerequisites:

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

Default Settings

This table lists the default settings for MSDP parameters.

Table 20: Default MSDP Parameters

Parameters	Default
Description	Peer has no description
Administrative shutdown	Peer is enabled when it is defined
MD5 password	No MD5 password is enabled
SA policy IN	All SA messages are received
SA policy OUT	All registered sources are sent in SA messages
SA limit	No limit is defined
Originator interface name	RP address of the local system
Group limit	No group limit is defined
SA interval	60 seconds

Configuring MSDP

You can establish MSDP peering by configuring the MSDP peers within each PIM domain.

To configure MSDP peering, follow these steps:

1. Select the routers to act as MSDP peers.
2. Enable the MSDP feature. See the Enabling the MSDP Feature section.
3. Configure the MSDP peers for each router identified in Step 1. See the Configuring MSDP Peers section.
4. Configure the optional MSDP peer parameters for each MSDP peer. See the Configuring MSDP Peer Parameters section.
5. Configure the optional global parameters for each MSDP peer. See the Configuring MSDP Global Parameters section.
6. Configure the optional mesh groups for each MSDP peer. See the Configuring MSDP Mesh Groups section.

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

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

Enabling the MSDP Feature

Procedure

	Command or Action	Purpose

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

Step 2	**feature msdp** **Example:** `switch# feature msdp`	Enables the MSDP feature so that you can enter MSDP commands. By default, the MSDP feature is disabled.
Step 3	(Optional) **show running-configuration | grep** *feature* **Example:** `switch# show running-configuration | grep feature`	Shows **feature** commands that you specified.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring MSDP Peers

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

Before you begin

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

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

Procedure

	Command or Action	Purpose

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

Step 2	**ip msdp peer** *peer-ip-address* **connect-source** *interface* [**remote-as** *as-number*] **Example:** `switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 2/1 remote-as 8`	Configures an MSDP peer with the specified peer IP address. The software uses the source IP address of the interface for the TCP connection with the peer. The interface can take the form of *type slot/port* . If the AS number is the same as the local AS, then the peer is within the PIM domain; otherwise, this peer is external to the PIM domain. By default, MSDP peering is disabled. **Note** MSDP peering is enabled when you use this command.
Step 3		Repeat Step 2 for each MSDP peering relationship by changing the peer IP address, the interface, and the AS number as appropriate. —
Step 4	(Optional) **show ip msdp summary** [**vrf** *vrf-name* | **all**] **Example:** `switch# show ip msdp summary`	Displays a summary of MDSP peers.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring MSDP Peer Parameters

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

Table 21: MSDP Peer Parameters

Parameter	Description
Description	Description string for the peer. By default, the peer has no description.

Parameter	Description
Administrative shutdown	Method to shut down the MSDP peer. The configuration settings are not affected by this command. You can use this parameter to allow configuration of multiple parameters to occur before making the peer active. The TCP connection with other peers is terminated by the shutdown. By default, a peer is enabled when it is defined.
MD5 password	MD5-shared password key used for authenticating the peer. By default, no MD5 password is enabled.
SA policy IN	Route-map policy for incoming SA messages. By default, all SA messages are received. **Note** To configure route-map policies, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.
SA policy OUT	Route-map policy for outgoing SA messages. By default, all registered sources are sent in SA messages. **Note** To configure route-map policies, see the Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.
SA limit	Number of (S, G) entries accepted from the peer and stored in the SA cache. By default, there is no limit.

For information about configuring multicast route maps, see the Configuring Route Maps to Control RP Information Distribution (PIM) section.

Note For information about configuring mesh groups, see the Configuring MSDP Mesh Groups section.

Before you begin

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

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
Step 2	**ip msdp description** *peer-ip-address description* **Example:** `switch(config)# ip msdp description 192.168.1.10 peer in Engineering network`	Sets a description string for the peer. By default, the peer has no description.
Step 3	**ip msdp shutdown** *peer-ip-address* **Example:** `switch(config)# ip msdp shutdown 192.168.1.10`	Shuts down the peer. By default, the peer is enabled when it is defined.
Step 4	**ip msdp password** *peer-ip-address password* **Example:** `switch(config)# ip msdp password 192.168.1.10 my_md5_password`	Enables an MD5 password for the peer. By default, no MD5 password is enabled.
Step 5	**ip msdp sa-policy** *peer-ip-address policy-name* **in** **Example:** `switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in`	Enables a route-map policy for incoming SA messages. By default, all SA messages are received.
Step 6	**ip msdp sa-policy** *peer-ip-address policy-name* **out** **Example:** `switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out`	Enables a route-map policy for outgoing SA messages. By default, all registered sources are sent in SA messages.
Step 7	**ip msdp sa-limit** *peer-ip-address limit* **Example:** `switch(config)# ip msdp sa-limit 192.168.1.10 5000`	Sets a limit on the number of (S, G) entries accepted from the peer. By default, there is no limit.
Step 8	(Optional) **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | *known-vrf-name* | **all**] **Example:** `switch# show ip msdp peer 1.1.1.1`	Displays detailed MDSP peer information.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring MSDP Global Parameters

You can configure the optional MSDP global parameters described in Table below:

Table 22: MSDP Global Parameters

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

Before you begin

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

Procedure

	Command or Action	Purpose

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

Step 2	**ip msdp originator-id** *interface* **Example:** `switch(config)# ip msdp originator-id loopback0`	Sets a description string for the peer. By default, the peer has no description. Sets the IP address used in the RP field of an SA message entry. By default, the software uses the RP address of the local system. **Note** We recommend that you use a loopback interface for the RP address.
Step 3	**ip msdp group-limit** *limit* **source** *source-prefix* **Example:** `switch(config)# ip msdp group-limit 1000 source 192.168.1.0/24`	Maximum number of (S, G) entries that the software creates for the specified prefix. The software ignores groups when the group limit is exceeded and logs a violation. By default, no group limit is defined.

	Command or Action	Purpose
Step 4	**ip msdp sa-interval** *seconds* **Example:** `switch(config)# ip msdp sa-interval 80`	Interval at which the software transmits Source-Active (SA) messages. The range is from 60 to 65,535 seconds. The default is 60 seconds.
Step 5	(Optional) **show ip msdp summary** [**vrf** *vrf-name* | **all**] **Example:** `switch(config)# show ip msdp summary`	Displays a summary of the MDSP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring MSDP Mesh Groups

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

Before you begin

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

Procedure

	Command or Action	Purpose

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

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

	Command or Action	Purpose
	`switch# show ip msdp mesh-group`	
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Restarting the MSDP Process

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

Before you begin

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

Procedure

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

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

Step 3	**ip msdp flush-routes** **Example:** `switch(config)# ip msdp flush-routes`	Removes routes when the MSDP process is restarted. By default, routes are not flushed.
Step 4	(Optional) **show running-configuration | include flush-routes** **Example:** `switch(config)# show running-configuration | include flush-routes`	Shows flush-routes configuration lines in the running configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Verifying the MSDP Configuration

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

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

For detailed information about the fields in the output from these commands, see the Cisco Nexus 3000 Series Command Reference.

Displaying Statistics

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

Displaying Statistics

You can display MSDP statistics using the commands listed in Table below.

Table 23: MSDP Statistics Commands

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

Clearing Statistics

You can clear the MSDP statistics using the commands listed in Table below

Table 24: Clear Statistics Commands

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

Configuration Examples for MSDP

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

1. Configure the MSDP peering relationship with other routers.

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

2. Configure the optional peer parameters.

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

3. Configure the optional global parameters.

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

4. Configure the peers in each mesh group.

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

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

RP 3: 192.168.3.10 (AS 7)

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

RP 5: 192.168.5.10 (AS 8)

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

RP 6: 192.168.6.10 (AS 9)

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

This example shows how to display information about IGMP snooping information on a switch that runs Cisco NX-OS Release 5.0(3)U2(1) and shows the status of multicast optimization on a virtual Port Channel (vPC):

```
switch# show ip igmp snooping
Global IGMP Snooping Information:
IGMP Snooping enabled
Optimised Multicast Flood (OMF) disabled
IGMPv1/v2 Report Suppression enabled
IGMPv3 Report Suppression disabled
Link Local Groups Suppression enabled
VPC Multicast optimization disabled
IGMP Snooping information for vlan 1
IGMP snooping enabled
Optimised Multicast Flood (OMF) disabled
IGMP querier present, address: 10.1.1.7, version: 2, interface Ethernet1/13
Switch-querier disabled
IGMPv3 Explicit tracking enabled
IGMPv2 Fast leave disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression disabled
Link Local Groups suppression enabled
Router port detection using PIM Hellos, IGMP Queries
Number of router-ports: 1
Number of groups: 0
Active ports:
Eth1/11 Eth1/13
switch#
```

Additional References

For additional information related to implementing MSDP, see the following sections:

- Related Documents
- Standards
- IETF RFCs for IP Multicast

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3000 Series Command Reference.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	-

Feature History for IGMP

Table below lists the release history for this feature.

Table 25: Feature History for MSDP

Feature Name	Releases	Feature Information
MSDP	5.0(3)U1(1)	This feature was introduced.

CHAPTER 7

Configuring Multicast VRF-Lite Route Leaking

This chapter describes how to configure Multicast VRF-Lite Route leaking on Cisco NX-OS switches.

This chapter includes the following sections:

- About Multicast VRF-Lite Route Leaking, on page 119
- Guidelines and Limitations for VRF-Lite Route Leaking, on page 119
- Configuring Multicast VRF-Lite Route Leaking, on page 120
- Verifying the Multicast VRF-Lite Route Leaking Configuration, on page 120
- Configuration Examples for Multicast VRF-Lite Route Leaking, on page 121
- Related Documents, on page 121
- Standards, on page 121
- Feature History for Multicast VRF-Lite Route Leaking, on page 122

About Multicast VRF-Lite Route Leaking

Beginning with Cisco NX-OS Release 7.0(3)I7(1), multicast receivers can forward IPv4 traffic across VRFs. In the previous releases, multicast traffic could flow within the same VRF.

With multicast VRF-lit route leaking, Reverse Path Forwarding (RPF) lookup for multicast routes in the receiver VRF can be performed in the source VRF. Therefore, traffic originating from the source VRF can be forwarded to the receiver VRF.

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

To support RPF selection in a different VRF, use the **ip multicast rpf select vrf** command.

Guidelines and Limitations for VRF-Lite Route Leaking

VRF-Lite Route Leaking has the following guidelines and limitations:

- VRF-Lite Route Leaking is not supported on the Cisco Nexus 34180YC platform switch.

Configuring Multicast VRF-Lite Route Leaking

Beginning with Cisco NX-OS Release 7.0(3)I7(1), you can configure multicast VRF-lite route leaking, which allows IPv4 multicast traffic across VRFs.

Before you begin

Ensure that you have installed the Enterprises Services license and enable the PIM or PIM6 feature.

Procedure

	Command or Action	Purpose

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

Step 2	**ip multicast rpf select vrf src-vrf-name group-list** **Example:** `sswitch(config)# ip multicast rpf select vrf red group-list 224.1.1.0/24`	Specifies which VRF to use for RPF lookup for a particular multicast group. To disable the support, use the **no** form of this command. *src-vrf-name* is the source VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive. *group-list* is the group range for the RPF select. The format is A.B.C.D/LEN with a maximum length of 32.
Step 3	(Optional) **show ip mroute** **Example:** `switch(config)# show ip mroute`	Shows the running-configuration information for IPv4 multicast routes.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Verifying the Multicast VRF-Lite Route Leaking Configuration

To display the multicast extranet configuration information, perform the following task:

Command	Purpose
show ip mroute	Displays the running-configuration information for IPv4 multicast routes.

Configuration Examples for Multicast VRF-Lite Route Leaking

This example shows how to display information about running-configuration for IPv4 multicast routes:

```
switch(config)# show ip mroute
IP Multicast Routing Table for VRF "default"


(*, 225.1.1.207/32), uptime: 00:13:33, ip pim

Incoming interface: Vlan147, RPF nbr: 147.147.147.2, uptime: 00:13:33

Outgoing interface list: (count: 0)


Extranet receiver in vrf blue:

(*, 225.1.1.207/32) OIF count: 1


(40.1.1.2/32, 225.1.1.207/32), uptime: 00:00:06, mrib ip pim

Incoming interface: Vlan147, RPF nbr: 147.147.147.2, uptime: 00:00:06

Outgoing interface list: (count: 0)


Extranet receiver in vrf blue:

(40.1.1.2/32, 225.1.1.207/32) OIF count: 1


switch(config)#
```

For detailed information about the fields in the output from these commands, see the Cisco Nexus 3000 Series Command Reference.

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3000 Series Command Reference.

Standards

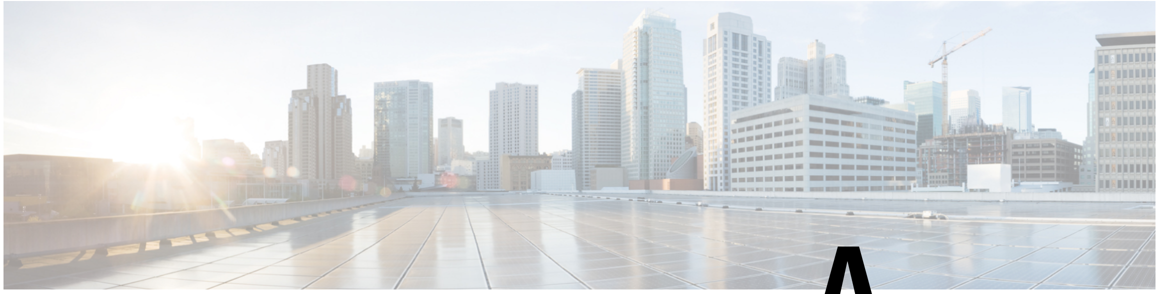
Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	-

Feature History for Multicast VRF-Lite Route Leaking

Table below lists the release history for this feature.

Table 26: Feature History for Multicast Extranet

Feature Name	Releases	Feature Information
Multicast VRF-lite route leaking	7.0(3)I7(1)	This feature was introduced.



APPENDIX A

IETF RFCs for IP Multicast

This appendix contains Internet Engineering Task Force (IETF) RFCs related to IP multicast. For information about IETF RFCs, see http://www.ietf.org/rfc.html.

- IETF RFCs for IP Multicast, on page 123

IETF RFCs for IP Multicast

RFCs	Title
RFC 2236	*Internet Group Management Protocol, Version 2*
RFC 2365	*Administratively Scoped IP Multicast*
RFC 2858	*Multiprotocol Extensions for BGP-4*
RFC 3376	*Internet Group Management Protocol, Version 3*
RFC 3446	*Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
RFC 3569	*An Overview of Source-Specific Multicast (SSM)*
RFC 3618	*Multicast Source Discovery Protocol (MSDP)*
RFC 4541	*Considerations for Internet Group Management Protocol (IGMP) Snooping Switches*
RFC 4601	*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*
RFC 4610	*Anycast-RP Using Protocol Independent Multicast (PIM)*
RFC 5132	*IP Multicast MIB*