Cisco Nexus 3548 Switch NX-OS Multicast Routing Configuration Guide, Release 10.3(x)

First Published: 2022-08-19

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

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 products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface ix

Audience ix

Document Conventions ix

Documentation Feedback x

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview 3

Licensing Requirements 3

Supported Platforms 3

Information About Multicast 3

Consistency Checker Commands for Cisco Nexus 3500 Series Switch 4

Multicast Distribution Trees 5

Source Trees 5

Shared Trees 6

Multicast Forwarding 7

Cisco NX-OS PIM 8

ASM 10

SSM 10

RPF Routes for Multicast 10

IGMP 10

IGMP Snooping 10

Interdomain Multicast 11

SSM 11

MSDP 11

MRIB 11
Troubleshooting Inconsistency Between SW and HW Multicast Routes 12
Additional References 13
Related Documents 13
Technical Assistance 13

CHAPTER 3 **Configuring IGMP 15**
Information About IGMP 15
IGMP Versions 15
IGMP Basics 16
Virtualization Support 18
Limitations 18
IGMP with VRFs 18
Default Settings for IGMP 19
Configuring IGMP Parameters 19
Configuring IGMP Interface Parameters 20
Configuring an IGMP SSM Translation 26
Configuring the Enforce Router Alert Option Check 27
Configuring IGMP Host Proxy 28
Overview of the feature 28
IGMP Join Process 28
IGMP Leave Process 28
IGMP Multicast Addresses 28
Guidelines and Limitations 29
How to Configure IGMP Host Proxy 29
Verifying the IGMP Configuration 30
Configuration Examples for IGMP 30
Where to Go Next 31

CHAPTER 4 **Configuring PIM 33**
Information about PIM 33
Hello Messages 34
Join-Prune Messages 35
State Refreshes 36

Rendezvous Points 36
Static RP 36
BSRs 36
Auto-RP 37
Anycast-RP 38
PIM Register Messages 39
Designated Routers 39
Administratively Scoped IP Multicast 40
Virtualization Support 40
Information about PIM-Bidir 40
PIM-Bidir 40
Bidirectional Shared Tree 40
DF Election 42
Bidirectional Group Tree Building 42
Packet Forwarding 43
Guidelines and Limitations for PIM 43
Guidelines and Limitations for PIM-Bidir 44
Default Settings for PIM 44
Configuring PIM 45
Enabling the PIM Feature 46
Configuring PIM Sparse Mode 46
Configuring ASM or Bidir 49
Configuring Static RPs (PIM) 49
Configuring BSRs 50
Configuring Auto-RP 52
Configuring a PIM Anycast RP Set (PIM) 55
Configuring Shared Trees Only for ASM (PIM) 56
Configuring SSM (PIM) 57
Configuring RPF Routes for Multicast 58
Configuring Route Maps to Control RP Information Distribution (PIM) 59
Configuring Message Filtering 60
Configuring Message Filtering 61
Flushing the Routes 63
Verifying the PIM Configuration 63

Displaying Statistics 64
Displaying PIM Statistics 64
Clearing PIM Statistics 65
Configuration Examples for PIM 65
Configuration Example for SSM 65
Configuration Example for BSR 66
Configuration Example for PIM Anycast-RP 66
Configuration Example for PIM-Bidir Using BSR 67
Configuring Multicast Service Reflection 68
Guidelines and Limitations for Multicast Service Reflection 68
Configuring Multicast Service Reflection Feature 69
Configuring the Multicast Service Reflect Loopback Port 69
Configuring the Multicast Service Reflect Mode 70
Configuring the Multicast Service Reflect Rule 71
Configuring the Regular Mode 72
Configuring the Fast-pass Mode 73
Viewing the Show Commands for the Regular Mode 75
Checking the Rate of the Stream 75
Checking the Multicast Route 75
Viewing the Multicast route 76
Viewing the Show Commands for the Fast-pass Mode 76
Checking the Rate of the Stream 77
Checking the Multicast Route 77
Viewing the Multicast route 77
Where to Go Next 78
Additional References 78
Related Documents 78
Standards 78
MIBs 79

CHAPTER 5 **Configuring IGMP Snooping 81**
Information About IGMP Snooping 81
IGMPv1 and IGMPv2 82
IGMPv3 83

IGMP Snooping Querier 83
IGMP Snooping Filter 83
Guidelines and Limitations for IGMP Snooping 83
Prerequisites for IGMP Snooping 84
Default Settings for IGMP Snooping 84
Configuring IGMP Snooping 85
Configuring IGMP Snooping Parameters 88
Verifying the IGMP Snooping Configuration 93
Displaying IGMP Snooping Statistics 94
Clearing IGMP Snooping Statistics 94
Configuration Examples for IGMP Snooping 94
Additional References 95
Related Documents 95
Standards 96

CHAPTER 6 **Configuring MSDP 97**
Information About MSDP 97
SA Messages and Caching 98
MSDP Peer-RPF Forwarding 99
MSDP Mesh Groups 99
Virtualization Support 99
Prerequisites for MSDP 99
Default Settings for MSDP 100
Configuring MSDP 100
Enabling the MSDP Feature 101
Configuring MSDP Peers 101
Configuring MSDP Peer Parameters 103
Configuring MSDP Global Parameters 105
Remote Multicast Source Support 107
Configuring MSDP Mesh Groups 107
Restarting the MSDP Process 108
Verifying the MSDP Configuration 109
Displaying Statistics 110
Displaying Statistics 110

Clearing Statistics 110
Configuration Examples for MSDP 111
Additional References 112
Related Documents 113
Standards 113

CHAPTER 7 **Configuring Multicast Extranet** 115
Information About Multicast Extranet 115
Guidelines and Limitations for Multicast Extranet 115
Configuring Multicast Extranet 116
Verifying the Multicast Extranet Configuration 116
Related Documents 117
Standards 117

APPENDIX A **IETF RFCs for IP Multicast** 119
IETF RFCs for IP Multicast 119

Preface

The preface contains the following sections:

- Audience, on page ix
- Document Conventions, on page ix
- Documentation Feedback, on page x

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

Document Conventions

Note As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.

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.

Convention	Description
[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.
`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.

This document uses the following conventions:

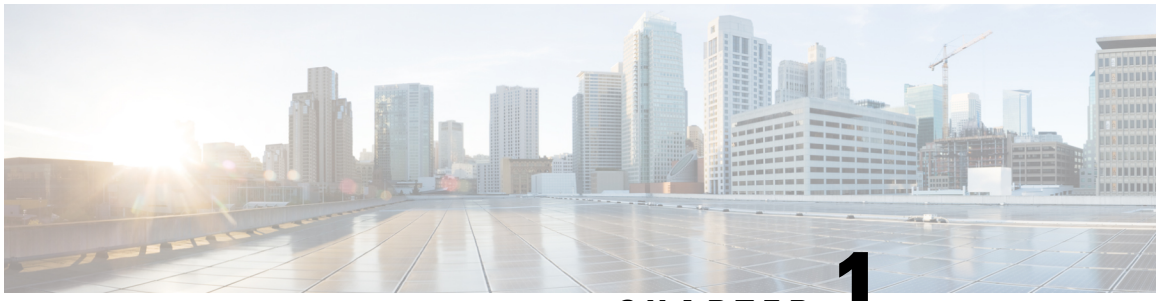
Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to: .

We appreciate your feedback.



CHAPTER 1

New and Changed Information

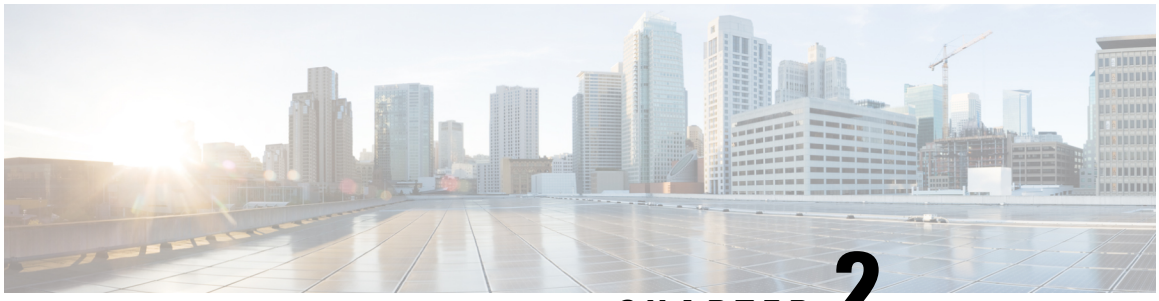
• New and Changed Information, on page 1

New and Changed Information

Table 1: New and Changed Features for Cisco NX-OS Release 10.3(x)

Feature	Description	Changed in Release	Where Documented
NA	No new features added for this release.	10.3(1)F	NA

New and Changed Information



CHAPTER 2

Overview

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

This chapter includes the following sections:

- Licensing Requirements, on page 3
- Supported Platforms, on page 3
- Information About Multicast, on page 3
- Troubleshooting Inconsistency Between SW and HW Multicast Routes , on page 12
- Additional References, on page 13
- Related Documents, on page 13
- Technical Assistance, on page 13

Licensing Requirements

See the Cisco NX-OS Licensing Guide and Cisco NX-OS Licensing Options Guide for Cisco NX-OS licensing recommendations and instructions to obtain and apply licenses.

Supported Platforms

See the Nexus Switch Platform Support Matrix to know from which Cisco NX-OS releases various Cisco Nexus 9000 and 3000 switches support a selected feature.

Information 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.

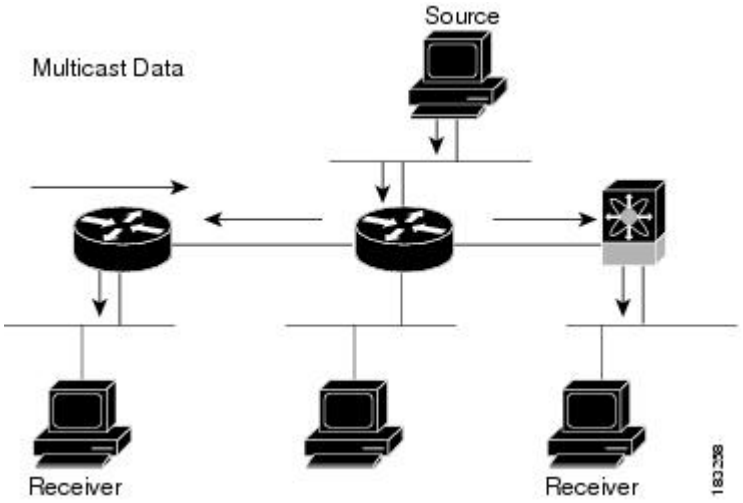
Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel. The Internet Assigned Number Authority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

Figure 1 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



Consistency Checker Commands for Cisco Nexus 3500 Series Switch

Consistency checker compares the software state of the network system, with the hardware state of supported modules. This helps to reduce increased troubleshooting time at a later period. Consistency checker supplements basic troubleshooting, and helps to identify scenarios where inconsistent state between software and hardware tables are causing issues in the network, thereby reducing the mean time to resolve the issue.

The following consistency checker commands are supported for Layer 2 from Cisco NX-OS Release 9.3(3):

- show consistency-checker membership vlan <vlanid> [native-vlan] —Determines that the VLAN membership in the software is the same as programmed in the hardware.
- show consistency-checker membership port-channels [interface <ch-id>]—Checks for port-channel membership in the hardware in all modules and validates it with the software state.
- show consistency-checker stp-state vlan <vlan>—Determines whether the spanning tree state in the software is the same as programmed in the hardware. This command is run only on interfaces that are operational (up).
- show consistency-checker l2 module <modnum>—Verifies that learned MAC addresses are consistent between the software and the hardware. It also shows extra entries that are present in the hardware but not in the software and missing entries in the hardware.

- show consistency-checker link-state module <moduleID>—Verifies the programming consistency between software and hardware for the link-state status of the interfaces.

The following consistency checker commands are supported for Layer 3 from Cisco NX-OS Release 9.3(3):

- show consistency-checker l3-interface module <moduleid>—Verifies the programming consistency between software and hardware for L3-interface ingress and egress forwarding tables.
- test forwarding ipv4 [unicast] inconsistency [suppress_transient] [vrf vrf-name] [stop] —Starts or stops a Layer 3 consistency check.
- show forwarding ipv4 [unicast] inconsistency [vrf vrf-name] —Displays the results of a Layer 3 consistency check.
- show consistency-checker forwarding single-route ipv4 <ip-prefix> vrf <vrf-name>—Displays the results of consistency check for a single route.
- clear forwarding [ipv4 | ip] [unicast] inconsistency—Clears the IP forwarding inconsistencies.
- show consistency-checker gwmacdb —Displays the results of consistency check for Router MAC.

The following consistency checker commands are supported for Multicast from Cisco NX-OS Release 9.3(3):

- show consistency-checker l2 multicast group <grp-address> source <src-address> vlan <vlan-id> [dump-debug-logs]—Verifies the Layer 2 multicast consistency for L2 IGMP entries between the software and the hardware.
- show consistency-checker l3 multicast group <grp-address> source <src-address> vrf <vrf-string> [dump-debug-logs]—Verifies the Layer 3 multicast consistency for L3 multicast route entries between the software and the hardware.

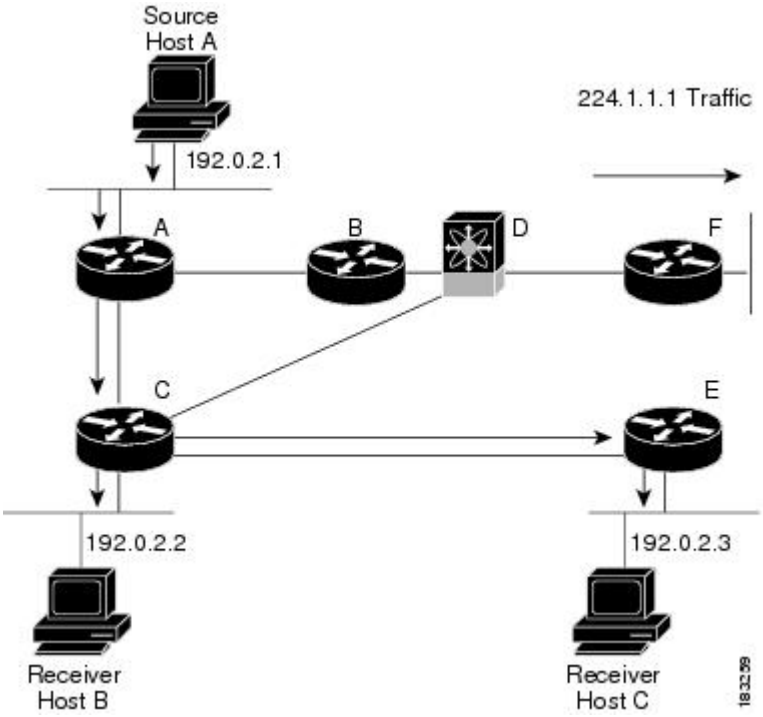
Multicast Distribution Trees

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). Figure 2 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

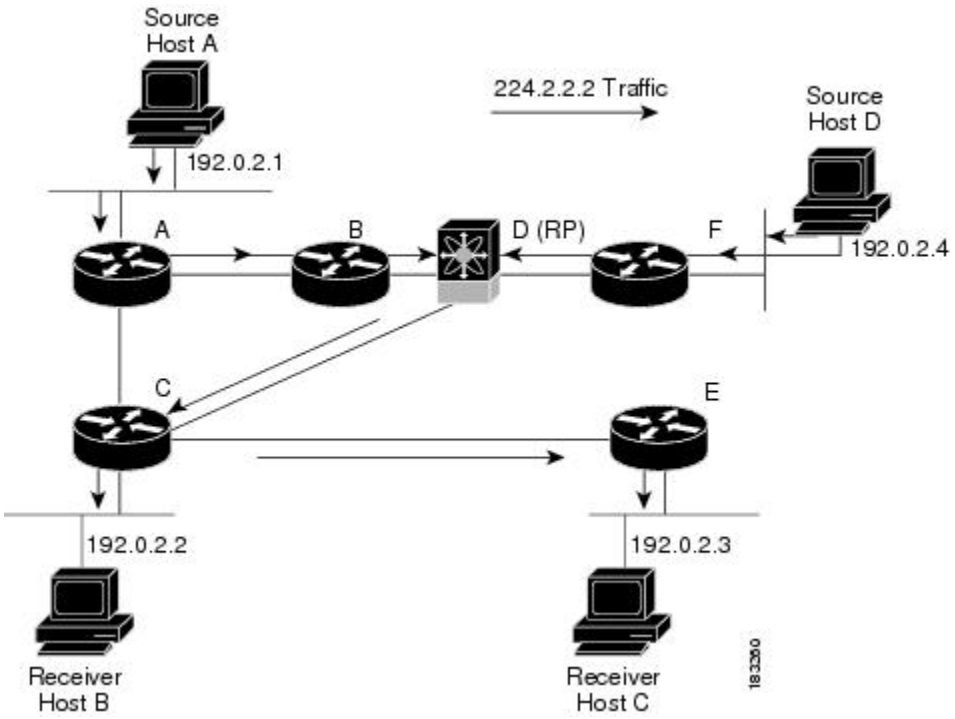


The notation (S, G) represents the multicast traffic from source S on group G. The SPT in Figure 2 is written (192.1.1.1, 224.1.1.1). Multiple sources can be transmitting on the same group.

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). Figure 3 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 3 is written (*, 224.2.2.2).

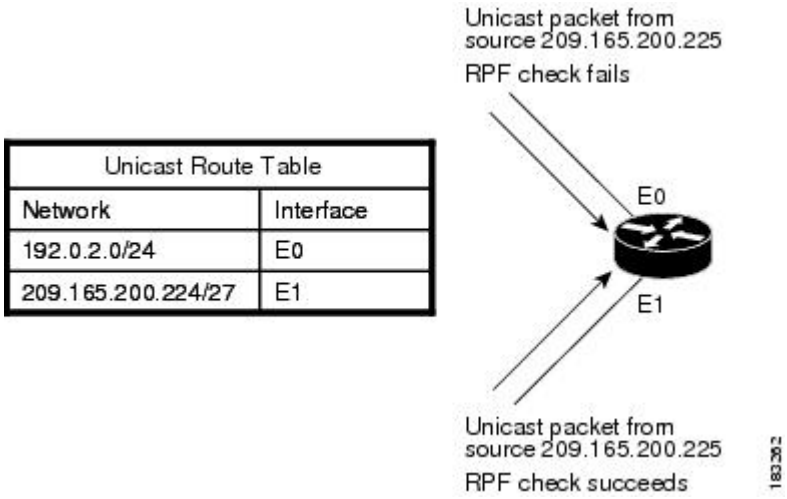
Multicast Forwarding

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.

Figure 4 shows an example of RPF checks on packets coming in from different interfaces. The packet that arrives on E0 fails the RPF check because the unicast route table lists the source of the network on interface E1. The packet that arrives on E1 passes the RPF check because the unicast route table lists the source of that network on interface E1.

Figure 4: RPF Check Example



Cisco NX-OS PIM

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

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

To access multicast commands, you must enable the PIM feature. Multicast is enabled only after you enable PIM on an interface of each router in a domain. You 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.

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 shows two PIM domains in an IPv4 network.

Figure 5: PIM Domains in an IPv4 Network

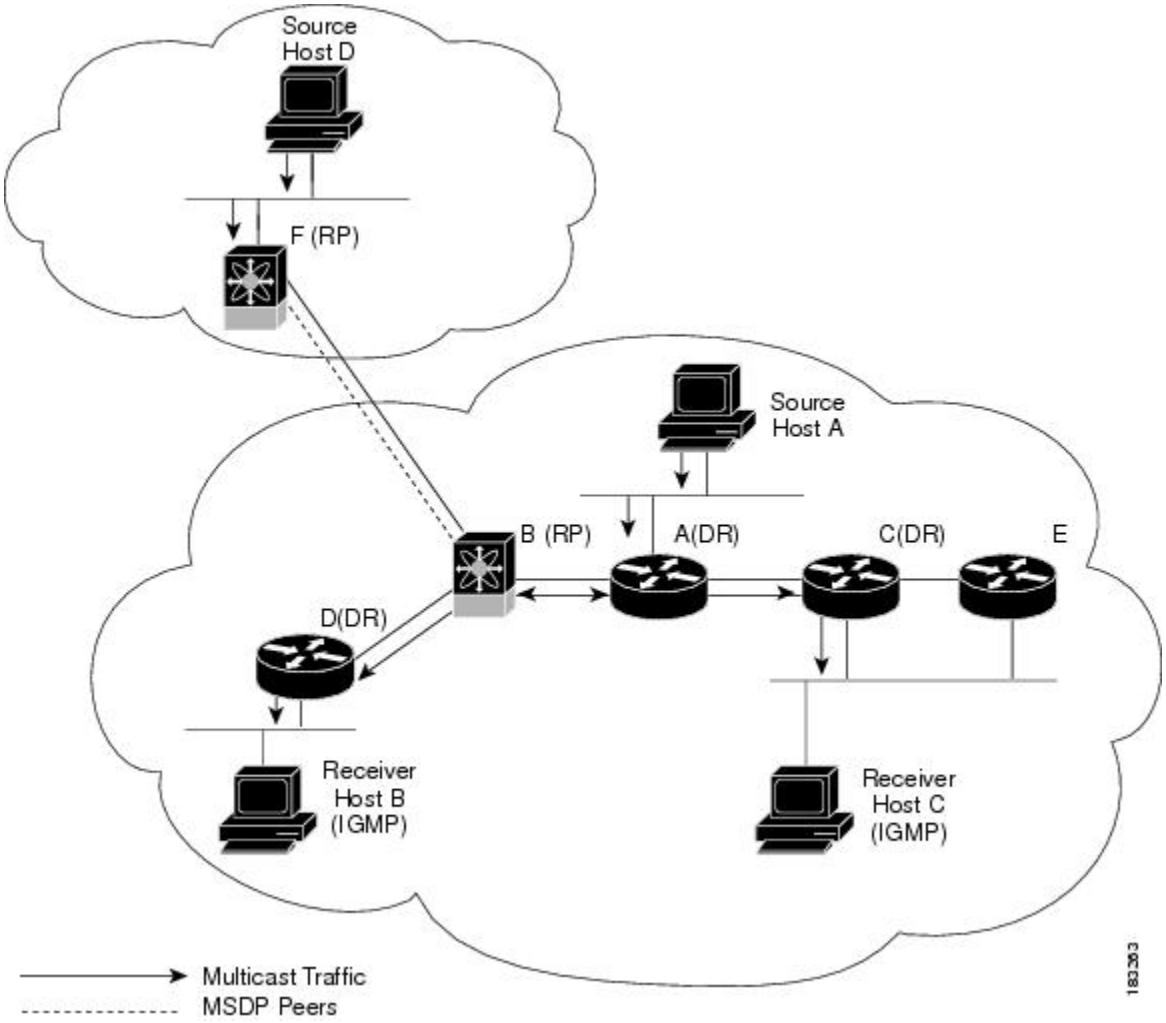


Figure 5 shows the following elements of PIM:

- 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 two 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 or 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 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, on page 15 .

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, on page 81.

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 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 section.

For information about MSDP, see Configuring MSDP.

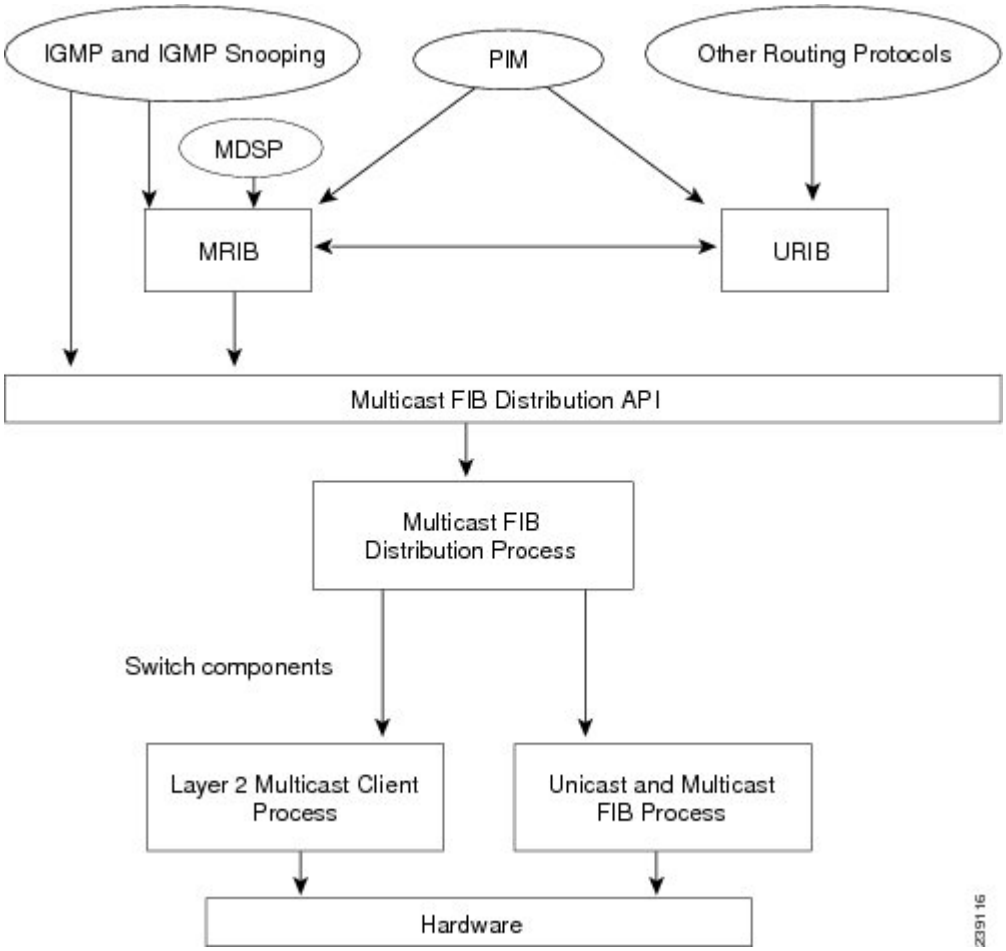
MRIB

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.

Figure 6 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



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:

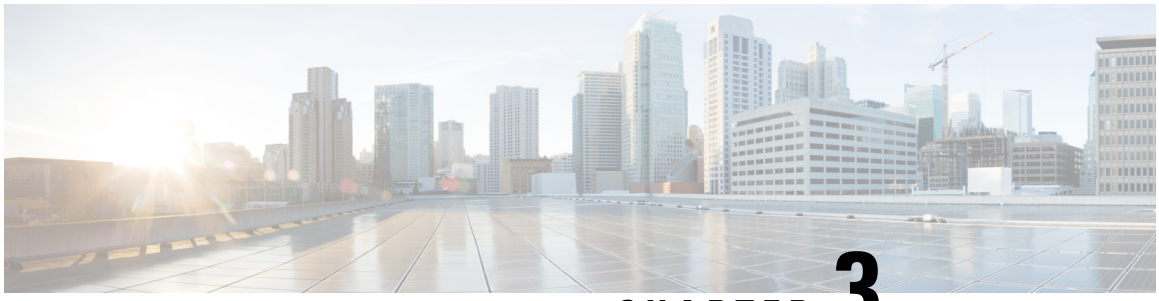
- Related Documents
- Appendix A, IETF RFCs for IP Multicast
- Technical Assistance

Related Documents

Related Topic	Document Title
CLI Commands	Cisco Nexus 3000 Series NX-OS Multicast Routing Command Reference

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:

- Information About IGMP, on page 15
- Default Settings for IGMP, on page 19
- Configuring IGMP Parameters, on page 19
- Configuring IGMP Host Proxy, on page 28
- Verifying the IGMP Configuration, on page 30
- Configuration Examples for IGMP, on page 30
- Where to Go Next, on page 31

Information 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.

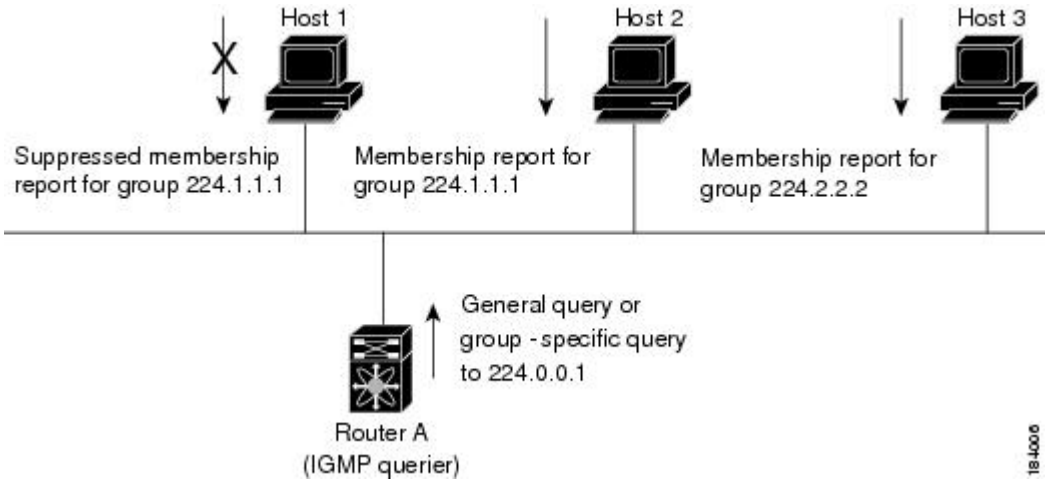
For detailed information about IGMPv2, see RFC 2236.

For detailed information about IGMPv3, see RFC 3376.

IGMP Basics

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

Figure 7: IGMPv1 and IGMPv2 Query-Response Process



In Figure 1, 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.

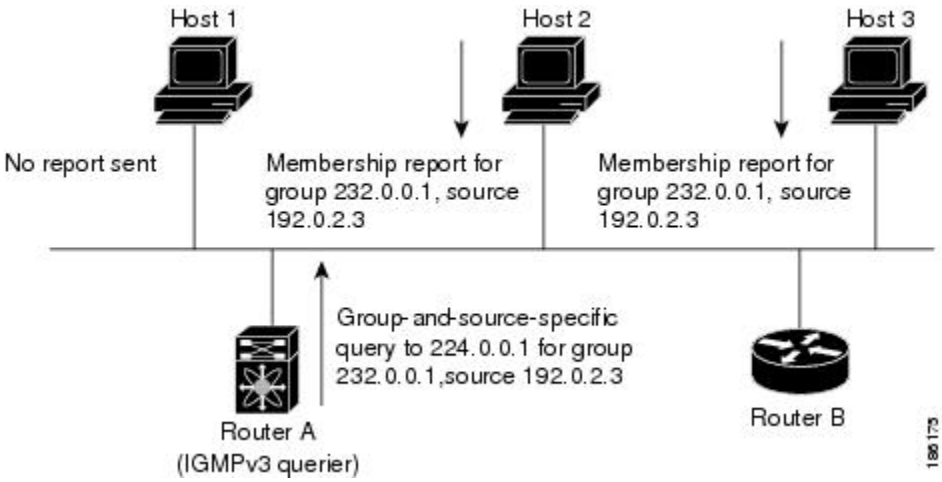
The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes 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 Figure 1, 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 Figure 2, 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 section.

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



Note IGMPv3 hosts do not perform IGMP membership report suppression.

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

Caution Changing the query interval can severely impact multicast forwarding.

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

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

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

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

Virtualization Support

Cisco NX-OS suports 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 3548 Switch NX-OS Unicast Routing Configuration Guide*.

Limitations

In Cisco NX-OS releases older than Cisco NX-OS Release 6.0(2)A1(1), you can use the ip igmp join-group command to bind a Nexus 3548 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 3548 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)A1(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 3548 switch to a multicast group, use the ip igmp static-oif command instead of the ip igmp join-group command.

IGMP 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 3548 Switch NX-OS Unicast Routing Configuration Guide*.

Default Settings for IGMP

Table 1 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.
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.

Parameter	Description
Query max response time	Maximum response time advertised in IGMP queries. You can tune the IGMP messages on the network by setting a larger value so that host responses are spread out over a longer time. This value must be less than the query interval. Values range from 1 to 25 seconds. The default is 10 seconds.
Query interval	Frequency at which the software sends IGMP host query messages. You can tune the number of IGMP messages on the network by setting a larger value so that the software sends IGMP queries less often. Values range from 1 to 18,000 seconds. The default is 125 seconds.
Last member query response interval	Interval in which the software sends a response to an IGMP query after receiving a host leave message from the last known active host on the subnet. If no reports are received in the interval, the group state is deleted. You can use this value to tune how quickly the software stops transmitting on the subnet. The software can detect the loss of the last member of a group or source more quickly when the values are smaller. Values range from 1 to 25 seconds. The default is 1 second.
Last member query count	Number of times that the software sends an IGMP query, separated by the last member query response interval, in response to a host leave message from the last known active host on the subnet. Values range from 1 to 5. The default is 2. Setting this value to 1 means that a missed packet in either direction causes the software to remove the multicast state from the queried group or channel. The software may wait until the next query interval before the group is added again.
Group membership timeout	Group membership interval that must pass before the router decides that no members of a group or source exist on the network. Values range from 3 to 65,535 seconds. The default is 260 seconds.
Report link local multicast groups	Option that enables sending reports for groups in 224.0.0.0/24. Link local addresses are used only by protocols on the local network. Reports are always sent for nonlink local groups. The default is disabled.
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 3548 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.

Parameter	Description
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.

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

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface*
3. **no switchport**
4. **ip igmp version** *value*
5. **ip igmp join-group** {**group** [**source** *source*] | **route-map** *policy-name*}
6. **ip igmp static-oif** {*group* [**source** *source*] | **route-map** *policy-name*}
7. **ip igmp startup-query-interval** *seconds*
8. **ip igmp startup-query-count** *count*
9. **ip igmp robustness-variable** *value*
10. **ip igmp querier-timeout** *seconds*
11. **ip igmp query-timeout** *seconds*
12. **ip igmp query-max-response-time** *seconds*
13. **ip igmp query-interval** *interval*
14. **ip igmp last-member-query-response-time** *seconds*
15. **ip igmp last-member-query-count** *count*
16. **ip igmp group-timeout** *seconds*
17. **ip igmp report-link-local-groups**
18. **ip igmp report-policy** *policy*
19. **ip igmp access-group** *policy*
20. **ip igmp immediate-leave**
21. (Optional) **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**]
22. (Optional) **copy running-config startup-config**

DETAILED STEPS

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:** `switch(config-if)# ip igmp last-member-query-count 3`	Sets the number of times that the software sends an IGMP query in response to a host leave message. Values can range from 1 to 5. The default is 2.

	Command or Action	Purpose
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	(Optional) **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] **Example:** `switch(config)# show ip igmp interface`	Displays IGMP information about the interface.
Step 22	(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.

Table 3 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

Table 4 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.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp ssm-translate** *group-prefix source-addr*
3. (Optional) **show running-configuration igmp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

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.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **[no] ip igmp enforce-router-alert**
3. (Optional) **show running-configuration igmp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
Step 2	(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.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring IGMP Host Proxy

This section contains the following information:

Overview of the feature

The IGMP host proxy feature helps to connect PIM enabled multicast network domain to a domain that does not understand PIM. This feature configures an interface as a proxy interface that proxies PIM joins/prunes that are received on the internal PIM network to IGMP joins/leaves.

IGMP Join Process

When a host wants to join a multicast group, the host sends one or more unsolicited Membership Reports for the multicast group that it wants to join.

IGMP Leave Process

IGMPv2 leaves are sent when the last host in the multicast network leaves. Therefore on receipt of the PIM prune from the last host, IGMPv2 leaves are sent upstream to indicate no more interest.

IGMP Multicast Addresses

IP multicast traffic uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

The multicast addresses in the range 224.0.0.0 to 224.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are transmitted using the IP multicast group addresses as follows:

- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the router is querying.
- IGMP group membership reports are destined to the group IP address for which the router is reporting.

- IGMPv2 Leave messages are destined to the address 224.0.0.2 (all routers on a subnet).

Guidelines and Limitations

See the following guidelines and limitations for configuring IGMP host proxy:

- Excluding or blocking a list of sources according to IGMPv3 (RFC 3376) is not supported.
- IGMP Host proxy proxies PIM joins/prunes received to IGMP joins/prunes on the proxy interface.
- Disable snooping if the proxy interface is a VLAN.
- It can be used to connect the network that understands only IGMP.
- The host proxy interface is a Layer 3 interface.
- The (S,G) entries have the RPF as the IGMP host proxy interfaces.
- The ideal configuration point is the RP.
- The IGMP host proxy can be in a query mode or unsolicited mode.
- If the reports need to be sent without the presence of a querier, configure the IGMP host proxy in unsolicited mode.
- Configure the IGMP host proxy unsolicited mode on a layer 3 physical port.
- The IGMP host proxy interface should have IP enabled.
- The PIM should not be enabled on the host proxy interface.
- The IGMP static/join group should not be configured on the IGMP host proxy interface.

How to Configure IGMP Host Proxy

Perform the following steps to configure IGMP host proxy:

Table 6: Configuring IGMP Host Proxy

Step	Command	Purpose
Step 1	**configure terminal** Example: `switch# configure terminal switch(config)#`	Enters configuration mode.
Step 2	**interface vlan** *interface*	Enters VLAN interface mode.
Step 3	**no shutdown**	Configures the interface in no shutdown mode.
Step 4	**ip address** *ip address*	Configures the IP address.

Step	Command	Purpose
Step 5	[**no**] **ip igmp host-proxy** [**unsolicited** [*time*] | **route-map** *route-map-name* [**unsolicited** [*time*]] | **prefix-list** *prefix-list-name* [**unsolicited** [*time*]]]	Configures the IGMP host proxy for the route-map.
Step 6	**show ip igmp groups**	Displays the IGMP connected group membership for VRF with H type for host proxy.
Step 7	**show ip igmp int vlan** *interface*	Displays the IGMP interfaces for VRF.
Step 8	**show ip igmp local-groups vlan** *interface*	Displays the IGMP locally joined group membership for VRF.
Step 9	show ip pim host-proxy	Displays the PIM host proxy interfaces.

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 Multicast Routing 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
```

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
```

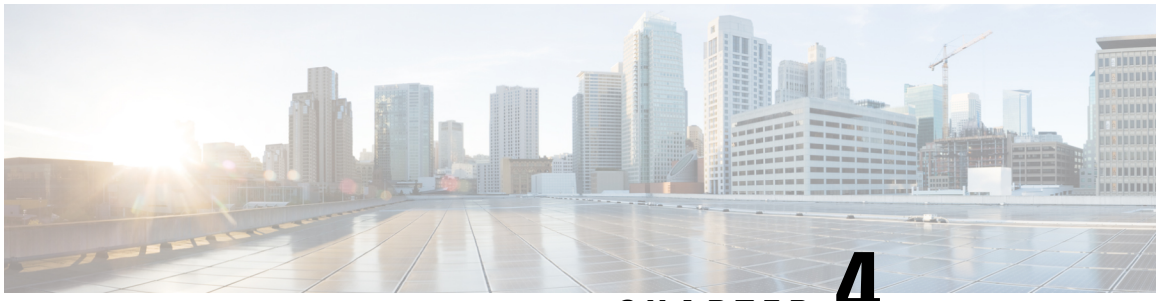
This example shows how to configure a route map that denies all multicast reports (joins):

```
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, on page 81
- Configuring MSDP, on page 97



CHAPTER 4

Configuring PIM

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

Note PIM Any Source Multicast (ASM) and Source-Specific Multicast (SSM) are unidirectional. PIM-Bidir is an enhanced form of PIM that allows bidirectional data flow. PIM-Bidir eliminates any source-specific state and allows trees to scale to an arbitrary number of sources. The differences between other PIM modes and PIM-Bidir are explained in the section Information about PIM-Bidir. Configuration of PIM and PIM-Bidir are similar. Textual notes and procedures indicate any configuration differences.

This chapter includes the following sections:

- Information about PIM, on page 33
- Information about PIM-Bidir, on page 40
- Guidelines and Limitations for PIM, on page 43
- Guidelines and Limitations for PIM-Bidir, on page 44
- Default Settings for PIM, on page 44
- Configuring PIM, on page 45
- Verifying the PIM Configuration, on page 63
- Displaying Statistics, on page 64
- Configuration Examples for PIM, on page 65
- Configuration Example for PIM-Bidir Using BSR, on page 67
- Configuring Multicast Service Reflection, on page 68
- Where to Go Next, on page 78
- Additional References, on page 78
- Related Documents, on page 78
- Standards, on page 78
- MIBs, on page 79

Information about PIM

PIM, which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees on which packets from

multiple sources are forwarded, as well as source distribution trees on which packets from a single source are forwarded. For more information about multicast, see the Information About Multicast section.

Cisco NX-OS supports PIM sparse mode for IPv4 networks (PIM). (In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it.) You can configure PIM to run simultaneously on a router. You can use PIM global parameters to configure rendezvous points (RPs), message packet filtering, and statistics. You can use PIM interface parameters to enable multicast, identify PIM borders, set the PIM hello message interval, and set the designated router (DR) priority. For more information, see the Configuring PIM 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 feature on each router and then enable PIM sparse mode on each interface that you want to participate in multicast. You can configure PIM for an IPv4 network. In an IPv4 network, if you have not already enabled IGMP on the router, PIM enables it automatically. For information about configuring IGMP, see Configuring IGMP, on page 15 .

You use the PIM global configuration parameters to configure the range of multicast group addresses to be handled by each of the two 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 that originates 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.

You can combine the modes to cover different ranges of group addresses. For more information, see the Configuring PIM, on page 33 section. For more information about PIM sparse mode and shared distribution trees used by the ASM mode, see RFC 4601.

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

For more information about PIM-Bidir, see RFC5015.

Note Multicast equal-cost multipathing (ECMP) is on by default in the Cisco NX-OS for the Cisco Nexus 3548 Switch; 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.

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. 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 (less than 10 seconds, or depending on your network environment), it may cause loss in multicast traffic.

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 switch 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 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 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 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 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. In PIM-Bidir mode, the Designated Forwarder (DF) is in charge of sending the PIM join message instead of the DR.

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 PIM-Bidir uses rendezvous points (RPs) and form bidirectional trees as explained in the section Information about PIM-Bidir.

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 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 section.

BSRs

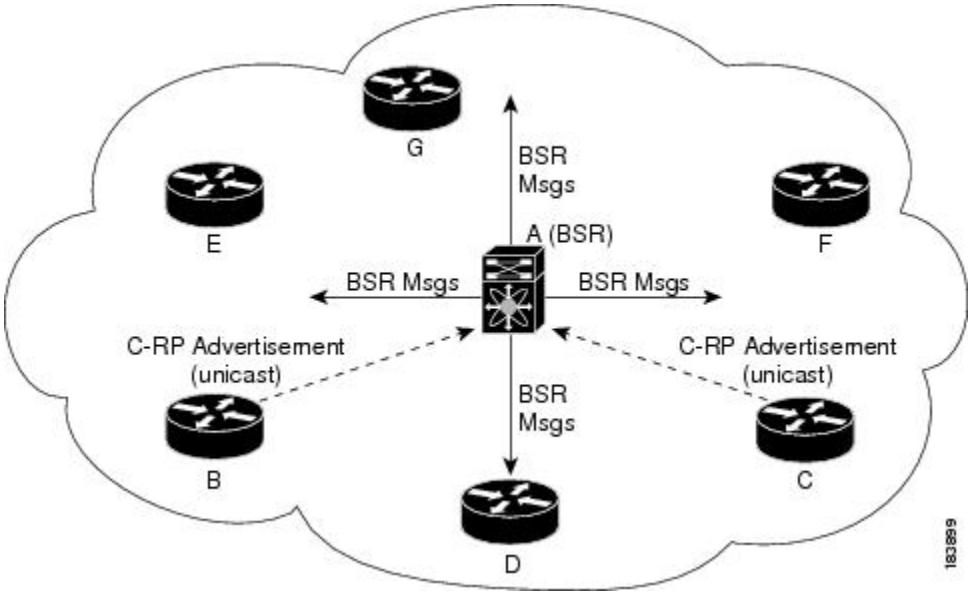
The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs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

Figure 1 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 sent by the BSR includes information about all of the candidate RPs. Each router uses a common algorithm to select the same RP address for a given multicast group.

Figure 9: BSR Mechanism



In the RP selection process, the RP address with the best priority is determined by the software. If the priorities match for two or more RP addresses, the software 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.

For information about configuring BSRs and candidate RPs, see the Configuring BSRs section.

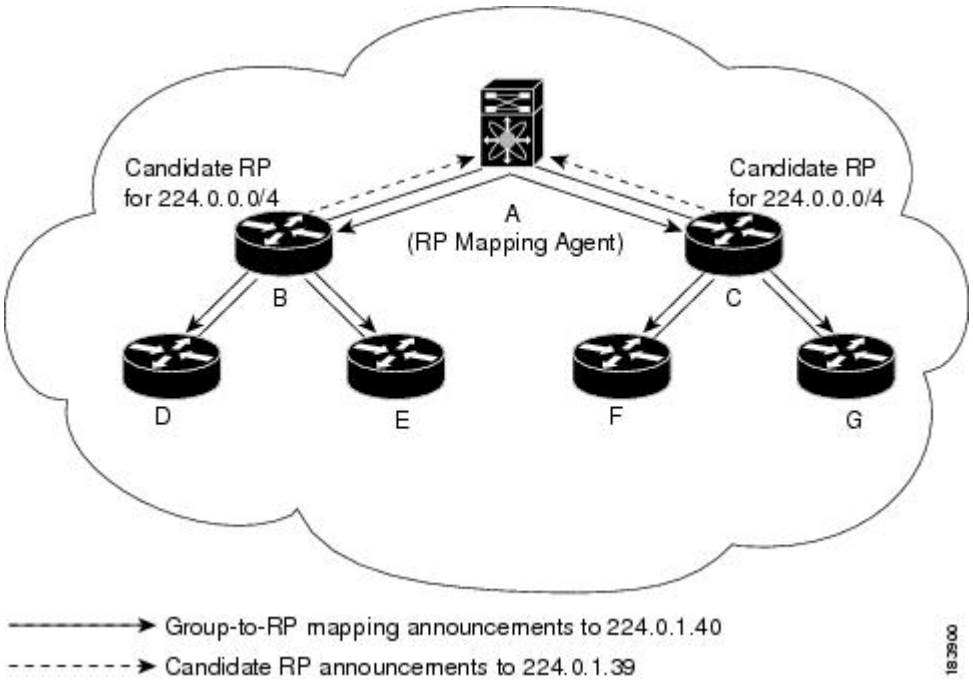
Auto-RP

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

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

Figure 2 shows the Auto-RP mechanism. Periodically, the RP mapping agent multicasts the RP information that it receives to the Cisco-RP-Discovery group 224.0.1.40 (shown by the solid lines in the figure).

Figure 10: Auto-RP Mechanism



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

For information about configuring Auto-RP, see the Configuring Auto-RP, on page 52 section.

Anycast-RP

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

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

PIM register messages are sent to the closest RP and PIM join-prune messages are sent in the direction of the closest RP as determined by the unicast routing protocols. If one of the RPs goes down, unicast routing ensures these message will be sent in the direction of the next-closest 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 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 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 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-OS, 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 Message Filtering 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 Hello Messages 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 Sparse Mode section.

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 Message Filtering section.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value. For more information, see the Configuring Auto-RP 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 3548 Switch NX-OS Unicast Routing Configuration Guide.

Information about PIM-Bidir

PIM-Bidir

The bidirectional mode for PIM (PIM-Bidir) is an enhancement of the PIM protocol that was designed for efficient many-to-many communications within an individual PIM domain. Multicast groups in bidirectional mode can scale to an arbitrary number of sources with only a minimal amount of additional overhead.

The shared trees that are created in PIM sparse mode are unidirectional. This means that a source tree must be created to bring the data stream to the root of the shared tree, or rendezvous point (RP), and then it can be forwarded down the branches to the receivers. Source data cannot flow up the shared tree toward the RP because this would be considered a bidirectional shared tree.

PIM-Bidir is derived from the mechanisms of PIM sparse mode (PIM-SM) and shares many of the shared tree operations. PIM-Bidir also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but PIM-Bidir differs in that it has no registering process for sources like those used in PIM-SM. These modifications in PIM-Bidir are necessary and sufficient to allow forwarding of traffic in all devices solely based on the (*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

Bidirectional Shared Tree

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In PIM-Bidir, the IP address of the RP acts as the key to having all devices establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a device, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. This technique is the preferred configuration method for establishing a redundant RP configuration for PIM-Bidir.

Membership in a bidirectional group is signaled by way of explicit Join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

Figure 3 and Figure 4 show the difference in state created per device for a unidirectional shared tree and source tree as compared to a bidirectional shared tree.

Figure 11: Unidirectional Shared Tree and Source Tree

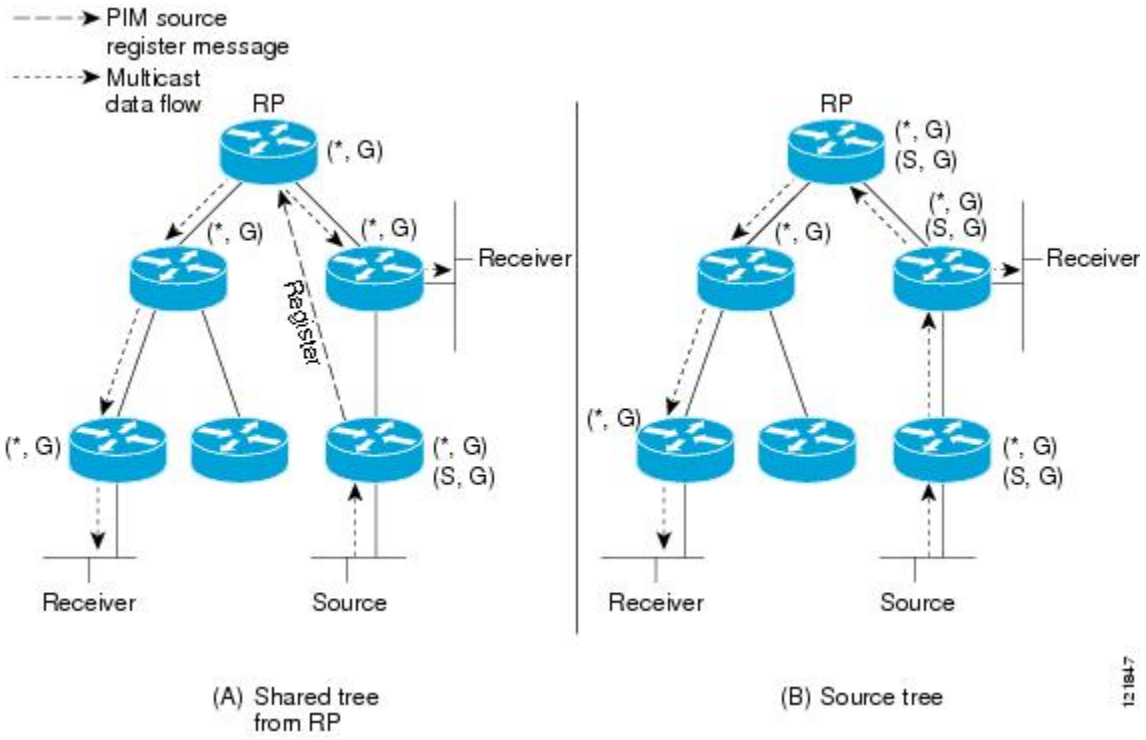
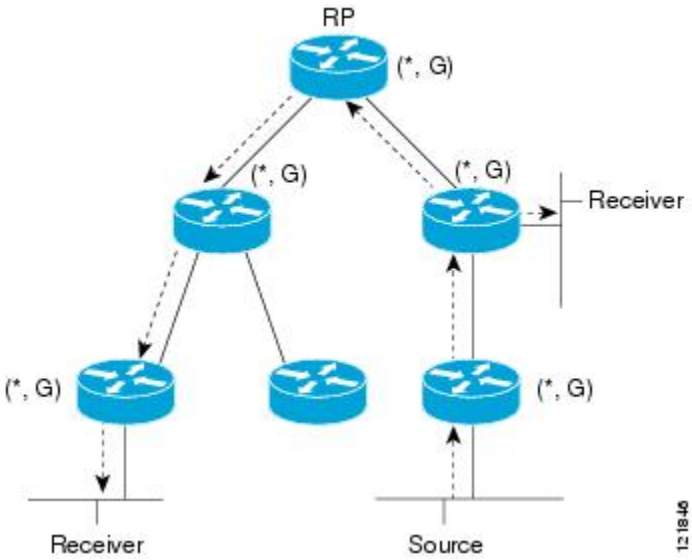


Figure 12: Bidirectional Shared Tree



For packets that are forwarded downstream from the RP toward receivers, there are no fundamental differences between PIM-Bidir and PIM sparse mode (PIM-SM). PIM-Bidir deviates substantially from PIM-SM for traffic that is passed from sources upstream toward the RP.

PIM-SM cannot forward traffic in the upstream direction of a tree because it accepts traffic from only one Reverse Path Forwarding (RPF) interface. This interface (for the shared tree) points toward the RP, thus allowing only downstream traffic flow. Upstream traffic is first encapsulated into unicast register messages, which are passed from the designated router (DR) of the source toward the RP. Second, the RP joins a source path tree (SPT) that is rooted at the source. Therefore, in PIM-SM, traffic from sources destined for the RP does not flow upstream in the shared tree, but downstream along the SPT of the source until it reaches the RP. From the RP, traffic flows along the shared tree toward all receivers.

In PIM-Bidir, the packet-forwarding rules have been improved over PIM-SM, allowing traffic to be passed up the shared tree toward the RP. To avoid multicast packet looping, PIM-Bidir introduces a new mechanism called designated forwarder (DF) election, which establishes a loop-free Rendezvous Point Tree (RPT) rooted at the RP.

DF Election

On every network segment and point-to-point link, all PIM devices participate in a procedure called designated forwarder (DF) election. The procedure selects one device as the DF for each rendezvous point (RP) of bidirectional groups. The DF is responsible for forwarding multicast packets received on that network.

The DF election is based on unicast routing metrics. The device with the most preferred unicast routing metric to the RP becomes the DF. Use of this method ensures that only one copy of every packet will be sent to the RP, even if there are parallel equal-cost paths to the RP.

A DF is selected for every RP of bidirectional groups. As a result, multiple devices may be elected as DF on any network segment, one for each RP. Any particular device can be elected as DF on more than one interface.

Bidirectional Group Tree Building

The procedure for joining the shared tree of a bidirectional group is nearly identical to that used in PIM Sparse Mode (PIM-SM). One main difference is that, for bidirectional groups, the role of the designated router (DR) is assumed by the designated forwarder (DF) for the rendezvous point (RP).

On a network that has local receivers, only the device elected as the DF populates the outgoing interface list (oiflist) upon receiving Internet Group Management Protocol (IGMP) Join messages, and sends (*, G) Join and Leave messages upstream toward the RP. When a downstream device wishes to join the shared tree, the reverse path forwarding (RPF) neighbor in the PIM Join and Leave messages is always the DF elected for the interface that leads to the RP.

When a device receives a Join or Leave message, and the device is not the DF for the receiving interface, the message is ignored. Otherwise, the device updates the shared tree in the same way as in sparse mode.

In a network where all devices support bidirectional shared trees, (S, G) Join and Leave messages are ignored. There is also no need to send PIM assert messages because the DF election procedure eliminates parallel downstream paths from any RP. An RP never joins a path back to the source, nor will it send any register stops.

Packet Forwarding

A device creates (*, G) entries only for bidirectional groups. The outgoing interface list (oiflist) of a (*, G) entry includes all the interfaces for which the device has been elected designated forwarder (DF) and that have received either an Internet Group Management protocol (IGMP) or Protocol Independent Multicast (PIM) Join message. If a device is located on a sender-only branch, it will also create a (*, G) state, but the oiflist will include only the RPF interface, unless the RP address belongs to a local interface of the router. In that case, the oiflist will be empty.

If a packet is received from the Reverse Path Forwarding (RPF) interface toward the rendezvous point (RP,) the packet is forwarded downstream according to the oiflist of the (*, G) entry. Otherwise, only the device that is the DF for the receiving interface forwards the packet upstream toward the RP; all other devices must discard the packet.

Guidelines and Limitations for PIM

PIM has the following guidelines and limitations:

- Cisco NX-OS PIM does not interoperate with any version of PIM dense mode or PIM sparse mode version 1.
- Cisco Nexus 3500 Series switches do not support PIM adjacency with a vPC leg or with a router behind a vPC.
- 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.
- OpenFlow is supported on the N3K-C3548-10GX platforms.
- The patchability feature is not supported on Cisco Nexus 3500 Series platforms.
- When the ACL log is configured matching a multicast stream where the flow is started, the corresponding S, G is not created because the ACL log consumes the packet. You must disable the log option to create the S, G route entry.
- RPF failure will not happen for *, G or S, G if RPF interface is SVI. In case of SVI as RPF, the match of entry in hardware happens based on VLAN, S, G as key. So, traffic on different VLAN does not hit and get punted to CPU as RPF failure.
- The **ip pim spt-threshold infinity group-list** and **ip pim use-shared-tree-only group-list** commands are supported for standalone (non-vPC) Last Hop Router (LHR) configurations.
- Configuring a secondary IP address as an RP address is not supported.

- PIM must be configured on all L3 interfaces between sources, receivers, and rendezvous points (RPs).

Guidelines and Limitations for PIM-Bidir

There are some limitations in the use of PIM-Bidir on the Cisco Nexus 3548 Switch. In particular, due to internal implementation, once a group range has been configured as Bidir for one VRF, the group-range may not be used again for other VRFs. For example, if the group-range 225.1.0.0/16 has been configured as Bidir in the default VRF, no group or part of this group-range can be re-used (as ASM, Bidir, or SSM) in a different VRF.

Default Settings for PIM

Table 1 lists the default settings for PIM parameters.

Table 7: Default PIM Parameters

Parameters	Default
Use shared trees only	Disabled
Flush routes on restart	Disabled
Log Neighbor changes	Disabled
Auto-RP message action	Disabled
BSR message action	Disabled
SSM multicast group range or policy	232.0.0.0/8 for IPv4
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

Parameters	Default
Neighbor adjacency policy	Become adjacent with all PIM neighbors

Configuring PIM

You can configure PIM for each interface.

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

You can configure separate ranges of addresses in the PIM domain using the multicast distribution modes described in 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	Source-specific multicast
RPF routes for multicast	No	RPF routes for multicast

To configure PIM, follow these steps:

Procedure

Step 1 From the multicast distribution modes described in Table 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 Features section.

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

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

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

Step 5 If you are configuring message filtering. See the Configuring Message Filtering section.

Enabling the PIM Feature

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

Before you begin

Ensure that you have installed the 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	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Shows the running-configuration information for PIM, including the **feature** command.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring PIM Sparse Mode

You configure PIM sparse mode on every switch interface that you want to participate in a sparse mode domain.

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

Note To configure the join-prune policy, see the Configuring Message Filtering section.

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:** `switch(config)# ip pim bsr forward`	Enables listening for or forwarding of BSR messages. The default is disabled, which means that the software does not listen for or forward BSR messages.
Step 4	(Optional) **ip pim 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 5	(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 6	(Optional) [**ip** |**ipv4**] **routing multicast holddown***holddown-period* **Example:** `switch(config)# ip routing multicast holddown 100`	Configures the initial holddown period in seconds. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Step 7	(Optional) **show running-configuration pim** **Example:** `switch(config)# show running-configuration pim`	Displays PIM running-configuration information, including the register rate limit.

Step 8	**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 9	**no switchport** **Example:** `sswitch(config-if)# no switchport`	Configures the interface as a Layer 3 routed interface.

	Command or Action	Purpose
Step 10	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. The default is disabled.
Step 11	(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 12	(Optional) **ip pim hello-authentication ah-md5** *auth-key* **Example:** `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	Enables an MD5 hash authentication key in PIM hello messages. You can enter an unencrypted (cleartext) key or one of these values followed by a space and the MD5 authentication key: • 0-Specifies an unencrypted (cleartext) key • 3-Specifies a 3-DES encrypted key • 7-Specifies a Cisco Type 7 encrypted key
Step 13	(Optional) **ip pim hello-interval** *interval* **Example:** `switch(config-if)# ip pim hello-interval 25000`	Configures the interval at which hello messages are sent in milliseconds. The range is from 1 to 4294967295. The default is 30000. **Note** The minimum value is 1 millisecond.
Step 14	(Optional) **ip pim border** **Example:** `switch(config-if)# ip pim border`	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.
Step 15	(Optional) **ip pim neighbor-policy prefix-list** *prefix-list* **Example:** `switch(config-if)# ip pim neighbor-policy prefix-list AllowPrefix`	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. Also configures which PIM neighbors to become adjacent to based on a prefix-list policy with the **ip prefix-list** *prefix-list* command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 16	(Optional) **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] **Example:** `switch(config-if)# show ip pim interface`	Displays PIM interface information.

	Command or Action	Purpose
Step 17	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Configuring ASM or Bidir

Any Source Multicast (ASM) and bidirectional shared trees (Bidir) are multicast distribution modes that require 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.

Note Before configuring ASM or PIM-Bidir, first enable PIM as described in the previous section.

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 If you are configuring unidirectional PIM, omit the parameter [bidir] at the end of the command in step 2, so that it would read: **ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **route-map** *policy-name*]

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*] **Example:**	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. The default group range is 224.0.0.0 through 239.255.255.255.

	Command or Action	Purpose
	`switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9`	The example configures PIM Bidir 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 BSRs

You configure BSRs by selecting candidate BSRs and RPs.

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

You can configure a candidate BSR with the arguments described in Table 3.

Table 9: Candidate BSR Arguments

Argument	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.
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 Table 4.

Table 10: 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.

Argument or Keyword	Description
interval	Number of seconds between sending candidate-RP messages. This value ranges f 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 1 seconds.
priority	Priority assigned to this RP. The software elects the RP with the highest priority 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 prio to 255 and has a default of 192. **Note** This priority differs from the BSR BSR-candidate priority, which prefers the hig value between 0 and 255.

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 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 Message Filtering section.

Configuring BSRs

Note If you are configuring PIM-ASM, omit the parameter bidir from the command in step 3, so that your command entry would read:

ip pim [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* [**priority** *priority*] [**interval** *interval*]

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* **Example:** `switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	Configures a candidate RP for BSR. The priority ranges from 0, the highest priority, to 65,535 and has a default of 192. The interval ranges from 1 to 65,535 seconds and has a default of 60. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures a PIM-Bidir candidate RP. **Note** To configure an ASM candidate RP, omit the parameter bidir at the end of the command.
Step 4	(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 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.

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 Table 5.

Table 11: 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 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 Table 6.

Table 12: 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 valu 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 minimur of 15 seconds.
bidir	If not specified, this RP will be in ASM mode. If specified, this RP will b 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 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 filtering. See the Configuring Message Filtering section.

Configuring Auto RP

Note Use the parameter bidir in the command shown in Step 3 only for bidirectional PIM (PIM-Bidir). If you are configuring unidirectional PIM, the command should read: **ip pim** {**send-rp-announce** | {**auto-rp rp-candidate**}} interface **group-list** *ip-prefix* [**scope** *ttl*] [**interval** *interval*]

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* [**scope** *ttl*] [**interval** *interval*] [**bidir**] **Example:** `switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir`	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 4-6. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures a bidirectional candidate RP. **Note** Omit the bidir parameter from the end of the command in this example to create an ASM candidate RP.

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

Configuring a PIM Anycast RP Set (PIM)

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

Step 1 Select the routers in the PIM Anycast-RP set.

Step 2 Select an IP address for the PIM Anycast-RP set.

Step 3 Configure each peer RP and local address in the PIM Anycast-RP set as described in this section.

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.

	Command or Action	Purpose
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**]]	Displays PIM modes and group ranges.
Step 8	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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. **Note** This command is supported only for standalone (non-vPC) Last Hop Router (LHR) configurations.

	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 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.

Note SSM cannot be configured in conjunction with PIM-Bidir.

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, on page 15.

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 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.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 2</td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Command</td><td>Purpose</td></tr>
<tr><td>ip pim ssm range {ip-prefix | none} | route-map policy-name}
Example:
<code>switch(config)# ip pim ssm range 239.128.1.0/24</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 match ip multicast command. The default range is 232.0.0.0/8. If the keyword none is specified, all group ranges are removed.</td></tr>
<tr><td>no ip pim ssm range {range ip-prefix | none} | route-map policy-name}
Example:
<code>switch(config)# no ip pim ssm range none</code></td><td>Removes the specified prefix from the SSM range, or removes the route-map policy. If the keyword none 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) show ip pim group-range [ip-prefix | vrf vrf-name]
Example:
<code>switch(config)# show ip pim group-range</code></td><td>Displays PIM modes and group ranges.</td></tr>
<tr><td>Step 4</td><td>(Optional) copy running-config startup-config
Example:
<code>switch(config)# copy running-config startup-config</code></td><td>Saves configuration changes.</td></tr>
</table>

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 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 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 preference is 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.

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 Message Filtering 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 PIM6.

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose

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 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`	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. **Note** BSR RP, auto-RP, and static RP cannot use the group-range keyword. This command allows both permit or deny. Some match mask commands do not allow permit or deny.
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 Message Filtering

You can configure filtering of the PIM and PIM6 messages described in Table 7.

Table 13: 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 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 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.

Message Type	Description
BSR policy	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy, where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.
Auto-RP candidate RP policy	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses, and the type ASM with the **match ip multicast** command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages.
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.
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 section.

Note For information on about configuring route-map policies, see the Cisco Nexus 3548 Switch NX-OS Unicast Routing Configuration Guide.

Configuring Message Filtering

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.

	Command or Action	Purpose
Step 2	(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 3	(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 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 4	(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 5	(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 6	(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 7	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the specified interface.

Step 8	**no switchport** **Example:** `switch(config-if)# no switchport`	Configures the interface as a Layer 3 routed interface.
Step 9	(Optional) **ip pim jp-policy** *policy-name* [**in** | **out**] **Example:** `switch(config-if)# ip pim jp-policy my_jp_policy`	Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the **match ip multicast** command. The default is no filtering of join-prune messages. This command filters messages in both incoming and outgoing directions.

	Command or Action	Purpose
Step 10	(Optional) **show run pim** **Example:** `switch(config-if)# show run pim`	Displays PIM configuration commands.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves configuration changes.

Flushing the Routes

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

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

Verifying the PIM Configuration

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

Command	Purpose
show ip mroute { *source* | *group* [*source*]} [**vrf** *vrf-name* | **all**]	Displays the IP multicast routing table.
show ip pim group-range [**vrf** *vrf-name* | **all**]	Displays the learned or configured group ranges and modes. For similar information, see also the **show ip pim rp** command.
show ip pim interface [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	Displays information by the interface.
show ip pim neighbor [**vrf** *vrf-name* | **all**]	Displays neighbors by the interface.
show ip pim oif-list *group* [*source*] [**vrf** *vrf-name* | **all**]	Displays all the interfaces in the OIF-list.
show ip 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 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 pim group-range** command.
show ip pim rp-hash [**vrf** *vrf-name* | **all**]	Displays the bootstrap router (BSR) RP hash information.
show running-configuration pim	Displays the running-configuration information.
show startup-configuration pim	Displays the running-configuration information.
show ip pim vrf [*vrf-name* | **all**] [**detail**]	Displays per-VRF information.

Displaying Statistics

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

Displaying PIM Statistics

You can display the PIM statistics and memory usage using the commands listed in the table below. Use the **show ip** form of the command for PIM.

Command	Description
show ip 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 NX-OS Multicast Routing Command Reference

Clearing PIM Statistics

You can clear the PIM and PIM6 statistics using the commands listed in Table 8. Use the **show ip** form of the command for PIM.

Table 14: PIM Commands to Clear Statistics

Command	Description
clear ippim interface statistics *interface*	Clears counters for the specified interface.
clear ip pim policy statistics	Clears policy counters for Register, RP, and join-prune message policies.
clear ip pim statistics [**vrf** *vrf-name* | **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.

Configuration Example for SSM

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, on page 15. 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
```

This example shows how to configure PIM in 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
```

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

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

3. **Step 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. **Step 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
```

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
no switchport
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
```

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. **Step 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. **Step 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
```

3. **Step 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
```

4. **Step 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. **Step 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
```

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

```
configure terminal
interface ethernet 2/1
no switchport
ip pim sparse-mode
exit
interface loopback 0
ip address 192.0.2.3/32
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
```

Configuration Example for PIM-Bidir Using BSR

The next section shows how to configure PIM-Bidir mode with BSR. The steps are similar to those used to configure PIM with Auto-RP or static RP for a given group-range.

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

1. **Step 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. **Step 2**: Configure whether that router should listen and forward BSR messages.

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

3. **Step 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. **Step 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 bidir
```

This example shows how to configure PIM Bidir mode using the BSR mechanism and, in particular, how to configure the BSR and RP on the same router:

```
configure terminal
interface ethernet 2/1
no switchport
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 bidir
```

Configuring Multicast Service Reflection

The multicast service reflection feature enables the users to translate externally received multicast destination addresses to addresses that confirm to their organization's internal addressing policy. It is the multicast network address translation (NAT) of an ingress multicast stream (S1,G1) to an egress (S2,G2) interface. This feature is commonly referred to as the multicast service reflection feature (SR feature).

The SR feature is supported in two flavors:

- Regular mode multicast NAT

In regular mode, the packets incoming as the S1, G1 interfaces are translated to S2,G2 interfaces and the destination MAC address of the outgoing packet is translated as the multicast MAC address of the G2 interface (for example, the translated group).

- Fast-pass and fast-pass with no-rewrite multicast NAT

In fast-pass mode, the S1, G1 interfaces are translated to S2,G2 interfaces and the destination MAC address of the outgoing packet has the multicast MAC address corresponding to the G1 interface (for example, the MAC address of the pre-translated group).

Note The multicast service reflection feature is supported only on Cisco Nexus 3548-X platforms from Release 7.0(3)I7(2) .

The SR feature is configured on a loopback interface. For more information on the SR feature, see the following sections:

Guidelines and Limitations for Multicast Service Reflection

Before configuring the SR feature on the Cisco Nexus 3548-X platform switches, read the following guidelines and limitations:

- The SR feature is supported on the N3K-C3548-10GX platforms only and it is not supported on the N3K-C3548-10GE platforms.
- The SR feature is supported in Protocol Independent Multicast (PIM) sparse mode only (ASM or SSM).
- The show ip mroute detail statistics are not available in fast-pass or fast-pass no-rewrite modes for SSM. ASM statistics are available.

- The multicast service reflection feature does not work in a VPC environment.
- The multicast service reflection feature uses a hardware loopback port that is defined by the CLI hardware profile **multicast service-reflect port x**.
- The selected hardware loopback port for a multicast service reflect configuration should be a physical port with a 'Link Down' state and no SFP connected.
- The total throughput of the multicast-NAT regular mode solution is 5 Gbps.
- The multicast NAT translation does not happen with the mask length 0 to 4. This mask length limitation is only for the group address and it is not for the source addresses.
- IP multicast allows creation of the multicast (S,G) routes for the sources that are non-directly connected if an RPF path to the source in question is available in the unicast routing table. The route could be static or dynamic (via the routing protocols) or through the multicast command **ip mroute** *ip-sa/mask gateway*.

Ingress and egress interface ACLs on a device configured for the Multicast Service Reflection feature have the following limitations:

- When an ingress ACL is applied to block the untranslated multicast traffic that is already flowing, the (S,G) entries are not removed. The reason is that the multicast route entries continue to be hit by the traffic, even though the ACL drops the packets.
- When an egress ACL is applied to block translated source traffic (S2,G2) on an egress interface, the egress ACL does not work because an egress ACL is not supported for the translated traffic.
- Multicast Service Reflect doesn't support source non-translation for Normal or fast-pass mode. The translated source should fall into subnet of loopback port configured as ingress multicast stream S1, G1 outgoing interface list (oiflist).
- Configuring a secondary IP address as an RP address is not supported.
- Multicast Forwarding for the source group (S1, G1) is not supported for Service Reflected multicast routes on the translation router.

Configuring Multicast Service Reflection Feature

Configure the multicast service reflection feature in the following sequence:

1. Configure the multicast service reflect loopback port first.
2. Configure the multicast service reflect mode.
3. Configure the multicast service reflect rule.

Configuring the Multicast Service Reflect Loopback Port

Configure the multicast service reflect loopback port using the CLI commands listed in Table 9 .

Table 15: Configuring the Multicast Service Reflect Loopback Port

Command	Description
hardware profile multicast service-reflect port ?<*1-48*> *Loopback port-num*	Creates a multicast service reflect loopback port from the range <1-48>.

Note The selected loopback port is no longer usable for any other purpose and it is dedicated to the multicast service reflection feature. A reload is required after configuring the loopback port.

The service-reflect port is required only in the regular mode and is not required in the fast-pass mode.

```
(config)# hardware profile multicast service-reflect port 12
```

Configuring the Multicast Service Reflect Mode

Configure the multicast service reflect mode using the CLI commands listed in Table 10 . The fast-pass mode with or without no-rewrite translates the UDP Destination Port D1 to a different Destination Port D2.

Note A reload is required after configuring the multicast service reflect mode.

Table 16: Configuring the Multicast Service Reflect Mode

Command	Description
ip service-reflect mode ? *regular* *fast-pass* *fast-pass no-rewrite*	Configures the multicast service reflect mode. The feature is supported in the following flavors: regular mode, fast-pass mode, and fast-pass no-rewrite mode. Regular Mode: The regular mode translates the G1 interface to G2 interface. It rewrites the MAC address for the G2 interface, as per the multicast protocol. The fast-pass mode translates the G1 interface to G2 interface. It does not rewrite the MAC address for the G2 interface. The MAC address of the G2 interface is still valid as per the multicast protocol, as the /9 mask-length restriction keeps the MAC address of the G2 interface same as the MAC address of the G1 interface. The mask-length for the group translation must-be less than or equal to 9 for this mode. The fast-pass mode with no-rewrite option translates the G1 interface to G2 interface but it does not rewrite the MAC address for the G2 interface. The MAC address of the G2 interface is not valid as per the multicast protocol. Use this mode option with due diligence, if the MAC address of the G2 interface is not taken into account in the topology. The mask-length for the group translation has no restriction.
ip service-reflect mode regular	Configures the regular mode.

Configuring the Multicast Service Reflect Rule

Next, configure the multicast service reflect rule using the CLI commands listed in Table 11 .

Note If the switch receives (S,G) traffic irrespective of the UDP port and you have multiple rules of the same S,G with different UDP Ports as key, then the states of all S,G UDP rules are created and the hardware resources get allocated.

Table 17: Configuring the Multicast Service Reflect Rule

Command	Description
config # **ip service-reflect destination** *G1* **to** *G2* **mask-len** *M1* **source** *S1* **to** *S2* **mask-len** *M2* *G1: A.B.C.D Incoming Group Address (Multicast)* *G2: A.B.C.D Outgoing Group Address (Multicast)* *M1: <0-32> Group Mask Length *Default value is 32* *S1: A.B.C.D Incoming Source Address* *S2: A.B.C.D Outgoing Source Address M2: <0-32> Source Mask Length *Default value is 32.*	Specifies the rule to SR translate the ingress interface (S1,G1) to an egress interface (S2,G2).
config # **ip service-reflect destination** *G1* **to** *G2* **mask-len** *M1***source** *S2* *G1: A.B.C.D Incoming Group Address (Multicast)* *G2: A.B.C.D Outgoing Group Address (Multicast)* *M1: <0-32> Group Mask Length* *S2: A.B.C.D Outgoing Source Address*	Specifies the rule to SR translate the ingress interface (*,G1) to (S2,G2) interface. **Note** * means S1: A.B.C.D Incoming Source Address would not be taken into the account.

See the following examples for the default (32) subnet-masks and non-default (less than 32) subnet-masks:

Example 1:

```
#ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to
12.0.0.2 mask-len 32
```

The configuration rule in example 1 installs the following (S1,G1) to (S2,G2) mapping rules:

```
a. (10.0.0.2, 225.0.0.2) -> (12.0.0.2, 226.0.0.2)
```

Example 2:

```
#ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 31 source 10.0.0.2 to
12.0.0.2 mask-len 31
```

The configuration rule in example 2 installs the following (S1,G1) to (S2,G2) mapping rules:

```
a. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
b. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
```

```
a. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
b. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
```

Example 3:

```
#ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 31 source 10.0.0.2 to
12.0.0.2 mask-len 32
```

The configuration rule in example 3 installs the following (S1,G1) to (S2,G2) mapping rules:

```
a. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
b. (10.0.0.2, 225.0.0.3) -> (12.0.0.2, 226.0.0.3)
```

Example 4:

```
ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to 12.0.0.2
 mask-len 32 udp-dest-port 3000
```

The configuration rule in example 4 installs the following (S1,G1) to (S2,G2) mapping rules:

```
a. (10.0.0.2, 225.0.0.2, 3000) -> (12.0.0.2, 226.0.0.2)
```

Example 5:

```
ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to 12.0.0.2
 mask-len 32 udp-dest-port 3000 to 4000
```

The configuration rule in example 5 installs the following (S1,G1) to (S2,G2) mapping rules:

```
a. (10.0.0.2, 225.0.0.2, 3000) -> (12.0.0.2, 226.0.0.2, 4000)
```

Configuring the Regular Mode

Configure the loopback port, the regular SR mode, and the SR rule for the regular mode using the CLI steps outlined in the table below.

Step	Command	Description
Step 1	**# feature pim**	Configures the PIM feature for the G1 and G2 interfaces.
Step 2	**# ip pim rp-address 10.0.0.2 group-list 225.0.0.2/32 //S1,G1**	
Step 3	**#ip pim rp-address 11.0.0.2 group-list 226.0.0.2/32 //S2,G2**	
Step 4	(config) # **hardware profile multicast service-reflect port 12**	Chooses the SR loopback port, for example, port 12 and configures loopback.
Step 5	(config) # **ip service-reflect mode regular**	Configures regular mode for multicast service reflection.
Step 6	**# ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to 12.0.0.2 mask-len 32 // G1 to G2, S1 to S2**	Configures the SR rule.

Step	Command	Description
Step 7	**# interface Ethernet1/10** **# no switchport** **# ip address 10.0.0.1/24** **# ip pim sparse-mode** **# no shutdown** **#interface Ethernet1/11** **# no switchport** **# ip address 11.0.0.1/24** **# ip pim sparse-mode** **# no shutdown**	Configures an ingress interface, for example, 1/10 and an egress interface, for example, 1/11 on the SR box.
Step 8	**# interface loopback0** **# ip address 12.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 225.0.0.2** **# interface loopback1** **# ip address 17.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 227.0.0.2**	Configures the loopback port on the SR box. This belongs to S2 subnet (translated S1). This is static OIF for G1. This belongs to S2 subnet (translated S1). This is static OIF for G1. For the multiple Multicast NAT rules, add loopback configuration per S2 unique subnet.
Step 9	(config) # **test ethpm l3 enable-show-iport**	Use the test ethpm l3 enable-show-iport command in regular mode to access the external loopback port.
Step 10	(config) # **copy r s** (config) # **reload**	Save the running configuration to the startup configuration and reload. Configurations described in steps (4) and (5) must be present for the regular mode feature and require a reload.

Configuring the Fast-pass Mode

Configure the loopback port, the fast-pass SR mode, and the SR rule for the fast-pass or fast-pass no rewrite using the CLI steps outlined in Table 12.

Note The hardware loopback port configuration is not required in fast-pass mode.

Table 18: Configuring the Fast-pass Mode

Step	Command	Description
Step 1	**# feature pim**	Configures the PIM feature for the G1 and G2 interfaces.
Step 2	**# ip pim rp-address 10.0.0.2 group-list 225.0.0.2/32 //RP for G1, G1**	
Step 3	**# ip pim rp-address 11.0.0.2 group-list 226.0.0.2/32 //S2,G2**	
Step 4	(config) # **ip service-reflect mode fast-pass** OR (config) # **ip service-reflect mode fast-pass no-rewrite**	Configures the fast-pass mode or the fast-pass mode no-rewrite mode for multicast service reflection.
Step 5	**# ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 9 source 10.0.0.2 to 12.0.0.2 mask-len 32 // G1 to G2, S1 to S2**	Configures the SR rule.
Step 6	**# interface Ethernet 1/10** **# no switchport** **# ip address 10.0.0.1/20** **# ip pim sparse-mode** **# no shutdown** **# interface Ethernet 1/11** **# no switchport** **# ip address 11.0.0.1/20** **# ip pim sparse-mode** **# no shutdown**	Configures an ingress interface, for example, 1/10 and an egress interface, for example, 1/11 on the SR box.
Step 7	**# interface loopback0** **# ip address 12.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 225.0.0.2** **# interface loopback1** **# ip address 17.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 227.0.0.2**	Configures the loopback port on the SR box. For the multiple Multicast NAT rules, add loopback configuration per S2 unique subnet.

Step	Command	Description
Step 8	(config) # **copy r s** (config) # **reload**	Save the running configuration to the startup configuration and reload. Configuration described in step (4) must be present for the fast-pass mode feature and requires a reload.

Viewing the Show Commands for the Regular Mode

See the following sections for viewing the show commands for the multicast service reflection feature:

- Checking the Rate of the Stream
- Checking the Multicast Route
- Viewing the Multicast route

Checking the Rate of the Stream

To display information about the interface configuration, use the show interface ethernet command.

Note The multicast group statistics in **show ip mroute detail** are not available in fast-pass mode and fast-pass no-rewrite with SSM. The statistics are available for ASM multicast.

Use the show int eth < *slot/port* > | i rate command to check the rate of the stream as displayed in the following examples:

 # show int eth 1/10 | i rate

```
30 seconds input rate 1536904 bits/sec, 3000 packets/sec \\ 1X of (S1,G1) UDP stream
0 seconds output rate 208 bits/sec, 0 packets/sec
input rate 1.54 Mbps, 3.00 Kpps; output rate 152 bps, 0 pps
```

 # show int eth 1/12 | i rate

```
30 seconds input rate 3072112 bits/sec, 5999 packets/sec \\ 2X Stream
30 seconds output rate 2811704 bits/sec, 5999 packets/sec \\ 2X Stream
input rate 3.07 Mbps, 6.00 Kpps; output rate 3.05 Mbps, 6.00 Kpps
```

The command listed above is required to execute the command over the loopback port:

```
# test ethpm l3 enable-show-iport // To show the loopback port
```

 # show int eth 1/11 | i rate

```
30 seconds input rate 160 bits/sec, 0 packets/sec
30 seconds output rate 1683024 bits/sec, 2999 packets/sec \\ 1X of (S2,G2) UDP stream
input rate 136 bps, 0 pps; output rate 1.52 Mbps, 3.00 Kpps
```

Checking the Multicast Route

Check the multicast route using the show ip mroute and show ip mroute sr command to display the service reflect routes only as explained in the following example:

 # show ip mroute sr

```
IP Multicast Routing Table for VRF "default"

(*, 225.0.0.2/32), uptime: 00:27:44, static pim ip // (*,G1) route
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:27:33
Outgoing interface list: (count: 1)
loopback0, uptime: 00:27:44, static

(10.0.0.2/32, 225.0.0.2/32), uptime: 00:24:01, ip mrib pim // (S1,G1) route
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:24:01
Outgoing interface list: (count: 1)
loopback0, uptime: 00:24:01, mrib

(10.1.1.11/32, 230.1.1.2/32), uptime: 00:15:57, pim mrib ip
Translated Route Info: (169.1.1.11, 225.1.1.2)
Incoming interface: Ethernet1/47, RPF nbr: 10.1.1.11, uptime: 00:15:57, internal
Outgoing interface list: (count: 1)
loopback0, uptime: 00:15:57, mrib

(12.0.0.2/32, 226.0.0.2/32), uptime: 00:24:01, ip pim // (S2,G2) route
Incoming interface: loopback0, RPF nbr: 12.0.0.2, uptime: 00:24:01
Outgoing interface list: (count: 1)
Ethernet1/11, uptime: 00:12:59, pim
```

Viewing the Multicast route

Use the **show forwarding multicast** route command to view the details of the forwarding multicast route as displayed in the following example:

 # show forwarding multicast route

```
IPv4 Multicast Routing table table-id:0x1
Total number of groups: 2


(*, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: G
Received Packets: 1 Bytes: 64
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 1
loopback0 Outgoing Packets:0 Bytes:0

(10.0.0.2/32, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: c
Received Packets: 507775 Bytes: 32497600
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 6000
Ethernet1/12 Outgoing Packets:0 Bytes:0

(12.0.0.2/32, 226.0.0.2/32), RPF Interface: loopback0, flags:
Received Packets: 0 Bytes: 0
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 3
Ethernet1/11 Outgoing Packets:0 Bytes:0
```

Viewing the Show Commands for the Fast-pass Mode

See the following sections for viewing the show commands for the fast-pass mode for the multicast service reflection feature:

- Checking the Rate of the Stream
- Checking the Multicast Route

- Viewing the Multicast route

Checking the Rate of the Stream

To display information about the interface configuration for the fast-pass mode, use the show interface ethernet command. Use the show int eth <slot/port> | i rate command to check the rate of the stream as displayed in the following examples:

 # show int eth 1/10 | i rate

```
30 seconds input rate 512632 bits/sec, 1000 packets/sec \\1X Stream of (S1,G1) Stream 30
seconds output rate 208 bits/sec, 0 packets/sec
input rate 95.38 Kbps, 168 pps; output rate 136 bps, 0 pps
```

 # show int eth 1/11 | i rate

```
30 seconds input rate 72 bits/sec, 0 packets/sec
30 seconds output rate 495584 bits/sec, 999 packets/sec \\ 1X stream of (S2,G2) stream input
 rate 144 bps, 0 pps; output rate 110.10 Kbps, 205 pps
```

Checking the Multicast Route

Check the multicast route using the show ip mroute and show ip mroute sr command to display the service reflect routes for the fast-pass mode as explained in the following example:

 # show ip mroute

 # show ip mroute sr (Display Service Reflect Routes only)

```
IP Multicast Routing Table for VRF "default"

(*, 225.0.0.2/32), uptime: 00:29:17, pim ip static
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:28:51 Outgoing interface
list: (count: 1)
loopback0, uptime: 00:16:15, static

(10.0.0.2/32, 225.0.0.2/32), uptime: 00:25:05, ip mrib pim
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:25:05 Outgoing interface
list: (count: 1)
loopback0, uptime: 00:16:15, mrib

(12.0.0.2/32, 226.0.0.2/32), uptime: 00:14:58, ip pim
Incoming interface: loopback0, RPF nbr: 12.0.0.2, uptime: 00:14:58 Outgoing interface list:
 (count: 1)
Ethernet1/11, uptime: 00:14:58, pim
```

Viewing the Multicast route

Use the show forwarding multicast route command to view the details of the forwarding multicast route as displayed in the following example:

 # show forwarding multicast route

```
IPv4 Multicast Routing table table-id:0x1
Total number of groups: 2

(*, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: G Received Packets: 10 Bytes: 640
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 2
loopback0 Outgoing Packets:0 Bytes:0

(10.0.0.2/32, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: c Received Packets: 1010555
```

```
 Bytes: 64675520
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 3
Ethernet1/11 Outgoing Packets:0 Bytes:0

(12.0.0.2/32, 226.0.0.2/32), RPF Interface: loopback0, flags: Received Packets: 0 Bytes: 0
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 3
Ethernet1/11 Outgoing Packets:0 Bytes:0
```

Where to Go Next

You can configure the following features that work with PIM:

Additional References

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

- Related Documents
- Standards
- MIBs
- Appendix A, IETF RFCs for IP Multicast

Related Documents

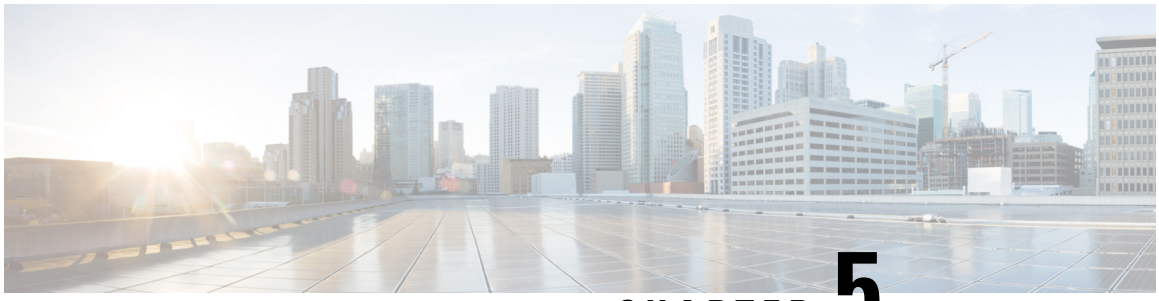
Related Topic	Document Title
CLI commands	Cisco Nexus 3000 Series Multicast Routing Command Reference
Configuring VRFs	Cisco Nexus 3548 Switch NX-OS Unicast Routing Configuration Guide

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 URL: http://mibs.cloudapps.cisco.com/ITDIT/MIBS/MainServlet



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:

- Information About IGMP Snooping, on page 81
- Guidelines and Limitations for IGMP Snooping, on page 83
- Prerequisites for IGMP Snooping, on page 84
- Default Settings for IGMP Snooping, on page 84
- Configuring IGMP Snooping, on page 85
- Configuring IGMP Snooping Parameters, on page 88
- Verifying the IGMP Snooping Configuration, on page 93
- Displaying IGMP Snooping Statistics, on page 94
- Clearing IGMP Snooping Statistics, on page 94
- Configuration Examples for IGMP Snooping, on page 94
- Additional References, on page 95
- Related Documents, on page 95
- Standards, on page 96

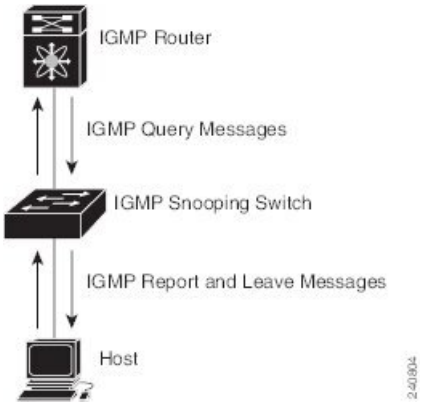
Information About IGMP Snooping

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

The Internet Group Management Protocol (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. The IGMP snooping feature 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 13: 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, on page 15.

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.
- Multicast forwarding based on IP address rather than MAC address.
- Optimized multicast flooding (OMF) that forwards unknown traffic to routers only and performs no data driven state creation.

For more information about IGMP snooping, see RFC 4541.

This section includes the following topics:

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, then 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, then 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 switch 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 switch 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.

Currently, you can configure the same SVI IP address for the switch querier and the IGMP snooping querier. Both queriers will then be active at the same time, and both queriers will send general queries to the VLAN periodically. To prevent this from happening, ensure that you use different IP addresses for the IGMP snooping querier and the switch querier.

IGMP Snooping Filter

Cisco NX-OS Release 6.0(2)A4(1) supports filtering of IGMP packets at the snooping layer. You can filter out IGMP snooping reports at the interface level. This filtering is based on a prefix-list or a route-map policy. The router compares a group to the prefix-list or route-map policy defined and performs the specified action. Thus, only groups that match the prefix-list or route-map that you specify will be filtered to the IGMP snooping reports.

Guidelines and Limitations for IGMP Snooping

IGMP snooping has the following guidelines and limitations:

- IGMP snooping is not supported with PVLAN.
- When IGMPv3 host on a VLAN leaves, it is possible that other hosts may experience traffic drop. This is seen mostly when a second consecutive leave is received from the port that already left and this impacts the other receivers on the VLAN.

To avoid this loss, you need to disable explicit host tracking under VLAN configuration using the **no ip igmp snooping explicit-tracking** command.

For example:

```
configure terminal
vlan configuration 10
no ip igmp snooping explicit-tracking
```

- In a hop-by-hop topology, the configuration of SVI on an intermediate box (second device) which is not an IGMP snooping querier causes traffic loss to hosts behind it when one of the other receivers ports behind another downstream L2 switch (third device) sends a leave. This is due to v3 suppression being disabled, IGMPv3 leave is consumed on second device. Workarounds for this issue is:
  - PIM DR and IGMP querier have to be co-located on the same box in the hop-by-hop topology. SVI in the first device should be configured with **ip pim dr-priority 10** to shift the DR from second device to the first device and the default suppression should be disabled on the second device, third device, and so on.
  - IGMPV3 suppression should be enabled under the VLAN configuration for the impacted VLAN on all the hops such as the second device and the third device.

For example:

```
configure terminal
vlan configuration 203
ip igmp snooping v3-report-suppression
```

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 for IGMP Snooping

The following table lists the default settings for IGMP snooping parameters.

Table 19: Default IGMP Snooping Parameters

Parameters	Default
IGMP snooping	Enabled
Explicit tracking	Enabled
Fast leave	Disabled
Last member query interval	1 second

Parameters	Default
Snooping querier	Disabled
Report suppression	Enabled
Link-local groups suppression	Enabled
IGMPv3 report suppression for the entire switch	Disabled
IGMPv3 report suppression per VLAN	Enabled

Note

- When a SPAN session is configured with a multicast router port being the source port, the destination port sees all the multicast traffic even when there is no traffic that is actually being forwarded to the source port. This is due to a current limitation of the multicast/SPAN implementation.
- Cisco Nexus 3548 Series switches replicate unknown multicast traffic to multicast router ports of all VLANs, although the multicast traffic is received in one particular VLAN. This is a default behavior and cannot be configured.

Configuring IGMP Snooping

Table 20: IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping. The default is enabled. **Note** If the global setting is disabled, all VLANs are treated as disabled, whether they are enabled or not.
Event history	Configures the size of the IGMP snooping history buffers. The default is small.
Group timeout	Configures the group membership timeout for all VLANs on the device.
Link-local groups suppression	Configures link-local groups suppression on the device. The default is enabled.
Optimise-multicast-flood	Configures optimized multicast flooding (OMF) on all VLANs on the device. The default is enabled.
Proxy	Configures the IGMP snooping proxy for the device. The default is 5 seconds.

Parameter	Description
Report suppression	Limits the membership report traffic sent to multicast-capable routers on the device. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.
IGMPv3 report suppression	Configures IGMPv3 report suppression and proxy reporting on the device. The default is disabled.

SUMMARY STEPS

1. **configure terminal**
2.
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**Option** / **Description** Command / Purpose **ip igmp snooping** Example: `switch(config-vlan-config)# ip igmp snooping` Enables IGMP snooping for the current VLAN. The default is enabled. **Note** If the global setting is disabled with the no form of this command, IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. If you disable IGMP snooping, Layer 2 multicast frames flood to all modules	

Command or Action		Purpose
Option	**Description**	
ip igmp snooping event-history Example: `switch(config)# ip igmp snooping event-history`	Configures the size of the event history buffer. The default is small.	
ip igmp snooping syslog-threshold percentage Example: `switch(config)# ip igmp snooping syslog-threshold 80`	Configures the syslog threshold of the IGMP snooping table.	
ip igmp snooping link-local-groups-suppression Example: `switch(config)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression for the entire device. The default is enabled.	
ip igmp snooping optimise-multicast-flood Example: `switch(config)# ip igmp snooping optimise-multicast-flood`	Optimizes OMF on all VLANs on the device. The default is enabled.	
ip igmp snooping v3-report-suppression Example: `switch(config)# ip igmp snooping v3-report-suppression`	Configures IGMPv3 report suppression and proxy reporting. The default is disabled for the global command for the entire switch and enabled per VLAN.	
ip igmp snooping report-suppression Example: `switch(config)# ip igmp snooping report-suppression`	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as-is to multicast-capable routers. The default is enabled.	

	Command or Action	Purpose
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Configuring IGMP Snooping Parameters

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

Table 21: IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping on a per-VLAN basis. The default is enabled. If the global setting is disabled, all VLANs are treated as disabled, whether they are enabled or not.
Access group	Filters IGMP packets at the snooping layer. The default is disabled.
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.
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.
Optimise-multicast-flood	Configures optimized multicast flooding (OMF) on specified VLANs. The default is enabled.
Report policy	Filters IGMP packets at the snooping layer. The default is disabled.

Parameter	Description
Snooping querier	Configures a snooping querier on an interface when you do not enable PIM because multicast traffic does not need to be routed. You can also configure the following values for the snooping querier: • timeout—Timeout value for IGMPv2. • interval—Time between query transmissions. • maximum response time—MRT for query messages. • startup count—Number of queries sent at startup. • startup interval—Interval between queries at startup.
Robustness variable	Configures the robustness value for the specified VLANs.
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.
Version	Configures the IGMP version number for the specified VLANs.

Note You configure the IGMP snooping parameters that you want by using this configuration mode; however, the configurations apply only after you specifically create the specified VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan configuration** *vlan-id*
4.
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td>configure terminal
Example:
<pre>switch# configure terminal
switch(config)#</pre></td><td>Enters global configuration mode.</td></tr>
<tr><td>Step 2</td><td>ip igmp snooping
Example:
<pre>switch(config)# ip igmp snooping</pre></td><td>Enables IGMP snooping for the device. The default is enabled.
Note
If the global setting is disabled with the no form of this command, IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. If you disable IGMP snooping, Layer 2 multicast frames flood to all modules.</td></tr>
<tr><td>Step 3</td><td>vlan configuration vlan-id
Example:
<pre>switch(config)# vlan configuration 100
switch(config-vlan-config)#</pre></td><td>Configures a VLAN and enters VLAN configuration mode.</td></tr>
<tr><td>Step 4</td><td><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Command</td><td>Purpose</td></tr>
<tr><td>ip igmp snooping
Example:
<pre>switch(config-vlan-config)#
ip igmp snooping</pre></td><td>Enables IGMP snooping for the current VLAN. The default is enabled.</td></tr>
<tr><td>ip igmp snooping access-group {prefix-list | route-map} policy-name interface interface slot/port
Example:
<pre>switch(config-vlan-config)#
ip igmp snooping access-group
 prefix-list plist interface
 ethernet 2/2</pre></td><td>Configures a filter for IGMP snooping access groups based on a prefix-list or route-map policy.</td></tr>
<tr><td>ip igmp snooping explicit-tracking
Example:</td><td>Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The</td></tr>
</table></td><td></td></tr>
</table>

Command or Action		Purpose
Option	**Description**	
`switch(config-vlan-config)# ip igmp snooping explicit-tracking`	default is enabled on all VLANs.	
ip igmp snooping fast-leave Example: `switch(config-vlan-config)# ip igmp snooping fast-leave`	Supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol. When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port. The default is disabled for all VLANs.	
ip igmp snooping last-member-query-interval *seconds* Example: `switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	Removes the group from the associated VLAN port if no hosts respond to an IGMP query message before the last member query interval expires. Values range from 1 to 25 seconds. The default is 1 second.	
ip igmp snooping link-local-groups-suppression Example: `switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression. 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-config)# ip igmp snooping mrouter interface ethernet 2/1`	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the	

Command or Action		Purpose
Option	**Description**	
	number, such as ethernet slot/port.	
ip igmp snooping optimise-multicast-flood Example: `switch(config-vlan-config)# ip igmp snooping optimise-multicast-flood`	Optimizes OMF on selected VLANs. The default is enabled.	
ip igmp snooping querier *ip-address* Example: `switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106`	Configures a snooping querier when you do not enable PIM because multicast traffic does not need to be routed. The IP address is used as the source in messages.	
ip igmp snooping querier-timeout *seconds* Example: `switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	Configures a snooping querier timeout value for IGMPv2 when you do not enable PIM because multicast traffic does not need to be routed. The default is 255 seconds.	
ip igmp snooping query-interval *seconds* Example: `switch(config-vlan-config)# ip igmp snooping query-interval 120`	Configures a snooping query interval when you do not enable PIM because multicast traffic does not need to be routed. The default value is 125 seconds.	
ip igmp snooping report-policy { **prefix-list** | **route-map** } **policy-name interface** *interface slot/port* Example: `switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 2/4`	Configures a filter for IGMP snooping reports based on a prefix-list or route-map policy.	
ip igmp snooping startup-query-count value	Configures snooping for a number of	

	Command or Action		Purpose
	Option	**Description**	
	Example: `switch(config-vlan-config)# ip igmp snooping startup-query-count 5`	queries sent at startup when you do not enable PIM because multicast traffic does not need to be routed.	
	ip igmp snooping startup-query-interval *seconds* Example: `switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000`	Configures a snooping query interval at startup when you do not enable PIM because multicast traffic does not need to be routed	
	ip igmp snooping robustness-variable value Example: `switch(config-vlan-config)# ip igmp snooping robustness-variable 5`	Configures the robustness value for the specified VLANs. The default value is 2.	
	ip igmp snooping static-group *group-ip-addr* [**source source -ip-addr**] **interface** *interface* Example: `switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 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 version value Example: `switch(config-vlan-config)# ip igmp snooping version 2`	Configures the IGMP version number for the specified VLANs.	
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 look-up mode [**vlan** *vlan-id*]	Displays IGMP snooping lookup mode information by VLAN.
show ip igmp snooping mac-oif [**detail** | **vlan** *vlan-id*]	Displays IGMP snooping static mac oif information by VLAN and by all details
show ip igmp snooping mroute [**vlan** *vlan-id*]	Displays multicast router ports by VLAN.
show ip igmp snooping otv groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*]	Displays IGMP snooping OTV information by VLAN.
show ip igmp snooping querier [**vlan** *vlan-id*]	Displays IGMP snooping queriers by VLAN.
show ip igmp snooping [**vlan** *vlan-id*]	Displays IGMP snooping configuration by VLAN.

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

Displaying IGMP Snooping Statistics

Command	Purpose
show ip igmp snooping statistics [**global** | **vlan** *vlan-id*]	Displays global or per VLAN packet and error counter statistics.

Clearing IGMP Snooping Statistics

You can clear the IGMP snooping statistics using these commands.

Command	Purpose
clear ip igmp snooping statistics vlan	Clears the IGMP snooping statistics.

Configuration Examples for IGMP Snooping

This example shows how to configure the IGMP snooping parameters:

```
configure terminal
ip igmp snooping
vlan configuration 2
ip igmp snooping
ip igmp snooping explicit-tracking
```

```
ip igmp snooping fast-leave
ip igmp snooping last-member-query-interval 3
ip igmp snooping querier 172.20.52.106
ip igmp snooping 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
```

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

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

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

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

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

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

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

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

Additional References

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

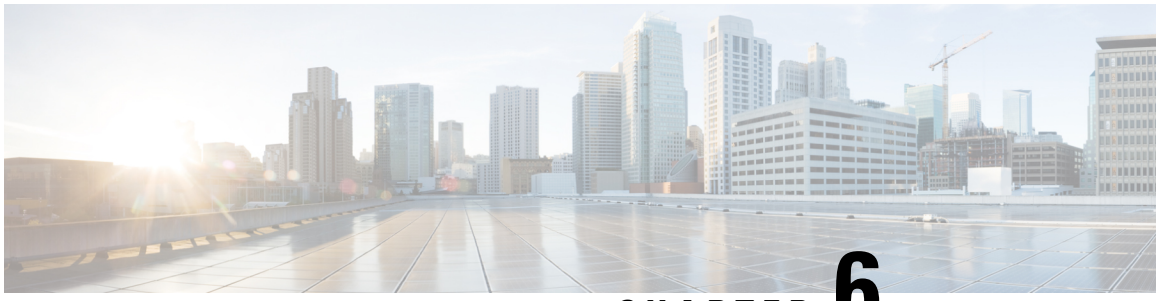
- Standards
- Related Documents

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3548 Switch Multicast Routing 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.	-



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:

- Information About MSDP, on page 97
- Prerequisites for MSDP, on page 99
- Default Settings for MSDP, on page 100
- Configuring MSDP, on page 100
- Verifying the MSDP Configuration, on page 109
- Displaying Statistics, on page 110
- Configuration Examples for MSDP, on page 111
- Additional References, on page 112
- Related Documents, on page 113
- Standards, on page 113

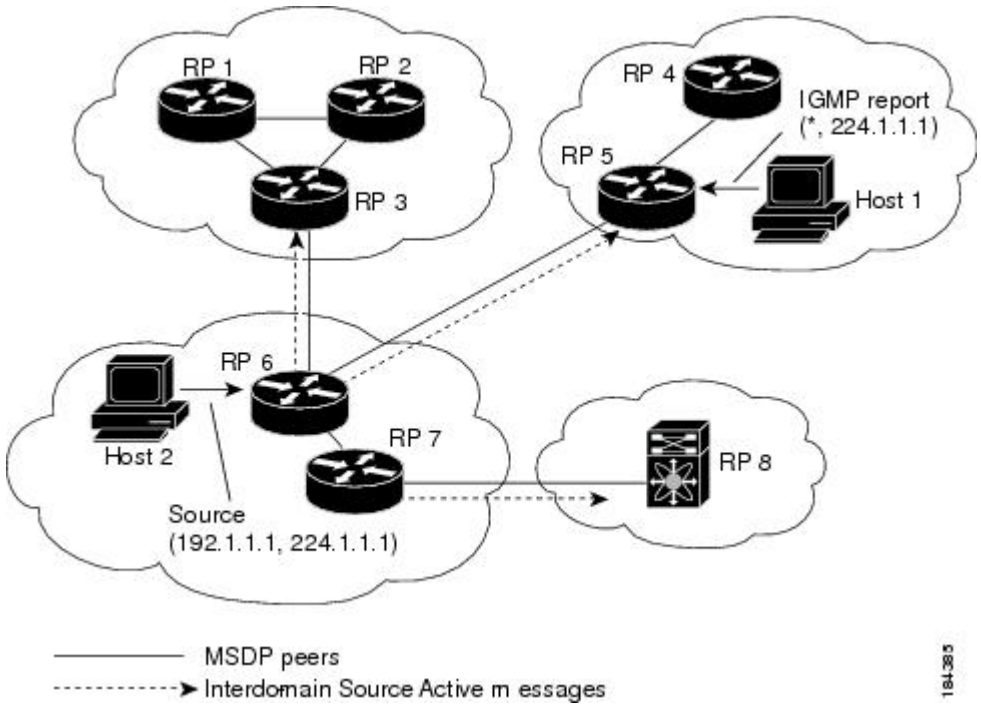
Information About MSDP

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, on page 33 For information about BGP, see the *Cisco Nexus 3548 Switch 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.

Figure 1 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 14: 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 section.

For detailed information about MSDP, see RFC 3618.

SA Messages and Caching

MSDP peers exchange Source-Active (SA) messages that the MSDP software uses 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 6-1, 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

You 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 3548 Switch 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 for MSDP

Table 1 lists the default settings for MSDP parameters.

Table 22: 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:

Step 1 Select the routers to act as MSDP peers.

Step 2 Enable the MSDP feature. See the Enabling the MSDP Feature section.

Step 3 Configure the MSDP peers for each router identified in Step 1. See the Configuring MSDP Peers section.

Step 4 Configure the optional MSDP peer parameters for each MSDP peer. See the Configuring MSDP Peer Parameters section.

Step 5 Configure the optional global parameters for each MSDP peer. See the Configuring MSDP Global Parameters section.

Step 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

SUMMARY STEPS

1. **configure terminal**
2. **feature msdp**
3. (Optional) **show running-configuration** | **grep** *feature*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

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.

SUMMARY STEPS

1. **configure terminal**
2. **ip msdp peer** *peer-ip-address* **connect-source** *interface* [**remote-as** *as-number*]
3. (Optional) **show ip msdp summary** [**vrf** *vrf-name* | **all**]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

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. **Note** Repeat Step 2 for each MSDP peering relationship by changing the peer IP address, the interface, and the AS number as appropriate.
Step 3	(Optional) **show ip msdp summary** [**vrf** *vrf-name*	**all**] **Example:** `switch# show ip msdp summary`	Displays a summary of MSDP peers.
Step 4	(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 Table 2. You configure these parameters in global configuration mode for each peer based on its IP address.

Table 23: MSDP Peer Parameters

Parameter	Description
Description	Description string for the peer. By default, the peer has no description.
Administrative shutdown	Method to shut down the MSDP peer. The configuration settings are not affected by this command. You can use this parameter to allow configuration of multiple parameters to occur before making the peer active. The TCP connection with other peers is terminated by the shutdown. By default, a peer is enabled when it is defined.
MD5 password	MD5-shared password key used for authenticating the peer. By default, no MD5 password is enabled.
SA policy IN	Route-map policy for incoming SA messages. By default, all SA messages are received. **Note** To configure route-map policies, see the *Cisco Nexus 3548 Switch 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 3548 Switch 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 section.

Note For information about configuring mesh groups, see the Configuring MSDP Mesh Groups, on page 107 section.

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **ip msdp description** *peer-ip-address description*
3. **ip msdp shutdown** *peer-ip-address*
4. **ip msdp password** *peer-ip-address password*
5. **ip msdp sa-policy** *peer-ip-address policy-name* **in**
6. **ip msdp sa-policy** *peer-ip-address policy-name* **out**
7. **ip msdp sa-limit** *peer-ip-address limit*
8. (Optional) **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | *known-vrf-name* | **all**]
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

	Command or Action	Purpose
Step 7	**ip msdp sa-limit** *peer-ip-address limit* **Example:** `switch(config)# ip msdp sa-limit 192.168.1.10 5000`	Sets a limit on the number of (S, G) entries accepted from the peer. By default, there is no limit.
Step 8	(Optional) **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | *known-vrf-name* | **all**] **Example:** `switch# show ip msdp peer 192.168.1.10`	Displays detailed MSDP 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 3:

Table 24: 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.

SUMMARY STEPS

1. **configure terminal**
2. **ip msdp originator-id** *interface*

3. **ip msdp group-limit** *limit* **source** *source-prefix*
4. **ip msdp sa-interval** *seconds*
5. (Optional) **show ip msdp summary** [**vrf** *vrf-name* | **all**]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

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.
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 MSDP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves configuration changes.

Remote Multicast Source Support

If multicast traffic is received from a source which is not attached, the (S,G) route is not formed and all traffic continuously hits the CPU. You can enable this feature to avoid sending traffic to the CPU and the traffic is then handled in the hardware with the configured mroute.

When this feature is enabled, static mroute to the source is configured using the **ip mroute** *src-ip next-hop* command and when the prebuild spt is enabled using the **ip pim pre-build-spt** command, the (S,G) route is formed without traffic hitting the CPU. Also, for these sources, register messages are sent periodically and MSDP SA messages are sent to the peer.

SUMMARY STEPS

1. **configure terminal**
2. **ip mfwd mstatic register**
3. (Optional) copy running-config startup-config

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip mfwd mstatic register** **Example:** `switch(config)# ip mfwd mstatic register`	Enables the remote multicast source support.
Step 3	(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 MSDP 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.

SUMMARY STEPS

1. **configure terminal**
2. **ip msdp mesh-group** *peer-ip-addr mesh-name*

3. (Optional) **show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name* | *known-vrf-name* | **all**]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

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. **Note** Repeat Step 2 for each MSDP peer in the mesh by changing the peer IP address.
Step 3	(Optional) **show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name*	*known-vrf-name*	**all**] **Example:** `switch# show ip msdp mesh-group`	Displays information about the MSDP mesh group configuration.
Step 4	(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.

SUMMARY STEPS

1. **restart msdp**
2. **configure terminal**
3. **ip msdp flush-routes**
4. (Optional) **show running-configuration | include flush-routes**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

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.

Command	Description
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 NX-OS Multicast Routing 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 4.

Table 25: 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 5.

Table 26: 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.

Command	Description
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:

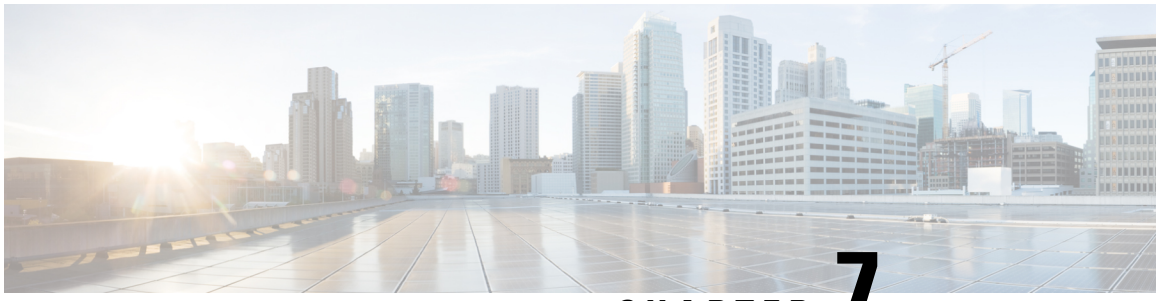
- Related Documents
- Standards
- Appendix A, IETF RFCs for IP Multicast

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3000 Series NX-OS Multicast Routing Comma

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.	-



CHAPTER 7

Configuring Multicast Extranet

This chapter describes how to configure Multicast Extranet on a Cisco NX-OS switch.

This chapter includes the following sections:

- Information About Multicast Extranet, on page 115
- Guidelines and Limitations for Multicast Extranet, on page 115
- Configuring Multicast Extranet, on page 116
- Verifying the Multicast Extranet Configuration, on page 116

Information About Multicast Extranet

In the current NX-OS multicast implementation, multicast traffic can only flow within the same VRF. In the multicast extranet feature, multicast receivers may exist in different VRFs from source in an enterprise network.

With the multicast extranet, the RPF lookup for multicast route in receiver VRF can be done in source VRF, thereby allowing to return a valid RPF interface. This forms a source or RP tree from receiver VRF to source VRF, thus enabling the traffic originated from source VRF to be forwarded to OIFs in receiver VRF.

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

Guidelines and Limitations for Multicast Extranet

Multicast Extranet has the following guidelines and limitations:

- The source and RP should be in the same VRF.
- Multicast NAT and multicast extranet should not coexist for the same group on the same box.
- Auto RP is not supported on multicast extranet.
- The number of multicast routes and VRFs required determine the memory consumption by multicast.
- Multicast VPN (MVPN) extranet is not supported on multicast extranet.
- The RPF lookup will be performed on the VRF specified by the **ip multicast rpf select vrf** command. Fallback mode is not supported.
- For ASM multicast group translation in the fast-pass mode, the static OIF for untranslated groups must be configured on IGMPv2 interface. Source specific static OIF configuration (IGMPv3) is not supported.

Configuring Multicast Extranet

Before you begin

Before you begin, ensure that the PIM is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **ip multicast rpf select vrf** *src-vrf-name* **group-list** *group-range*
3. (Optional) **show ip mroute**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**ip multicast rpf select vrf** *src-vrf-name* **group-list** *group-range* **Example:** `switch(config)# ip multicast rpf select vrf red group-list 224.1.1.0/24`	Supports RPF selection in a different VRF. To disable the support, use the **no** form of this command. **vrf** *src-vrf-name* is the source VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive. **group-list** *group-range* 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 Extranet Configuration

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

Table 27:

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

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)#
```

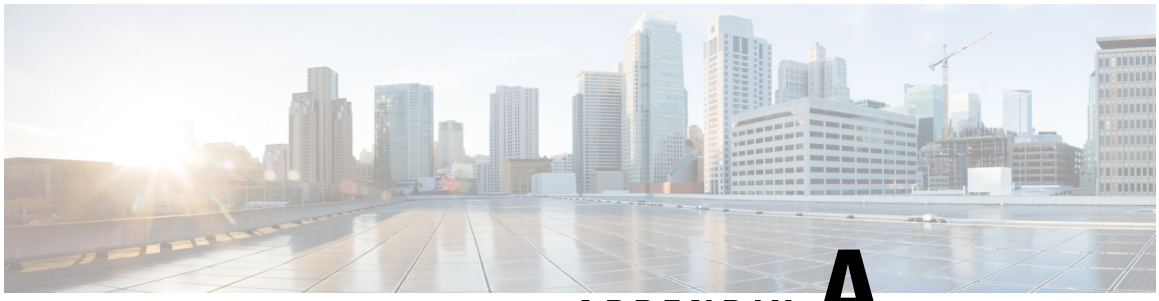
For detailed information about the fields in the output from these commands, see the Cisco Nexus 3000 Series Multicast Routing Command Reference

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3000 Series Multicast Routing 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.	—



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 119

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*

IETF RFCs for IP Multicast