



Cisco IOS XR Multicast Configuration Guide

Cisco IOS XR Software Release 3.6

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

Text Part Number: OL-14354-01

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

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

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

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

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

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

Cisco IOS XR Multicast Configuration Guide
© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface 3v

Implementing Multicast Routing on Cisco IOS XR Software MCC-1

Contents MCC-2

Prerequisites for Implementing Multicast Routing on Cisco IOS XR Software MCC-2

Information About Implementing Multicast Routing on Cisco IOS XR Software MCC-2

Key Protocols and Features Supported in the Cisco IOS XR Software Multicast Routing Implementation MCC-3

Multicast Routing Functional Overview MCC-4

Internet Group Management Protocol and Multicast Listener Discovery MCC-5

Protocol Independent Multicast MCC-7

PIM Shared Tree and Source Tree (Shortest Path Tree) MCC-8

Multicast-Intact MCC-9

Designated Routers MCC-10

Rendezvous Points MCC-11

Auto-RP MCC-12

PIM Bootstrap Router MCC-12

Reverse Path Forwarding MCC-13

Multicast VPN MCC-13

Multicast Source Discovery Protocol MCC-14

Multicast Nonstop Forwarding MCC-15

Multicast Quality of Service MCC-15

Multicast Configuration Submodes MCC-16

Understanding Interface Configuration Inheritance MCC-17

Understanding Enabling and Disabling Interfaces MCC-18

Multicast Routing Information Base MCC-18

Multicast Forwarding Information Base MCC-18

MSDP MD5 Password Authentication MCC-18

How to Implement Multicast on Cisco IOS XR Software MCC-19

Configuring PIM-SM and PIM-SSM MCC-19

Configuring a Static RP and Allowing Backward Compatibility MCC-22

Configuring Auto-RP to Automate Group-to-RP Mappings MCC-24

Configuring the BSR MCC-26

Configuring Multicast Nonstop Forwarding MCC-30

Configuring Multicast VPN	MCC-33
Interconnecting PIM-SM Domains with MSDP	MCC-40
Controlling Source Information on MSDP Peer Routers	MCC-43
Configuring Multicast Quality of Service	MCC-45
Configuring MSDP MD5 Password Authentication	MCC-47
Configuration Examples for Implementing Multicast Routing on Cisco IOS XR Software	MCC-49
MSDP Anycast RP Configuration on Cisco IOS XR Software: Example	MCC-49
Bidir-PIM Configuration on Cisco IOS XR Software: Example	MCC-50
Preventing Auto-RP Messages from Being Forwarded on Cisco IOS XR Software: Example	MCC-51
Inheritance in MSDP on Cisco IOS XR Software: Example	MCC-51
Multicast QoS: Example	MCC-52
Multicast VPN: Example	MCC-52
Additional References	MCC-60
Related Documents	MCC-60
Standards	MCC-60
MIBs	MCC-60
RFCs	MCC-61
Technical Assistance	MCC-61

Index



Preface

The *Cisco IOS XR Multicast Routing Configuration Guide* preface contains the following sections:

- [Changes to This Document](#), page MCC-v
- [Obtaining Documentation and Submitting a Service Request](#), page MCC-v

Changes to This Document

[Table 1](#) lists the technical changes made to this document since it was first printed.

Table 1 *Changes to This Document*

Revision	Date	Change Summary
OL-14354-01	December 2007	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



Implementing Multicast Routing on Cisco IOS XR Software

Multicast routing is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferencing; corporate communications; distance learning; and distribution of software, stock quotes, and news.

This document assumes that you are familiar with IPv4 and IPv6 multicast routing configuration tasks and concepts for Cisco IOS XR software.

Multicast routing allows a host to send packets to a subset of all hosts as a group transmission rather than to a single host, as in unicast transmission, or to all hosts, as in broadcast transmission. The subset of hosts is known as *group members* and are identified by a single multicast group address that falls under the IP Class D address range from 224.0.0.0 through 239.255.255.255.

For detailed conceptual information about multicast routing and complete descriptions of the multicast routing commands listed in this module, you can refer to the [“Related Documents” section on page MCC-54](#). To locate documentation for other commands that might appear in the course of executing a configuration task, search online in the Cisco IOS XR software master command index.

Feature History for Configuring Multicast Routing on Cisco IOS XR Software

Release	Modification
Release 2.0	This feature was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	Support was added for the Cisco XR 12000 Series Router. Support was added for the IPv6 routing protocol on the Cisco CRS-1. Support was added for the bootstrap router (BSR) feature.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	Multicast VPN was supported.
Release 3.6.0	No modification.

Contents

- [Prerequisites for Implementing Multicast Routing on Cisco IOS XR Software](#), page MCC-2
- [Information About Implementing Multicast Routing on Cisco IOS XR Software](#), page MCC-2
- [How to Implement Multicast on Cisco IOS XR Software](#), page MCC-19
- [Configuration Examples for Implementing Multicast Routing on Cisco IOS XR Software](#), page MCC-49
- [Additional References](#), page MCC-54

Prerequisites for Implementing Multicast Routing on Cisco IOS XR Software

The following prerequisites are required to implement multicast routing on your multicast network:

- You must install and activate a Package Installation Envelope (PIE) for the multicast routing software.
For detailed information about optional PIE installation, see *Cisco IOS XR Getting Started Guide*.
- You must be in a user group associated with a task group that includes the proper task IDs for multicast routing commands. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.
- You must be familiar with IPv4 and IPv6 multicast routing configuration tasks and concepts.
- Unicast routing must be operational.

Information About Implementing Multicast Routing on Cisco IOS XR Software

To implement the multicast routing features described in this document you must understand the following concepts:

- [Key Protocols and Features Supported in the Cisco IOS XR Software Multicast Routing Implementation](#), page MCC-3
- [Multicast Routing Functional Overview](#), page MCC-4
- [Internet Group Management Protocol and Multicast Listener Discovery](#), page MCC-5
- [Protocol Independent Multicast](#), page MCC-7
- [PIM Shared Tree and Source Tree \(Shortest Path Tree\)](#), page MCC-8
- [Multicast-Intact](#), page MCC-9
- [Designated Routers](#), page MCC-10
- [Rendezvous Points](#), page MCC-11
- [Auto-RP](#), page MCC-12
- [PIM Bootstrap Router](#), page MCC-12

- [Reverse Path Forwarding](#), page MCC-13
- [Multicast VPN](#), page MCC-13
- [Multicast Source Discovery Protocol](#), page MCC-14
- [Multicast Nonstop Forwarding](#), page MCC-15
- [Multicast Quality of Service](#), page MCC-15
- [Multicast Configuration Submodes](#), page MCC-16
- [Understanding Interface Configuration Inheritance](#), page MCC-17
- [Understanding Enabling and Disabling Interfaces](#), page MCC-18
- [Multicast Routing Information Base](#), page MCC-18
- [Multicast Forwarding Information Base](#), page MCC-18
- [MSDP MD5 Password Authentication](#), page MCC-18

Key Protocols and Features Supported in the Cisco IOS XR Software Multicast Routing Implementation

Table 1 lists the supported features for IPv4 and IPv6 multicast routing in Cisco IOS XR software.

Table 1 Supported Features for IPv4 and IPv6

Feature	IPv4 Support	IPv6 Support
Dynamic host registration	Yes (IGMP v1/2/3)	Yes (MLD v1/2)
Explicit tracking of hosts, groups, and channels	Yes (IGMP v3)	Yes (MLD v2)
PIM-SM ¹	Yes	Yes
PIM-SSM ²	Yes	Yes
PIM-Bidir ³	No	No
Auto-RP	Yes	No
Multicast VPN	Yes	No
BSR ⁴	Yes	Yes
MSDP ⁵	Yes	No
BGP ⁶	Yes	Yes
Multicast NSF ⁷	Yes	Yes
OOR handling ⁸	Yes	No

1. Protocol Independent Multicast in sparse mode
2. Protocol Independent Multicast in Source-Specific Multicast
3. Protocol Independent Multicast Bidirectional
4. PIM bootstrap router
5. Multicast Source Discovery Protocol
6. Multiprotocol Border Gateway Protocol
7. Nonstop forwarding
8. Out of resource

Multicast Routing Functional Overview

Traditional IP communication allows a host to send packets to a single host (*unicast transmission*) or to all hosts (*broadcast transmission*). Multicast provides a third scheme, allowing a host to send a single data stream to a subset of all hosts (*group transmission*) at about the same time. IP hosts are known as *group members*.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IP unicast packets.

The multicast environment consists of senders and receivers. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

A multicast address is chosen for the receivers in a multicast group. Senders use that group address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it may be very short-lived. Membership in a group can change constantly. A group that has members may have no activity.

Routers use the Internet Group Management Protocol (IGMP) (IPv4) and Multicast Listener Discovery (MLD) (IPv6) to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending IGMP or MLD report messages.

Many multimedia applications involve multiple participants. Multicast is naturally suitable for this communication paradigm.

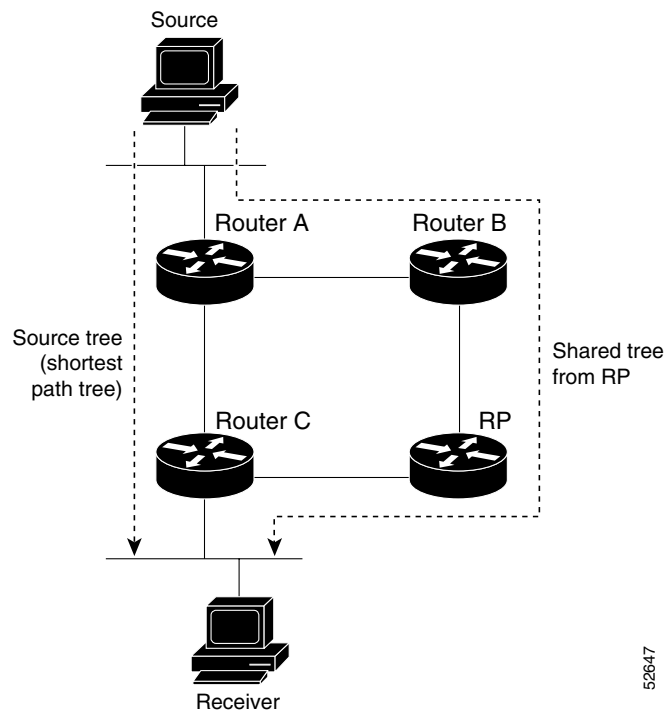
Cisco IOS XR Multicast Routing Implementation

Cisco IOS XR software supports the following protocols to implement multicast routing:

- IGMP and MLD are used (depending on the IP protocol) between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members.
- Protocol Independent Multicast in sparse mode (PIM-SM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses), to an IP multicast address.
- PIM-SSM is made possible by IGMPv3 and MLDv2. Hosts can now indicate interest in specific sources using IGMPv3 and MLDv2. SSM does not require a rendezvous point (RP) to operate.

Figure 1 shows IGMP/MLD and PIM-SM operating in a multicast environment.

Figure 1 Multicast Routing Protocols Supported for Cisco IOS XR Software



Internet Group Management Protocol and Multicast Listener Discovery

Cisco IOS XR software provides support for the following protocols:

- Internet Group Management Protocol (IGMP) over IPv4, and
- Multicast Listener Discovery (MLD) over IPv6.

IGMP and MLD provide a means for hosts to indicate which multicast traffic they are interested in and for routers to control and limit the flow of multicast traffic throughout the network. Routers build state by means of IGMP and MLD messages; that is, router queries and host reports.

A set of queries and hosts that receive multicast data streams from the same source is called a *multicast group*. Hosts use IGMP and MLD messages to join and leave multicast groups.



Note

IGMP messages use group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is guaranteed not to be assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

IGMP and MLD Versions

The following points describe IGMP versions 1, 2, and 3:

- IGMP Version 1 provides for the basic query-response mechanism that allows the multicast router to determine which multicast groups are active and for other processes that enable hosts to join and leave a multicast group.

- IGMP Version 2 extends IGMP allowing such features as the IGMP query timeout and the maximum query-response time. See RFC 2236.

**Note**

MLDv1 provides the same functionality (under IPv6) as IGMP Version 2.

- IGMP Version 3 permits joins and leaves for certain source and group pairs instead of requesting traffic from all sources in the multicast group.

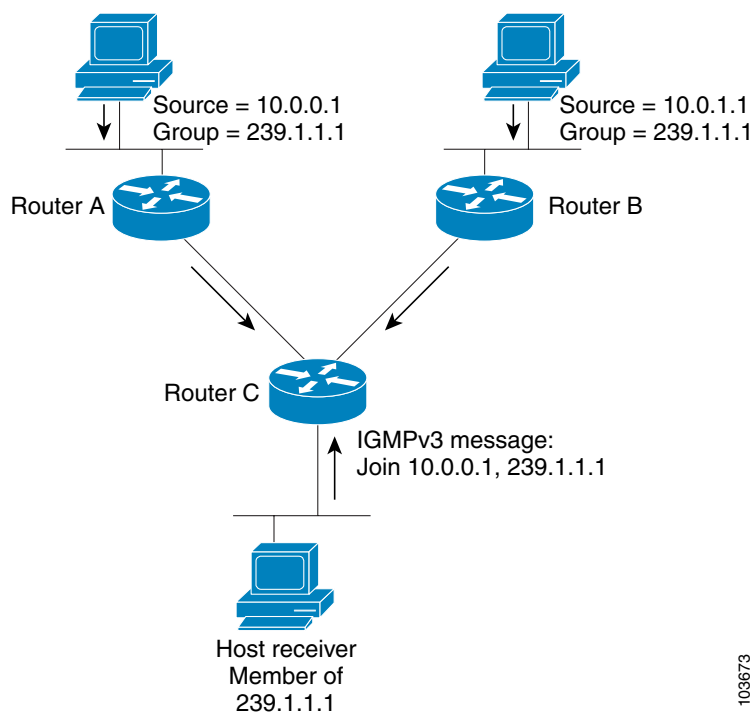
**Note**

MLDv2 provides the same functionality (under IPv6) as IGMP Version 3.

IGMP Routing Example

Figure 2 illustrates two sources, 10.0.0.1 and 10.0.1.1, that are multicasting to group 239.1.1.1. The receiver wants to receive traffic addressed to group 239.1.1.1 from source 10.0.0.1 but not from source 10.0.1.1. The host must send an IGMPv3 message containing a list of sources and groups (S, G) that it wants to join and a list of sources and groups (S, G) that it wants to leave. Router C can now use this information to prune traffic from Source 10.0.1.1 so that only Source 10.0.0.1 traffic is being delivered to Router C.

Figure 2 IGMPv3 Signaling

**Note**

When configuring IGMP, ensure that all systems on the subnet support the same IGMP version. The router does not automatically detect Version 1 systems. Configure the router for Version 2 if your hosts do not support Version 3.

Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a routing protocol designed to send and receive multicast routing updates. Proper operation of multicast depends on knowing the unicast paths towards a source or an RP. PIM relies on unicast routing protocols to derive this Reverse Path Forwarding (RPF) information. As the name PIM implies, it functions independently of the unicast protocols being used. PIM relies on the Routing Information Base (RIB) for RPF information. If the multicast subsequent address family identifier (SAFI) is configured for Border Gateway Protocol (BGP), or if multicast intact is configured, a separate multicast unicast RIB is created and populated with the BGP multicast SAFI routes, the intact information, and any IGP information in the unicast RIB. Otherwise, PIM gets information directly from the unicast SAFI RIB. Both multicast unicast and unicast databases are outside of the scope of PIM.

The Cisco IOS XR implementation of PIM is based on RFC 4601 *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*. For more information, see RFC 4601 and the *Protocol Independent Multicast (PIM): Motivation and Architecture* Internet Engineering Task Force (IETF) Internet draft.

**Note**

Cisco IOS XR software supports PIM-SM, PIM-SSM, PIM Bidir, and PIM Version 2 only. PIM Version 1 hello messages that arrive from neighbors are rejected.

PIM-Sparse Mode

Typically, PIM in sparse mode (PIM-SM) operation is used in a multicast network when relatively few routers are involved in each multicast. Routers do not forward multicast packets for a group, unless there is an explicit request for traffic. Requests are accomplished using PIM join messages, which are sent hop by hop toward the root node of the tree. The root node of a tree in PIM-SM is the rendezvous point (RP) in the case of a shared tree or the first-hop router that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups, and the sources that send multicast packets are registered with the RP by the first-hop router of the source.

As a PIM join travels up the tree, routers along the path set up the multicast forwarding state so that the requested multicast traffic is forwarded back down the tree. When multicast traffic is no longer needed, a router sends a PIM prune message up the tree toward the root node to prune (or remove) the unnecessary traffic. As this PIM prune travels hop by hop up the tree, each router updates its forwarding state appropriately. Ultimately, the forwarding state associated with a multicast group or source is removed. Additionally, if prunes are not explicitly sent, the PIM state will timeout and be removed in the absence of any further join messages.

PIM-SM is the best choice for multicast networks that have potential members at the end of WAN links.

PIM-Source Specific Multicast

PIM-SSM is derived from PIM-SM. However, where PIM-SM allows for the data transmission of all sources sending to a particular group in response to PIM join messages, the SSM feature forwards traffic to receivers only from those sources that the receivers have explicitly joined. Because PIM joins and prunes are sent directly towards the source sending traffic, an RP and shared trees are unnecessary and are disallowed. SSM is used to optimize bandwidth utilization and deny unwanted Internet broadcast traffic. The source is provided by interested receivers through IGMPv3 membership reports.

In SSM, delivery of datagrams is based on (S,G) channels. Traffic for one (S,G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems receive traffic by becoming members of the (S,G) channel. Signaling is not required,

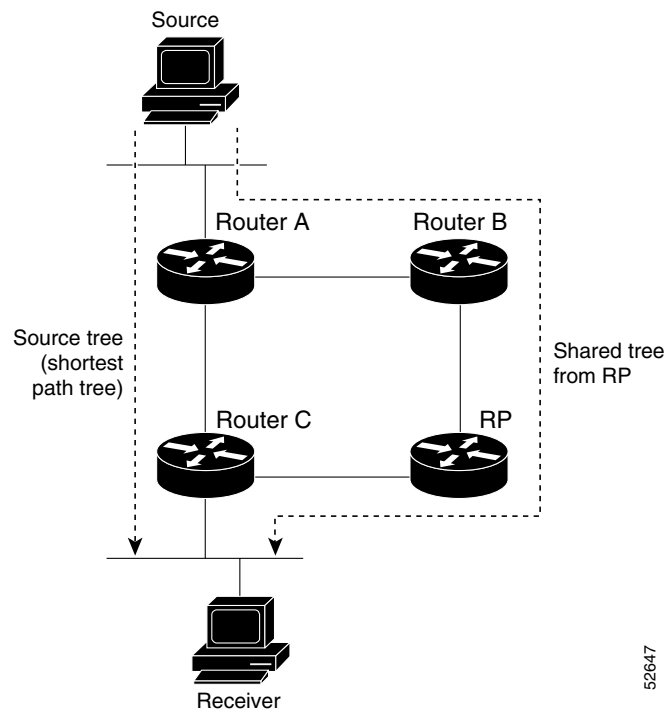
but receivers must subscribe or unsubscribe to (S,G) channels to receive or not receive traffic from specific sources. Channel subscription signaling uses IGMP to include mode membership reports, which are supported only in Version 3 of IGMP (IGMPv3).

To run SSM with IGMPv3, SSM must be supported on the multicast router, the host where the application is running, and the application itself. Cisco IOS XR software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use addresses in the SSM range, unless the application is modified to use explicit (S,G) channel subscription.

PIM Shared Tree and Source Tree (Shortest Path Tree)

In PIM-SM, the rendezvous point (RP) is used to bridge sources sending data to a particular group with receivers sending joins for that group. In the initial setup of state, interested receivers receive data from senders to the group across a single data distribution tree rooted at the RP. This type of distribution tree is called a shared tree or rendezvous point tree (RPT) as illustrated in [Figure 3](#). Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

Figure 3 Shared Tree and Source Tree (Shortest Path Tree)



Unless the `spt-threshold infinity` command is configured, this initial state gives way as soon as traffic is received on the leaf routers (designated router closest to the host receivers). When the leaf router receives traffic from the RP on the RPT, the router initiates a switch to a data distribution tree rooted at the source sending traffic. This type of distribution tree is called a *shortest path tree* or *source tree*. By default, the Cisco IOS XR software switches to a source tree when it receives the first data packet from a source.

The following process describes the move from shared tree to source tree in more detail:

1. Receiver joins a group; leaf Router C sends a join message toward RP.
2. RP puts link to Router C in its outgoing interface list.
3. Source sends data; Router A encapsulates data in Register and sends it to RP.
4. RP forwards data down the shared tree to Router C and sends a join message toward Source. At this point, data may arrive twice at the RP, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at RP, RP sends a register-stop message to Router A.
6. By default, receipt of the first data packet prompts Router C to send a join message toward Source.
7. When Router C receives data on (S,G), it sends a prune message for Source up the shared tree.
8. RP deletes the link to Router C from outgoing interface of (S,G). RP triggers a prune message toward Source.

Join and prune messages are sent for sources and RPs. They are sent hop by hop and are processed by each PIM router along the path to the source or RP. Register and register-stop messages are not sent hop by hop. They are exchanged using direct unicast communication between the designated router that is directly connected to a source and the RP for the group.

**Tip**

The **spt-threshold infinity** command lets you configure the router so that it never switches to the shortest path tree (SPT).

Multicast-Intact

The multicast-intact feature provides the ability to run multicast routing (PIM) when Interior Gateway Protocol (IGP) shortcuts are configured and active on the router. Both Open Shortest Path First version 2 (OSPFv2) and Intermediate System-to-Intermediate System (IS-IS) support the multicast-intact feature. Multiprotocol Label Switching Traffic Engineering (MPLS-TE) and IP multicast coexistence is supported in Cisco IOS XR software by using the **mpls traffic-eng multicast-intact IS-IS** or **OSPF** router command. See *Cisco IOS XR Routing Configuration Guide* for information on configuring multicast intact using IS-IS and OSPF commands.

You can enable multicast-intact in the IGP when multicast routing protocols (PIM) are configured and IGP shortcuts are configured on the router. IGP shortcuts are MPLS tunnels that are exposed to IGP. The IGPs route the IP traffic over these tunnels to destinations that are downstream from the egress router of the tunnel (from an SPF perspective). PIM cannot use IGP shortcuts for propagating PIM joins because reverse path forwarding (RPF) cannot work across a unidirectional tunnel.

When you enable multicast-intact on an IGP, the IGP publishes a parallel or alternate set of equal-cost next-hops for use by PIM. These next-hops are called *mcast-intact next-hops*. The *mcast-intact next-hops* have the following attributes:

- They are guaranteed not to contain any IGP shortcuts.
- They are not used for unicast routing but are used only by PIM to look up an IPv4 next hop to a PIM source.
- They are not published to the Forwarding Information Base (FIB).
- When multicast-intact is enabled on an IGP, all IPv4 destinations that were learned through link-state advertisements are published with a set equal-cost mcast-intact next-hops to the RIB. This attribute applies even when the native next-hops have no IGP shortcuts.

- In IS-IS, the max-paths limit is applied by counting both the native and mcast-intact next-hops together. (In OSPFv2, the behavior is slightly different.)

Designated Routers

Cisco routers use PIM-SM to forward multicast traffic and follow an election process to select a designated router (DR) when there is more than one router on a LAN segment.

The designated router is responsible for sending PIM register and PIM join and prune messages toward the RP to inform it about host group membership.

If there are multiple PIM-SM routers on a LAN, a designated router must be elected to avoid duplicating multicast traffic for connected hosts. The PIM router with the highest IP address becomes the DR for the LAN unless you choose to force the DR election by use of the **dr-priority** command. The DR priority option allows you to specify the DR priority of each router on the LAN segment (default priority = 1) so that the router with the highest priority is elected as the DR. If all routers on the LAN segment have the same priority, the highest IP address is again used as the tiebreaker.

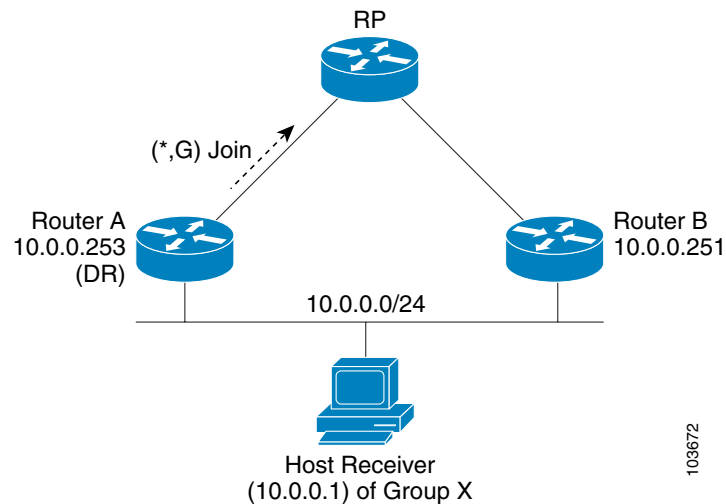
Figure 4 illustrates what happens on a multiaccess segment. Router A (10.0.0.253) and Router B (10.0.0.251) are connected to a common multiaccess Ethernet segment with Host A (10.0.0.1) as an active receiver for Group A. As the Explicit Join model is used, only Router A, operating as the DR, sends joins to the RP to construct the shared tree for Group A. If Router B were also permitted to send (*, G) joins to the RP, parallel paths would be created and Host A would receive duplicate multicast traffic. When Host A begins to source multicast traffic to the group, the DR's responsibility is to send register messages to the RP. Again, if both routers were assigned the responsibility, the RP would receive duplicate multicast packets.

If the DR fails, the PIM-SM provides a way to detect the failure of Router A and to elect a failover DR. If the DR (Router A) were to become inoperable, Router B would detect this situation when its neighbor adjacency with Router A timed out. Because Router B has been hearing IGMP membership reports from Host A, it already has IGMP state for Group A on this interface and immediately sends a join to the RP when it becomes the new DR. This step reestablishes traffic flow down a new branch of the shared tree using Router B. Additionally, if Host A were sourcing traffic, Router B would initiate a new *register* process immediately after receiving the next multicast packet from Host A. This action would trigger the RP to join the SPT to Host A, using a new branch through Router B.



Tip

Two PIM routers are neighbors if there is a direct connection between them. To display your PIM neighbors, use the **show pim neighbor EXEC** command.

Figure 4 Designated Router Election on a Multiaccess Segment**Note**

DR election process is required only on multiaccess LANs. The last-hop router directly connected to the host is the DR.

Rendezvous Points

When PIM is configured in sparse mode, you must choose one or more routers to operate as a rendezvous point (RP). A rendezvous point is a single common root placed at a chosen point of a shared distribution tree, as illustrated in [Figure 3](#). A rendezvous point can be either configured statically in each box or learned through a dynamic mechanism.

PIM DRs forward data from directly connected multicast sources to the rendezvous point for distribution *down* the shared tree. Data is forwarded to the rendezvous point in one of two ways:

- Encapsulated in register packets and unicast directly to the rendezvous point by the first-hop router operating as the DR.
- Multicast forwarded by the RPF forwarding algorithm, described in the [“Reverse Path Forwarding” section on page MCC-13](#), if the rendezvous point has itself joined the source tree.

The rendezvous point address is used by first-hop routers to send PIM register messages on behalf of a host sending a packet to the group. The rendezvous point address is also used by last-hop routers to send PIM join and prune messages to the rendezvous point to inform it about group membership. You must configure the rendezvous point address on all routers (including the rendezvous point router).

A PIM router can be a rendezvous point for more than one group. Only one rendezvous point address can be used at a time within a PIM domain. The conditions specified by the access list determine for which groups the router is a rendezvous point.

You can manually configure a PIM router to function as a rendezvous point or allow the rendezvous point to learn group-to-RP mappings automatically by configuring Auto-RP or BSR (see the [“Auto-RP” section on page MCC-12](#) and [“PIM Bootstrap Router” section on page MCC-12](#)).

Auto-RP

Automatic route processing (Auto-RP) is a feature that automates the distribution of group-to-RP mappings in a PIM network. This feature has the following benefits:

- It is easy to use multiple RPs within a network to serve different group ranges.
- It allows load splitting among different RPs and arrangement of RPs according to the location of group participants.
- It avoids inconsistent, manual RP configurations that can cause connectivity problems.

Multiple RPs can be used to serve different group ranges or to serve as hot backups of each other. To ensure that Auto-RP functions, configure routers as candidate RPs so that they can announce their interest in operating as the RP for certain group ranges. Additionally, a router must be designated as an *RP-mapping agent* that receives the RP-announcement messages from the candidate RPs and arbitrates conflicts. The RP-mapping agent sends the consistent group-to-RP mappings to all remaining routers. Thus, all routers automatically discover which RP to use for the groups they support.



Tip

By default, if a given group address is covered by group-to-RP mappings from both static RP configuration and is discovered using Auto-RP or PIM BSR, the Auto-RP or PIM BSR range is preferred. To override the default to use RP mapping only, use the **rp-address override** keyword.



Note

If you configure PIM in sparse mode and do not configure Auto-RP, you must statically configure an RP as described in the [“Configuring a Static RP and Allowing Backward Compatibility”](#) section on page MCC-22.

When router interfaces are configured in sparse mode, Auto-RP can still be used if all routers are configured with a static RP address for the Auto-RP groups.



Note

Auto-RP is supported in the IPv4 address family only.

PIM Bootstrap Router

The PIM bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism that simplifies the Auto-RP process. This feature is enabled by default allowing routers to dynamically learn the group-to-RP mappings.

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function accomplished by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP on Cisco routers.

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is elected among the candidate BSRs automatically. Candidates use bootstrap messages to discover which BSR has the highest priority. The candidate with the highest priority sends an announcement to all PIM routers in the PIM domain that it is the BSR.

Routers that are configured as candidate RPs unicast to the BSR the group range for which they are responsible. The BSR includes this information in its bootstrap messages and disseminates it to all PIM routers in the domain. Based on this information, all routers are able to map multicast groups to specific RPs. As long as a router is receiving the bootstrap message, it has a current RP map.

Reverse Path Forwarding

RPF is an algorithm used for forwarding multicast datagrams. It functions as follows:

- If a router receives a datagram on an interface it uses to send unicast packets to the source, the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a router forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM uses both source trees and RP-rooted shared trees to forward datagrams; the RPF check is performed differently for each, as follows:

- If a PIM router has source-tree state (that is, an (S,G) entry is present in the multicast routing table), the router performs the RPF check against the IP address of the source of the multicast packet.
- If a PIM router has shared-tree state (and no explicit source-tree state), it performs the RPF check on the address of the RP (which is known when members join the group).

Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S,G) joins (which are source-tree states) are sent toward the source. (*,G) joins (which are shared-tree states) are sent toward the RP.

Multicast VPN

The Multicast VPN (MVPN) feature is based on the multicast domain (MD) concept in which provider edge (PE) routers establish virtual PIM neighbor connections with other PE routers connected to the same customer VPN, forming a secure, virtual multicast domain over the provider network. Multicast traffic is transmitted across the core network from one site to another, as if the traffic were going through a dedicated provider network. Separate multicast routing and forwarding tables are maintained for each individual VPN routing and forwarding (VRF) instance. Traffic is sent through VPN tunnels across the service provider backbone.

MVPN is supported on Generic Routing Encapsulation (GRE) tunnels over the service provider network. Multicast is supported in this release.

Multicast VPN Routing and Forwarding

Dedicated multicast routing and forwarding tables are created for each VPN to separate traffic in one VPN from another VPN. The VPN-specific multicast routing and forwarding database is referred to as MVRF. On a PE router, an MVRF is created when multicast is enabled for a VRF. Protocol Independent Multicast (PIM), and Internet Group Management Protocol (IGMP) protocols run in the context of MVRF, and all routes created by a MVRF protocol instance are associated with the corresponding MVRF. In addition to VRFs, which hold VPN-specific protocol states, a PE router always has a global VRF containing all the routing and forwarding information for the provider network.

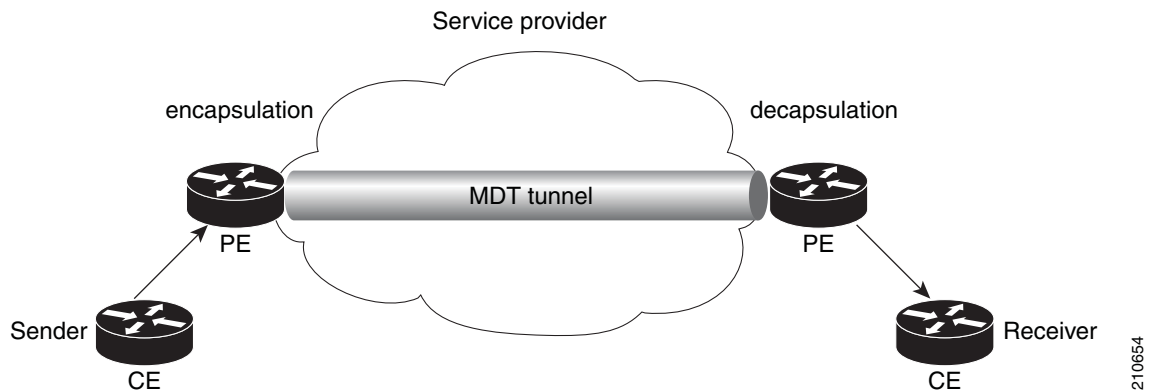
Multicast Distribution Tree Tunnels

The multicast distribution tree (MDT) can span multiple customer sites and the provider network, allowing traffic to flow from one source to multiple receivers.

Secure data transmission is achieved by encapsulating multicast packets in a provider header from the sending customer edge (CE) router at the ingress PE router and transmitting the packets across the core. At the egress PE router, the encapsulated packets are decapsulated then sent to the CE receiving routers.

Multicast distribution tree (MDT) tunnels are point-to-multipoint. Packets sent to an MDT tunnel interface are received by multiple receiving routers. Packets sent to an MDT tunnel interface are encapsulated, and packets received from a MDT tunnel interface are decapsulated. [Figure 5](#) shows a virtual peer connection between two PE routers over an MDT tunnel interface.

Figure 5 Virtual PIM Peer Connection over an MDT Tunnel Interface



Encapsulating multicast packets in a provider header allows PE routers to be unaware of the packet origin—all VPN packets passing through the provider network are viewed as native multicast packets and are routed based on the routing information in the core network. PE routers only need to support native multicast routing to support MVPN.

MVPN also supports optimized VPN traffic forwarding for high-bandwidth applications that have sparsely distributed receivers. A dedicated multicast group can be used to encapsulate packets from a specific source, and an optimized MDT can be created to send traffic only to PE routers with interested receivers.

BGP Requirements

PE routers are the only routers that need to be MVPN-aware and able to signal remote PEs with information regarding the MVPN. It is fundamental that all PE routers have a BGP relationship with each other, either directly or through a route reflector because the PE routers use the BGP peering address information to derive the RPF PE peer within a given VRF. Also, PIM-SSM MDT tunnels cannot be set up without the BGP MDT address-family configured because PIM-SSM MDT tunnels are established using the BGP connector attribute.

See the *Implementing BGP on Cisco IOS XR Software* module of *Cisco IOS XR Routing Configuration Guide* for information on BGP support for Multicast VPN.

Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains.

An RP in a PIM-SM domain has MSDP peering relationships with MSDP-enabled routers in other domains. Each peering relationship occurs over a TCP connection, which is maintained by the underlying routing system.

MSDP speakers exchange messages called Source Active (SA) messages. When an RP learns about a local active source, typically through a PIM register message, the MSDP process encapsulates the register in an SA message and forwards the information to its peers. The message contains the source and group information for the multicast flow, as well as any encapsulated data. If a neighboring RP has local joiners for the multicast group, the RP installs the S, G route, forwards the encapsulated data contained in the SA message, and sends PIM joins back towards the source. This process describes how a multicast path can be built between domains.

**Note**

Although you should configure BGP or Multiprotocol BGP for optimal MSDP interdomain operation, these features are not considered necessary in the Cisco IOS XR software implementation. For information about how BGP or Multiprotocol BGP may be used with MSDP, see the MSDP RPF rules listed in the *Multicast Source Discovery Protocol (MSDP)*, Internet Engineering Task Force (IETF) Internet draft.

Multicast Nonstop Forwarding

The Cisco IOS XR nonstop forwarding (NSF) feature for multicast enhances high availability (HA) of multicast packet forwarding. NSF prevents hardware or software failures on the control plane from disrupting the forwarding of existing packet flows through the router.

How does multicast NSF work? The contents of the Multicast Forwarding Information Base (MFIB) are frozen during a control plane failure. Subsequently, PIM attempts to recover normal protocol processing and state before the neighboring routers time out the PIM hello neighbor adjacency for the problematic router. This behavior prevents the NSF-capable router from being transferred to neighbors that will otherwise detect the failure through the timed-out adjacency. Routes in MFIB are marked as stale after entering NSF, and traffic continues to be forwarded (based on those routes) until NSF completion. On completion, MRIB notifies MFIB and MFIB performs a mark-and-sweep to synchronize MFIB with the current MRIB route info.

**Note**

Nonstop forwarding is not supported for PIM bidirectional routes. If a PIM or MRIB failure (including RP failover) happens with multicast-routing NSF enabled, PIM bidirectional routes in the MFIBs will be purged immediately and forwarding on these routes stops. Routes are reinstalled and forwarding recommences after NSF recovery has ended. This impacts only bidirectional routes. PIM-SM and PIM-SSM routes are forwarded with NSF during the failure. This exception is designed to prevent possible multicast routing loops from forming when the control plane is not able to participate in the BiDir Designated Forwarder election.

Multicast Quality of Service

Cisco IOS XR software provides for the configuration of multicast quality of service (QoS). When configured on specific interfaces, system-wide, general QoS operations are applied to multicast traffic as well as to general network traffic.

QoS expedites the handling of mission-critical applications, while sharing network resources with noncritical applications. QoS also ensures available bandwidth and minimum delays required by time-sensitive multimedia and voice applications. It also gives network managers control over network applications, improves cost efficiency of WAN connections, and enables advanced differentiated services.

For supported multicast QoS commands and general QoS commands, refer to *Cisco IOS XR Modular Quality of Service Command Reference*.

Multicast Configuration Submodes

Cisco IOS XR software moves control plane CLI configurations to protocol-specific submodes to provide mechanisms for enabling, disabling, and configuring multicast features on a large number of interfaces.

The Cisco IOS XR software allows you to issue most commands available under submodes as one single command string from global configuration mode.

For example, the **ssm** command could be executed from the multicast-routing configuration submode like this:

```
RP/0/RP0/CPU0:router(config)# multicast-routing  
RP/0/RP0/CPU0:router(config-mcast-ipv4)# ssm range
```

Alternatively, you could issue the same command from global configuration mode like this:

```
RP/0/RP0/CPU0:router(config)# multicast-routing ssm range
```

The following multicast protocol-specific submodes are available through these configuration submodes:

- [Multicast-routing Configuration Submode, page MCC-16](#)
- [Router PIM Configuration Submode, page MCC-16](#)
- [Router IGMP Configuration Submode, page MCC-16](#)
- [Router MSDP Configuration Submode, page MCC-17](#)

Multicast-routing Configuration Submode

When you issue the **multicast-routing ipv4** or **multicast-routing ipv6** command, all default multicast components (PIM, IGMP, MLD, MFWD, and MRIB) are automatically started, and the CLI prompt changes to “config-mcast-ipv4” or “config-mcast-ipv6”, indicating that you have entered multicast-routing configuration submode.

Router PIM Configuration Submode

When you issue the **router pim** command, the CLI prompt changes to “config-pim-ipv4” indicating that you have entered router pim configuration submode. To enter router pim configuration submode for IPv6, use the **address-family ipv6** keywords with the **router pim** command.

Router IGMP Configuration Submode

When you issue the **router igmp** command, the CLI prompt changes to “config-igmp”, indicating that you have entered router IGMP configuration submode.

Router MLD Configuration Submode

When you issue the **router mld** command, the CLI prompt changes to “config-ml”, indicating that you have entered router MLD configuration submode.

Router MSDP Configuration Submode

When you issue the **router msdp** command, the CLI prompt changes to “config-msdp”, indicating that you have entered router MSDP configuration submode.

Understanding Interface Configuration Inheritance

The Cisco IOS XR software allows you to configure commands for a large number of interfaces by applying command configuration within a multicast routing submode that could be inherited by all interfaces. To override the inheritance mechanism, you can enter interface configuration submode and explicitly enter a different command parameter.

For example, in the following configuration you could quickly specify (under router PIM configuration mode) that all existing and new PIM interfaces on your router will use the hello interval parameter of 420 seconds. However, Packet-over-SONET/SDH (POS) interface 0/1/0/1 overrides the global interface configuration and uses the hello interval time of 210 seconds.

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# hello-interval 420
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# hello-interval 210
```

The following is a listing of commands (specified under the appropriate router submode) that use the inheritance mechanism:

```
multicast-routing
  interface all enable

router pim
  interface all disable
  dr-priority
  hello-interval
  join-prune-interval

router igmp
  interface all router disable
  version
  query-interval
  query-max-response-time
  explicit-tracking

router mld
  interface all disable
  version
  query-interval
  query-max-response-time
  explicit-tracking

router msdp
  connect-source
  sa-filter
  filter-sa-request list
  remote-as
  ttl-threshold
```

Understanding Enabling and Disabling Interfaces

When the Cisco IOS XR multicast routing feature is configured on your router, by default, no interfaces are enabled.

To enable multicast routing and protocols on a single interface or multiple interfaces, you must explicitly enable interfaces using the **interface** command in multicast routing configuration mode.

To set up multicast routing on all interfaces, enter the **interface all** command in multicast routing configuration mode. For any interface to be fully enabled for multicast routing, it must be enabled specifically (or be default) in multicast routing configuration mode, and it must not be disabled in the PIM and IGMP/MLD configuration modes.

For example, in the following configuration, all interfaces are explicitly configured from multicast routing configuration submode:

```
RP/0/RP0/CPU0:router(config)# multicast-routing  
RP/0/RP0/CPU0:router(config-mcast)# interface all enable
```

To disable an interface that was globally configured from the multicast routing configuration submode, enter interface configuration submode, as illustrated in the following example:

```
RP/0/RP0/CPU0:router(config-mcast)# interface pos 0/1/0/0  
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# disable
```

Multicast Routing Information Base

The Multicast Routing Information Base (MRIB) is a protocol-independent multicast routing table that describe a logical network in which one or more multicast routing protocols are running. The tables contain generic multicast routes installed by individual multicast routing protocols. There is an MRIB for every logical network (VPN) in which the router is configured. MRIBs do not redistribute routes among multicast routing protocols; they select the preferred multicast route from comparable ones, and they notify their clients of changes in selected attributes of any multicast route.

Multicast Forwarding Information Base

Multicast Forwarding Information Base (MFIB) is a protocol-independent multicast forwarding system that contains unique multicast forwarding entries for each source or group pair known in a given network. There is a separate MFIB for every logical network (VPN) in which the router is configured. Each MFIB entry resolves a given source or group pair to an incoming interface (IIF) for reverse forwarding (RPF) checking and an outgoing interface list (olist) for multicast forwarding.

MSDP MD5 Password Authentication

MSDP MD5 password authentication is an enhancement to support Message Digest 5 (MD5) signature protection on a TCP connection between two Multicast Source Discovery Protocol (MSDP) peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.

MSDP MD5 password authentication verifies each segment sent on the TCP connection between MSDP peers. The **password** command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified.

**Note**

MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made.

MSDP MD5 password authentication uses an industry-standard MD5 algorithm for improved reliability and security.

How to Implement Multicast on Cisco IOS XR Software

This section contains instructions for the following tasks. The first two tasks are required to configure a basic multicast configuration. The remaining tasks are optional tasks that help you to optimize, debug, and discover the routers in your multicast network.

- [Configuring PIM-SM and PIM-SSM](#), page MCC-19 (required)
- [Configuring a Static RP and Allowing Backward Compatibility](#) (required)
- [Configuring Auto-RP to Automate Group-to-RP Mappings](#), page MCC-24 (optional)
- [Configuring the BSR](#), page MCC-26 (optional)
- [Configuring Multicast Nonstop Forwarding](#), page MCC-30 (optional)
- [Configuring Multicast VPN](#), page MCC-33 (optional)
- [Interconnecting PIM-SM Domains with MSDP](#), page MCC-40 (optional)
- [Controlling Source Information on MSDP Peer Routers](#), page MCC-43 (optional)
- [Configuring Multicast Quality of Service](#), page MCC-45 (optional)
- [Configuring MSDP MD5 Password Authentication](#), page MCC-47 (optional)

Configuring PIM-SM and PIM-SSM

PIM is an efficient IP routing protocol that is “independent” of a routing table, unlike other multicast protocols such as Multicast Open Shortest Path First (MOSPF) or Distance Vector Multicast Routing Protocol (DVMRP).

Cisco IOS XR software supports Protocol Independent Multicast in sparse mode (PIM-SM) and Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM), permitting both to operate on your router at the same time.

This task configures PIM-SM and PIM-SSM.

PIM-SM Operations

PIM in sparse mode operation is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic.

For more information about PIM-SM, see the “[PIM-Sparse Mode](#)” section on page MCC-7.

PIM-SSM Operations

PIM in Source Specific Multicast operation uses information found on source addresses for a multicast group provided by receivers and performs source filtering on traffic.

- By default, PIM-SSM operates in the 232.0.0.0/8 multicast group range for IPv4 and ff3x::/32 (where x is any valid scope) in IPv6. To configure these values, use the **ssm range** command.
- If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers must be upgraded with Cisco IOS XR software that supports the SSM feature.
- No MSDP SA messages within the SSM range are accepted, generated, or forwarded.

For more information about PIM-SSM, see the [“PIM-Source Specific Multicast” section on page MCC-7](#).

Restrictions

Interoperability with SSM

PIM-SM operations within the SSM range of addresses change to PIM-SSM. In this mode, only PIM (S, G) join and prune messages are generated by the router, and no (S,G) RP shared tree or (*,G) shared tree messages are generated.

IGMP Version

To report multicast memberships to neighboring multicast routers, routers use IGMP and all routers on the subnet must be configured with the same version of IGMP.

A router running Cisco IOS XR software does not automatically detect Version 1 systems. You must use the **version** command in router IGMP configuration submode to configure the IGMP version.

MLD Version

To report multicast memberships to neighboring multicast routers, routers use MLD, and all routers on the subnet must be configured with the same version of MLD.

SUMMARY STEPS

1. **configure**
2. **multicast-routing** [address-family {ipv4 | ipv6}]
3. **interface all enable**
4. **exit**
5. **router** {igmp | mld}
6. **version** {1 | 2 | 3}
7. **end**
or
commit
8. **show pim** [ipv4 | ipv6] **group-map** [ip-address-name] [**info-source**]
9. **show pim** [vrf vrf-name] [ipv4 | ipv6] **topology** [source-ip-address [group-ip-address] | **entry-flag** flag | **interface-flag** | **summary**] [**route-count**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	multicast-routing [address-family { ipv4 ipv6 }] Example: RP/0/RP0/CPU0:router(config)# multicast-routing	Enters multicast routing configuration mode. <ul style="list-style-type: none"> The following multicast processes are started: MRIB, MFWD, PIM, IGMP, and MLD. For IPv4, IGMP version 3 is enabled by default; for IPv6, MLD version 1 is enabled by default. For IPv4, use the address-family ipv4 keywords. For IPv6, use the address-family ipv6 keywords.
Step 3	interface all enable Example: RP/0/RP0/CPU0:router(config-mcast-ipv4)# interface all enable	Enables multicast routing and forwarding on all new and existing interfaces.
Step 4	exit Example: RP/0/RP0/CPU0:router(config-mcast-ipv4)# exit	Exits multicast routing configuration mode, and returns the router to the parent configuration mode.
Step 5	router { igmp mls } Example: RP/0/RP0/CPU0:router(config)# router igmp	(Optional) Enters router IGMP or MLD configuration mode.
Step 6	version { 1 2 3 } Example: RP/0/RP0/CPU0:router(config-igmp)# version 3	(Optional) Selects the IGMP or MLD version that the router interface uses. <ul style="list-style-type: none"> The default for IGMP is version 3; the default for MLD is version 1. Host receivers must support IGMPv3 for PIM-SSM operation. If this command is configured in router IGMP or router MLD configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.

	Command or Action	Purpose
Step 7	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config-igmp)# end or RP/0/RP0/CPU0:router(config-igmp)# commit</p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 8	<pre>show pim [ipv4 ipv6] group-map [ip-address-name] [info-source]</pre> <p>Example: RP/0//CPU0:router# show pim ipv4 group-map</p>	(Optional) Displays group-to-PIM mode mapping.
Step 9	<pre>show pim [vrf vrf-name] [ipv4 ipv6] topology [source-ip-address [group-ip-address] entry-flag flag interface-flag summary] [route-count]</pre> <p>Example: RP/0/RP0/CPU0:router# show pim topology</p>	(Optional) Displays PIM topology table information for a specific group or all groups.

Configuring a Static RP and Allowing Backward Compatibility

When PIM is configured in sparse mode, you must choose one or more routers to operate as a rendezvous point (RP) for a multicast group. An RP is a single common root placed at a chosen point of a shared distribution tree. An RP can either be configured statically in each router, or learned through Auto-RP or BSR.

This task configures a static RP. For more information about RPs, see the [“Rendezvous Points” section on page MCC-11](#). For configuration information for Auto-RP, see the [“Configuring Auto-RP to Automate Group-to-RP Mappings” section on page MCC-24](#).

SUMMARY STEPS

1. **configure**
2. **router pim [address-family {ipv4 | ipv6}]**
3. **rp-address ip-address [group-access-list] [bidir] [override]**

4. **old-register-checksum**
5. **exit**
6. **{ipv4 | ipv6} access-list name**
7. **[sequence-number] permit source [source-wildcard]**
8. **end**
or
commit
9. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	router pim [address-family {ipv4 ipv6}] Example: RP/0/RP0/CPU0:router(config)# router pim	Enters router PIM configuration mode.
Step 3	rp-address ip-address [group-access-list] [bidir] [override] Example: RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rp-address 172.16.6.22 rp-access	Assigns an RP to multicast groups. <ul style="list-style-type: none"> • If you specify a <i>group-access-list-number</i> value, you must configure that access list using the ipv4 access-list command.
Step 4	old-register-checksum Example: RP/0/RP0/CPU0:router(config-pim-ipv4)# old-register-checksum	(Optional) Allows backward compatibility on the RP that uses old register checksum methodology.
Step 5	exit Example: RP/0/RP0/CPU0:router(config-pim-ipv4)# exit	Exits PIM configuration mode, and returns the router to the parent configuration mode.
Step 6	{ipv4 ipv6} access-list name Example: RP/0/RP0/CPU0:router(config)# ipv4 access-list rp-access	(Optional) Enters access list configuration mode and configures the RP access list. <ul style="list-style-type: none"> • The access list called “rp-access” permits multicast group 239.1.1.0 0.0.255.255.

	Command or Action	Purpose
Step 7	<pre>[sequence-number] permit source [source-wildcard]</pre> <p>Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 239.1.1.0 0.0.255.255 </p>	<p>(Optional) Permits multicast group 239.1.1.0 0.0.255.255 for the “rp-access” list.</p> <p>Tip The commands in Step 6 and Step 7 can be combined in one command string and entered from global configuration mode like this: ipv4 access-list rp-access permit 239.1.1.0 0.0.255.255.</p>
Step 8	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# end or RP/0/RP0/CPU0:router(config-ipv4-acl)# commit </p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 9	<pre>show version</pre> <p>Example: RP/0/RP0/CPU0:router# show version </p>	<p>Displays the software release version.</p>

Configuring Auto-RP to Automate Group-to-RP Mappings

This task configures the Auto-RP mechanism to automate the distribution of group-to-RP mappings in your network. In a network running Auto-RP, at least one router must operate as an RP candidate and another router must operate as an RP mapping agent.

For more information about Auto-RP, see the [“Auto-RP” section on page MCC-12](#).

SUMMARY STEPS

1. **configure**
2. **router pim [address-family ipv4]**
3. **auto-rp candidate-rp type instance scope ttl-value [group-list access-list-name] [interval seconds] [bidir]**
4. **auto-rp mapping-agent type number scope ttl-value [interval seconds]**
5. **exit**

6. **ipv4 access-list** *name*
7. [*sequence-number*] **permit** *source* [*source-wildcard*]
8. **end**
or
commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	router pim [address-family ipv4] Example: RP/0/RP0/CPU0:router(config)# router pim	Enters router PIM configuration mode.
Step 3	auto-rp candidate-rp <i>type instance scope</i> <i>t1l-value</i> [group-list <i>access-list-name</i>] [interval seconds] [bidir] Example: RP/0/RP0/CPU0:router(config-pim-ipv4)# auto-rp candidate-rp pos 0/1/0/1 scope 31 group-list 2	Configures an RP candidate that sends messages to the CISCO-RP-ANNOUNCE multicast group (224.0.1.39). <ul style="list-style-type: none"> • This example sends RP announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as an RP is the IP address associated with POS interface 0/1/0/1. • Access list 2 designates the groups this router serves as RP. • If you specify group-list, you must configure the optional access-list command.
Step 4	auto-rp mapping-agent <i>type number scope</i> <i>t1l-value</i> [interval seconds] Example: RP/0/RP0/CPU0:router(config-pim-ipv4)# auto-rp mapping-agent pos 0/1/0/1 scope 20	Configures the router to be an RP mapping agent on a specified interface. <ul style="list-style-type: none"> • After the router is configured as an RP mapping agent and determines the RP-to-group mappings through the CISCO-RP-ANNOUNCE (224.0.1.39) group, the router sends the mappings in an Auto-RP discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40). • A PIM DR listens to this well-known group to determine which RP to use. • This example limits Auto-RP discovery messages to 20 hops.
Step 5	exit Example: RP/0/RP0/CPU0:router(config-pim-ipv4)# exit	Exits PIM configuration mode and returns the router to the parent configuration mode.

	Command or Action	Purpose
Step 6	<pre>ipv4 access-list name</pre> <p>Example: RP/0/RP0/CPU0:router(config)# ipv4 access-list 2</p>	(Optional) Defines the RP access list.
Step 7	<pre>[sequence-number] permit source [source-wildcard]</pre> <p>Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 239.1.1.1 0.0.0.0</p>	(Optional) Permits multicast group 239.1.1.1 for the RP access list. Tip The commands in Step 6 and Step 7 can be combined in one command string and entered from global configuration mode like this: ipv4 access-list rp-access permit 239.1.1.1 0.0.0.0
Step 8	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# end or RP/0/RP0/CPU0:router(config-ipv4-acl)# commit</p>	Saves configuration changes. <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring the BSR

This task configures one or more candidate BSRs and a BSR mapping agent. This task also connects and locates the candidate BSRs in the backbone portion of the network.

For more information about BSR see the “PIM Bootstrap Router” section on page MCC-12.

SUMMARY STEPS

1. **configure**
2. **router pim [address-family {ipv4 | ipv6}]**
3. **bsr candidate-bsr ip-address [hash-mask-len length] [priority value]**
4. **bsr candidate-rp ip-address [group-list access-list] [interval seconds] [priority value]**
5. **interface type number**
6. **bsr border**

7. **exit**
8. **exit**
9. **{ ipv4 | ipv6 } access-list name**
10. **[sequence-number] permit source [source-wildcard]**
or
[sequence-number] permit source-prefix dest-prefix
11. **end**
or
commit
12. **clear pim [vrf vrf-name] [ipv4 | ipv6] bsr**
13. **show pim [vrf vrf-name] [ipv4 | ipv6] bsr candidate-rp**
14. **show pim [vrf vrf-name] [ipv4 | ipv6] bsr election**
15. **show pim [vrf vrf-name] [ipv4 | ipv6] bsr rp-cache**
16. **show pim [vrf vrf-name] [ipv4 | ipv6] group-map [ip-address-name] [info-source]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	router pim [address-family { ipv4 ipv6 }] Example: RP/0/RP0/CPU0:router(config)# router pim	Enters router PIM configuration mode.
Step 3	bsr candidate-bsr ip-address [hash-mask-len length] [priority value] Example: RP/0/RP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-bsr 10.0.0.1 hash-mask-len 30	Configures the router to announce its candidacy as a BSR.
Step 4	bsr candidate-rp ip-address [group-list access-list] [interval seconds] [priority value] Example: RP/0/RP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-rp 172.16.0.0 group-list 4	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR. <ul style="list-style-type: none"> • See Step 9 for group list 4 configuration.
Step 5	interface type number Example: RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0	(Optional) Enters interface configuration mode for the PIM protocol.

	Command or Action	Purpose
Step 6	bsr-border Example: RP/0/RP0/CPU0:router(config-pim-ipv4-if)# bsr-border	(Optional) Stops the forwarding of bootstrap router (BSR) messages on a Protocol Independent Multicast (PIM) router interface.
Step 7	exit Example: RP/0/RP0/CPU0:router(config-pim-ipv4-if)# exit	(Optional) Exits PIM interface configuration mode, and returns the router to PIM configuration mode.
Step 8	exit Example: RP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit	Exits PIM configuration mode, and returns the router to global configuration mode.
Step 9	{ ipv4 ipv6 } access-list <i>name</i> Example: RP/0/RP0/CPU0:router(config)# ipv4 access-list 4	(Optional) Defines the candidate group list to the BSR. <ul style="list-style-type: none"> Access list number 4 specifies the group prefix associated with the candidate RP address 172.16.0.0. (See Step 4). This RP is responsible for the groups with the prefix 239.
Step 10	[<i>sequence-number</i>] permit <i>source</i> [<i>source-wildcard</i>] OR [<i>sequence-number</i>] permit <i>source-prefix</i> <i>dest-prefix</i> Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 239.1.1.1 0.255.255.255	(Optional) Permits multicast group 239.1.1.1 for the candidate group list. <p>Tip The commands in Step 6 and Step 7 can be combined in one command string and entered from global configuration mode like this: ipv4 access-list rp-access permit 239.1.1.1 0.255.255.255</p>

	Command or Action	Purpose
Step 11	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# end OR RP/0/RP0/CPU0:router(config-ipv4-acl)# commit </p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 12	<pre>clear pim [vrf vrf-name] [ipv4 ipv6] bsr</pre> <p>Example: RP/0/RP0/CPU0:router# clear pim bsr </p>	<p>(Optional) Clears BSR entries from the PIM RP group mapping cache.</p>
Step 13	<pre>show pim [vrf vrf-name] [ipv4 ipv6] bsr candidate-rp</pre> <p>Example: RP/0/RP0/CPU0:router# show pim bsr candidate-rp </p>	<p>(Optional) Displays PIM candidate RP information for the BSR.</p>
Step 14	<pre>show pim [vrf vrf-name] [ipv4 ipv6] bsr election</pre> <p>Example: RP/0/RP0/CPU0:router# show pim bsr election </p>	<p>(Optional) Displays PIM candidate election information for the BSR.</p>
Step 15	<pre>show pim [vrf vrf-name] [ipv4 ipv6] bsr rp-cache</pre> <p>Example: RP/0/RP0/CPU0:router# show pim bsr rp-cache </p>	<p>(Optional) Displays PIM RP cache information for the BSR.</p>
Step 16	<pre>show pim [vrf vrf-name] [ipv4 ipv6] group-map [ip-address-name] [info-source]</pre> <p>Example: RP/0/RP0/CPU0:router# show pim ipv4 group-map </p>	<p>(Optional) Displays group-to-PIM mode mapping.</p>

Configuring Multicast Nonstop Forwarding

This task configures the nonstop forwarding (NSF) feature for multicast packet forwarding for the purpose of alleviating network failures, or software upgrades and downgrades.

Although we strongly recommend that you use the NSF lifetime default values, the optional [Step 4](#) through [Step 9](#) allow you to modify the NSF timeout values for Protocol Independent Multicast (PIM) and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD). Use these commands when PIM and IGMP or MLD are configured with nondefault interval or query intervals for join and prune operations.

Generally, configure the IGMP NSF and PIM NSF lifetime values to equal or exceed the query or join query interval. For example, if you set the IGMP query interval to 120 seconds, set the IGMP NSF lifetime to 120 seconds (or greater).

If the Cisco IOS XR software control plane does not converge and reconnect after NSF is enabled on your router, multicast packet forwarding continues for up to 15 minutes, then packet forwarding stops.

Prerequisites

For NSF to operate in your multicast network, you must also enable NSF for the unicast protocols (such as IS-IS, OSPF, and BGP) that PIM relies on for Reverse Path Forwarding (RPF) information. See the appropriate configuration modules to learn how to configure NSF for unicast protocols.

SUMMARY STEPS

1. **configure**
2. **multicast-routing** [address-family {ipv4 | ipv6}]
3. **nsf** [lifetime *seconds*]
4. **exit**
5. **router pim** [address-family {ipv4 | ipv6}]
6. **nsf lifetime** *seconds*
7. **exit**
8. **router** {igmp | mld}
9. **nsf lifetime** *seconds*
10. **end**
or
commit
11. **show** {igmp | mld} [old-output] nsf
12. **show mfib** [ipv4 | ipv6] nsf [location *node-id*]
13. **show mrrib** [ipv4 | ipv6] [old-output] nsf
14. **show pim** [ipv4 | ipv6] nsf

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	multicast-routing [address-family { ipv4 ipv6 }] Example: RP/0/RP0/CPU0:router(config)# multicast-routing	Enters multicast routing configuration mode. <ul style="list-style-type: none">The following multicast processes are started: MRIB, MFWD, PIM, IGMP, and MLD.For IPv4, IGMP version 3 is enabled by default; for IPv6, MLD version 1 is enabled by default.
Step 3	nsf [lifetime <i>seconds</i>] Example: RP/0/RP0/CPU0:router(config-mcast)# nsf	Turns on NSF capability for the multicast routing system.
Step 4	exit Example: RP/0/RP0/CPU0:router(config-mcast)# exit	(Optional) Exits multicast routing configuration mode, and returns the router to the parent configuration mode.
Step 5	router pim [address-family { ipv4 ipv6 }] Example: RP/0/RP0/CPU0:router(config)# router pim	(Optional) Enters router PIM configuration mode.
Step 6	nsf lifetime <i>seconds</i> Example: RP/0/RP0/CPU0:router(config-pim-default-ipv4)# nsf lifetime 30	(Optional) Configures the NSF timeout value for multicast forwarding route entries under the PIM process. Note If you configure the PIM hello interval to a nondefault value, configure the PIM NSF lifetime to a value less than the hello hold time. Typically the value of the hold-time field is 3.5 times the interval time value, or 120 seconds if the PIM hello interval time is 30 seconds.
Step 7	exit Example: RRP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit	(Optional) Exits PIM configuration mode and returns the router to the parent configuration mode.
Step 8	router { igmp mld } Example: RP/0/RP0/CPU0:router(config)# router igmp	(Optional) Enters router IGMP or MLD configuration mode.

	Command or Action	Purpose
Step 9	<p>nsf lifetime <i>seconds</i></p> <p>Example: RP/0/RP0/CPU0:router(config-igmp)# nsf lifetime 30</p>	(Optional) Configures the NSF timeout value for multicast forwarding route entries under the IGMP or MLD process.
Step 10	<p>end or commit</p> <p>Example: RP/0/RP0/CPU0:router(config-igmp)# end or RP/0/RP0/CPU0:router(config-igmp)# commit</p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <ul style="list-style-type: none"> Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 11	<p>show {igmp mld} [old-output] nsf</p> <p>Example: RP/0/RP0/CPU0:router# show igmp nsf</p>	(Optional) Displays the state of NSF operation in IGMP or MLD.
Step 12	<p>show mfib [ipv4 ipv6] nsf [location node-id]</p> <p>Example: RP/0/RP0/CPU0:router# show mfib nsf</p>	(Optional) Displays the state of NSF operation for the MFIB line cards.
Step 13	<p>show mrib [ipv4 ipv6] [old-output] nsf</p> <p>Example: RP/0/RP0/CPU0:router# show mrib nsf</p>	(Optional) Displays the state of NSF operation in the MRIB.
Step 14	<p>show pim [ipv4 ipv6] nsf</p> <p>Example: RP/0/RP0/CPU0:router# show pim nsf</p>	(Optional) Displays the state of NSF operation for PIM.

Configuring Multicast VPN

This task configures multicast VPN (MVPN).

Prerequisites

When configuring MVPN, the following prerequisites must be met:

- PIM and multicast forwarding must be configured on all interfaces being used by multicast traffic. In an MVPN, enable PIM and multicast forwarding on the following interfaces using the multicast-routing configuration mode:
 - Physical interface on a provider edge (PE) router that is connected to the backbone.
 - Loopback interface used for BGP peering.
 - Loopback interface used as the source for the sparse PIM rendezvous point router address.

Also, associate MVRFs with interfaces over which they are going to forward multicast traffic.

- BGP should already be configured and operational on all routers that are sending or receiving multicast traffic. Multicast distribution trees (MDTs) must be included in BGP to support the use of MDTs in the network. See the *Configuring an MDT Address Family Session in BGP* section in *Cisco IOS XR Routing Configuration Guide*.
- All provider edge (PE) routers in the multicast domain must be running a Cisco IOS XR software image that supports MVPN.
- PE routers in a VPN appear as PIM neighbors over a virtual multicast distribution tree (MDT) tunnel interface. Therefore, the virtual MDT tunnel interface must be defined in the MVPN configuration. An MDT tunnel interface is created when multicast VPN is configured on a PE router. The creation of the tunnel interface also triggers PIM joins towards the root (a rendezvous point or a source) of the MDT in the provider network and results in the (S,G) or (*,G) state on core routers.
- Global VRF must be defined.
- Each multicast VRF domain must have an associate PIM RP definition.

Restrictions

Intermediate System-to-Intermediate System (IS-IS) is not supported between the PE and customer edge (CE) routers.

Configuring a VRF Entry

This task configures a VRF entry and the route-target extended community.

SUMMARY STEPS

1. **configure**
2. **vrf** *vrf-name*
3. **address-family** {*ipv4* | *ipv6*} **unicast**
4. **import route-target** [*as-number:nn* | *ip-address:nn*]
5. **export route-target** [*as-number:nn* | *ip-address:nn*]

```

6. end
   or
   commit

```

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	vrf vrf-name Example: RP/0/RP0/CPU0:router(config)# vrf vrf_A	Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode.
Step 3	address-family {ipv4 ipv6} unicast Example: RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast	Enters address family configuration mode.
Step 4	import route-target [as-number:nn ip-address:nn] Example: RP/0/RP0/CPU0:router(config-vrf-af)# import route-target 1:1	Configures a VRF import route-target extended community.

	Command or Action	Purpose
Step 5	<pre>export route-target [as-number:nn ip-address:nn]</pre> <p>Example: RP/0/RP0/CPU0:router(config-vrf-af)# export route-target 1:1 </p>	Configures a VRF export route-target extended community.
Step 6	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config)# end or RP/0/RP0/CPU0:router(config)# commit </p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Enabling Multicast VRF Forwarding

This task enables multicast VPN routing and forwarding (VRF) forwarding.

SUMMARY STEPS

- configure**
- multicast-routing** [address-family {ipv4 | ipv6}]
- vrf** vrf-name
- mdt default** mdt-group-address
- mdt data** mdt-group-address/prefix-length **threshold** threshold acl-name
- interface all enable**
- exit**
- vrf default**
- mdt source** type interface-id
- interface all enable**
- end**
or
commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	multicast-routing [address-family {ipv4 ipv6}] Example: RP/0/RP0/CPU0:router(config)# multicast-routing address-family ipv4	Enters multicast routing configuration mode.
Step 3	vrf vrf-name Example: RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# vrf vrf_A	Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode.
Step 4	mdt default mdt-group-address Example: RP/0/RP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt default 172.16.10.1	Specifies the multicast distribution tree (MDT) default group address.
Step 5	mdt data mdt-group-address/prefix-length threshold threshold acl-name Example: RP/0/RP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt data 172.23.2.2/24 threshold 1200 acl_A	Specifies the data MDT group.
Step 6	interface all enable Example: RP/0/RP0/CPU0:router(config-mcast-vrf_A-ipv4)#	Enables multicast routing and forwarding on all new and existing interfaces.
Step 7	exit Example: RP/0/RP0/CPU0:router(config-mcast-vrf_A-ipv4)#	Exits the current configuration mode.
Step 8	vrf default Example: RP/0/RP0/CPU0:router(config-mcast)# vrf default	Enters the default VRF configuration mode.
Step 9	mdt source type interface-id Example: RP/0/RP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt source pos 0/1/0/0	Specifies the MDT source address. Note The MDT source interface name should be the same as the one used for BGP peerings.

	Command or Action	Purpose
Step 10	<pre>interface all enable</pre> <p>Example: RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # interface all enable </p>	Enables multicast routing and forwarding on all new and existing interfaces.
Step 11	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # end or RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # commit </p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Specifying the PIM VRF Instance

This task specifies the PIM VPN routing and forwarding (VRF) instance.

SUMMARY STEPS

- configure**
- router pim vrf** *vrf-name* **address-family** {**ipv4** | **ipv6**}
- rp-address** *ip-address* [*group-access-list-number*] [**bidir**] [**override**]
- end**
or
commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	router pim vrf <i>vrf-name</i> address-family { ipv4 ipv6 } Example: RP/0/RP0/CPU0:router(config)# router pim vrf vrf_A address-family ipv4	Enters PIM configuration mode.
Step 3	rp-address <i>ip-address</i> [<i>group-access-list-number</i>] [bidir] [override] Example: RP/0/RP0/CPU0:router(config-pim-vrf_A-ipv4)# rp-address 10.0.0.0	Configures the PIM RP address.
Step 4	end or commit Example: RP/0/RP0/CPU0:router(config-pim-vrf_A-ipv4)# end or RP/0/RP0/CPU0:router(config-pim-vrf_A-ipv4)# commit	Saves configuration changes. <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Specifying the IGMP VRF Instance

This task specifies the IGMP VPN routing and forwarding (VRF) instance.

SUMMARY STEPS

1. **configure**
2. **router igmp**

3. **vrf** *vrf-name*
4. **end**
or
commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	router igmp Example: RP/0/RP0/CPU0:router(config)# router igmp	Enters IGMP configuration mode.
Step 3	vrf <i>vrf-name</i> Example: RP/0/RP0/CPU0:router(config-igmp)# vrf vrf_B	Configures a VRF instance.
Step 4	end or commit Example: RP/0/RP0/CPU0:router(config-igmp-vrf_B)# end or RP/0/RP0/CPU0:router(config-igmp-vrf_B)# commit	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> – Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Interconnecting PIM-SM Domains with MSDP

To set up an MSDP peering relationship with MSDP-enabled routers in another domain, you configure an MSDP peer to the local router.

If you do not want to have or cannot have a BGP peer in your domain, you could define a default MSDP peer from which to accept all Source-Active (SA) messages.

Finally, you can change the Originator ID when you configure a logical RP on multiple routers in an MSDP mesh group.

Prerequisites

You must configure MSDP default peering, if the addresses of all MSDP peers are not known in BGP or multiprotocol BGP.

SUMMARY STEPS

1. **configure**
2. **interface** *type number*
3. **ipv4 address** *address mask*
4. **end**
5. **router msdp**
6. **default-peer** *ip-address* [**prefix-list** *list*]
7. **originator-id** *type interface-id*
8. **peer** *peer-address*
9. **connect-source** *type interface-id*
10. **mesh-group** *name*
11. **remote-as** *as-number*
12. **end**
or
commit
13. **show msdp** [**ipv4**] **globals**
14. **show msdp** [**ipv4**] **peer** [*peer-address*]
15. **show msdp** [**ipv4**] **rpf** *rpf-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	interface <i>type number</i> Example: RP/0/RP0/CPU0:router(config)# interface loopback 0	(Optional) Enters interface configuration mode to define the IPv4 address for the interface. Note This step is required if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection.
Step 3	ipv4 address <i>address mask</i> Example: RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.1.3 255.255.255.0	(Optional) Defines the IPv4 address for the interface. Note This step is required only if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection. See optional Step 9 for information about configuring the connect-source command.
Step 4	end Example: RP/0/RP0/CPU0:router(config-if)# end	Exits interface configuration mode, and returns the router to global configuration mode.
Step 5	router msdp Example: RP/0/RP0/CPU0:router(config)# router msdp	Enters MSDP protocol configuration mode.
Step 6	default-peer <i>ip-address [prefix-list list]</i> Example: RP/0/RP0/CPU0:router(config-msdp)# default-peer 172.23.16.0	(Optional) Defines a default peer from which to accept all MSDP SA messages.
Step 7	originator-id <i>type interface-id</i> Example: RP/0/RP0/CPU0:router(config-msdp)# originator-id pos 0/1/1/0	(Optional) Allows an MSDP speaker that originates a (Source-Active) SA message to use the IP address of the interface as the RP address in the SA message.
Step 8	peer <i>peer-address</i> Example: RP/0/RP0/CPU0:router(config-msdp)# peer 172.31.1.2	Enters MSDP peer configuration mode and configures an MSDP peer. <ul style="list-style-type: none"> • Configure the router as a BGP neighbor. • If you are also BGP peering with this MSDP peer, use the same IP address for MSDP and BGP. You are not required to run BGP or multiprotocol BGP with the MSDP peer, as long as there is a BGP or multiprotocol BGP path between the MSDP peers.

	Command or Action	Purpose
Step 9	<p>connect-source <i>type interface-id</i></p> <p>Example: RP/0/RP0/CPU0:router(config-msdp-peer)# connect-source loopback 0</p>	(Optional) Configures a source address used for an MSDP connection.
Step 10	<p>mesh-group <i>name</i></p> <p>Example: RP/0/RP0/CPU0:router(config-msdp-peer)# mesh-group internal</p>	(Optional) Configures an MSDP peer to be a member of a mesh group.
Step 11	<p>remote-as <i>as-number</i></p> <p>Example: RP/0/RP0/CPU0:router(config-msdp-peer)# remote-as 250</p>	(Optional) Configures the remote autonomous system number of this peer.
Step 12	<p>end OR commit</p> <p>Example: RP/0/RP0/CPU0:router(config-msdp-peer)# end OR RP/0/RP0/CPU0:router(config-msdp-peer)# commit</p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 13	<p>show msdp [<i>ipv4</i>] globals</p> <p>Example: RP/0/RP0/CPU0:router# show msdp globals</p>	Displays the MSDP global variables.

	Command or Action	Purpose
Step 14	<pre>show msdp [ipv4] peer [peer-address]</pre> <p>Example: RP/0/RP0/CPU0:router# show msdp peer 172.31.1.2 </p>	Displays information about the MSDP peer.
Step 15	<pre>show msdp [ipv4] rpf rpf-address</pre> <p>Example: RP/0/RP0/CPU0:router# show msdp rpf 172.16.10.13 </p>	Displays the RPF lookup.

Controlling Source Information on MSDP Peer Routers

Your MSDP peer router can be customized to control source information that is originated, forwarded, received, cached, and encapsulated.

When originating Source-Active (SA) messages, you can control to whom you will originate source information, based on the source that is requesting information.

When forwarding SA messages you can do the following:

- Filter all source/group pairs
- Specify an extended access list to pass only certain source/group pairs
- Filter based on match criteria in a route map

When receiving SA messages you can do the following:

- Filter all incoming SA messages from an MSDP peer
- Specify an extended access list to pass certain source/group pairs
- Filter based on match criteria in a route map

In addition, you can use time to live (TTL) to control what data is encapsulated in the first SA message for every source. For example, you could limit internal traffic to a TTL of eight hops. If you want other groups to go to external locations, you send those packets with a TTL greater than eight hops.

By default, MSDP automatically sends SA messages to peers when a new member joins a group and wants to receive multicast traffic. You are no longer required to configure an SA request to a specified MSDP peer.

SUMMARY STEPS

1. **configure**
2. **router msdp**
3. **sa-filter {in | out} {ip-address | peer-name} [list access-list-name] [rp-list access-list-name]**
4. **cache-sa-state [list access-list-name] [rp-list access-list-name]**
5. **ttl-threshold ttl-value**
6. **exit**
7. **ipv4 access-list name [sequence-number] permit source [source-wildcard]**

```

8. end
   or
   commit

```

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	router msdp Example: RP/0/RP0/CPU0:router(config)# router msdp	Enters MSDP protocol configuration mode.
Step 3	sa-filter {in out} {ip-address peer-name} [list access-list-name] [rp-list access-list-name] Example: RP/0/RP0/CPU0:router(config-msdp)# sa-filter out router.cisco.com list 100	Configures an incoming or outgoing filter list for messages received from the specified MSDP peer. <ul style="list-style-type: none"> If you specify both the list and rp-list keywords, all conditions must be true to pass any source, group (S, G) pairs in outgoing Source-Active (SA) messages. You must configure the ipv4 access-list command in Step 7. If all match criteria are true, a permit from the route map passes routes through the filter. A deny filters routes. This example allows only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer named router.cisco.com.
Step 4	cache-sa-state [list access-list-name] [rp-list access-list-name] Example: RP/0/RP0/CPU0:router(config-msdp)# cache-sa-state 100	Creates and caches source/group pairs from received Source-Active (SA) messages and controls pairs through access lists.
Step 5	t1-threshold ttl-value Example: RP/0/RP0/CPU0:router(config-msdp)# t1-threshold 8	(Optional) Limits which multicast data is sent in SA messages to an MSDP peer. <ul style="list-style-type: none"> Only multicast packets with an IP header TTL greater than or equal to the <i>ttl-value</i> argument are sent to the MSDP peer specified by the IP address or name. Use this command if you want to use TTL to examine your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, send those packets with a TTL greater than 8. This example configures a TTL threshold of eight hops.

	Command or Action	Purpose
Step 6	<pre>exit</pre> <p>Example: RP/0/RP0/CPU0:router(config-msdp)# exit </p>	Exits the current configuration mode.
Step 7	<pre>ipv4 access-list name [sequence-number] permit source [source-wildcard]</pre> <p>Example: RP/0/RP0/CPU0:router(config)# ipv4 access-list 100 20 permit 239.1.1.1 0.0.0.0 </p>	<p>Defines an IPv4 access list to be used by SA filtering.</p> <ul style="list-style-type: none"> In this example, the access list 100 permits multicast group 239.1.1.1. The ipv4 access-list command is required if the keyword list is configured for SA filtering in Step 3.
Step 8	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# end or RP/0/RP0/CPU0:router(config-ipv4-acl)# commit </p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Multicast Quality of Service

This task describes how to configure multicast QoS to permit system-wide, general QoS operations to apply to multicast traffic on Cisco XR 12000 Series Routers.



Note

There are no commands to specifically enable Multicast QoS on Cisco CRS-1 routers. The commands to configure QoS apply to multicast and unicast. See *Cisco IOS XR Modular Quality of Service Configuration Guide* for information on configuring QoS on Cisco CRS-1 routers.

This single task describes how to enable multicast QoS and assign a priority queue level to the multicast traffic.

**Note**

The following commands apply to Cisco XR 12000 Series Router Engine 3 line cards only: **hw-module qos multicast** and **hw-module qos multicast priorityq disable**. For Engine 5 line cards, there is no requirement for a command to enable QoS. On Engine 5 line cards, multicast QoS behaves like unicast QoS (when a policy is attached to an interface).

**Note**

For supported multicast QoS commands and general QoS commands, refer to *Cisco IOS XR Modular Quality of Service Command Reference*.

SUMMARY STEPS

1. **configure**
2. **hw-module qos multicast [location node-id]**
3. **hw-module qos multicast priorityq disable {location node-id}**
4. **end**
or
commit
5. **show mfib [vrf vrf-name] [ipv4 | ipv6] hardware route {* | source-address | group-address [prefix-length]} location node-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	hw-module qos multicast [location node-id] Example: RP/0/RP0/CPU0:router(config)# hw-module qos multicast POS 0/7/0/3	Enables multicast QoS on an interface.
Step 3	hw-module qos multicast priorityq disable [location node-id] Example: RP/0/RP0/CPU0:router(config)# hw-module qos multicast priorityq disable POS 0/7/0/3	Assigns a QoS priority value on the specified interface and diverts traffic from the priority to the default queue.

	Command or Action	Purpose
Step 4	<pre>end or commit</pre> <p>Example: RP/0/RP0/CPU0:router(config)# end OR RP/0/RP0/CPU0:router(config)# commit</p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 5	<pre>show mfib [vrf vrf-name] [ipv4 ipv6] hardware route {* source-address group-address [/prefix-length]} location node-id</pre> <p>Example: RP/0/RP0/CPU0:router# show mfib hardware route * location 0/1/cpu0</p>	<p>Displays multicast routes configured with multicast QoS and the associated parameters.</p>

Configuring MSDP MD5 Password Authentication

This task describes how to configure Multicast Source Discovery Protocol (MSDP) MD5 password authentication.

SUMMARY STEPS

- configure**
- router msdp**
- peer** *peer-address*
- password** {**clear** | **encrypted**} *password*
- end**
or
commit
- show mfib** [**vrf** *vrf-name*] [**ipv4** | **ipv6**] **hardware route** {***** | *source-address* | *group-address* [/prefix-length]} **location** *node-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure</p> <p>Example: RP/0/RP0/CPU0:router# configure</p>	Enters global configuration mode.
Step 2	<p>router msdp</p> <p>Example: RP/0/RP0/CPU0:router(config)# router msdp</p>	Enters MSDP configuration mode.
Step 3	<p>peer peer-address</p> <p>Example: RP/0/RP0/CPU0:router(config-msdp)# peer 10.0.5.4</p>	Configures the MSDP peer.
Step 4	<p>password {clear encrypted} password</p> <p>Example: RP/0/RP0/CPU0:router(config-msdp-peer)# password encrypted a34bi5m</p>	Configures the password.
Step 5	<p>end OR commit</p> <p>Example: RP/0/RP0/CPU0:router(config-msdp-peer)# end OR RP/0/RP0/CPU0:router(config-msdp-peer)# commit</p>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 6	<p>show mfib [vrf vrf-name] [ipv4 ipv6] hardware route {* source-address group-address [/prefix-length]} location node-id</p> <p>Example: RP/0/RP0/CPU0:router# show mfib hardware route * location 0/1/cpu0</p>	Displays multicast routes configured with multicast QoS and the associated parameters.

Configuration Examples for Implementing Multicast Routing on Cisco IOS XR Software

This section provides the following configuration examples:

- [MSDP Anycast RP Configuration on Cisco IOS XR Software: Example, page MCC-49](#)
- [Bidir-PIM Configuration on Cisco IOS XR Software: Example, page MCC-50](#)
- [Preventing Auto-RP Messages from Being Forwarded on Cisco IOS XR Software: Example, page MCC-51](#)
- [Inheritance in MSDP on Cisco IOS XR Software: Example, page MCC-51](#)
- [Multicast QoS: Example, page MCC-52](#)
- [Multicast VPN: Example, page MCC-52](#)

MSDP Anycast RP Configuration on Cisco IOS XR Software: Example

Anycast RP allows two or more RPs to share the load for source registration and to act as hot backup routers for each other. MSDP is the key protocol that makes Anycast RP possible.

In Anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. Configure the Anycast RP loopback address with a 32-bit mask, making it a host address. Configure all downstream routers to “know” that the Anycast RP loopback address is the IP address of the local RP. IP routing automatically selects the topologically closest RP for each source and receiver.

As a source may register with one RP and receivers may join to a different RP, a method is needed for the RPs to exchange information about active sources. This information exchange is done with MSDP.

In Anycast RP, all the RPs are configured to be MSDP peers of each other. When a source registers with one RP, a Source-Active (SA) message is sent to the other RPs, informing them that there is an active source for a particular multicast group. The result is that each RP knows about the active sources in the area of the other RPs. If any of the RPs fails, IP routing converges and one of the RPs becomes the active RP in more than one area. New sources register with the backup RP, and receivers join the new RP.

Note that the RP is usually needed only to start new sessions with sources and receivers. The RP facilitates the shared tree so that sources and receivers can directly establish a multicast data flow. If a multicast data flow is already directly established between a source and the receiver, an RP failure does not affect that session. Anycast RP ensures that new sessions with sources and receivers can begin at any time.

The following Anycast RP example configures Router A and Router B as Anycast RPs. The Anycast RP IP address assignment is 10.0.0.1.

Router A

```
interface loopback 0
  ipv4 address 10.0.0.1/32
  no shutdown
interface loopback 1
  ipv4 address 10.2.0.1/32
  no shutdown
multicast-routing
  interfaces all enable
router pim
  rp-address 10.0.0.1
router msdp
```

```
connect-source loopback 1
peer 10.2.0.2
```

Router B

```
interface loopback 0
  ipv4 address 10.0.0.1/32
  no shutdown
interface loopback 1
  ipv4 address 10.2.0.2/32
  no shutdown
multicast-routing
  interfaces all enable
router pim
  rp-address 10.0.0.1
router msdp
  connect-source loopback 1
  peer 10.2.0.1
```

Apply the following configuration to all network routers:

```
multicast-routing
router pim
  rp-address 10.0.0.1
```

Bidir-PIM Configuration on Cisco IOS XR Software: Example

An access list on the RP can be used to specify a list of groups to be advertised as bidirectional PIM (bidir-PIM).

The following example shows how to configure an RP for both PIM-SM and the bidir-PIM mode groups. The bidir-PIM groups are configured as 224/8 and 227/8, with the remaining multicast group range (224/4) configured as PIM-SM.

```
interface loopback 0
  ipv4 address 10.0.0.1/24
  no shutdown
interface loopback 1
  ipv4 address 10.2.0.1/24
  no shutdown
ipv4 access-list bidir_acl
  10 permit 224.0.0.0 0.255.255.255 any
  20 permit 225.0.0.0 0.255.255.255 any
multicast-routing
  interface all enable
router pim
  auto-rp mapping-agent loopback 0 scope 15 interval 60
  auto-rp candidate-rp loopback 0 scope 15 group-list bidir_acl interval 60 bidir
  auto-rp candidate-rp loopback 1 scope 15 group-list 224/4 interval 60
```

**Tip**

Issue the **show pim group-map** command and verify the output to ensure that the configured mappings are learned correctly.

Preventing Auto-RP Messages from Being Forwarded on Cisco IOS XR Software: Example

The following example shows that Auto-RP messages are prevented from being sent out of the Packet over SONET/SDH (POS) interface 0/3/0/0. It also shows that access list 111 is used by the Auto-RP candidate and access list 222 is used by the **boundary** command to contain traffic on POS interface 0/3/0/0.

```
ipv4 access-list 111
 10 permit 224.1.0.0 0.0.255.255 any
 20 permit 224.2.0.0 0.0.255.255 any
!
!Access list 111 is used by the Auto-RP candidate.
!
ipv4 access-list 222
 10 deny any host 224.0.1.39
 20 deny any host 224.0.1.40
!
!Access list 222 is used by the boundary command to contain traffic (on POS0/3/0/0) that
is sent to groups 224.0.1.39 and 224.0.1.40.
!
router pim
 auto-rp mapping-agent loopback 2 scope 32 interval 30
 auto-rp candidate-rp loopback 2 scope 15 group-list 111 interval 30
 multicast-routing
 interface pos 0/3/0/0
 boundary 222
!
```

Inheritance in MSDP on Cisco IOS XR Software: Example

The following MSDP commands can be inherited by all MSDP peers when configured under router MSDP configuration mode. In addition, commands can be configured under the peer configuration mode for specific peers to override the inheritance feature.

- **connect-source**
- **sa-filter**
- **ttl-threshold**

If a command is configured in both the router msdp and peer configuration modes, the peer configuration takes precedence.

In the following example, MSDP on Router A filters Source-Active (SA) announcements on all peer groups in the address range 226/8 (except IP address 172.16.0.2); and filters SAs sourced by the originator RP 172.16.0.3 to 172.16.0.2.

MSDP peers (172.16.0.1, 172.16.0.2, and 172.17.0.1) use the loopback 0 address of Router A to set up peering. However, peer 192.168.12.2 uses the IPv4 address configured on the Packet-over-SONET/SDH (POS) interface to peer with Router A.

Router A

```
!
ipv4 access-list 111
 10 deny ip host 172.16.0.3 any
 20 permit any any
!
```

```

ipv4 access-list 112
 10 deny any 226.0.0.0 0.255.255.255
 30 permit any any
!
router msdp
 connect-source loopback 0
 sa-filter in rp-list 111
 sa-filter out rp-list 111
 peer 172.16.0.1
!
 peer 172.16.0.2
 sa-filter out list 112
!
 peer 172.17.0.1
!
 peer 192.168.12.2
 connect-source pos 0/2/0/0
!

```

Multicast QoS: Example

The following example shows how to configure a multicast QoS shaping policy.

```

class-map match-any class1
 match precedence flash-override
!
policy-map policy1
 class class1
  shape average 200 kbps

interface POS0/0/3/3
 service-policy output class1
 vrf mvpn1
 ipv4 address 25.25.25.1 255.255.255.0
 keepalive disable

```

Multicast VPN: Example

The following example shows how to configure a multicast VPN.

1. Configure basic VRF

```

vrf vpn1
 address-family ipv4 unicast
  import route-target
  1:1
  export route-target
  1:1
interface GigabitEthernet0/8/0/0.1
 vrf vpn1
 ipv4 address 101.1.1.1 255.255.255.0
 load-interval 30
 dot1q vlan 1 i

```

2. Configure VRF specific routing (CE to PE)

```

!router ospf 1
 redistribute bgp 100
 area 0
 vrf vpn1
  router-id 1.1.1.1
  redistribute bgp 100

```

```
area 0
 interface GigabitEthernet0/8/0/0.1
 !
 interface GigabitEthernet0/10/0/0.1
```

3. Configure MDT SAFI (PE to PE)!

```
router bgp 100
 bgp router-id 1.1.1.1
 address-family ipv4 unicast
 address-family vpnv4 unicast
 address-family ipv4 mdt
 !
 neighbor 9.9.9.9
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
  address-family vpnv4 unicast
  address-family ipv4 mdt
 !
```

4. Configure BGP to advertise VRF routes (PE to PE)

```
router bgp 100
 bgp router-id 1.1.1.1
 address-family ipv4 unicast
 address-family vpnv4 unicast
 address-family ipv4 mdt
 !
 neighbor 9.9.9.9
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
  address-family vpnv4 unicast
  address-family ipv4 mdt
 !
 vrf vpn1
  rd 1:1
  address-family ipv4 unicast
  redistribute ospf 1
```

5. Define core mcast RP address

```
router pim vrf default address-family ipv4
 rp-address 1.1.1.1
```

6. Define VRF mcast RP address

```
router pim vrf vpn1 address-family ipv4
 rp-address 11.11.11.11
 log neighbor changes
```

7. Define default / data MDT addresses

```
multicast-routing
 vrf vpn1 address-family ipv4
 mdt data 239.192.20.32/24 threshold 10 mc225
 mdt default 226.0.0.1
 interface all enable
```

Additional References

The following sections provide references related to implementing multicast routing on Cisco IOS XR software.

Related Documents

Related Topic	Document Title
Multicast command reference document	<i>Cisco IOS XR Multicast Command Reference</i>
Cisco CRS-1 router getting started material	<i>Cisco IOS XR Getting Started Guide</i>
Information about user groups and task IDs	<i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>
Modular quality of service command reference document	<i>Cisco IOS XR Modular Quality of Service Command Reference</i>

Standards

Standards	Title
draft-ietf-pim-sm-v2-new	<i>Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification</i>

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
RFC 2362	<i>Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification</i>
RFC 2385	<i>Protection of BGP Sessions via the TCP MD5 Signature Option</i>
RFC 2710	<i>Multicast Listener Discovery (MLD) for IPv6</i>
RFC 3376	<i>Internet Group Management Protocol, Version 3</i>
RFC 3446	Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
RFC 3618	<i>Multicast Source Discovery Protocol (MSDP)</i>
RFC 3810	<i>Multicast Listener Discovery Version 2 (MLDv2) for IPv6</i>

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport



INDEX

HC	Cisco IOS XR Interface and Hardware Component Configuration Guide
IC	Cisco IOS XR IP Addresses and Services Configuration Guide
MCC	Cisco IOS XR Multicast Configuration Guide
MNC	Cisco IOS XR System Monitoring Configuration Guide
MPC	Cisco IOS XR MPLS Configuration Guide
QC	Cisco IOS XR Modular Quality of Service Configuration Guide
RC	Cisco IOS XR Routing Configuration Guide
SBC	Cisco IOS XR Session Border Controller Configuration Guide
SC	Cisco IOS XR System Security Configuration Guide
SMC	Cisco IOS XR System Management Configuration Guide

B

BSR (Bootstrap Router)
See multicast routing, BSR

C

Class D IP addresses [MCC-5](#)
clear pim bsr command [MCC-29](#)

D

DR (Designated Router)
See multicast routing, DR

G

Generic Routing Encapsulation tunnels [MCC-13](#)
global configuration mode
 access-list command [MCC-23](#), [MCC-26](#), [MCC-28](#)
 hw-module qos multicast enable command [MCC-46](#)
 hw-module qos multicast priority queue
 command [MCC-46](#)

interface command [MCC-40](#)
ipv4 access-list command [MCC-43](#)
permit [MCC-26](#)
permit command [MCC-24](#)
vrf command [MCC-34](#)

I

interface submode
 ipv4 address command [MCC-40](#), [MCC-41](#)
IPv4 multicast routing [MCC-3](#)
IPv6 multicast routing [MCC-3](#)

M

MFIB (Multicast Forwarding Information Base)
 See multicast routing, Multicast Forwarding Information Base
mpls traffic-eng multicast-intact command [MCC-9](#)
MRIB (Multicast Routing Information Base)
 See multicast routing, Multicast Routing Information Base
MSDP (Multicast Source Discovery Protocol)
 See multicast routing, MSDP
multicast
 See multicast routing
multicast domain [MCC-13](#)
multicast intact [MCC-9](#)
multicast NSF (multicast nonstop forwarding)
 See multicast routing, multicast NSF
multicast routing
 Auto-RP
 configuring [MCC-24](#)
 description [MCC-12](#)

- RP-mapping agent [MCC-12](#)
- bootstrap router
 - configuring [MCC-26](#)
 - description [MCC-12](#)
- BSR
 - description
- DR
 - dr-priority command [MCC-10](#)
 - failure [MCC-10](#)
 - multiaccess segment [MCC-10](#)
 - purpose [MCC-10](#)
- IGMP
 - description [MCC-5](#)
 - host group addresses [MCC-5](#)
 - router IGMP submode, description [MCC-16](#)
 - versions [MCC-5, MCC-6](#)
- interfaces
 - configuration inheritance [MCC-17](#)
 - enabling and disabling [MCC-18](#)
- MLD
 - description [MCC-5](#)
 - router MLD submode, description [MCC-17](#)
 - versions [MCC-5](#)
- MSDP
 - default, SA messages [MCC-43](#)
 - default peering [MCC-40](#)
 - logical RP [MCC-40](#)
 - PIM-SM domains, interconnecting [MCC-40](#)
 - router MSDP submode, description [MCC-17](#)
 - source information, controlling [MCC-43](#)
- MSDP MD5 password authentication [MCC-18](#)
 - configuring [MCC-47](#)
- Multicast Forwarding Information Base [MCC-18](#)
- multicast NSF
 - configuring [MCC-30](#)
 - converge and reconnect [MCC-30](#)
 - high availability [MCC-15](#)
 - prerequisites [MCC-30](#)
 - timeout values [MCC-30](#)
- Multicast Routing Information Base [MCC-18](#)
- multicast VPN
 - BGP requirements [MCC-14](#)
 - description [MCC-13](#)
 - enabling multicast VRF forwarding [MCC-35](#)
 - multicast distribution tree [MCC-13](#)
 - specifying IGMP VRF instance [MCC-38](#)
 - specifying PIM VRF instance [MCC-37](#)
 - VRF entry [MCC-33](#)
- PIM
 - leaf routers [MCC-8](#)
 - multicast-intact [MCC-9](#)
 - restrictions, configuration [MCC-20](#)
 - router PIM submode, description [MCC-16](#)
 - shared tree to source tree process [MCC-9](#)
 - shortest path tree [MCC-8](#)
 - show pim neighbor command [MCC-10](#)
 - source tree [MCC-8](#)
- PIM-SM
 - configuring [MCC-19](#)
 - description [MCC-7](#)
 - RP [MCC-7](#)
- PIM-SSM
 - configuring [MCC-20](#)
 - datagrams, delivery [MCC-7](#)
 - description [MCC-7](#)
 - IGMPv3 support [MCC-8](#)
 - shared tree [MCC-8](#)
 - shortest path tree [MCC-8](#)
 - source tree [MCC-8](#)
- QOS
 - configuring [MCC-45](#)
 - differentiated services [MCC-16](#)
 - overview [MCC-15](#)
- RP, description [MCC-11](#)
- RPF [MCC-13](#)
 - static RP, configuring [MCC-22](#)
- multicast-routing command [MCC-21, MCC-31, MCC-36](#)
- multicast-routing submode

description [MCC-16](#)
 interface all command [MCC-20](#)
 interface all enable [MCC-36](#)
 interface all enable command [MCC-21](#)
 mdt data command [MCC-36](#)
 mdt default [MCC-36](#)
 nsf command [MCC-31](#)
 See multicast-routing command
 vrf [MCC-36](#)
 vrf default [MCC-36](#)

N

nsf lifetime command [MCC-32](#)

P

peer submode

remote-as command [MCC-42](#)

PIM-SSM (Protocol Independent Multicast in Source Specific Multicast)

See multicast routing, PIM-SSM

Protocol Independent Multicast (PIM) [MCC-7](#)

R

remote-as command [MCC-42](#)

RFC 2236 [MCC-6](#)

RFC 4601 [MCC-7](#)

router command [MCC-20](#)

router igmp command [MCC-21](#), [MCC-31](#), [MCC-39](#)

router igmp submode

nsf lifetime command [MCC-32](#)

version command [MCC-20](#), [MCC-21](#)

router mld command [MCC-21](#), [MCC-31](#)

router mld submode

nsf lifetime command [MCC-32](#)

version command [MCC-20](#), [MCC-21](#)

router msdp command [MCC-40](#), [MCC-43](#), [MCC-48](#)

router msdp submode

cache-sa-state command [MCC-43](#)

connect-source command [MCC-40](#)

default-peer command [MCC-40](#)

mesh-group command [MCC-40](#)

originator-id command [MCC-40](#)

password command [MCC-48](#)

peer command [MCC-40](#), [MCC-48](#)

remote-as command [MCC-40](#)

sa-filter command [MCC-43](#)

ttl-threshold command [MCC-43](#)

router pim command [MCC-23](#), [MCC-25](#), [MCC-27](#), [MCC-31](#), [MCC-38](#)

router pim submode

auto-rp candidate-rp command [MCC-25](#)

auto-rp mapping-agent command [MCC-25](#)

bsr border command [MCC-28](#)

bsr candidate-bsr command [MCC-27](#)

bsr candidate-rp command [MCC-27](#)

interface command [MCC-27](#)

nsf lifetime command [MCC-31](#)

old-register-checksum [MCC-23](#)

rp-address command [MCC-23](#), [MCC-38](#), [MCC-39](#)

RPF (Reverse Path Forwarding)

See multicast routing, RPF

S

show igmp nsf command [MCC-32](#)

show mfib hardware route command [MCC-46](#), [MCC-48](#)

show mfib nsf command [MCC-32](#)

show mld nsf command [MCC-32](#)

show mrrib nsf command [MCC-32](#)

show msdp globals command [MCC-40](#)

show msdp peer command [MCC-40](#)

show msdp rpf command [MCC-40](#)

show pim {ipv4 | ipv6} group-map command [MCC-20](#)

show pim bsr candidate-rp command [MCC-29](#)

show pim bsr election command [MCC-29](#)

show pim bsr rp-cache command [MCC-29](#)
show pim group-map command [MCC-22](#), [MCC-29](#)
show pim nsf command [MCC-32](#)
show pim topology command [MCC-20](#), [MCC-22](#)
show version command [MCC-24](#)
spt-threshold infinity command [MCC-8](#)

V

vrf submode
 address-family command [MCC-34](#)
 export route-target [MCC-35](#)
 import route-target [MCC-34](#)