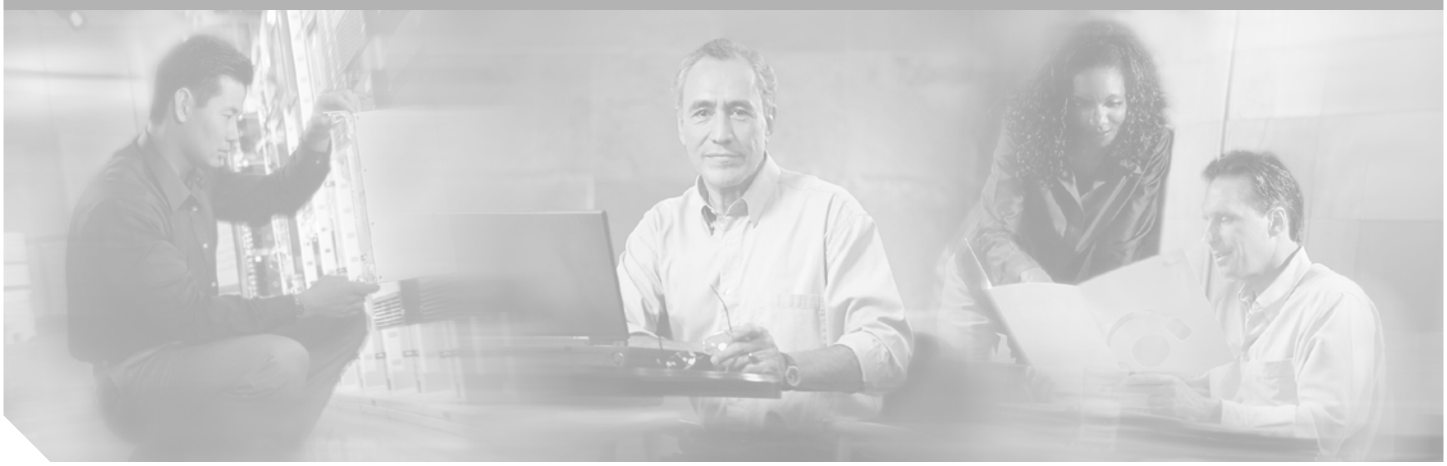
CISCO SYSTEMS



Cisco IOS XR Multicast Configuration Guide

Cisco IOS XR Software Release 3.4

Corporate 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: 408 526-4100

Text Part Number: OL-10950-02

CONTENTS

Preface

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

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-10950-01	October 2006	Initial release of this document.
OL-10950-02	April 2008	Added the following procedure: *Calculating Rates per Route*

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 of this module. 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.

Contents

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, refer to the *Cisco CRS-1 Series Carrier Routing System 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. Task IDs for commands are listed in the *Cisco IOS XR Task ID Reference Guide*.

  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.

Information About Implementing Multicast Routing on Cisco IOS XR Software

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

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

Table 2 lists the supported features for IPv4 and IPv6 multicast routing in Cisco IOS XR software.

Table 2 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
Auto-RP	Yes	No
BSR[3]	Yes	Yes
MSDP[4]	Yes	No
BGP[5]	Yes	Yes
Multicast NSF[6]	Yes	Yes
OOR handling[7]	Yes	Yes

1. Protocol Independent Multicast in sparse mode
2. Protocol Independent Multicast in Source-Specific Multicast
3. PIM bootstrap router
4. Multicast Source Discovery Protocol
5. Multiprotocol Border Gateway Protocol
6. Nonstop forwarding
7. 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 IGMP (IPv4) and 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.

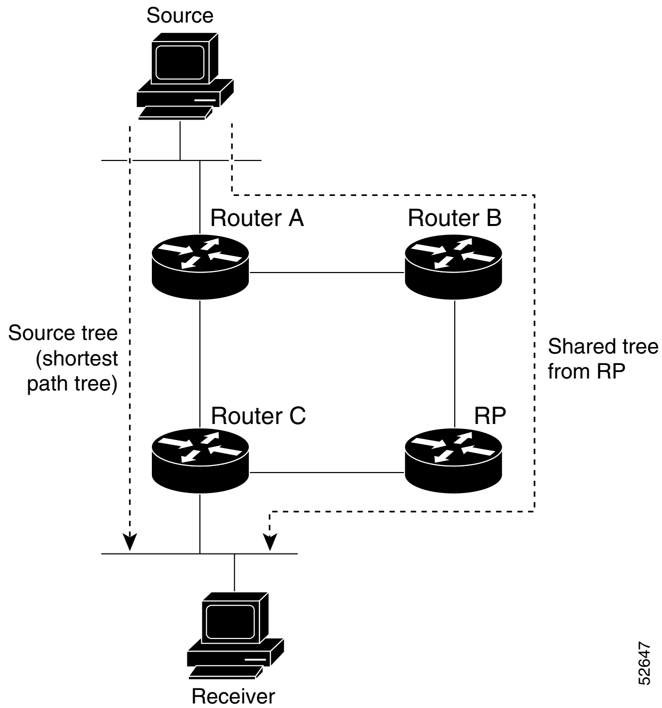
Cisco IOS XR Multicast Routing Implementation

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.
- 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.
- 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

- 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/MLD messages: 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/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/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.

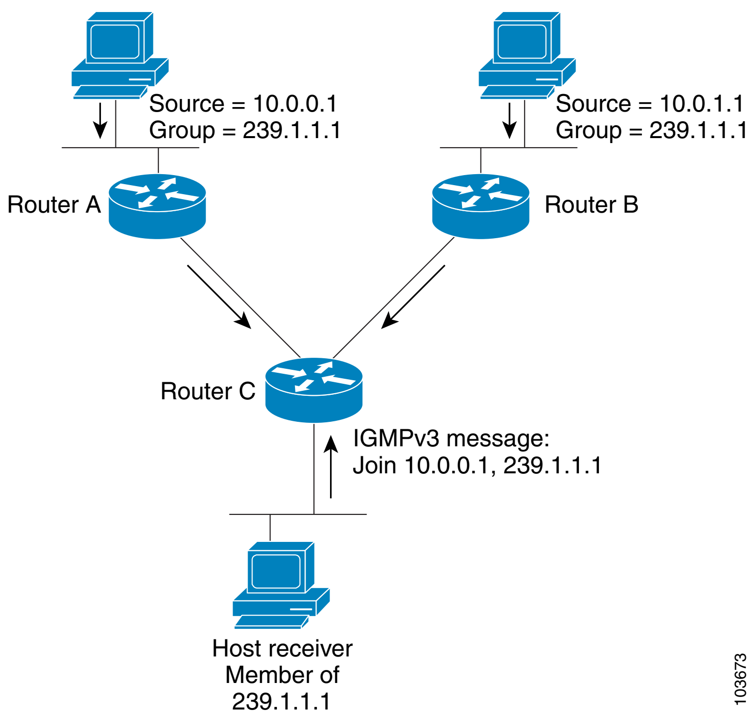
- IGMP Version 3 permits joins and leaves for certain source/group pairs instead of requesting traffic from all sources in the multicast group.

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)s that it wants to join and a list of sources and groups (S, G)s 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

PIM is an efficient IP routing protocol that is independent of the unicast routing table to perform send and receive multicast route updates like other protocols, such as Multicast Open Shortest Path First (MOSPF) or Distance Vector Multicast Routing Protocol (DVMRP). In other words, regardless of which unicast routing protocols are being used in the LAN to populate the unicast routing table, Cisco IOS XR PIM implementation leverages the existing unicast table content to perform the Reverse Path Forwarding (RPF) check function instead of building and maintaining its own separate multicast route table.

PIM is defined in RFC 2362, *Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*. For more information, see the following Internet Engineering Task Force (IETF) Internet drafts:

- *Protocol Independent Multicast (PIM): Motivation and Architecture*
- *Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*

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

PIM-Sparse Mode

Typically, 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. 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 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 hosts that send multicast packets are registered with the RP by that host's first-hop router.

How does PIM-SM work? As a PIM join travels up the tree, routers along the path set up 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.

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 the routing protocol that supports the implementation of SSM and is derived from PIM-SM. However, unlike PIM-SM where *all* multicast sources are sent when there is a PIM join, the SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined; thus optimizing bandwidth utilization and denying unwanted Internet broadcast traffic. Further, instead of the use of RP and shared trees, SSM uses information found on source addresses for a multicast group. This information is provided by receivers through the source addresses relayed to the last-hop routers by IGMPv3 membership reports resulting in source-specific trees.

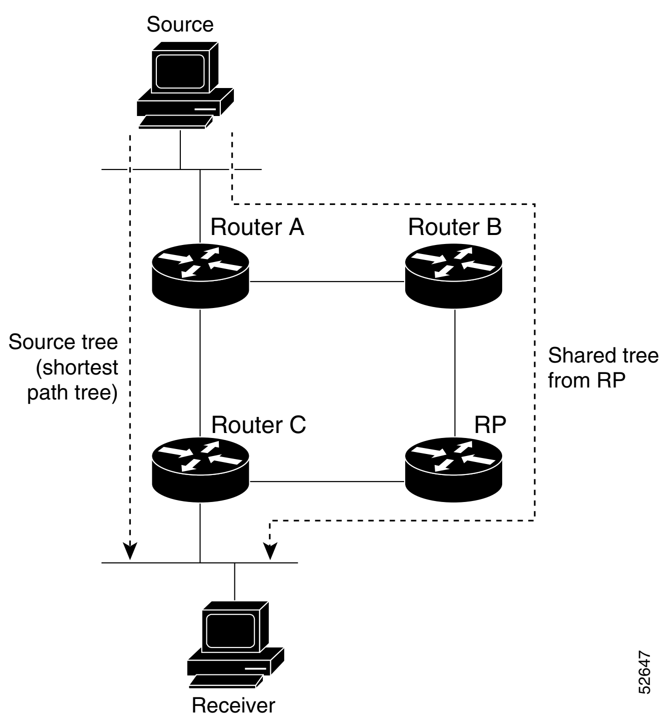
In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the (S, G) channel. Signaling is 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 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 will 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)

By default, members of a group 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)



If the data threshold warrants, leaf routers on the shared tree may initiate a switch to the data distribution tree rooted at the source. 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 upon receiving 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 sent by the designated router that is directly connected to a source and are received by the RP for the group.

Tip The **spt-threshold infinity** command lets you configure the router so that it never switches to the SPT.

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.

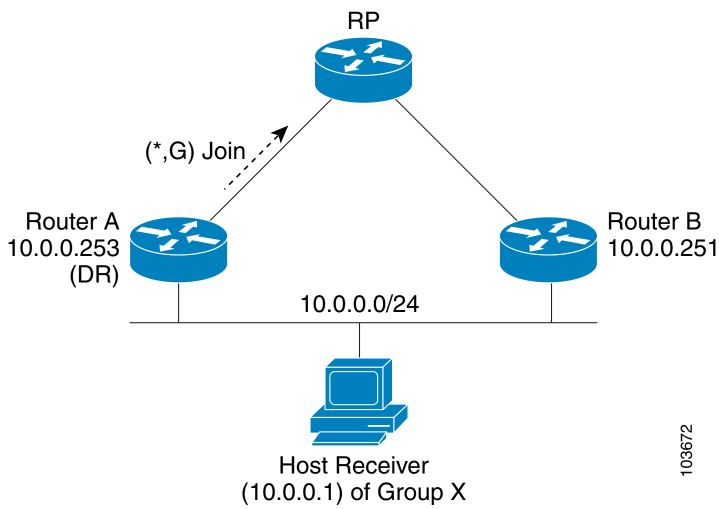
If there are multiple PIM-SM routers on a LAN, a designated router must be elected to avoid duplicating multicast traffic for connected hosts. The PIM router with the highest IP address becomes the DR for the LAN unless you choose to force the DR election by use of the **dr-priority** command. The DR priority option will allow 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 was also permitted to send (*, G) joins to the RP, parallel paths are created and Host A receive duplicate multicast traffic. Once 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 receives duplicate multicast packets.

What happens if the DR fails? The PIM-SM provides a way to detect the failure of Router A and elect a failover DR. If the DR (Router A) became inoperable, Router B detects this situation when its neighbor adjacency with Router A timed out. As 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 became 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 initiates a new Register process immediately after receiving the next multicast packet from Host A. This action triggers 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, 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" and "PIM Bootstrap Router" sections).

Auto-RP

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 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 "Configuring a Static RP and Allowing Backward Compatibility".

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.

Auto-RP is supported under IPv4 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 RP's address (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 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 a SA message and forwards the information to its peers. The message will contain 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 will install the S, G route, forward the encapsulated data contained in the SA message, and send 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 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) is 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. Upon completion, MRIB notifies MFIB and MFIB performs a mark-and-sweep to synchronize MFIB with the current MRIB route info.

Note Non-stop 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 will stop. Routes will be reinstalled and forwarding will recommence after NSF recovery has ended. This will only impact bidirectional routes. PIM SM/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 QoS. When configured on specific interfaces, system-wide, general QoS operations are applied to multicast traffic as well as 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 can 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
- Router PIM Configuration Submode
- Router IGMP Configuration Submode
- Router MDSP Configuration Submode

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.

In the following sample output, the question mark (?) online help function displays all the commands available under the multicast-routing configuration submode:

```
RP/0/RP0/CPU0:router(config)# multicast-routing ipv4
RP/0/RP0/CPU0:router(config-mcast-ipv4)# ?
  accounting       Enable/disable Accounting
  interface        Multicast interface configuration subcommands
  log-traps        Enable logging trap events
  maximum          Maximum state limits
  multipath        Enable equal-cost multipath routing
  nsf              Global multicast NSF configuration commands
  oom-handling     Enable out-of-memory handling
  rate-per-route   Enable/disable per (S,G) rate calculation
  ssm              Configure a group range for Source-Specific use
  static-rpf       Configure a static RPF rule for a given prefix/mask
```

The following example shows the available options for IPv6:

```
RP/0/RP0/CPU0:router(config)# multicast-routing ipv6
RP/0/RP0/CPU0:router(config-mcast-ipv6)# ?
  accounting       Enable/disable Accounting
  commit           Commit the configuration changes to running
  describe         Describe a command without taking real actions
  do               Run an exec command
  exit             Exit from this submode
  interface        Multicast interface configuration subcommands
  log-traps        Enable logging trap events
  maximum          Maximum state limits
  multipath        Enable equal-cost multipath routing
  no               Negate a command or set its defaults
  nsf              Global multicast NSF configuration commands
  rate-per-route   Enable/disable per (S,G) rate calculation
  root             Exit to the global configuration mode
  show             Show contents of configuration
  ssm              Configure a group range for Source-Specific use
  static-rpf       Configure a static RPF rule for a given prefix/mask
```

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.

In the following sample output, the question mark (?) online help function displays all the commands available under the router PIM configuration submode.

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-ipv4)# ?

  accept-register         Registers accept filter
  auto-rp                 Auto-RP Commands
  commit                  Commit the configuration changes to running
  default                 Set a command to its defaults
  describe                Describe a command without taking real actions
  do                      Run an exec command
  dr-priority             Inherited by all interfaces : PIM Hello DR priority
  exit                    Exit from this submode
  hello-interval          Inherited by all interfaces : Hello interval in seconds
  interface               PIM interface configuration subcommands
  join-prune-interval     Inherited by all interfaces : Join-Prune interval
  neighbor-filter         Neighbor filter
  no                      Negate a command or set its defaults
  nsf                     Configure Non-stop forwarding (NSF) options
  old-register-checksum   Generate registers compatible with older IOS versions
  rp-address              Configure Rendezvous Point
  show                    Show contents of configuration
  spt-threshold           Configure threshold for switching to SPT on last-hop
```

The following example shows the available options for IPv6:

```
RP/0/RP0/CPU0:router(config)# router pim address-family ipv6
RP/0/RP0/CPU0:router(config-pim-ipv6)# ?

  accept-register           Registers accept filter
  assert-batching-disable   Disable batching asserts
  bsr                       BSR Configurations
  commit                    Commit the configuration changes to running
  convergence-timeout       Timeout value for the RIB convergence notification
  describe                  Describe a command without taking real actions
  do                        Run an exec command
  dr-priority               Inherited by all interfaces : PIM Hello DR priority
  embedded-rp               Set Embedded RP processing support
  exit                      Exit from this submode
  hello-interval            Inherited by all interfaces : Hello interval in seconds
  interface                 PIM interface configuration subcommands
  join-prune-interval       Inherited by all interfaces : Join-Prune interval
  log                       Enable PIM logging
  maximum                   Maximum state limits
  neighbor-check-on-recv    Check for PIM neighbor before rcv'ing control message
```

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.

In the following sample output, the question mark (?) online help function displays all the commands available under router IGMP configuration submode:

```
RP/0/RP0/CP0:router(config)# router igmp
RP/0/RP0/CP0:router(config-igmp)# ?

  access-group             IGMP group access group
  commit                   Commit the configuration changes to running
  default                  Set a command to its defaults
  describe                 Describe a command without taking real actions
  do                       Run an exec command
  exit                     Exit from this submode
  explicit-tracking        IGMPv3 explicit host tracking
  interface                IGMP interface configuration subcommands
  no                       Negate a command or set its defaults
  nsf                      Configure NSF specific options
  query-interval           IGMP host query interval
  query-max-response-time  IGMP max query response value
  query-timeout            IGMP previous querier timeout
  show                     Show contents of configuration
  version                  IGMP version
```

Router MLD Configuration Submode

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

In the following sample output, the question mark (?) online help function displays all the commands available under router MLD configuration submode:

```
RP/0/RP0/CP0:router(config)# router mld
RP/0/RP0/CP0:router(config-mld)# ?

  access-group             MLD group access group
  commit                   Commit the configuration changes to running
  default                  Set a command to its defaults
  describe                 Describe a command without taking real actions
  do                       Run an exec command
  exit                     Exit from this submode
  explicit-tracking        MLD explicit host tracking
  interface                MLD interface configuration subcommands
  no                       Negate a command or set its defaults
  nsf                      Configure NSF specific options
  query-interval           MLD host query interval
  query-max-response-time  MLD max query response value
  query-timeout            MLD previous querier timeout
  show                     Show contents of configuration
  version                  MLD version
```

Router MDSP Configuration Submode

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

In the following sample output, the question mark (?) online help function displays all the commands available under router MSDP configuration submode.

```
RP/0/RP0/CP0:router(config)# router msdp
RP/0/RP0/CP0:router(config-msdp)# ?

  cache-sa-holdtime  Configure Cache SA State holdtime period
  cache-sa-state     Configure this systems SA cache access-lists
  commit             Commit the configuration changes to running
  connect-source     Configure source address used for MSDP connection
  default            Set a command to its defaults
```

```
  default-peer       Default MSDP peer to accept SA messages from
  describe           Describe a command without taking real actions
  do                 Run an exec command
  exit               Exit from this submode
  no                 Negate a command or set its defaults
  originator-id      Configure MSDP Originator ID
  peer               MSDP Peer configuration subcommands
  sa-filter          Filter SA messages from peer
  show               Show contents of configuration
  ttl-threshold      Configure TTL Threshold for MSDP Peer
```

Understanding Interface Configuration Inheritance

The Cisco IOS XR software allows you to configure commands for a large number of interfaces by simply 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 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-ipv4)# hello-interval 420
RP/0/RP0/CPU0:router(config-pim-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
  interface all disable

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

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

router mld
  interface all disable
  interface all enable
  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-ipv4)# interface all enable
```

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

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

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 in optimizing, debugging and discovering 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-23 (optional)
- Configuring the BSR, page MCC-25 (optional)
- Calculating Rates per Route, page MCC-28 (optional)
- Configuring Multicast Nonstop Forwarding, page MCC-30 (optional)
- Interconnecting PIM-SM Domains with MSDP, page MCC-32 (optional)
- Controlling Source Information on MSDP Peer Routers, page MCC-35 (optional)
- Configuring Multicast Quality of Service, page MCC-38 (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 MOSPF or DVMRP.

Cisco IOS XR software supports PIM-SM and PIM-SSM permitting both to operate on your router at the same time.

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.

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.

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**
3. **interface all**
4. **exit**
5. **router {igmp | mld}**
6. **version {1 | 2 | 3}**
7. **end**
   or
   commit
8. **show pim {ipv4 | ipv6} group-map**
9. **show pim topology**

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 ipv6**] **Example:** `RP/0/RP0/CPU0:router(config)# multicast-routing`	Enters multicast routing configuration mode. • 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 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** | **mld**} **Example:** `RP/0/RP0/CPU0:router(config)# router igmp`	(Optional) Enters router IGMP or MLD configuration mode.

	Command or Action	Purpose
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. • 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.

Step 7	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config-igmp)# end`
	or
	`RP/0/RP0/CPU0:router(config-igmp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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 8	**show pim** [**ipv4** | **ipv6**] **group-map** **Example:** `RP/0//CPU0:router# show pim ipv4 group-map`	(Optional) Displays group-to-PIM mode mapping.
Step 9	**show pim** [**ipv4** | **ipv6**] **topology** **Example:** `RP/0/RP0/CPU0:router# show pim topology`	(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. For configuration information for Auto-RP, see the "Configuring Auto-RP to Automate Group-to-RP Mappings" section.

SUMMARY STEPS

1. **configure**
2. **router pim** [**address-family ipv6**]
3. **rp-address** *ip-address* [*group-access-list-number*] [**bidir**] [**override**]
4. **old-register-checksum**
5. **exit**
6. **ipv4 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**] **Example:** `RP/0/RP0/CPU0:router(config)# router pim`	Enters router PIM configuration mode.
Step 3	**rp-address** *ip-address* [*group-access-list-number*] [**bidir**] [**override**] **Example:** `RP/0/RP0/CPU0:router(config-pim-ipv4)# rp-address 172.16.6.22 rp-access`	Assigns an RP to multicast groups. • If you specify a *group-access-list-number* value, you must configure the optional **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.

	Command or Action	Purpose
Step 6	**ipv4 access-list** *name* **Example:** `RP/0/RP0/CPU0:router(config)# ipv4 access-list rp-access`	(Optional) Enters IPv4 access list configuration mode and configures the RP access list. • The access list called "rp-access" permits multicast group 239.1.1.1.
Step 7	[*sequence-number*] **permit** *source* [*source-wildcard*] **Example:** `RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 239.1.1.1`	(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.**

Step 8	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config-ipv4-acl)# end`
	or
	`RP/0/RP0/CPU0:router(config-ipv4-acl)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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 9	**show version** **Example:** `RP/0/RP0/CPU0:router# show version`	Displays the software release version.

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.

SUMMARY STEPS

1. **configure**
2. **router pim** [**address-family ipv4**]

3. **auto-rp candidate-rp** *interface-type interface-number* **scope** *ttl-value* [**group-list** *access-list-number*] [**interval** *seconds*] [**bidir**]
4. **auto-rp mapping-agent** *interface-type interface-number* **scope** *ttl-value* [**interval** *seconds*]
5. **exit**
6. **ipv4 access-list** *name* [*sequence-number*] **permit** *source* [*source-wildcard*]
7. **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 ipv6`**] **Example:** `RP/0/RP0/CPU0:router(config)# router pim`	Enters router PIM configuration mode.
Step 3	**`auto-rp candidate-rp`** *`interface-type interface-number`* **`scope`** *`ttl-value`* [**`group-list`** *`access-list-number`*] [**`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). • 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`** *`interface-type interface-number`* **`scope`** *`ttl-value`* [**`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 a RP mapping agent on a specified interface. • 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.

	Command or Action	Purpose
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 access-list** *name* [*sequence-number*] **permit** *source* [*source-wildcard*] **Example:** `RP/0/RP0/CPU0:router(config)# ipv4 access-list 2 permit 239.1.1.1 0.0.0.0`	(Optional) Defines the RP access list. • Access list 2 permits multicast group 239.1.1.1.

Step 7	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config)# end`
	or
	`RP/0/RP0/CPU0:router(config)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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.

Configuring the BSR

Configure one or more candidate BSRs and a BSR mapping agent. Connect and locate the candidate BSRs in the backbone portion of the network.

For more information about BSR see the "PIM Bootstrap Router" section.

SUMMARY STEPS

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

8. **ipv4 access-list** *name* [*sequence-number*] **permit** *source* [*source-wildcard*]
9. **end**
   or
   commit
10. **clear pim** [**ipv4** | **ipv6**] **bsr**
11. **show pim** [**ipv4** | **ipv6**] **bsr candidate-rp**
12. **show pim** [**ipv4** | **ipv6**] **bsr election**
13. **show pim** [**ipv4** | **ipv6**] **bsr rp-cache**
14. **show pim** [**ipv4** | **ipv6**] **group-map**

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 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-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*] [**priority** *value*] **Example:** `RP/0/RP0/CPU0:router(config-pim-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. • See Step 8 for group list 4 configuration.
Step 5	**interface** *type number* **Example:** `RP/0/RP0/CPU0:router(config-pim-ipv4)# interface pos 0/1/0/0`	Enters interface configuration mode for the PIM protocol.
Step 6	**bsr-border** **Example:** `RP/0/RP0/CPU0:router(config-pim-ipv4-if)# bsr-border`	Stops the forwarding of bootstrap router (BSR) messages on a Protocol Independent Multicast (PIM) router interface,

	Command or Action	Purpose
Step 7	**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 8	**ipv4 access-list** *name* [*sequence-number*] **permit** *source* [*source-wildcard*] or **ipv6 access-list** *name* [*sequence-number*] **permit** *source-prefix dest-prefix* **Example:** `RP/0/RP0/CPU0:router(config)# ipv4 access-list 4 permit 239.0.0.0 0.255.255.255`	(Optional) Defines the candidate group list to the BSR. • 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 9	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config)# end`
	or
	`RP/0/RP0/CPU0:router(config)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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 10	**clear pim** [**ipv4** | **ipv6**] **bsr** **Example:** `RP/0/RP0/CPU0:router# clear pim bsr`	(Optional) Clears BSR entries from the PIM RP group mapping cache.
Step 11	**show pim** [**ipv4** | **ipv6**] **bsr candidate-rp** **Example:** `RP/0/RP0/CPU0:router# show pim bsr candidate-rp`	(Optional) Displays PIM candidate RP information for the BSR.
Step 12	**show pim** [**ipv4** | **ipv6**] **bsr election** **Example:** `RP/0/RP0/CPU0:router# show pim bsr election`	(Optional) Displays PIM candidate election information for the BSR.

	Command or Action	Purpose
Step 13	**show pim** [**ipv4** | **ipv6**] **bsr rp-cache** **Example:** `RP/0/RP0/CPU0:router# show pim bsr rp-cache`	(Optional) Displays PIM RP cache information for the BSR.
Step 14	**show pim** [**ipv4** | **ipv6**] **group-map** **Example:** `RP/0/RP0/CPU0:router# show pim ipv4 group-map`	(Optional) Displays group-to-PIM mode mapping.

Calculating Rates per Route

This procedure enables multicast hardware forward rate counters on a per VRF family basis.

SUMMARY STEPS

1. **configure**
2. **multicast-routing [vrf** *vrf-name*] [**address-family** {**ipv4** | **ipv6**}]
3. **rate-per-route**
4. **interface {***type interface-id* **| all} enable**
5. **accouting per-prefix**
6. **end**
   or
   commit
7. **show mfib route rate** [**vrf** *vrf-name*] [**ipv4** | **ipv6**] **route** [**rate** | **statistics**] [* | *source-address*] [*group-address* [*/prefix-length*] [**detail** | **old-output**] | **summary**] [**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	**multicast-routing** [**vrf** *vrf-name*] [**address-family** {**ipv4** | **ipv6**}] **Example:** `RP/0/RP0/CPU0:router(config)# multicast-routing address-family ipv4`	Enters multicast routing configuration mode. • 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	**rate-per-route** **Example:** `RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# rate-per-route`	Enables a per (S,G) rate calculation for a particular route.

	Command or Action	Purpose

Step 4	**interface** {*type interface-id* | **all**} **enable**
	
	Example:
	`RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # interface all enable`
	or
	`RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # interface FastEthernet0/3/3/1 enable`
		Enables multicast routing on all interfaces.

Step 5	**accounting per-prefix** **Example:** `RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # accounting per-prefix`	Enables per-prefix counters in hardware. Cisco IOS XR software counters are always present. When enabled, every existing and new (S, G) route is assigned forward, punt, and drop counters on the ingress route and forward and punt counters on the egress route. The (*, G) routes are assigned a single counter.

Step 6	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # end`
	or
	`RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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 7	**show mfib route rate** [**vrf** *vrf-name*] [**ipv4** | **ipv6**] **route** [**rate** | **statistics**] [* | *source-address*] [*group-address* [/*prefix-length*] [**detail** | **old-output**] | **summary**] [**location** *node-id*] **Example:** `RP/0/RP0/CPU0:router# show mfib route rate ipv4 IP Multicast Forwarding Rates Source Address, Group Address HW Forwarding Rates: bps In/pps In/bps Out/pps Out`	Displays route entries in the Multicast Forwarding Information Base (MFIB) table. • When the **rate** keyword is used with the *source-* and *group-address* arguments, the command displays the cumulative rates per route for all line cards in the Multicast Forwarding Information Base (MFIB) table . • When the **statistics** keyword is used, the command displays the rate per route for one line card in the Multicast Forwarding Information Base (MFIB) table .

Configuring Multicast Nonstop Forwarding

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

Although we strongly recommended that you use the NSF lifetime default values, the optional Step 4 through Step 9 allow you to modify the NSF timeout values for PIM and IGMP/MLD. Use these commands when PIM and IGMP/MLD are configured with non-default 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 and 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**
3. **nsf**
4. **exit**
5. **router pim** [**address-family ipv6**]
6. **nsf lifetime** *seconds*
7. **exit**
8. **router** {**igmp** | **mld**}
9. **nsf lifetime** *seconds*
10. **end**
    or
    commit
11. **show** {**igmp** | **mld**} **nsf**
12. **show mfib nsf** [**location** *node-id*]
13. **show mrib nsf**
14. **show pim 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 ipv6**] **Example:** `RP/0/RP0/CPU0:router(config)# multicast-routing`	Enters multicast routing configuration mode. • 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** **Example:** `RP/0/RP0/CPU0:router(config-mcast-ipv4)# nsf`	Turns on NSF capability for the multicast routing system.
Step 4	**exit** **Example:** `RP/0/RP0/CPU0:router(config-mcast-ipv4)# exit`	(Optional) Exits multicast routing configuration mode, and returns the router to the parent configuration mode.
Step 5	**router pim** [**address-family ipv6**] **Example:** `RP/0/RP0/CPU0:router(config)# router pim`	(Optional) Enters router PIM configuration mode.
Step 6	**nsf lifetime** *seconds* **Example:** `RP/0/RP0/CPU0:router(config-pim-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 non-default 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-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.
Step 9	**nsf lifetime** *seconds* **Example:** `RP/0/RP0/CPU0:router(config-igmp)# nsf lifetime 30`	(Optional) Configures the NSF timeout value for multicast forwarding route entries under the IGMP or MLD process.

	Command or Action	Purpose

Step 10	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config-igmp)# end`
	or
	`RP/0/RP0/CPU0:router(config-igmp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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	**show** {**igmp** | **mld**} **nsf** **Example:** `RP/0/RP0/CPU0:router# show igmp nsf`	(Optional) Displays the state of NSF operation in IGMP or MLD.
Step 12	**show mfib** [**ipv4** | **ipv6**] **nsf** [**location** *node-id*] **Example:** `RP/0/RP0/CPU0:router# show mfib nsf`	(Optional) Displays the state of NSF operation for the MFIB line cards.
Step 13	**show mrib** [**ipv4** | **ipv6**] **nsf** **Example:** `RP/0/RP0/CPU0:router# show mrib nsf`	(Optional) Displays the state of NSF operation in the MRIB.
Step 14	**show pim** [**ipv4** | **ipv6**] **nsf** **Example:** `RP/0/RP0/CPU0:router# show pim nsf`	(Optional) Displays the state of NSF operation for PIM.

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* | *dns-name*} [**prefix-list**]
7. **originator-id** *interface-type interface-number*
8. **peer** {*peer-name* | *peer-address*}
9. **connect-source** *interface-type interface-number*
10. **mesh-group** *name*
11. **remote-as**-*number*
12. **end**
    or
    commit
13. **show msdp globals**
14. **show msdp peer** {*peer-address* | *peer-name*}
15. **show msdp rpf** {*rpf-address* | *host-name*}

DETAILED STEPS

	Command or Action	Purpose

Step 1	`configure`
	
	Example:
	`RP/0/RP0/CPU0:router# configure`
		Enters global configuration mode.

Step 2	`interface` *type number* **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 the interface type and number whose primary address becomes the source IP address for the TCP connection.
Step 3	`ipv4 address` *address mask* **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 the 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.

	Command or Action	Purpose
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** {*ip-address* | *dns-name*} [**prefix-list** *list*] **Example:** `RP/0/RP0/CPU0:router(config-msdp)# default-peer router.cisco.com`	(Optional) Defines a default peer from which to accept all MSDP SA messages.
Step 7	**originator-id** *interface-type interface-number* **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** {*peer-name* | *peer-address*} **Example:** `RP/0/RP0/CPU0:router(config-msdp)# peer 172.31.1.2`	Enters MSDP peer configuration mode and configures an MSDP peer. • 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.
Step 9	**connect-source** *interface-type interface-number* **Example:** `RP/0/RP0/CPU0:router(config-msdp-peer)# connect-source interface loopback 0`	(Optional) Configures a source address used for an MSDP connection.
Step 10	**mesh-group** *name* **Example:** `RP/0/RP0/CPU0:router(config-msdp-peer)# mesh-group internal`	(Optional) Configures an MSDP peer to be a member of a mesh group.
Step 11	**remote-as** *as-number* **Example:** `RP/0/RP0/CPU0:router(config-msdp-peer)# remote-as 250`	(Optional) Configures the remote autonomous system number of this peer.

	Command or Action	Purpose

Step 12	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config-msdp-peer)# end`
	or
	`RP/0/RP0/CPU0:router(config-msdp-peer)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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 13	**show msdp globals** **Example:** `RP/0/RP0/CPU0:router# show msdp globals`	Displays the MSDP global variables.
Step 14	**show msdp peer** {*peer-address* | *peer-name*} **Example:** `RP/0/RP0/CPU0:router# show msdp peer 172.31.1.2`	Displays information about the MSDP peer.
Step 15	**show msdp rpf** {*rpf-address* | *host-name*} **Example:** `RP/0/RP0/CPU0:router# show msdp rpf 172.16.10.13`	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 whom you will originate source information to based on the source that is requesting information

When forwarding SA messages you can:

- 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:

- Filter all incoming Source-Active 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 Source-Active (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 will 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. **ipv4 access-list** *name* [*sequence-number*] **permit** *source* [*source-wildcard*]
7. **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.

	Command or Action	Purpose
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-peer)# sa-filter out router.cisco.com list 100`	Configures an incoming or outgoing filter list for messages received from the specified MSDP peer. • 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 6. • If all match criteria are true, a **permit** from the route map will pass routes through the filter. A **deny** will filter 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-peer)# cache-sa-state 100`	Creates and caches source/group pairs from received Source-Active (SA) messages and controls pairs through access lists.
Step 5	**ttl-threshold** *ttl-value* **Example:** `RP/0/RP0/CPU0:router(config-msdp-peer)# ttl-threshold 8`	(Optional) Limits which multicast data s are sent in SA messages to an MSDP peer. • Only multicast packets with an IP header TTL greater than or equal to the *ttl-value* 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	**ipv4 access-list** *name* [*sequence-number*] **permit** *source* [*source-wildcard*] **Example:** `RP/0/RP0/CPU0:router(config-msdp-peer)# ipv4 access-list 100 20 permit 239.1.1.1 0.0.0.0`	Defines an IPv4 access list to be used by SA filtering. • 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 7	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config-msdp-peer)# end`
	or
	`RP/0/RP0/CPU0:router(config-msdp-peer)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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.

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.

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

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 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# 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# 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.

Step 4	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(config-if)# end`
	or
	`RP/0/RP0/CPU0:router(config-if)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`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 5	**show mfib hardware route** {***** | *source-address* | *group-address* [/*prefix-length*]} **location** *node-id* **Example:** `RP/0/RP0/CPU0:router# show mfib hardware route * location 0/1/cpu0`	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

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, an 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 were to fail, IP routing will converge 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 will 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 (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 are inheritable by all MSDP peers when configured under the 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 (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

```
pv4 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
!
```

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 documents	*Cisco IOS XR Multicast Command Reference*, Release 3.3.0
Cisco CRS-1 router getting started material	*Cisco IOS XR Getting Started Guide*, Release 3.3.0
Information about user groups and task IDs	*Configuring AAA Services on Cisco IOS XR Software module* of the *Cisco IOS XR System Security Configuration Guide*, Release 3.3.0

Standards

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

MIBs

MIBs	MIBs Link
—	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	*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*
RFC 2710	*Multicast Listener Discovery (MLD) for IPv6*
RFC 3446	*Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
RFC 3810	*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
RFC 3618	*Multicast Source Discovery Protocol (MSDP)*
RFC 3376	*Internet Group Management Protocol, Version 3*
draft-ietf-pim-sm-v2-new	*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised),* March 6, 2003

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

A

B

C

D

H

I

M

N

O

P

Q

R

S

T

V