IP Multicast: PIM Configuration Guide, Cisco IOS XE Release 2

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

CONTENTS

IP Multicast Technology Overview

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

This module contains a technical overview of IP multicast. IP multicast is an efficient way to use network resources, especially for bandwidth-intensive services such as audio and video. Before beginning to configure IP multicast, it is important that you understand the information presented in this module.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP Multicast Technology

Role of IP Multicast in Information Delivery

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

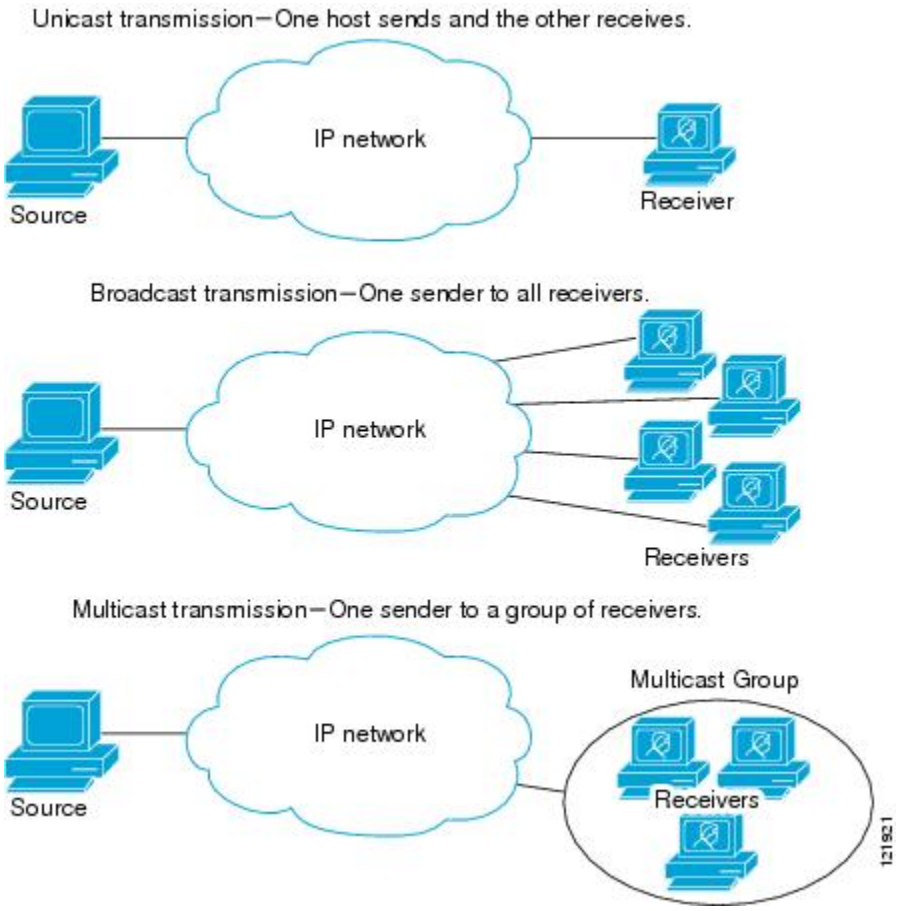
IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packet and IP multicast routers and multilayer switches forward incoming IP multicast packets out all interfaces that lead to the members of the multicast group. 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.

Multicast Group Transmission Scheme

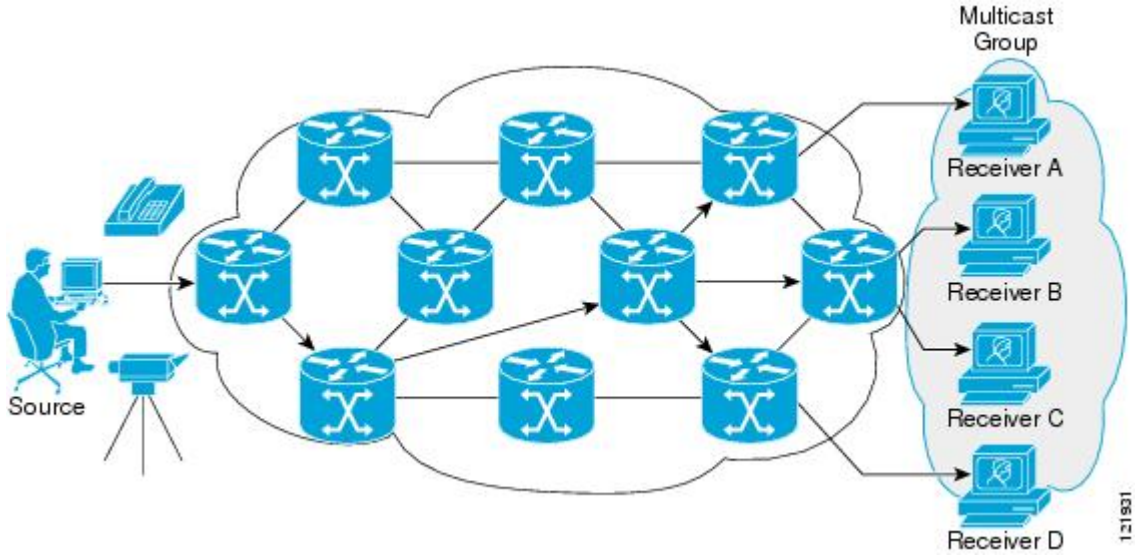
IP communication consists of hosts that act as senders and receivers of traffic as shown in the first figure. Senders are called sources. Traditional IP communication is accomplished by a single host source sending packets to another single host (unicast transmission) or to all hosts (broadcast transmission). IP multicast provides a third scheme, allowing a host to send packets to a subset of all hosts (multicast transmission). This subset of receiving hosts is called a multicast group. The hosts that belong to a multicast group are called group members.

Multicast is based on this group concept. A multicast group is an arbitrary number of receivers that join a group in order to receive a particular data stream. This multicast group has no physical or geographical boundaries--the hosts can be located anywhere on the Internet or on any private internetwork. Hosts that are interested in receiving data from a source to a particular group must join that group. Joining a group is accomplished by a host receiver by way of the Internet Group Management Protocol (IGMP).

In a multicast environment, any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group can receive packets sent to that group. Multicast packets are delivered to a group using best-effort reliability, just like IP unicast packets.



In the next figure, the receivers (the designated multicast group) are interested in receiving the video data stream from the source. The receivers indicate their interest by sending an IGMP host report to the routers in the network. The routers are then responsible for delivering the data from the source to the receivers. The routers use Protocol Independent Multicast (PIM) to dynamically create a multicast distribution tree. The video data stream will then be delivered only to the network segments that are in the path between the source and the receivers.



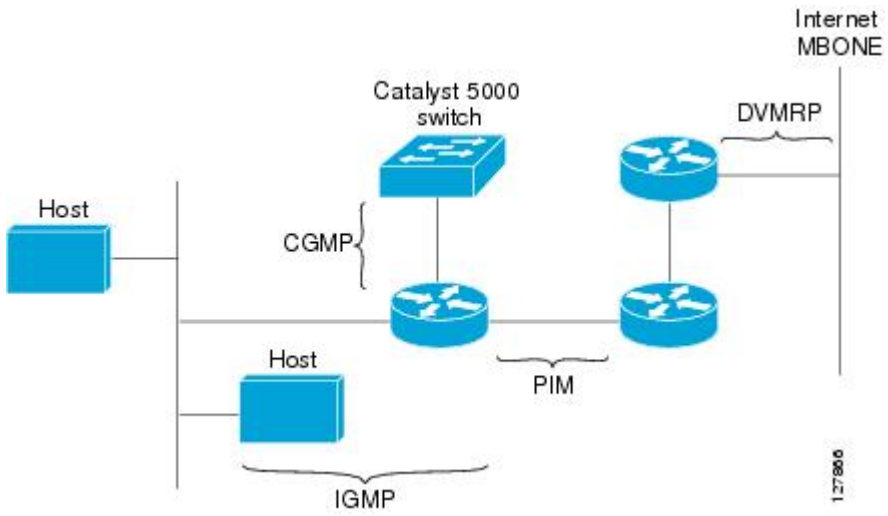
IP Multicast Routing Protocols

The software supports the following protocols to implement IP multicast routing:

- IGMP is used between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members.
- Protocol Independent Multicast (PIM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- Distance Vector Multicast Routing Protocol (DVMRP) is used on the MBONE (the multicast backbone of the Internet). The software supports PIM-to-DVMRP interaction.
- Cisco Group Management Protocol (CGMP) is used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP.

The figure shows where these protocols operate within the IP multicast environment.

Figure 1 IP Multicast Routing Protocols



IP Multicast Group Addressing

A multicast group is identified by its multicast group address. Multicast packets are delivered to that multicast group address. Unlike unicast addresses that uniquely identify a single host, multicast IP addresses do not identify a particular host. To receive the data sent to a multicast address, a host must join the group that address identifies. The data is sent to the multicast address and received by all the hosts that have joined the group indicating that they wish to receive traffic sent to that group. The multicast group address is assigned to a group at the source. Network administrators who assign multicast group addresses must make sure the addresses conform to the multicast address range assignments reserved by the Internet Assigned Numbers Authority (IANA).

- IP Class D Addresses, page 5

IP Class D Addresses

IP multicast addresses have been assigned to the IPv4 Class D address space by IANA. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255. A multicast address is chosen at the source (sender) for the receivers in a multicast group.

Note The Class D address range is used only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

IP Multicast Address Scoping

The multicast address range is subdivided to provide predictable behavior for various address ranges and for address reuse within smaller domains. The table provides a summary of the multicast address ranges. A brief summary description of each range follows.

Table 1 Multicast Address Range Assignments

Name	Range	Description
Reserved Link-Local Addresses	224.0.0.0 to 224.0.0.255	Reserved for use by network protocols on a local network segment.
Globally Scoped Addresses	224.0.1.0 to 238.255.255.255	Reserved to send multicast data between organizations and across the Internet.
Source Specific Multicast	232.0.0.0 to 232.255.255.255	Reserved for use with the SSM datagram delivery model where data is forwarded only to receivers that have explicitly joined the group.
GLOP Addresses	233.0.0.0 to 233.255.255.255	Reserved for statically defined addresses by organizations that already have an assigned autonomous system (AS) domain number.

Name	Range	Description
Limited Scope Address	239.0.0.0 to 239.255.255.255	Reserved as administratively or limited scope addresses for use in private multicast domains.

Reserved Link-Local Addresses

The IANA has reserved the range 224.0.0.0 to 224.0.0.255 for use by network protocols on a local network segment. Packets with an address in this range are local in scope and are not forwarded by IP routers. Packets with link local destination addresses are typically sent with a time-to-live (TTL) value of 1 and are not forwarded by a router.

Within this range, reserved link-local addresses provide network protocol functions for which they are reserved. Network protocols use these addresses for automatic router discovery and to communicate important routing information. For example, Open Shortest Path First (OSPF) uses the IP addresses 224.0.0.5 and 224.0.0.6 to exchange link-state information.

IANA assigns single multicast address requests for network protocols or network applications out of the 224.0.1.xxx address range. Multicast routers forward these multicast addresses.

Globally Scoped Addresses

Addresses in the range 224.0.1.0 to 238.255.255.255 are called globally scoped addresses. These addresses are used to send multicast data between organizations across the Internet. Some of these addresses have been reserved by IANA for use by multicast applications. For example, the IP address 224.0.1.1 is reserved for Network Time Protocol (NTP).

Source Specific Multicast Addresses

Addresses in the range 232.0.0.0/8 are reserved for Source Specific Multicast (SSM) by IANA. In Cisco IOS software, you can use the **ip pim ssm**command to configure SSM for arbitrary IP multicast addresses also. SSM is an extension of Protocol Independent Multicast (PIM) that allows for an efficient data delivery mechanism in one-to-many communications. SSM is described in the IP Multicast Delivery Modes, page 7 section.

GLOP Addresses

GLOP addressing (as proposed by RFC 2770, GLOP Addressing in 233/8) proposes that the 233.0.0.0/8 range be reserved for statically defined addresses by organizations that already have an AS number reserved. This practice is called GLOP addressing. The AS number of the domain is embedded into the second and third octets of the 233.0.0.0/8 address range. For example, AS 62010 is written in hexadecimal format as F23A. Separating the two octets F2 and 3A results in 242 and 58 in decimal format. These values result in a subnet of 233.242.58.0/24 that would be globally reserved for AS 62010 to use.

Limited Scope Addresses

The range 239.0.0.0 to 239.255.255.255 is reserved as administratively or limited scoped addresses for use in private multicast domains. These addresses are constrained to a local group or organization. Companies, universities, and other organizations can use limited scope addresses to have local multicast applications that will not be forwarded outside their domain. Routers typically are configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an AS or domain, the limited scope address range can be further subdivided so that local multicast boundaries can be defined.

Note Network administrators may use multicast addresses in this range, inside a domain, without conflicting with others elsewhere in the Internet.

Layer 2 Multicast Addresses

Historically, network interface cards (NICs) on a LAN segment could receive only packets destined for their burned-in MAC address or the broadcast MAC address. In IP multicast, several hosts need to be able to receive a single data stream with a common destination MAC address. Some means had to be devised so that multiple hosts could receive the same packet and still be able to differentiate between several multicast groups. One method to accomplish this is to map IP multicast Class D addresses directly to a MAC address. Using this method, NICs can receive packets destined to many different MAC address.

Cisco Group Management Protocol (CGMP) is used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP. CGMP is necessary for those Catalyst switches that cannot distinguish between IP multicast data packets and IGMP report messages, both of which are addressed to the same group address at the MAC level.

IP Multicast Delivery Modes

IP multicast delivery modes differ only for the receiver hosts, not for the source hosts. A source host sends IP multicast packets with its own IP address as the IP source address of the packet and a group address as the IP destination address of the packet.

- Any Source Multicast, page 7
- Source Specific Multicast, page 7

Any Source Multicast

For the Any Source Multicast (ASM) delivery mode, an IP multicast receiver host can use any version of IGMP to join a multicast group. This group is notated as G in the routing table state notation. By joining this group, the receiver host is indicating that it wants to receive IP multicast traffic sent by any source to group G. The network will deliver IP multicast packets from any source host with the destination address G to all receiver hosts in the network that have joined group G.

ASM requires group address allocation within the network. At any given time, an ASM group should only be used by a single application. When two applications use the same ASM group simultaneously, receiver hosts of both applications will receive traffic from both application sources. This may result in unexpected excess traffic in the network. This situation may cause congestion of network links and malfunction of the application receiver hosts.

Source Specific Multicast

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology for the Cisco implementation of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S,G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Protocol Independent Multicast

The Protocol Independent Multicast (PIM) protocol maintains the current IP multicast service mode of receiver-initiated membership. PIM is not dependent on a specific unicast routing protocol; it is IP routing protocol independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and static routes. PIM uses unicast routing information to perform the multicast forwarding function.

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

PIM is defined in RFC 2362, Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification .

PIM can operate in dense mode or sparse mode. The router can handle both sparse groups and dense groups at the same time. The mode determines how the router populates its multicast routing table and how the router forwards multicast packets it receives from its directly connected LANs.

For information about PIM forwarding (interface) modes, see the following sections:

- PIM Dense Mode, page 8
- PIM Sparse Mode, page 9
- Sparse-Dense Mode, page 9
- Bidirectional PIM, page 10

PIM Dense Mode

PIM dense mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network. This push model is a method for delivering data to the receivers without the receivers requesting the data. This method is efficient in certain deployments in which there are active receivers on every subnet in the network.

In dense mode, a router assumes that all other routers want to forward multicast packets for a group. If a router receives a multicast packet and has no directly connected members or PIM neighbors present, a prune message is sent back to the source. Subsequent multicast packets are not flooded to this router on this pruned branch. PIM builds source-based multicast distribution trees.

PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats every 3 minutes.

Routers accumulate state information by receiving data streams through the flood and prune mechanism. These data streams contain the source and group information so that downstream routers can build up their multicast forwarding table. PIM-DM supports only source trees--that is, (S,G) entries--and cannot be used to build a shared distribution tree.

Note Dense mode is not often used and its use is not recommended. For this reason it is not specified in the configuration tasks in related modules.

PIM Sparse Mode

PIM sparse mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic.

Unlike dense mode interfaces, sparse mode interfaces are added to the multicast routing table only when periodic Join messages are received from downstream routers, or when a directly connected member is on the interface. When forwarding from a LAN, sparse mode operation occurs if an RP is known for the group. If so, the packets are encapsulated and sent toward the RP. When no RP is known, the packet is flooded in a dense mode fashion. If the multicast traffic from a specific source is sufficient, the first hop router of the receiver may send Join messages toward the source to build a source-based distribution tree.

PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least, initially), it requires the use of a rendezvous point (RP). The RP must be administratively configured in the network. See the Rendezvous Points, page 11 section for more information.

In sparse mode, a router assumes that other routers do not want to forward multicast packets for a group, unless there is an explicit request for the traffic. When hosts join a multicast group, the directly connected routers send PIM Join messages toward the RP. The RP keeps track of multicast groups. Hosts that send multicast packets are registered with the RP by the first hop router of that host. The RP then sends Join messages toward the source. At this point, packets are forwarded on a shared distribution tree. If the multicast traffic from a specific source is sufficient, the first hop router of the host may send Join messages toward the source to build a source-based distribution tree.

Sources register with the RP and then data is forwarded down the shared tree to the receivers. The edge routers learn about a particular source when they receive data packets on the shared tree from that source through the RP. The edge router then sends PIM (S,G) Join messages toward that source. Each router along the reverse path compares the unicast routing metric of the RP address to the metric of the source address. If the metric for the source address is better, it will forward a PIM (S,G) Join message toward the source. If the metric for the RP is the same or better, then the PIM (S,G) Join message will be sent in the same direction as the RP. In this case, the shared tree and the source tree would be considered congruent.

If the shared tree is not an optimal path between the source and the receiver, the routers dynamically create a source tree and stop traffic from flowing down the shared tree. This behavior is the default behavior in software. Network administrators can force traffic to stay on the shared tree by using the **ip pim spt-threshold infinity** command.

PIM-SM scales well to a network of any size, including those with WAN links. The explicit join mechanism prevents unwanted traffic from flooding the WAN links.

Sparse-Dense Mode

If you configure either sparse mode or dense mode on an interface, then sparseness or denseness is applied to the interface as a whole. However, some environments might require PIM to run in a single region in sparse mode for some groups and in dense mode for other groups.

An alternative to enabling only dense mode or only sparse mode is to enable sparse-dense mode. In this case, the interface is treated as dense mode if the group is in dense mode; the interface is treated in sparse

mode if the group is in sparse mode. You must have an RP if the interface is in sparse-dense mode and you want to treat the group as a sparse group.

If you configure sparse-dense mode, the idea of sparseness or denseness is applied to the groups for which the router is a member.

Another benefit of sparse-dense mode is that Auto-RP information can be distributed in a dense mode; yet, multicast groups for user groups can be used in a sparse mode manner. Therefore there is no need to configure a default RP at the leaf routers.

When an interface is treated in dense mode, it is populated in the outgoing interface list of a multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- There are PIM neighbors and the group has not been pruned.

When an interface is treated in sparse mode, it is populated in the outgoing interface list of a multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- An explicit Join message has been received by a PIM neighbor on the interface.

Bidirectional PIM

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

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

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the RP for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router address, but can be any unassigned IP address on a network that is reachable throughout the PIM domain.

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

Multicast Group Modes

In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco implementation of PIM supports four modes for a multicast group:

- PIM Bidirectional mode
- PIM Sparse mode
- PIM Dense mode
- PIM Source Specific Multicast (SSM) mode

A router can simultaneously support all four modes or any combination of them for different multicast groups.

Bidirectional Mode

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

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

Sparse Mode

Sparse mode operation centers around a single unidirectional shared tree whose root node is called the rendezvous point (RP). Sources must register with the RP to get their multicast traffic to flow down the shared tree by way of the RP. This registration process actually triggers a shortest path tree (SPT) Join by the RP toward the source when there are active receivers for the group in the network.

A sparse mode group uses the explicit join model of interaction. Receiver hosts join a group at a rendezvous point (RP). Different groups can have different RPs.

Multicast traffic packets flow down the shared tree to only those receivers that have explicitly asked to receive the traffic.

Dense Mode

Dense mode operates using the broadcast (flood) and prune model.

In populating the multicast routing table, dense mode interfaces are always added to the table. Multicast traffic is forwarded out all interfaces in the outgoing interface list to all receivers. Interfaces are removed from the outgoing interface list in a process called pruning. In dense mode, interfaces are pruned for various reasons including that there are no directly connected receivers.

A pruned interface can be reestablished, that is, grafted back so that restarting the flow of multicast traffic can be accomplished with minimal delay.

Rendezvous Points

A rendezvous point (RP) is a role that a router performs when operating in PIM-SM mode. An RP is required only in networks running PIM-SM. In PIM-SM, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data is in contrast to the PIM dense mode (PIM-DM) model. In PIM-DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the first hop router of the receiver learns about the source, it will send a Join message

directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

In most cases, the placement of the RP in the network is not a complex decision. By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM version 2, the RP performs less processing than in PIM version 1 because sources must only periodically register with the RP to create state.

Auto-RP

In the first version of PIM-SM, all leaf routers (routers directly connected to sources or receivers) were required to be manually configured with the IP address of the RP. This type of configuration is also known as static RP configuration. Configuring static RPs is relatively easy in a small network, but it can be laborious in a large, complex network.

Following the introduction of PIM-SM version 1, Cisco implemented a version of PIM-SM with the Auto-RP feature. Auto-RP automates the distribution of group-to-RP mappings in a PIM network. Auto-RP has the following benefits:

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

Multiple RPs can be used to serve different group ranges or serve as backups to each other. For Auto-RP to work, a router must be designated as an RP-mapping agent, which receives the RP-announcement messages from the RPs and arbitrates conflicts. The RP-mapping agent then sends the consistent group-to-RP mappings to all other routers. Thus, all routers automatically discover which RP to use for the groups they support.

Note If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must statically configure an RP.

Note If 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.

To make Auto-RP work, a router must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts. The RP mapping agent then sends the consistent group-to-RP mappings to all other routers by dense mode flooding. Thus, all routers automatically discover which RP to use for the groups they support. The Internet Assigned Numbers Authority (IANA) has assigned two group addresses, 224.0.1.39 and 224.0.1.40, for Auto-RP. One advantage of Auto-RP is that any change to the RP designation must be configured only on the routers that are RPs and not on the leaf routers. Another advantage of Auto-RP is that it offers the ability to scope the

RP address within a domain. Scoping can be achieved by defining the time-to-live (TTL) value allowed for the Auto-RP advertisements.

Each method for configuring an RP has its own strengths, weaknesses, and level of complexity. In conventional IP multicast network scenarios, we recommend using Auto-RP to configure RPs because it is easy to configure, well-tested, and stable. The alternative ways to configure an RP are static RP, Auto-RP, and bootstrap router.

Sparse-Dense Mode for Auto-RP

A prerequisite of Auto-RP is that all interfaces must be configured in sparse-dense mode using the **ip pim sparse-dense-mode** interface configuration command. An interface configured in sparse-dense mode is treated in either sparse mode or dense mode of operation, depending on which mode the multicast group operates. If a multicast group has a known RP, the interface is treated in sparse mode. If a group has no known RP, by default the interface is treated in dense mode and data will be flooded over this interface. (You can prevent dense-mode fallback; see the module "Configuring Basic IP Multicast.")

To successfully implement Auto-RP and prevent any groups other than 224.0.1.39 and 224.0.1.40 from operating in dense mode, we recommend configuring a "sink RP" (also known as "RP of last resort"). A sink RP is a statically configured RP that may or may not actually exist in the network. Configuring a sink RP does not interfere with Auto-RP operation because, by default, Auto-RP messages supersede static RP configurations. We recommend configuring a sink RP for all possible multicast groups in your network, because it is possible for an unknown or unexpected source to become active. If no RP is configured to limit source registration, the group may revert to dense mode operation and be flooded with data.

Bootstrap Router

Another RP selection model called bootstrap router (BSR) was introduced after Auto-RP in PIM-SM version 2. BSR performs similarly to Auto-RP in that it uses candidate routers for the RP function and for relaying the RP information for a group. RP information is distributed through BSR messages, which are carried within PIM messages. PIM messages are link-local multicast messages that travel from PIM router to PIM router. Because of this single hop method of disseminating RP information, TTL scoping cannot be used with BSR. A BSR performs similarly as an RP, except that it does not run the risk of reverting to dense mode operation, and it does not offer the ability to scope within a domain.

Multicast Source Discovery Protocol

In the PIM sparse mode model, multicast sources and receivers must register with their local rendezvous point (RP). Actually, the router closest to a source or a receiver registers with the RP, but the key point to note is that the RP "knows" about all the sources and receivers for any particular group. RPs in other domains have no way of knowing about sources that are located in other domains. Multicast Source Discovery Protocol (MSDP) is an elegant way to solve this problem.

MSDP is a mechanism that allows RPs to share information about active sources. RPs know about the receivers in their local domain. When RPs in remote domains hear about the active sources, they can pass on that information to their local receivers. Multicast data can then be forwarded between the domains. A useful feature of MSDP is that it allows each domain to maintain an independent RP that does not rely on other domains, but it does enable RPs to forward traffic between domains. PIM-SM is used to forward the traffic between the multicast domains.

The RP in each domain establishes an MSDP peering session using a TCP connection with the RPs in other domains or with border routers leading to the other domains. When the RP learns about a new multicast source within its own domain (through the normal PIM register mechanism), the RP encapsulates the first data packet in a Source-Active (SA) message and sends the SA to all MSDP peers. Each receiving peer

uses a modified Reverse Path Forwarding (RPF) check to forward the SA, until the SA reaches every MSDP router in the interconnected networks--theoretically the entire multicast internet. If the receiving MSDP peer is an RP, and the RP has a (*, G) entry for the group in the SA (there is an interested receiver), the RP creates (S,G) state for the source and joins to the shortest path tree for the source. The encapsulated data is decapsulated and forwarded down the shared tree of that RP. When the last hop router (the router closest to the receiver) receives the multicast packet, it may join the shortest path tree to the source. The MSDP speaker periodically sends SAs that include all sources within the domain of the RP.

MSDP was developed for peering between Internet service providers (ISPs). ISPs did not want to rely on an RP maintained by a competing ISP to provide service to their customers. MSDP allows each ISP to have its own local RP and still forward and receive multicast traffic to the Internet.

Anycast RP

Anycast RP is a useful application of MSDP. Originally developed for interdomain multicast applications, MSDP used for Anycast RP is an intradomain feature that provides redundancy and load-sharing capabilities. Enterprise customers typically use Anycast RP for configuring a Protocol Independent Multicast sparse mode (PIM-SM) network to meet fault tolerance requirements within a single multicast domain.

In Anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. The Anycast RP loopback address should be configured with a 32-bit mask, making it a host address. All the downstream routers should be configured to “know” that the Anycast RP loopback address is the IP address of their local RP. IP routing automatically will select the topologically closest RP for each source and receiver. Assuming that the sources are evenly spaced around the network, an equal number of sources will register with each RP. That is, the process of registering the sources will be shared equally by all the RPs in the network.

Because 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 SA message will be sent to the other RPs informing them that there is an active source for a particular multicast group. The result is that each RP will know about the active sources in the area of the other RPs. If any of the RPs were to fail, IP routing would converge and one of the RPs would become the active RP in more than one area. New sources would register with the backup RP. Receivers would join toward the new RP and connectivity would be maintained.

Note The RP is normally 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, then an RP failure will not affect that session. Anycast RP ensures that new sessions with sources and receivers can begin at any time.

Multicast Forwarding

Forwarding of multicast traffic is accomplished by multicast-capable routers. These routers create distribution trees that control the path that IP multicast traffic takes through the network in order to deliver traffic to all receivers.

Multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared tree) or a separate distribution tree can be built for each source (a source tree). The shared tree may be one-way or bidirectional.

Before describing the structure of source and shared trees, it is helpful to explain the notations that are used in multicast routing tables. These notations include the following:

- (S,G) = (unicast source for the multicast group G, multicast group G)
- (*,G) = (any source for the multicast group G, multicast group G)

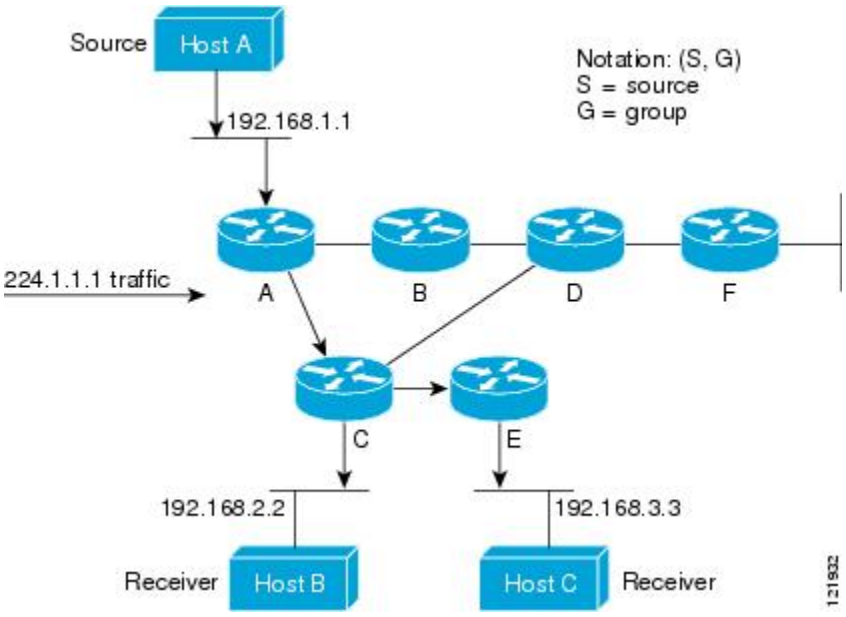
The notation of (S,G), pronounced “S comma G,” enumerates a shortest path tree where S is the IP address of the source and G is the multicast group address.

Shared trees are (*,G) and the source trees are (S,G) and always routed at the sources.

Multicast Distribution Source Tree

The simplest form of a multicast distribution tree is a source tree. A source tree has its root at the source host and has branches forming a spanning tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).

The figure shows an example of an SPT for group 224.1.1.1 rooted at the source, Host A, and connecting two receivers, Hosts B and C.



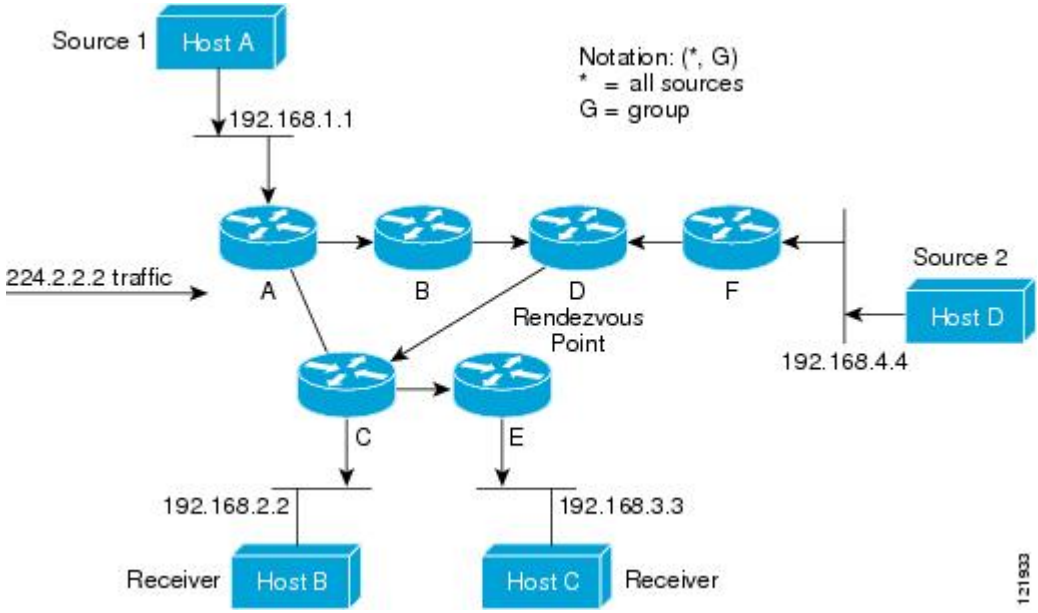
Using standard notation, the SPT for the example shown in the figure would be (192.168.1.1, 224.1.1.1).

The (S,G) notation implies that a separate SPT exists for each individual source sending to each group--which is correct.

Multicast Distribution Shared Tree

Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).

The figure below shows a shared tree for the group 224.2.2.2 with the root located at Router D. This shared tree is unidirectional. Source traffic is sent towards the RP on a source tree. The traffic is then forwarded down the shared tree from the RP to reach all of the receivers (unless the receiver is located between the source and the RP, in which case it will be serviced directly).



In this example, multicast traffic from the sources, Hosts A and D, travels to the root (Router D) and then down the shared tree to the two receivers, Hosts B and C. Because all sources in the multicast group use a common shared tree, a wildcard notation written as (*, G), pronounced “star comma G,” represents the tree. In this case, * means all sources, and G represents the multicast group. Therefore, the shared tree shown in the figure above would be written as (*, 224.2.2.2).

Both source trees and shared trees are loop-free. Messages are replicated only where the tree branches. Members of multicast groups can join or leave at any time; therefore the distribution trees must be dynamically updated. When all the active receivers on a particular branch stop requesting the traffic for a particular multicast group, the routers prune that branch from the distribution tree and stop forwarding traffic down that branch. If one receiver on that branch becomes active and requests the multicast traffic, the router will dynamically modify the distribution tree and start forwarding traffic again.

Source Tree Advantage

Source trees have the advantage of creating the optimal path between the source and the receivers. This advantage guarantees the minimum amount of network latency for forwarding multicast traffic. However, this optimization comes at a cost. The routers must maintain path information for each source. In a network that has thousands of sources and thousands of groups, this overhead can quickly become a resource issue on the routers. Memory consumption from the size of the multicast routing table is a factor that network designers must take into consideration.

Shared Tree Advantage

Shared trees have the advantage of requiring the minimum amount of state in each router. This advantage lowers the overall memory requirements for a network that only allows shared trees. The disadvantage of shared trees is that under certain circumstances the paths between the source and receivers might not be the optimal paths, which might introduce some latency in packet delivery. For example, in the figure above the shortest path between Host A (source 1) and Host B (a receiver) would be Router A and Router C. Because we are using Router D as the root for a shared tree, the traffic must traverse Routers A, B, D and then C. Network designers must carefully consider the placement of the rendezvous point (RP) when implementing a shared tree-only environment.

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination address and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)--which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is described in the following section.

Reverse Path Forwarding

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination network and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)--which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is an algorithm used for forwarding multicast datagrams.

Protocol Independent Multicast (PIM) uses the unicast routing information to create a distribution tree along the reverse path from the receivers towards the source. The multicast routers then forward packets along the distribution tree from the source to the receivers. RPF is a key concept in multicast forwarding. It enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will forward a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop-free.

RPF Check

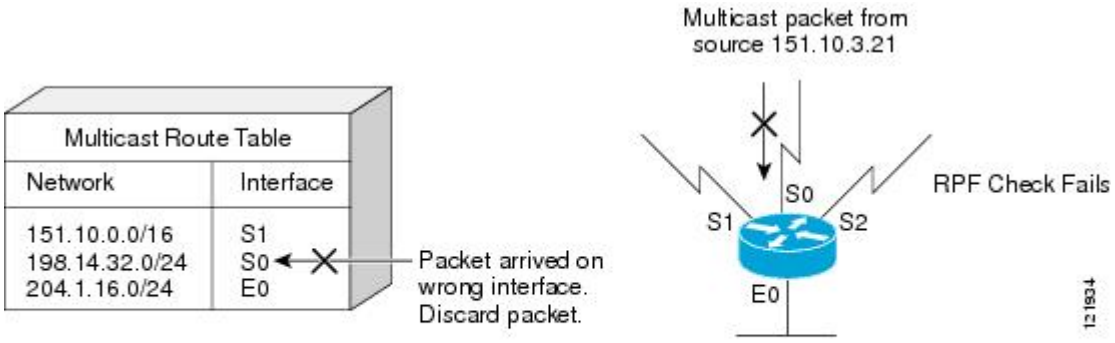
When a multicast packet arrives at a router, the router performs an RPF check on the packet. If the RPF check succeeds, the packet is forwarded. Otherwise, it is dropped.

For traffic flowing down a source tree, the RPF check procedure works as follows:

1. The router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source.
2. If the packet has arrived on the interface leading back to the source, the RPF check succeeds and the packet is forwarded out the interfaces present in the outgoing interface list of a multicast routing table entry.
3. If the RPF check in Step 2 fails, the packet is dropped.

The figure shows an example of an unsuccessful RPF check.

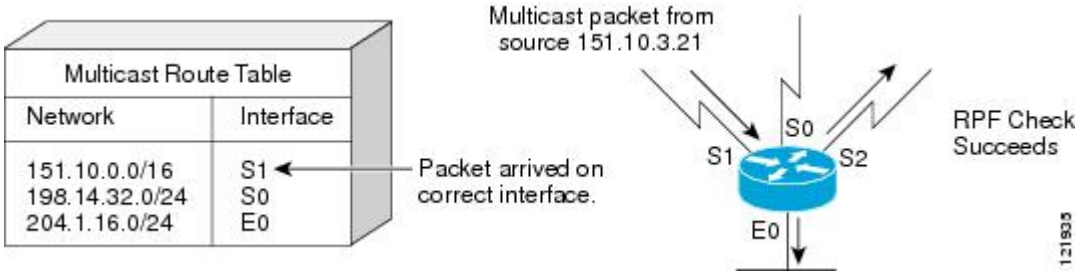
Figure 2 RPF Check Fails



As the figure illustrates, a multicast packet from source 151.10.3.21 is received on serial interface 0 (S0). A check of the unicast route table shows that S1 is the interface this router would use to forward unicast data to 151.10.3.21. Because the packet has arrived on interface S0, the packet is discarded.

The figure shows an example of a successful RPF check.

Figure 3 RPF Check Succeeds



In this example, the multicast packet has arrived on interface S1. The router refers to the unicast routing table and finds that S1 is the correct interface. The RPF check passes, and the packet is forwarded.

PIM Dense Mode Fallback

If you use IP multicast in mission-critical networks, you should avoid the use of PIM-DM (dense mode).

Dense mode fallback describes the event of the PIM mode changing (falling back) from sparse mode (which requires an RP) to dense mode (which does not use an RP). Dense mode fallback occurs when RP information is lost.

If all interfaces are configured with the **ip pim sparse-mode** command, there is no dense mode fallback because dense mode groups cannot be created over interfaces configured for sparse mode.

Cause and Effect of Dense Mode Fallback

PIM determines whether a multicast group operates in PIM-DM or PIM-SM mode based solely on the existence of RP information in the group-to-RP mapping cache. If Auto-RP is configured or a bootstrap router (BSR) is used to distribute RP information, there is a risk that RP information can be lost if all RPs, Auto-RP, or the BSR for a group fails due to network congestion. This failure can lead to the network either partially or fully falling back into PIM-DM.

If a network falls back into PIM-DM and AutoRP or BSR is being used, dense mode flooding will occur. Routers that lose RP information will fallback into dense mode and any new states that must be created for the failed group will be created in dense mode.

Effects of Preventing Dense Mode Fallback

Prior to the introduction of PIM-DM fallback prevention, all multicast groups without a group-to-RP mapping would be treated as dense mode.

With the introduction of PIM-DM fallback prevention, the PIM-DM fallback behavior has been changed to prevent dense mode flooding. By default, if all of the interfaces are configured to operate in PIM sparse mode (using the **ip pim sparse-mode** command), there is no need to configure the **no ip pim dm-fallback** command (that is, the PIM-DM fallback behavior is enabled by default). If any interfaces are not configured using the **ip pim sparse-mode**command (for example, using the **ip pim sparse-dense-mode** command), then the PIM-DM fallback behavior can be explicit disabled using the **no ip pim dm-fallback**command.

When the **no ip pim dm-fallback** command is configured or when **ip pim sparse-mode** is configured on all interfaces, any existing groups running in sparse mode will continue to operate in sparse mode but will use an RP address set to 0.0.0.0. Multicast entries with an RP address set to 0.0.0.0 will exhibit the following behavior:

- Existing (S, G) states will be maintained.
- No PIM Join or Prune messages for (*, G) or (S, G, RPbit) are sent.
- Received (*, G) or (S, G, RPbit) Joins or Prune messages are ignored.
- No registers are sent and traffic at the first hop is dropped.
- Received registers are answered with register stop.
- Asserts are unchanged.
- The (*, G) outgoing interface list (olist) is maintained only for the Internet Group Management Protocol (IGMP) state.
- Multicast Source Discovery Protocol (MSDP) source active (SA) messages for RP 0.0.0.0 groups are still accepted and forwarded.

Guidelines for Choosing a PIM Mode

Before beginning the configuration process, you must decide which PIM mode needs to be used. This determination is based on the applications you intend to support on your network.

Basic guidelines include the following:

- In general, if the application is one-to-many or many-to-many in nature, then PIM-SM can be used successfully.
- For optimal one-to-many application performance, SSM is appropriate but requires IGMP version 3 support.
- For optimal many-to-many application performance, bidirectional PIM is appropriate but hardware support is limited to Cisco devices and the Catalyst 6000 series switches with Sup720.

Where to Go Next

- To configure basic IP multicast, see the “ Configuring Basic IP Multicast ” module.

Additional References

Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	*Cisco IOS IP Multicast Command Reference*

MIBs

MIB	MIBs Link
--	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1112	Host Extensions for IP Multicasting
RFC 2113	IP Router Alert Option
RFC 2362	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
RFC 3180	GLOP Addressing in 233/8

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP Multicast Technology Overview

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for IP Multicast Technology Overview

Feature Names	Releases	Feature Configuration Information
CGMP	Cisco IOS XE Release 2.1	Cisco Group Management Protocol (CGMP) is used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP.
IGMP Version 2	Cisco IOS XE Release 2.1	
IGMP Version 3	Cisco IOS XE Release 2.1	
Uni-Directional Link Routing (UDLR)	Cisco IOS XE Release 2.1	

Feature Names	Releases	Feature Configuration Information
PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss	Cisco IOS XE Release 2.1	The PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss feature enables you to prevent PIM-DM fallback when all RPs fail. Preventing the use of dense mode is very important to multicast networks whose reliability is critical. This feature provides a mechanism to keep the multicast groups in sparse mode, thereby preventing dense mode flooding.
PIM Version 2	Cisco IOS XE Release 3.5S	Protocol Independent Multicast (PIM) version 2 is a multicast routing protocol with two basic operating modes: sparse-mode and dense-mode. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.

Glossary

basic multicast--Interactive intra-domain multicast. Supports multicast applications within an enterprise campus. Also provides an additional integrity in the network with the inclusion of a reliable multicast transport, PGM.

bidir PIM--Bidirectional PIM is an extension to the PIM suite of protocols that implements shared sparse trees with bidirectional flow of data. In contrast to PIM-SM, bidir-PIM avoids keeping source specific state in router and thus allows trees to scale to an arbitrary number of sources.

broadcast--One-to-all transmission where the source sends one copy of the message to all nodes, whether they wish to receive it or not.

Cisco Group Management Protocol (CGMP)--Cisco-developed protocol that allows Layer 2 switches to leverage IGMP information on Cisco routers to make Layer 2 forwarding decisions. It allows the switches to forward multicast traffic to only those ports that are interested in the traffic.

dense mode (DM) (Internet Draft Spec)--Actively attempts to send multicast data to all potential receivers (flooding) and relies upon their self-pruning (removal from group) to achieve desired distribution.

designated router (DR)--The router in a PIM-SM tree that instigates the Join/Prune message cascade upstream to the RP in response to IGMP membership information it receives from IGMP hosts.

distribution tree--Multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared-tree), or a separate distribution tree can be built for each source (a source-tree). The shared-tree may be one-way or bidirectional.

IGMP messages--IGMP messages are encapsulated in standard IP datagrams with an IP protocol number of 2 and the IP Router Alert option (RFC 2113).

IGMP snooping--IGMP snooping requires the LAN switch to examine, or “snoop,” some Layer 3 information in the IGMP packet sent from the host to the router. When the switch hears an IGMP report from a host for a particular multicast group, the switch adds the host’s port number to the associated multicast table entry. When it hears an IGMP Leave Group message from a host, it removes the host’s port from the table entry.

IGMP unidirectional link routing--Cisco’s other UDLR solution is to use IP multicast routing with IGMP, which has been enhanced to accommodate UDLR. This solution scales very well for many satellite links.

Internet Group Management Protocol v2 (IGMP)--Used by IP routers and their immediately connected hosts to communicate multicast group membership states.

Internet Group Management Protocol v3 (IGMP)--IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. Version 3 of IGMP adds support for “source filtering,” that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.

multicast--A routing technique that allows IP traffic to be sent from one source or multiple sources and delivered to multiple destinations. Instead of sending individual packets to each destination, a single packet is sent to a group of destinations known as a multicast group, which is identified by a single IP destination group address. Multicast addressing supports the transmission of a single IP datagram to multiple hosts.

multicast routing monitor (MRM)--A management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

Multicast Source Discovery Protocol (MSDP)--A mechanism to connect multiple PIM sparse mode (PIM-SM) 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 runs MSDP over TCP to discover multicast sources in other domains. MSDP is also used to announce sources sending to a group. These announcements must originate at the domain’s RP. MSDP depends heavily on MBGP for interdomain operation.

Protocol Independent Multicast (PIM)--A multicast routing architecture defined by the IETF that enables IP multicast routing on existing IP networks. Its key point is its independence from any underlying unicast protocol such as OSPF or BGP.

prune--Multicast routing terminology indicating that the multicast-enabled router has sent the appropriate multicast messages to remove itself from the multicast tree for a particular multicast group. It will stop receiving the multicast data addressed to that group and, therefore, cannot deliver the data to any connected hosts until it rejoins the group.

query--IGMP messages originating from the router(s) to elicit multicast group membership information from its connected hosts.

rendezvous point (RP)--The multicast router that is the root of the PIM-SM shared multicast distribution tree.

report--IGMP messages originating from the hosts that are joining, maintaining, or leaving their membership in a multicast group.

source tree--A multicast distribution path that directly connects the source’s and receivers’ designated router (or the rendezvous point) to obtain the shortest path through the network. Results in most efficient routing of data between source and receivers, but may result in unnecessary data duplication throughout the network if built by anything other than the RP.

sparse mode (SM) (RFC 2362)--Relies upon an explicitly joining method before attempting to send multicast data to receivers of a multicast group.

UDLR tunnel--Uses a back channel (another link) so the routing protocols believe the one-way link is bidirectional. The back channel itself is a special, unidirectional, generic route encapsulation (GRE) tunnel through which control traffic flows in the opposite direction of the user data flow. This feature allows IP and its associated unicast and multicast routing protocols to believe the unidirectional link is logically bidirectional. This solution accommodates all IP unicast and multicast routing protocols without changing them. However, it does not scale and no more than 20 tunnels should feed into the upstream router. The purpose of the unidirectional GRE tunnel is to move control packets from a downstream node to an upstream node.

Unicast--Point-to-point transmission requiring the source to send an individual copy of a message to each requester.

unidirectional Link Routing Protocol (UDLR)--A routing protocol that provides a way to forward multicast packets over a physical unidirectional interface (such as a satellite link of high bandwidth) to stub networks that have a back channel.

URL rendezvous directory (URD)--URD is a multicast-lite solution that directly provides the network with information about the specific source of a content stream. It enables the network to quickly establish the most direct distribution path from the source to the receiver, thus significantly reducing the time and effort required in receiving the streaming media. URD allows an application to identify the source of the content stream through a web page link or web directly. When that information is sent back to the application it is then conveyed back to the network using URD.

In this feature, a URD-capable web page provides information about the source, the group, and the application (via media-type) on a web page. An interested host will click on the web page pulling across the information in an HTTP transaction. The last-hop router to receiver would intercept this transaction and send it to a special port allocated by IANA. The last-hop router is also URD capable and uses the information to initiate the PIM source, group (S,G) join on behalf of the host.

Configuring Basic IP Multicast

IP multicast is a bandwidth-conserving technology that reduces traffic by delivering a single stream of information simultaneously to potentially thousands of corporate businesses and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news. This module describes the tasks used to configure basic IP multicast.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Basic IP Multicast

- Before performing the tasks in this module, you should be familiar with the concepts explained in the “IP Multicast Technology Overview” module.
- To determine which of the tasks contained in this module you will have to perform, you must decide which Protocol Independent Multicast (PIM) mode will be used. This determination is based on the applications you intend to support on your network.
- All access lists you intend to use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the “ Creating an IP Access List and Applying It to an Interface ” module.

Information About Configuring Basic IP Multicast

Auto-RP Overview

The Role of Auto-RP in a PIM Network

Auto-RP automates the distribution of group-to-rendezvous point (RP) mappings in a PIM network. To make Auto-RP work, a router must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts. The RP mapping agent then sends the consistent group-to-RP mappings to all other routers by way of dense mode flooding.

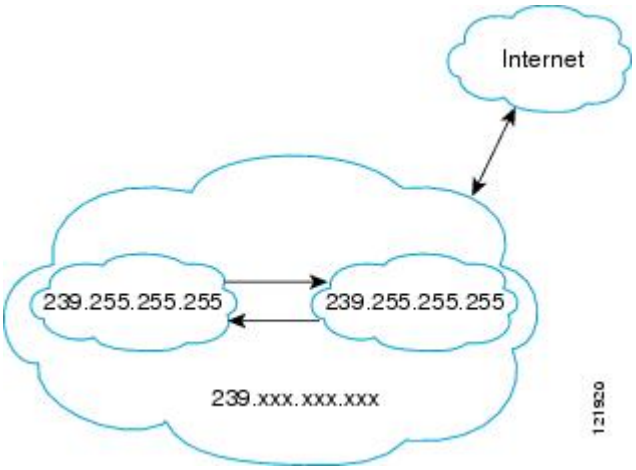
Thus, all routers automatically discover which RP to use for the groups they support. The Internet Assigned Numbers Authority (IANA) has assigned two group addresses, 224.0.1.39 and 224.0.1.40, for Auto-RP.

The mapping agent receives announcements of intention to become the RP from Candidate-RPs. The mapping agent then announces the winner of the RP election. This announcement is made independently of the decisions by the other mapping agents.

IP Multicast Boundary

As shown in the figure, address scoping defines domain boundaries so that domains with RPs that have the same IP address do not leak into each other. Scoping is performed on the subnet boundaries within large domains and on the boundaries between the domain and the Internet.

Figure 4 Address Scoping at Boundaries



You can set up an administratively scoped boundary on an interface for multicast group addresses using the **ip multicast boundary** command with the *access-list* argument. A standard access list defines the range of addresses affected. When a boundary is set up, no multicast data packets are allowed to flow across the boundary from either direction. The boundary allows the same multicast group address to be reused in different administrative domains.

The Internet Assigned Numbers Authority (IANA) has designated the multicast address range 239.0.0.0 to 239.255.255.255 as the administratively scoped addresses. This range of addresses can be reused in domains administered by different organizations. They would be considered local, not globally unique.

You can configure the **filter-autorp** keyword to examine and filter Auto-RP discovery and announcement messages at the administratively scoped boundary. Any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary access control list (ACL) are removed. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Benefits of Auto-RP in a PIM Network

- Auto-RP allows any change to the RP designation to be configured only on the routers that are RPs, not on the leaf routers.
- Auto-RP offers the ability to scope the RP address within a domain. Scoping can be achieved by using the **ip multicast boundary** command with the **filter-autorp** keyword.

Anycast RP Overview

Anycast RP is a useful application of MSDP. Originally developed for interdomain multicast applications, MSDP used for Anycast RP is an intradomain feature that provides redundancy and load-sharing capabilities. Enterprise customers typically use Anycast RP for configuring a Protocol Independent Multicast sparse mode (PIM-SM) network to meet fault tolerance requirements within a single multicast domain.

In anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. The anycast RP loopback address should be configured with a 32-bit mask, making it a host address. All the downstream routers should be configured so that the anycast RP loopback address is the IP address of their local RP. IP routing will automatically select the topologically closest RP for each source and receiver. Assuming that the sources are evenly spaced around the network, an equal number of sources will register with each RP. That is, the process of registering the sources will be shared equally by all the RPs in the network.

Because 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 SA message will be sent to the other RPs informing them that there is an active source for a particular multicast group. The result is that each RP will know about the active sources in the area of the other RPs. If any of the RPs were to fail, IP routing would converge, and one of the RPs would become the active RP in more than one area. New sources would register with the backup RP. Receivers would join the new RP and connectivity would be maintained.

The RP is normally needed only to start new sessions with sources and receivers. The RP facilitates the shared tree so that sources and receivers can establish a direct multicast data flow. If a multicast data flow is already 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.

BSR Overview

BSR Election and Functionality

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 performed 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; they use bootstrap messages to discover which BSR has the highest priority. This router then announces to all PIM routers in the PIM domain that it is the BSR.

Following the election of the BSR, candidate RPs use unicast to announce to the BSR their willingness to be the RP. The BSR advertises the entire group-to-RP mapping set to the router link local address 224.0.0.13. Unlike the RP mapping agent in Auto-RP, which is used by Auto-RP to select the RP, every router in the BSR network is responsible for selecting the RP.

BSR lacks the ability to scope RP advertisements; however, BSR is used when vendor interoperability or open standard adherence is a requirement.

BSR Border Interface

A border interface in a PIM sparse mode domain requires precautions to prevent exchange of certain traffic with a neighboring domain reachable through that interface, especially if that domain is also running PIM sparse mode. BSR and Auto-RP messages should not be exchanged between different domains, because routers in one domain may elect RPs in the other domain, resulting in protocol malfunction or loss of isolation between the domains. Configure a BSR border interface to prevent BSR messages from being sent or received through an interface.

Static RP Overview

If you are configuring PIM sparse mode, you must configure a PIM RP for a multicast group. An RP can either be configured statically in each device, or learned through a dynamic mechanism. This task explains how to statically configure an RP, as opposed to the router learning the RP through a dynamic mechanism such as Auto-RP.

PIM designated routers (DRs) forward data from directly connected multicast sources to the RP for distribution down the shared tree. Data is forwarded to the RP in one of two ways. It is encapsulated in register packets and unicast directly to the RP, or, if the RP has itself joined the source tree, it is multicast forwarded per the RPF forwarding algorithm. Last hop routers directly connected to receivers may, at their discretion, join themselves to the source tree and prune themselves from the shared tree.

A single RP can be configured for multiple groups that are defined by an access list. If no RP is configured for a group, the router treats the group as dense using the PIM dense mode techniques. (You can prevent this occurrence by configuring the **no ip pim dm-fallback**command.)

If dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping (with the **ip pim rp-address override**command) will take precedence.

Note If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.

SSM Overview

Source Specific Multicast (SSM). SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.

SSM Components

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569. The following two components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

Protocol Independent Multicast (PIM) SSM, or PIM-SSM, is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which is required for SSM. IGMP For SSM to run with IGMPv3, SSM must be supported in the router, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The standard IP multicast infrastructure in the Internet and many enterprise intranets is based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have proved to be reliable, extensive, and efficient. However, they are bound to the complexity and functionality limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic. With SSM, this information is provided by receivers through the source addresses relayed to the last-hop routers by IGMPv3. SSM is an incremental response to the issues associated with ISM and is intended to coexist in the network with the protocols developed for ISM. In general, SSM provides IP multicast service for applications that utilize SSM.

ISM service is described in RFC 1112. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary 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 host group. Membership in a host group simply requires signaling the host group through IGMP Version 1, 2, or 3.

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. In both SSM and ISM, no signaling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signaling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMP Version 3.

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Internet Assigned Numbers Authority (IANA) has reserved the address range from 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. The software allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 through 239.255.255.255. When an SSM range is defined, an existing IP multicast receiver application will not receive any traffic when it tries to use addresses in the SSM range unless the application is modified to use explicit (S, G) channel subscription or is SSM-enabled through a URL Rendezvous Directory (URD).

SSM Operations

An established network in which IP multicast service is based on PIM-SM can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM. That is, SSM does not require an RP, so there is no need for an RP mechanism such as Auto-RP, MSDP, or bootstrap router (BSR).

If SSM is deployed in a network that is already configured for PIM-SM, then only the last-hop routers must be upgraded to a software image that supports SSM. Routers that are not directly connected to receivers do not have to upgrade to a software image that supports SSM. In general, these non-last-hop routers must only run PIM-SM in the SSM range. They may need additional access control configuration to suppress MSDP signaling, registering, or PIM-SM shared-tree operations from occurring within the SSM range.

The SSM mode of operation is enabled by configuring the SSM range using the **ip pim ssm** global configuration command. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 INCLUDE mode membership reports.
- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-SM. In this mode, only PIM (S, G) Join and Prune messages are generated by the router. Incoming messages related to rendezvous point tree (RPT) operations are ignored or rejected, and incoming PIM register messages are immediately answered with Register-Stop messages. PIM-SSM is backward-compatible with PIM-SM unless a router is a last-hop router. Therefore, routers that are not last-hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- For groups within the SSM range, no MSDP Source-Active (SA) messages within the SSM range will be accepted, generated, or forwarded.

IGMPv3 Host Signaling

IGMPv3 is the third version of the IETF standards track protocol in which hosts signal membership to last-hop routers of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership that allows filtering capabilities with respect to sources. A host can signal either that it wants to receive traffic from all sources sending to a group except for some specific sources (a mode called EXCLUDE) or that it wants to receive traffic only from some specific sources sending to the group (a mode called INCLUDE).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode reports are accepted by the last-hop router. In SSM, only INCLUDE mode reports are accepted by the last-hop router.

Benefits of Source Specific Multicast

IP Multicast Address Management Not Required

In the ISM service, applications must acquire a unique IP multicast group address because traffic distribution is based only on the IP multicast group address used. If two applications with different sources and receivers use the same IP multicast group address, then receivers of both applications will receive traffic from the senders of both applications. Even though the receivers, if programmed appropriately, can filter out the unwanted traffic, this situation would cause generally unacceptable levels of unwanted traffic.

Allocating a unique IP multicast group address for an application is still a problem. Most short-lived applications use mechanisms like Session Description Protocol (SDP) and Session Announcement Protocol (SAP) to get a random address, a solution that does not work well with a rising number of applications in the Internet. The best current solution for long-lived applications is described in RFC 2770, but this solution suffers from the restriction that each autonomous system is limited to only 255 usable IP multicast addresses.

In SSM, traffic from each source is forwarded between routers in the network independent of traffic from other sources. Thus different sources can reuse multicast group addresses in the SSM range.

Denial of Service Attacks from Unwanted Sources Inhibited

In SSM, multicast traffic from each individual source will be transported across the network only if it was requested (through IGMPv3, IGMP v3lite, or URD memberships) from a receiver. In contrast, ISM forwards traffic from any active source sending to a multicast group to all receivers requesting that multicast group. In Internet broadcast applications, this ISM behavior is highly undesirable because it allows unwanted sources to easily disturb the actual Internet broadcast source by simply sending traffic to the same multicast group. This situation depletes bandwidth at the receiver side with unwanted traffic and thus disrupts the undisturbed reception of the Internet broadcast. In SSM, this type of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

Easy to Install and Manage

SSM is easy to install and provision in a network because it does not require the network to maintain which active sources are sending to multicast groups. This requirement exists in ISM (with IGMPv1, IGMPv2, or IGMPv3).

The current standard solutions for ISM service are PIM-SM and MSDP. Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or BSR) and MSDP is required only for the network to learn about active sources. This management is not necessary in SSM, which makes SSM easier than ISM to install and manage, and therefore easier than ISM to operationally scale in deployment. Another factor that contributes to the ease of installation of SSM is the fact that it can leverage preexisting PIM-SM networks and requires only the upgrade of last hop routers to support IGMPv3, IGMP v3lite, or URD.

Ideal for Internet Broadcast Applications

The three benefits previously described make SSM ideal for Internet broadcast-style applications for the following reasons:

- The ability to provide Internet broadcast services through SSM without the need for unique IP multicast addresses allows content providers to easily offer their service (IP multicast address allocation has been a serious problem for content providers in the past).
- The prevention against DoS attacks is an important factor for Internet broadcast services because, with their exposure to a large number of receivers, they are the most common targets for such attacks.
- The ease of installation and operation of SSM makes it ideal for network operators, especially in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains).

Bidir-PIM Overview

Bidir-PIM shares many of its shortest path tree (SPT) operations with PIM-SM. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but has no registering process for sources as in PIM-SM. These modifications allow forwarding of traffic in all routers based solely on the (*, G) multicast routing entries. This form of forwarding eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

Multicast Group Modes

In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco implementation of PIM supports four modes for a multicast group:

- PIM bidirectional mode
- PIM dense mode
- PIM sparse mode
- PIM Source Specific Mode (SSM)

A router can simultaneously support all four modes or any combination of them for different multicast groups.

Bidirectional Shared Tree

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

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

The figures show the difference in state created per router for a unidirectional shared tree and source tree versus a bidirectional shared tree.

Figure 5 Unidirectional Shared Tree and Source Tree

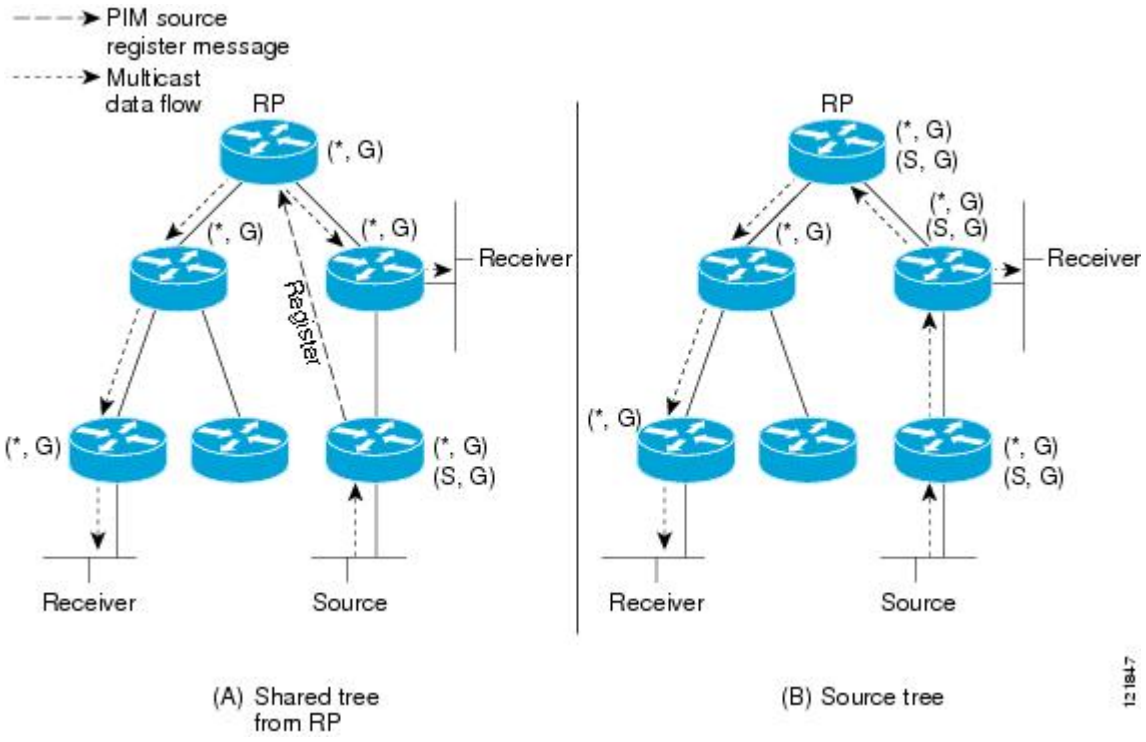
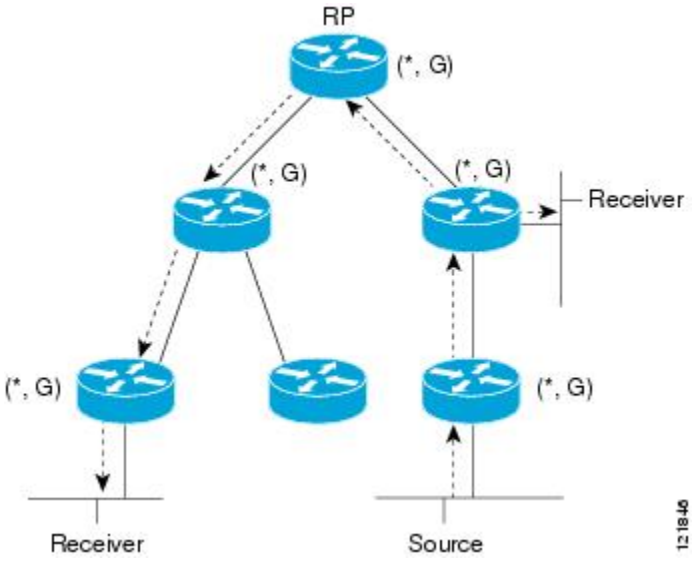


Figure 6 Bidirectional Shared Tree



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

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

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

DF Election

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

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

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

Bidirectional Group Tree Building

The procedure for joining the shared tree of a bidirectional group is almost identical to that used in PIM-SM. One main difference is that, for bidirectional groups, the role of the DR is assumed by the DF for the RP.

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

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

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

Packet Forwarding

A router creates (*, G) entries only for bidirectional groups. The olist of a (*, G) entry includes all the interfaces for which the router has been elected DF and that have received either an IGMP or PIM Join message. If a router is located on a sender-only branch, it will also create a (*, G) state, but the olist will not include any interfaces.

If a packet is received from the RPF interface toward the RP, the packet is forwarded downstream according to the olist of the (*, G) entry. Otherwise, only the router that is the DF for the receiving interface forwards the packet upstream toward the RP; all other routers must discard the packet.

Benefits of Bidirectional PIM

- Bidir-PIM removes the performance cost of maintaining a routing state table for a large number of sources.
- Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional PIM mode can scale to an arbitrary number of sources without incurring overhead due to the number of sources.

How to Configure Basic IP Multicast

The tasks described in this section configure the basic IP multicast modes. No single task in this section is required; however, at least one of the tasks must be performed to configure IP multicast in a network. More than one of the tasks may be needed.

- Configuring Sparse Mode with Auto-RP, page 35
- Configuring Sparse Mode with Anycast RP, page 40
- Configuring Sparse Mode with a Bootstrap Router, page 44
- Configuring Sparse Mode with a Single Static RP, page 49
- Configuring Source Specific Multicast, page 52
- Configuring Bidirectional PIM, page 54

Configuring Sparse Mode with Auto-RP

This section contains information about and instructions on how to configure auto-rendezvous point (Auto-RP). Auto-RP can also be optionally used with anycast RP.

Note The simultaneous deployment of Auto-RP and bootstrap router (BSR) is not supported.

- When configuring Auto-RP, you must either configure the Auto-RP listener feature using the **ip pim autorp listener** command (Step 5) and specify sparse mode using the **ip pim sparse-mode** command (Step 7) or specify sparse-dense mode (Step 8) using the **ip pim sparse-dense mode** command.

Note When you configure sparse-dense mode, dense mode failover may result in a network dense-mode flood. To avoid this condition, use PIM sparse mode with the Auto-RP listener feature.

- An interface configured in sparse-dense mode is treated in either sparse mode or dense mode of operation, depending on the mode in which the multicast group operates. You must decide how to configure your interfaces.
- All access lists that are needed when Auto-RP is configured should be configured prior to beginning the configuration task. For information about how to configure an access list, see the “ Creating an IP Access List and Applying It to an Interface ” module.

- If a group has no known RP and the interface is configured to be sparse-dense mode, the interface is treated as if it were in dense mode, and data is flooded over the interface. To avoid this data flooding, configure the Auto-RP listener using the **ip pim autorp listener** command and then configure the interface as sparse mode using the **ip pim sparse mode** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. Either perform Steps 5 through 7 or perform Steps 6 and 8.
5. **ip pim autorp listener**
6. **interface** *type number*
7. **ip pim sparse-mode**
8. **ip pim sparse-dense-mode**
9. **exit**
10. Repeat Steps 1 through 9 on all PIM interfaces.
11. **ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]
12. **ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*]
13. **ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list*
14. **no ip pim dm-fallback**
15. **interface** *type number*
16. **ip multicast boundary** *access-list* [**filter-autorp**]
17. **end**
18. **show ip pim autorp**
19. **show ip pim rp** [**mapping**] [*rp-address*]
20. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
21. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enabled Multicast Distributed Switching.
Step 4	Either perform Steps 5 through 7 or perform Steps 6 and 8.	--
Step 5	**ip pim autorp listener** **Example:** `Router(config)# ip pim autorp listener`	Causes IP multicast traffic for the two Auto-RP groups 224.0.1.39 and 224.0.1.40 to be PIM dense mode flooded across interfaces operating in PIM sparse mode. • Skip this step if you are configuring sparse-dense mode in Step 8.
Step 6	**interface** *type number* **Example:** `Router(config)# interface Gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 7	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on an interface. When configuring Auto-RP in sparse mode, you must also configure the Auto-RP listener in the next step. • Skip this step if you are configuring sparse-dense mode in Step 8.
Step 8	**ip pim sparse-dense-mode** **Example:** `Router(config-if)# ip pim sparse-dense-mode`	Enables PIM sparse-dense mode on an interface. • Skip this step if you configured sparse mode in Step 7.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 10	Repeat Steps 1 through 9 on all PIM interfaces.	--

Command or Action	Purpose
Step 11 **ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**] **Example:** `Router(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5`	Sends RP announcements out all PIM-enabled interfaces. • Perform this step on the RP router only. • Use the *interface-type*and *interface-number* arguments to define which IP address is to be used as the RP address. • Use the *ip-address* argument to specify a directly connected IP address as the RP address. **Note** If the *ip-address* argument is configured for this command, the RP-announce message will be sourced by the interface to which this IP address is connected (that is, the source address in the IP header of the RP-announce message is the IP address of that interface). • This example shows that the interface is enabled with a maximum of 31 hops. The IP address by which the router wants to be identified as RP is the IP address associated with loopback interface 0. Access list 5 describes the groups for which this router serves as RP.
Step 12 **ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*] **Example:** `Router(config)# ip pim send-rp-discovery loopback 1 scope 31`	Configures the router to be an RP mapping agent. • Perform this step on RP mapping agent routers or on combined RP/RP mapping agent routers. **Note** Auto-RP allows the RP function to run separately on one router and the RP mapping agent to run on one or multiple routers. It is possible to deploy the RP and the RP mapping agent on a combined RP/RP mapping agent router. • Use the optional *interface-type* and *interface-number* arguments to define which IP address is to be used as the source address of the RP mapping agent. • Use the **scope** keyword and *ttl-value* argument to specify the Time-to-Live (TTL) value in the IP header of Auto-RP discovery messages. • Use the optional **interval** keyword and *seconds* argument to specify the interval at which Auto-RP discovery messages are sent. **Note** Lowering the interval at which Auto-RP discovery messages are sent from the default value of 60 seconds results in more frequent floodings of the group-to-RP mappings. In some network environments, the disadvantages of lowering the interval (more control packet overhead) may outweigh the advantages (more frequent group-to-RP mapping updates). • The example shows limiting the Auto-RP discovery messages to 31 hops on loopback interface 1.

	Command or Action	Purpose
Step 13	**ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list* **Example:** `Router(config)# ip pim rp-announce-filter rp-list 1 group-list 2`	Filters incoming RP announcement messages sent from candidate RPs (C-RPs) to the RP mapping agent. • Perform this step on the RP mapping agent only.
Step 14	**no ip pim dm-fallback** **Example:** `Router(config)# no ip pim dm-fallback`	(Optional) Prevents PIM dense mode fallback. • Skip this step if all interfaces have been configured to operate in PIM sparse mode. **Note** The **no ip pim dm-fallback** command behavior is enabled by default if all the interfaces are configured to operate in PIM sparse mode (using the **ip pim sparse-mode** command).
Step 15	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 16	**ip multicast boundary** *access-list* [**filter-autorp**] **Example:** `Router(config-if)# ip multicast boundary 10 filter-autorp`	Configures an administratively scoped boundary. • Perform this step on the interfaces that are boundaries to other routers. • The access list is not shown in this task. • An access list entry that uses the **deny** keyword creates a multicast boundary for packets that match that entry.
Step 17	**end** **Example:** `Router(config-if)# end`	Returns to global configuration mode.
Step 18	**show ip pim autorp** **Example:** `Router# show ip pim autorp`	(Optional) Displays the Auto-RP information.

	Command or Action	Purpose
Step 19	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Router# show ip pim rp mapping`	(Optional) Displays RPs known in the network and shows how the router learned about each RP.
Step 20	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `Router# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP). • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
Step 21	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `Router# show ip mroute cbone-audio`	(Optional) Displays the contents of the IP multicast routing (mroute) table.

• What to Do Next, page 40

What to Do Next

Proceed to the “ Verifying IP Multicast Operation ” module.

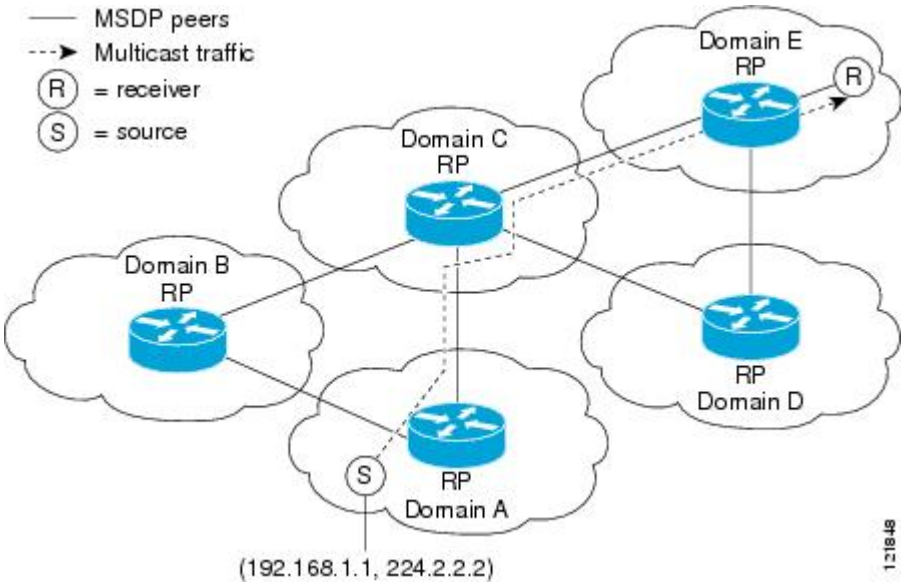
Configuring Sparse Mode with Anycast RP

This section describes how to configure sparse mode with anycast RP for RP redundancy.

Anycast RPs are configured statically, and interfaces are configured to operate in Protocol Independent Multicast-Sparse Mode (PIM-SM). In an anycast RP configuration, two or more RPs are configured with the same IP address on loopback interfaces. The Anycast RP loopback address should be configured with a 32-bit mask, making it a host address. An Anycast RP configuration is easy to configure and troubleshoot because the same host address is used as the RP address regardless of which router it is configured on.

Anycast RP allows two or more rendezvous points (RPs) to share the load for source registration and have the ability to act as hot backup routers for each other. Multicast Source Discovery Protocol (MSDP) is the key protocol that makes anycast RP possible.

Figure 7 MSDP Sharing Source Information Between RPs in Each Domain



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **ip pim rp-address** *rp-address*
7. Repeat Steps 1 through 6 on two or more routers assigning the same RP address to each.
8. **interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
9. **interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
10. **exit**
11. **ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type* **interface-number**] [**remote-as** *as-number*]
12. **ip msdp originator-id loopback** [*interface*]
13. Repeat Steps 8 through 12 on the redundant RPs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables sparse mode.
Step 6	**ip pim rp-address** *rp-address* **Example:** `Router(config-if)# ip pim rp-address 10.0.0.1`	Configures the address of a PIM RP for a particular group.
Step 7	Repeat Steps 1 through 6 on two or more routers assigning the same RP address to each.	--

	Command or Action	Purpose

Step 8	**interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
	
	Example:
	`Router(config-if)# interface loopback 0`
	
	Example:
	`ip address 10.0.0.1 255.255.255.255`
		Configures the interface loopback IP address for the RP router.
		• Perform this step on the RP routers.

Step 9	**interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
	
	Example:
	`Router(config-if)# interface loopback 1`
	
	Example:
	`ip address 10.1.1.1 255.255.255.255`
		Configures the interface loopback IP address for MSDP peering.

Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type* **interface-number**] [**remote-as** *as-number*] **Example:** `Router(config)# ip msdp peer 10.1.1.2 connect-source loopback 1`	Configures an MSDP peer. • Perform this step on the RP routers.
Step 12	**ip msdp originator-id loopback** [*interface*] **Example:** `Router(config)# ip msdp originator-id loopback 1`	Allows an MSDP speaker that originates a SA message to use the IP address of the interface as the RP address in the SA message. • Perform this step on the RP routers.
Step 13	Repeat Steps 8 through 12 on the redundant RPs.	--

• What to Do Next, page 44

What to Do Next

Proceed to the " Verifying IP Multicast Operation " module.

Configuring Sparse Mode with a Bootstrap Router

This section describes how to configure a bootstrap router (BSR), which provides a fault-tolerant, automated RP discovery and distribution mechanism so that routers learn the group-to-RP mappings dynamically.

Note The simultaneous deployment of Auto-RP and BSR is not supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **end**
7. Repeat Steps 1 through 6 on every multicast-enabled interface on every router.
8. **ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]
9. **ip pim rp-candidate** *interface-type interface-number* [group-list *access-list*] [**interval** seconds] [**priority** *value*]
10. Repeat Steps 8 through 10 on all RP and BSR routers.
11. **interface** *type number*
12. **ip pim bsr-border**
13. **end**
14. Repeat Steps 11 through 13 on all the routers that have boundary interfaces where the messages should not be sent or received.
15. **show ip pim rp** [**mapping**] [*rp-address*]
16. **show ip pim rp-hash** [*group-address*] [*group-name*]
17. **show ip pim bsr-router**
18. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
19. **show ip mroute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables sparse mode.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to global configuration mode.
Step 7	Repeat Steps 1 through 6 on every multicast-enabled interface on every router.	--

	Command or Action	Purpose
Step 8	**ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]] **Example:** `Router(config)# ip pim bsr-candidate gigibitethernet 0/0/0 0 192`	Configures the router to announce its candidacy as a bootstrap router (BSR). • Perform this step on the RP or on combined RP/BSR routers. **Note** BSR allows the RP function to run separately on one router and the BSR to run on one or multiple routers. It is possible to deploy the RP and the BSR on a combined RP/BSR router. • This command configures the router to send BSR messages to all its PIM neighbors, with the address of the designated interface (configured for the *interface-type* and *interface-number*arguments) as the BSR address. • Use the optional *hash-mask-length* argument to set the length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0. • Use the optional *priority* argument (after you set the hash mask length) to specify the priority of the BSR as a C-RP. The priority range is from 0 to 255. The BSR C-RP with the highest priority (the lowest priority value) is preferred. If the priority values are the same, the router with the higher IP address is preferred. The default priority value is 0. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.

	Command or Action	Purpose
Step 9	**ip pim rp-candidate** *interface-type interface-number* [group-list *access-list*] [**interval** seconds] [**priority** *value*] **Example:** `Router(config)# ip pim rp-candidate gigabitethernet 2/0/0 group-list 4 priority 192`	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR. • Perform this step on the RP or on combined RP/BSR routers. **Note** BSR allows the RP function to run separately on one router and the BSR to run on one or multiple routers. It is possible to deploy the RP and the BSR on a combined RP/BSR router. • When an interval is specified, the candidate RP advertisement interval is set to the number of seconds specified. The default interval is 60 seconds. Tuning this interval down can reduce the time required to fail over to a secondary RP at the expense of generating more PIMv2 messages. • The Cisco IOS and Cisco IOS XE implementation of PIM BSR selects an RP from a set of candidate RPs using a method that is incompatible with the specification in RFC 2362. See the BSR and RFC 2362 Interoperable Candidate RP Example, page 59 section for a configuration workaround. See CSCdy56806 using the Cisco Bug Toolkit for more information. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.
Step 10	Repeat Steps 8 through 10 on all RP and BSR routers.	--
Step 11	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 12	**ip pim bsr-border** **Example:** `Router(config-if)# ip pim bsr-border`	Prevents the bootstrap router (BSR) messages from being sent or received through an interface. • See the BSR Border Interface, page 28 section for more information.

	Command or Action	Purpose
Step 13	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 14	Repeat Steps 11 through 13 on all the routers that have boundary interfaces where the messages should not be sent or received.	--
Step 15	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Router# show ip pim rp`	(Optional) Displays active rendezvous points (RPs) that are cached with associated multicast routing entries.
Step 16	**show ip pim rp-hash** [*group-address*] [*group-name*] **Example:** `Router# show ip pim rp-hash 239.1.1.1`	(Optional) Displays which rendezvous point (RP) is being selected for a specified group.
Step 17	**show ip pim bsr-router** **Example:** `Router# show ip pim bsr-router`	(Optional) Displays the bootstrap router (BSR) information.
Step 18	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `Router# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the router and that were learned through IGMP. • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
Step 19	**show ip mroute** **Example:** `Router# show ip mroute cbone-audio`	(Optional) Displays the contents of the IP mroute table.

• What to Do Next, page 49

What to Do Next

Proceed to the " Verifying IP Multicast Operation " module.

Configuring Sparse Mode with a Single Static RP

A rendezvous point (RP) is required in networks running Protocol Independent Multicast sparse mode (PIM-SM). In PIM-SM, traffic will be forwarded only to network segments with active receivers that have explicitly requested multicast data.

This section describes how to configure sparse mode with a single static RP.

All access lists that are needed when sparse mode is configured with a single static RP should be configured prior to beginning the configuration task.

Note The same RP address cannot be used for both bidirectional and sparse mode PIM groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. Repeat Steps 1 through 5 on every interface that uses IP multicast.
7. **exit**
8. **ip pim rp-address** *rp-address* [*access-list*] [**override**]
9. **end**
10. **show ip pim rp** [**mapping**] [*rp-address*]
11. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
12. **show ip mroute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM on an interface. You must use sparse mode.
Step 6	Repeat Steps 1 through 5 on every interface that uses IP multicast.	--
Step 7	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 8	**ip pim rp-address** *rp-address* [*access-list*] [**override**] **Example:** `Router(config)# ip pim rp-address 192.168.0.0`	Configures the address of a PIM RP for a particular group. • The optional *access-list* argument is used to specify the number or name a standard access list that defines the multicast groups to be statically mapped to the RP. **Note** If no access list is defined, the RP will map to all multicast groups, 224/4. • The optional **override** keyword is used to specify that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. **Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
Step 9	**end** **Example:** `Router(config)# end`	Ends the current configuration session and returns to EXEC mode.
Step 10	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Router# show ip pim rp mapping`	(Optional) Displays RPs known in the network and shows how the router learned about each RP.
Step 11	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `Router# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the router and that were learned through IGMP. • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
Step 12	**show ip mroute** **Example:** `Router# show ip mroute`	(Optional) Displays the contents of the IP mroute table.

• What to Do Next, page 51

What to Do Next

Proceed to the “ Verifying IP Multicast Operation ” module.

Configuring Source Specific Multicast

This section describes how to configure Source Specific Multicast (SSM).

If you want to use an access list to define the SSM range, configure the access list before you reference the access list in the **ip pim ssm** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **ip pim ssm** {**default** | **range** *access-list*}
5. **interface** *type number*
6. **ip pim sparse-mode**
7. Repeat Steps 1 through 6 on every interface that uses IP multicast.
8. **ip igmp version 3**
9. Repeat Step 8 on all host-facing interfaces.
10. **end**
11. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
12. **show ip mroute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.

	Command or Action	Purpose
Step 4	**ip pim ssm** {**default** | **range** *access-list*} **Example:** `Router(config)# ip pim ssm default`	Configures SSM service. • The **default** keyword defines the SSM range access list as 232/8. • The **range** keyword specifies the standard IP access list number or name that defines the SSM range.
Step 5	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
Step 6	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM on an interface. You must use sparse mode.
Step 7	Repeat Steps 1 through 6 on every interface that uses IP multicast.	--
Step 8	**ip igmp version 3** **Example:** `Router(config-if)# ip igmp version 3`	Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2. Version 3 is required by SSM.
Step 9	Repeat Step 8 on all host-facing interfaces.	--
Step 10	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 11	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `Router# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the router and that were learned through IGMP. • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.

	Command or Action	Purpose
Step 12	**show ip mroute** **Example:** `Router# show ip mroute`	(Optional) Displays the contents of the IP mroute table. • This command displays whether a multicast group is configured for SSM service or a source-specific host report has been received.

• What to Do Next, page 54

What to Do Next

Proceed to the " Verifying IP Multicast Operation " module.

Configuring Bidirectional PIM

This section describes how to configure bidirectional PIM (bidir-PIM).

All access lists needed when configuring bidirectional PIM must be configured prior to beginning the configuration task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **exit**
7. **ip pim bidir-enable**
8. **ip pim rp-address** *rp-address* [*access-list*] [**override**] **bidir**
9. **end**
10. Repeat Steps 2 through 9 on every multicast-enabled interface on every router.
11. **show ip pim rp** [**mapping**] [*rp-address*]
12. **show ip mroute**
13. **show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables sparse mode.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**ip pim bidir-enable** **Example:** `Router(config)# ip pim bidir-enable`	Enables bidir-PIM on a router. • Perform this step on every router.

	Command or Action	Purpose
Step 8	**ip pim rp-address** *rp-address* [*access-list*] [**override**] **bidir** **Example:** `Router(config)# ip pim rp-address 10.0.1.1 45 bidir`	Configures the address of a PIM RP for a particular group. • Perform this step on every router. • This command defines the RP as bidirectional and defines the bidirectional group by way of the access list. • The optional **override** keyword is used to specify that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. **Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
Step 9	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 10	Repeat Steps 2 through 9 on every multicast-enabled interface on every router.	--
Step 11	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Router# show ip pim rp`	(Optional) Displays active RPs that are cached with associated multicast routing entries.
Step 12	**show ip mroute** **Example:** `Router# show ip mroute`	(Optional) Displays the contents of the IP mroute table.
Step 13	**show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] **Example:** `Router# show ip pim interface`	(Optional) Displays information about the elected DF for each RP of an interface, along with the unicast routing metric associated with the DF.

Configuration Examples for Basic IP Multicast

Sparse Mode with Auto-RP Example

The following example configures sparse mode with Auto-RP:

```
ip multicast-routing
ip pim autorp listener
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
no ip pim dm-fallback
access-list 1 permit 239.254.2.0 0.0.0.255
access-list 1 permit 239.254.3.0 0.0.0.255
.
.
.
access-list 10 permit 224.0.1.39
access-list 10 permit 224.0.1.40
access-list 10 permit 239.254.2.0 0.0.0.255
access-list 10 permit 239.254.3.0 0.0.0.255
```

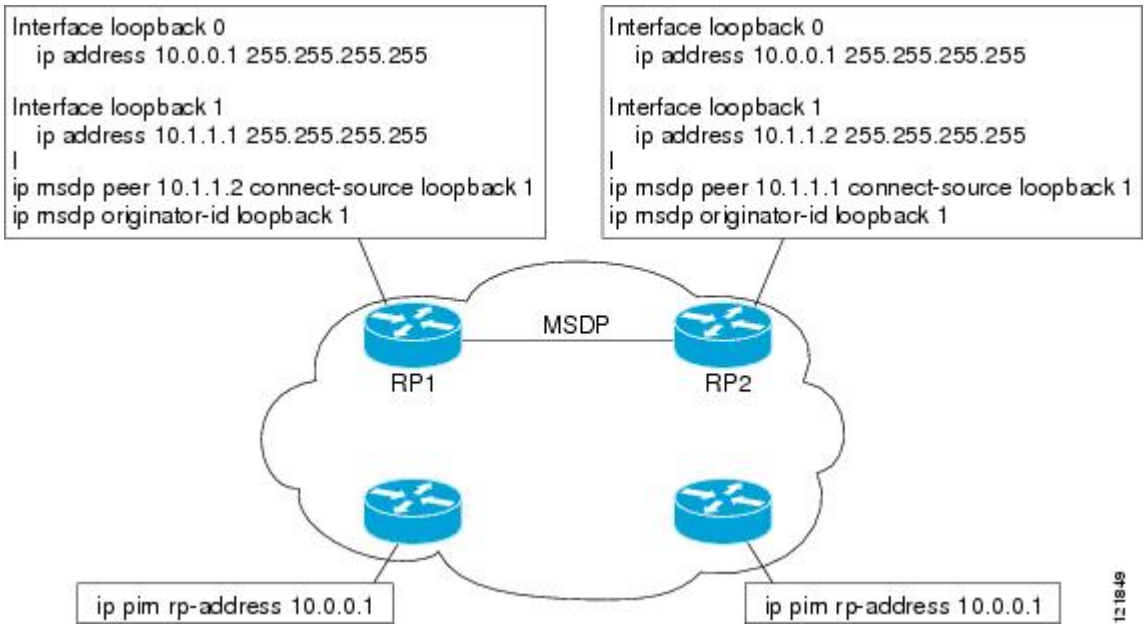
Sparse Mode with Anycast RP Example

The main purpose of an Anycast RP implementation is that the downstream multicast routers will have just one address for an RP. The example given in the figure below shows how loopback interface 0 of the RPs (RP1 and RP2) is configured with the 10.0.0.1 IP address. If this 10.0.0.1 address is configured on all RPs as the address for loopback interface 0 and then configured as the RP address, IP routing will converge on the closest RP. This address must be a host route; note the 255.255.255.255 subnet mask.

The downstream routers must be informed about the 10.0.0.1 RP address. In the figure below, the routers are configured statically with the **ip pim rp-address 10.0.0.1**global configuration command. This configuration could also be accomplished using the Auto-RP or bootstrap router (BSR) features.

The RPs in the figure below must also share source information using MSDP. In this example, loopback interface 1 of the RPs (RP1 and RP2) is configured for MSDP peering. The MSDP peering address must be different from the anycast RP address.

Figure 8 AnyCast RP Configuration



Many routing protocols choose the highest IP address on loopback interfaces for the router ID. A problem may arise if the router selects the anycast RP address for the router ID. It is recommended that you avoid this problem by manually setting the router ID on the RPs to the same address as the MSDP peering address (for example, the loopback 1 address in the figure above). In Open Shortest Path First (OSPF), the router ID is configured using the **router-id**router configuration command. In Border Gateway Protocol (BGP), the router ID is configured using the **bgp router-id** router configuration command. In many BGP topologies, the MSDP peering address and the BGP peering address must be the same in order to pass the RPF check. The BGP peering address can be set using the **neighbor update-source** router configuration command.

The anycast RP example above uses IP addresses taken from RFC 1918. These IP addresses are normally blocked at interdomain borders and therefore are not accessible to other ISPs. You must use valid IP addresses if you want the RPs to be reachable from other domains.

The following example shows how to perform an Anycast RP configuration.

On RP 1

```
ip pim rp-address 10.0.0.1
interface loopback 0
 ip address 10.0.0.1 255.255.255.255
!
interface loopback 1
 ip address 10.1.1.1. 255.255.255.255
!
 ip msdp peer 10.1.1.2 connect-source loopback 1
 ip msdp originator-id loopback 1
```

On RP 2

```
ip pim rp-address 10.0.0.1
interface loopback 0
 ip address 10.0.0.1 255.255.255.255
interface loopback 1
 ip address 10.1.1.2. 255.255.255.255
!
 ip msdp peer 10.1.1.1 connect-source loopback 1
 ip msdp originator-id loopback 1
```

All Other Routers

```
ip pim rp-address 10.0.0.1
```

Sparse Mode with Bootstrap Router Example

The following example is a configuration for a candidate BSR, which also happens to be a candidate RP:

```
!
ip multicast-routing
!
interface GigabitEthernet0/0/0
 ip address 172.69.62.35 255.255.255.240
 ip pim sparse-mode
!
interface GigabitEthernet1/0/0
 ip address 172.21.24.18 255.255.255.248
 ip pim sparse-mode
!
interface GigabitEthernet2/0/0
 ip address 172.21.24.12 255.255.255.248
 ip pim sparse-mode
!
ip pim bsr-candidate GigabitEthernet2/0/0 30 10
ip pim rp-candidate GigabitEthernet2/0/0 group-list 5
access-list 5 permit 239.255.2.0 0.0.0.255
```

BSR and RFC 2362 Interoperable Candidate RP Example

When Cisco and non-Cisco routers are being operated in a single PIM domain with PIM Version 2 BSR, care must be taken when configuring candidate RPs because the Cisco implementation of the BSR RP selection is not fully compatible with RFC 2362.

RFC 2362 specifies that the BSR RP be selected as follows (RFC 2362, 3.7):

1. Select the candidate RP with the highest priority (lowest configured priority value).
2. If there is a tie in the priority level, select the candidate RP with the highest hash function value.
3. If there is a tie in the hash function value, select the candidate RP with the highest IP address.

Cisco routers always select the candidate RP based on the longest match on the announced group address prefix before selecting an RP based on priority, hash function, or IP address.

Inconsistent candidate RP selection between Cisco and non-Cisco RFC 2362-compliant routers in the same domain if multiple candidate RPs with partially overlapping group address ranges are configured can occur. Inconsistent candidate RP selection can prevent connectivity between sources and receivers in the PIM domain. A source may register with one candidate RP and a receiver may connect to a different candidate RP even though it is in the same group.

The following example shows a configuration that can cause inconsistent RP selection between a Cisco and a non-Cisco router in a single PIM domain with PIM Version 2 BSR:

```
access-list 10 permit 224.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet1/0/0 group-list 10 priority 20
access-list 20 permit 224.0.0.0 15.255.255.255
ip pim rp-candidate gigabitethernet2/0/0 group-list 20 priority 10
```

In this example, a candidate RP on GigabitEthernet interface 1/0/0 announces a longer group prefix of 224.0.0.0/5 with a lower priority of 20. The candidate RP on GigabitEthernet interface 2/0/0 announces a shorter group prefix of 224.0.0.0/4 with a higher priority of 10. For all groups that match both ranges a Cisco router will always select the candidate RP on Ethernet interface 1 because it has the longer announced group prefix. A non-Cisco fully RFC 2362-compliant router will always select the candidate RP on GigabitEthernet interface 2/0/0 because it is configured with a higher priority.

To avoid this interoperability issue, do not configure different candidate RPs to announce partially overlapping group address prefixes. Configure any group prefixes that you want to announce from more than one candidate RP with the same group prefix length.

The following example shows how to configure the previous example so that there is no incompatibility between a Cisco router and a non-Cisco router in a single PIM domain with PIM Version 2 BSR:

```
access-list 10 permit 224.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet1/0/0 group-list 10 priority 20
access-list 20 permit 224.0.0.0  7.255.255.255
access-list 20 permit 232.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet2/0/0 group-list 20 priority 10
```

In this configuration the candidate RP on Ethernet interface 2 announces group address 224.0.0.0/5 and 232.0.0.0/5 which equal 224.0.0.0/4, but gives the interface the same group prefix length (5) as the candidate RP on Ethernet 1. As a result, both a Cisco router and an RFC 2362-compliant router will select the RP Ethernet interface 2.

Sparse Mode with a Single Static RP Example

The following example sets the PIM RP address to 192.168.1.1 for all multicast groups and defines all groups to operate in sparse mode:

```
ip multicast-routing
interface gigiabitethernet 1/0/0
 ip pim sparse-mode
ip pim rp-address 192.168.1.1
```

Note The same RP cannot be used for both bidirectional and sparse mode groups.

The following example sets the PIM RP address to 172.16.1.1 for the multicast group 225.2.2.2 only:

```
access list 1 225.2.2.2 0.0.0.0
 ip pim rp-address 172.17.1.1
```

SSM with IGMPv3 Example

The following example shows how to configure a router (running IGMPv3) for SSM:

```
ip multicast-routing
!
```

```
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
    ip pim sparse-mode
!
interface GigabitEthernet3/2/0
    ip address 131.108.1.2 255.255.255.0
    ip pim sparse-mode
    description ethernet connected to hosts
    ip igmp version 3
!
ip pim ssm default
```

SSM Filtering Example

The following example shows how to configure filtering on legacy RP routers running software releases that do not support SSM routing. This filtering will suppress all unwanted PIM-SM and MSDP traffic in the SSM range. Without this filtering, SSM will still operate, but there may be additional RPT traffic if legacy first hop and last hop routers exist in the network.

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The “ip pim accept-register” command
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. “Filtered on receipt” means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

Bidir-PIM Example

By default, a bidirectional RP advertises all groups as bidirectional. An access list on the RP can be used to specify a list of groups to be advertised as bidirectional. Groups with the **deny** keyword will operate in dense mode. A different, nonbidirectional RP address is required for groups that operate in sparse mode because a single access list only allows either a **permit** or **deny** keyword.

The following example shows how to configure an RP for both sparse mode and bidirectional mode groups. The groups identified as 224/8 and 227/8 are bidirectional groups, and 226/8 is a sparse mode group. The RP must be configured to use different IP addresses for the sparse mode and bidirectional mode operations. Two loopback interfaces are used to allow this configuration. The addresses of these loopback interfaces must be routed throughout the PIM domain in such a way that the other routers in the PIM domain can communicate with the RP.

```
ip multicast-routing
!
.
.
.
```

```
!
interface loopback 0
 description One loopback address for this router’s Bidir Mode RP function
 ip address 10.0.1.1 255.255.255.0
!
interface loopback 1
description One loopback address for this router’s Sparse Mode RP function
 ip address 10.0.2.1 255.255.255.0
!
.
.
.
!
ip pim bidir-enable
ip pim rp-address 10.0.1.1 45 bidir
ip pim rp-address 10.0.2.1 46
!
access-list 45 permit 224.0.0.0 0.255.255.255
access-list 45 permit 227.0.0.0 0.255.255.255
access-list 46 permit 226.0.0.0 0.255.255.255
```

Additional References

Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

Standard	Title
draft-kouvelas-pim-bidir-new-00.txt	A New Proposal for Bi-directional PIM

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1112	Host Extensions for IP Multicasting
RFC 1918	Address Allocation for Private Internets

RFC	Title
RFC 2770	GLOP Addressing in 233/8
RFC 3569	An Overview of Source-Specific Multicast (SSM)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Basic IP Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3 Feature Information for Configuring Basic IP Multicast

Feature Name	Releases	Feature Information
Multicast Source Discovery Protocol (MSDP)	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
IGMP Version 3	Cisco IOS XE Release 2.1	
Source Specific Multicast (SSM)	Cisco IOS XE Release 2.1	SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.
Bidirectional PIM	Cisco IOS XE Release 2.2	
AutoRP Enhancement	Cisco IOS XE Release 2.1	Auto-RP automates the distribution of group-to-rendezvous point (RP) mappings in a PIM network. To make Auto-RP work, a router must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts.

Feature Name	Releases	Feature Information
PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss	Cisco IOS XE Release 2.1	The PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss feature enables you to prevent PIM-DM fallback when all RPs fail. Preventing the use of dense mode is very important to multicast networks whose reliability is critical. This feature provides a mechanism to keep the multicast groups in sparse mode, thereby preventing dense mode flooding. The following command was introduced by this feature: **ip pim dm-fallback**.

Using MSDP to Interconnect Multiple PIM-SM Domains

This module describes the tasks associated with using Multicast Source Discovery Protocol (MSDP) to interconnect multiple PIM-SM domains. The tasks explain how to configure MSDP peers, mesh groups, and default peers, how to use filters to control and scope MSDP activity, and how to monitor and maintain MSDP. Using MSDP with PIM-SM greatly reduces the complexity of connecting multiple PIM-SM domains.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Using MSDP to Interconnect Multiple PIM-SM Domains

Before you configure MSDP, the addresses of all MSDP peers must be known in Border Gateway Protocol (BGP).

Information About Using MSDP to Interconnect Multiple PIM-SM Domains

Benefits of Using MSDP to Interconnect Multiple PIM-SM Domains

- Allows a rendezvous point (RP) to dynamically discover active sources outside of its domain.
- Introduces a more manageable approach for building multicast distribution trees between multiple domains.

Use of MSDP to Interconnect Multiple PIM-SM Domains

MSDP is a mechanism to connect multiple PIM-SM domains. The purpose of MSDP is to discover multicast sources in other PIM domains. The main advantage of MSDP is that it reduces the complexity of interconnecting multiple PIM-SM domains by allowing PIM-SM domains to use an interdomain source tree (rather than a common shared tree). When MSDP is configured in a network, RPs exchange source information with RPs in other domains. An RP can join the interdomain source tree for sources that are sending to groups for which it has receivers. The RP can do that because it is the root of the shared tree within its domain, which has branches to all points in the domain where there are active receivers. When a last-hop router learns of a new source outside the PIM-SM domain (through the arrival of a multicast packet from the source down the shared tree), it then can send a join toward the source and join the interdomain source tree.

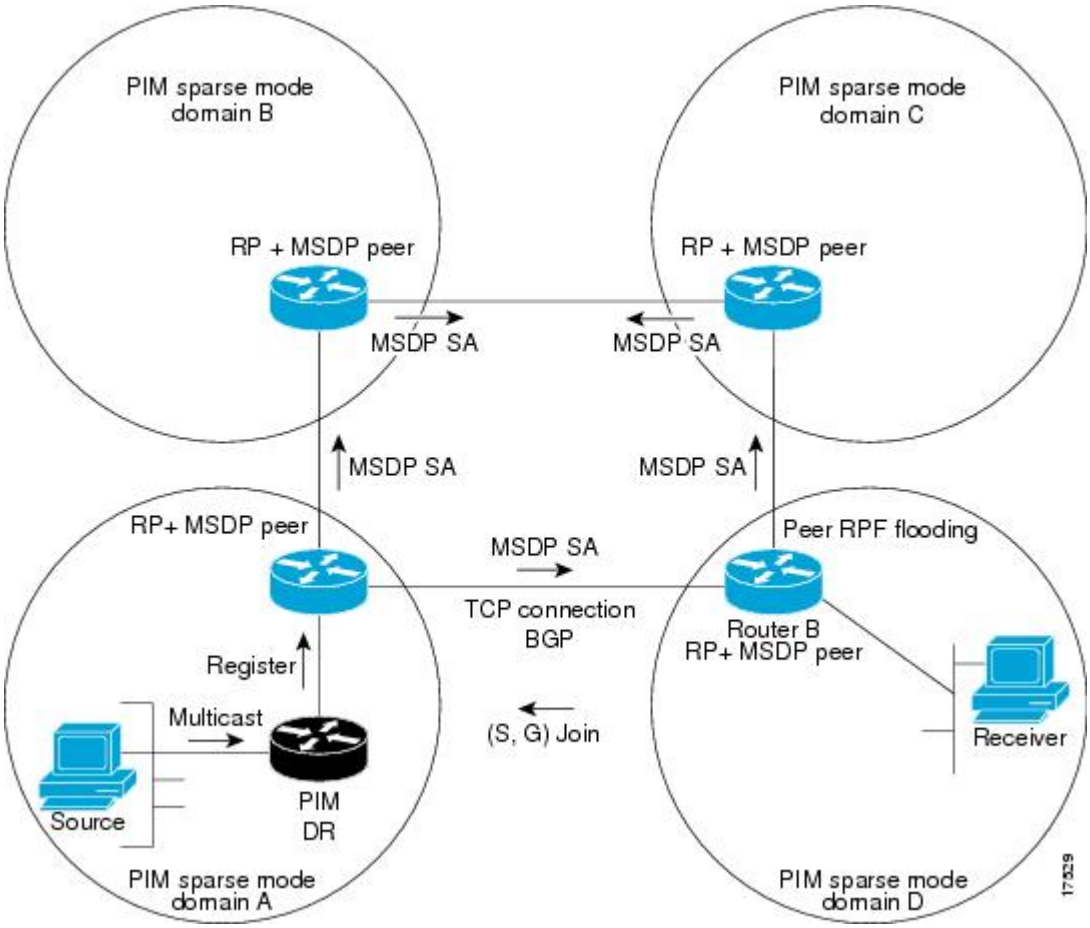
Note If the RP either has no shared tree for a particular group or a shared tree whose outgoing interface list is null, it does not send a join to the source in another domain.

When MSDP is enabled, an RP in a PIM-SM domain maintains MSDP peering relationships with MSDP-enabled routers in other domains. This peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. MSDP uses TCP (port 639) for its peering connections. As with BGP, using point-to-point TCP peering means that each peer must be explicitly configured. The TCP connections between RPs, moreover, are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism provided by PIM-SM. MSDP is also used to announce sources sending to a group. These announcements must originate at the RP of the domain.

Note MSDP depends on BGP or multiprotocol BGP (MBGP) for interdomain operation. We recommended that you run MSDP on RPs sending to global multicast groups.

The figure illustrates MSDP operating between two MSDP peers. PIM uses MSDP as the standard mechanism to register a source with the RP of a domain.

Figure 9 MSDP Running Between RP Peers



When MSDP is implemented, the following sequence of events occurs:

1. When a PIM designated router (DR) registers a source with its RP as illustrated in the figure, the RP sends a Source-Active (SA) message to all of its MSDP peers.

Note The DR sends the encapsulated data to the RP only once per source (when the source goes active). If the source times out, this process happens again when it goes active again. This situation is different from the periodic SA message that contains all sources that are registered to the originating RP. Those SA messages are MSDP control packets, and, thus, do not contain encapsulated data from active sources.

1. The SA message identifies the source address, the group that the source is sending to, and the address or the originator ID of the RP, if configured.
2. Each MSDP peer that receives the SA message floods the SA message to all of its peers downstream from the originator. In some cases (such as the case with the RPs in PIM-SM domains B and C in the figure), an RP may receive a copy of an SA message from more than one MSDP peer. To prevent looping, the RP consults the BGP next-hop database to determine the next hop toward the originator of the SA message. If both MBGP and unicast BGP are configured, MBGP is checked first, and then unicast BGP. That next-hop neighbor is the RPF-peer for the originator. SA messages that are received from the originator on any interface other than the interface to the RPF peer are dropped. The SA message flooding process, therefore, is referred to as peer-RPF flooding. Because of the peer-RPF flooding mechanism, BGP or MBGP must be running in conjunction with MSDP.

Note (M)BGP is not required in MSDP mesh group scenarios. For more information about MSDP mesh groups, see the Configuring an MSDP Mesh Group, page 95 section.

Note (M)BGP is not required in default MSDP peer scenarios or in scenarios where only one MSDP peer is configured. For more information, see the Configuring a Default MSDP Peer, page 94 section.

1. When an RP receives an SA message, it checks to see whether there are any members of the advertised groups in its domain by checking to see whether there are interfaces on the group's (*, G) outgoing interface list. If there are no group members, the RP does nothing. If there are group members, the RP sends an (S, G) join toward the source. As a result, a branch of the interdomain source tree is constructed across autonomous system boundaries to the RP. As multicast packets arrive at the RP, they are then forwarded down its own shared tree to the group members in the RP's domain. The members' DRs then have the option of joining the rendezvous point tree (RPT) to the source using standard PIM-SM procedures.
2. The originating RP continues to send periodic SA messages for the (S, G) state every 60 seconds for as long as the source is sending packets to the group. When an RP receives an SA message, it caches the SA message. Suppose, for example, that an RP receives an SA message for (172.16.5.4, 228.1.2.3) from originating RP 10.5.4.3. The RP consults its mroute table and finds that there are no active members for group 228.1.2.3, so it passes the SA message to its peers downstream of 10.5.4.3. If a host in the domain then sends a join to the RP for group 228.1.2.3, the RP adds the interface toward the host to the outgoing interface list of its (*, 224.1.2.3) entry. Because the RP caches SA messages, the router will have an entry for (172.16.5.4, 228.1.2.3) and can join the source tree as soon as a host requests a join.

Note In all current and supported software releases, caching of MSDP SA messages is mandatory and cannot be manually enabled or disabled. By default, when an MSDP peer is configured, the **ip multicast cache-sa-state** command will automatically be added to the running configuration.

MSDP Message Types

There are four basic MSDP message types, each encoded in their own Type, Length, and Value (TLV) data format.

SA Messages

SA messages are used to advertise active sources in a domain. In addition, these SA messages may contain the initial multicast data packet that was sent by the source.

SA messages contain the IP address of the originating RP and one or more (S, G) pairs being advertised. In addition, the SA message may contain an encapsulated data packet.

Note For more information about SA messages, see the SA Message Origination Receipt and Processing, page 72 section.

SA Request Messages

SA request messages are used to request a list of active sources for a specific group. These messages are sent to an MSDP SA cache that maintains a list of active (S, G) pairs in its SA cache. Join latency can be reduced by using SA request messages to request the list of active sources for a group instead of having to wait up to 60 seconds for all active sources in the group to be readvertised by originating RPs.

Note For more information about SA request messages, see the Requesting Source Information from MSDP Peers, page 100 section.

SA Response Messages

SA response messages are sent by the MSDP peer in response to an SA request message. SA response messages contain the IP address of the originating RP and one or more (S, G) pairs of the active sources in the originating RP’s domain that are stored in the cache.

Note For more information about SA response messages, see the Controlling the Response to Outgoing SA Request Messages from MSDP Peers Using SA Request Filters, page 102 section.

Keepalive Messages

Keepalive messages are sent every 60 seconds in order to keep the MSDP session active. If no keepalive messages or SA messages are received for 75 seconds, the MSDP session is reset.

Note For more information about keepalive messages, see the Adjusting the MSDP Keepalive and Hold-Time Intervals, page 90 section.

SA Message Origination Receipt and Processing

The section describes SA message origination, receipt, and processing in detail.

SA Message Origination

SA messages are triggered by an RP (assuming MSDP is configured) when any new source goes active within a local PIM-SM domain. A local source is a source that is directly connected to the RP or is the first-hop DR that has registered with it. An RP originates SA messages only for local sources in its PIM-SM domain; that is, for local sources that register with it.

Note A local source is denoted by the A flag being set in the (S, G) mroute entry on the RP (which can be viewed in the output of the **show ip mroute** command). This flag indicates that the source is a candidate for advertisement by the RP to other MSDP peers.

When a source is in the local PIM-SM domain, it causes the creation of (S, G) state in the RP. New sources are detected by the RP either by the receipt of a register message or the arrival of the first (S, G) packet from a directly connected source. The initial multicast packet sent by the source (either encapsulated in the register message or received from a directly connected source) is encapsulated in the initial SA message.

SA Message Receipt

SA messages are only accepted from the MSDP RPF peer that is in the best path back toward the originator. The same SA message arriving from other MSDP peers must be ignored or SA loops can occur. Deterministically selecting the MSDP RPF peer for an arriving SA message requires knowledge of the MSDP topology. However, MSDP does not distribute topology information in the form of routing updates. MSDP infers this information by using (M)BGP routing data as the best approximation of the MSDP topology for the SA RPF check mechanism. An MSDP topology, therefore, must follow the same general topology as the BGP peer topology. Besides a few exceptions (such as default MSDP peers and MSDP peers in MSDP mesh groups), MSDP peers, in general should also be (M)BGP peers.

How RPF Check Rules Are Applied to SA Messages

The rules that apply to RPF checks for SA messages are dependent on the BGP peerings between the MSDP peers:

- Rule 1: Applied when the sending MSDP peer is also an interior (M)BGP peer.
- Rule 2: Applied when the sending MSDP peer is also an exterior (M)BGP peer.
- Rule 3: Applied when the sending MSDP peer is not an (M)BGP peer.

RPF checks are not performed in the following cases:

- If the sending MSDP peer is the only MSDP peer, which would be the case if only a single MSDP peer or a default MSDP peer is configured.
- If the sending MSDP peer is a member of a mesh group.
- If the sending MSDP peer address is the RP address contained in the SA message.

How the Software Determines the Rule to Apply to RPF Checks

The software uses the following logic to determine which RPF rule to apply to RPF checks:

- Find the (M)BGP neighbor that has the same IP address as the sending MSDP peer.
  - If the matching (M)BGP neighbor is an internal BGP (iBGP) peer, apply Rule 1.
  - If the matching (M)BGP neighbor is an external BGP (eBGP) peer, apply Rule 2.
  - If no match is found, apply Rule 3.

Note The implication of the RPF check rule selection is as follows: The IP address used to configure an MSDP peer on a router must match the IP address used to configure the (M)BGP peer on the same router.

Rule 1 of RPF Checking of SA Messages in MSDP

Rule 1 of RPF checking in MSDP is applied when the sending MSDP peer is also an i(M)BGP peer. When Rule 1 is applied, the RPF check proceeds as follows:

1. The peer searches the BGP Multicast Routing Information Base (MRIB) for the best path to the RP that originated the SA message. If a path is not found in the MRIB, the peer then searches the Unicast Routing Information Base (URIB). If a path is still not found, the RPF check fails.
2. If the previous search succeeds (that is, the best path is found), the peer then determines the address of the BGP neighbor for this best path, which will be the address of the BGP neighbor that sent the peer the path in BGP update messages.

Note The BGP neighbor address is not the same as the next-hop address in the path. Because i(M)BGP peers do not update the next-hop attribute of a path, the next-hop address usually is not the same as the address of the BGP peer that sent us the path.

Note The BGP neighbor address is not necessarily the same as the BGP router ID of the peer that sent the peer the path.

1. If the IP address of the sending MSDP peer is the same as the BGP neighbor address (that is, the address of the BGP peer that sent the peer the path), then the RPF check succeeds; otherwise it fails.

Implications of Rule 1 of RPF Checking on MSDP

The MSDP topology must mirror the (M)BGP topology. In general, wherever there is an i(M)BGP peer connection between two routers, an MSDP peer connection should be configured. More specifically, the IP address of the far-end MSDP peer connection must be the same as the far-end i(M)BGP peer connection. The addresses must be the same because the BGP topology between i(M)BGP peers inside an autonomous system is not described by the AS path. If it were always the case that i(M)BGP peers updated the next-hop address in the path when sending an update to another i(M)BGP peer, then the peer could rely on the next-hop address to describe the i(M)BGP topology (and hence the MSDP topology). However, because the default behavior for i(M)BGP peers is to not update the next-hop address, the peer cannot rely on the next-hop address to describe the (M)BGP topology (MSDP topology). Instead, the i(M)BGP peer uses the address of the i(M)BGP peer that sent the path to describe the i(M)BGP topology (MSDP topology) inside the autonomous system.

Tip Care should be taken when configuring the MSDP peer addresses to make sure that the same address is used for both i(M)BGP and MSDP peer addresses.

Rule 2 of RPF Checking of SA Messages in MSDP

Rule 2 of RPF checking in MSDP is applied when the sending MSDP peer is also an e(M)BGP peer. When Rule 2 is applied, the RPF check proceeds as follows:

1. The peer searches the BGP MRIB for the best path to the RP that originated the SA message. If a path is not found in the MRIB, the peer then searches the URIB. If a path is still not found, the RPF check fails.
2. If the previous search succeeds (that is, the best path is found), the peer then examines the path. If the first autonomous system in the best path to the RP is the same as the autonomous system of the e(M)BGP peer (which is also the sending MSDP peer), then the RPF check succeeds; otherwise it fails.

Implications of Rule 2 of RPF Checking on MSDP

The MSDP topology must mirror the (M)BGP topology. In general, wherever there is an e(M)BGP peer connection between two routers, an MSDP peer connection should be configured. As opposed to Rule 1, the IP address of the far-end MSDP peer connection does not have to be the same as the far-end e(M)BGP peer connection.The reason that the addresses do not have to be identical is that BGP topology between two e(M)BGP peers is not described by the AS path.

Rule 3 of RPF Checking of SA Messages in MSDP

Rule 3 of RPF checking is applied when the sending MSDP peer is not a (M)BGP peer at all. When Rule 3 is applied, the RPF check proceeds as follows:

1. The peer searches the BGP MRIB for the best path to the RP that originated the SA message. If a path is not found in the MRIB, the peer then searches the URIB. If a path is still not found, the RPF check fails.
2. If the previous search succeeds (that is, the best path to the RP that originated the SA message is found), the peer then searches the BGP MRIB for the best path to the MSDP peer that sent the SA message. If a path is not found in the MRIB, the peer then searches the URIB. If a path is still not found, the RPF check fails.

Note The autonomous system of the MSDP peer that sent the SA is the origin autonomous system, which is the last autonomous system in the AS path to the MSDP peer.

1. If the first autonomous system in the best path to the RP is the same as the autonomous system of the sending MSDP peer, then the RPF check succeeds; otherwise it fails.

SA Message Processing

The following steps are taken by an MSDP peer whenever it processes an SA message:

1. Using the group address G of the (S, G) pair in the SA message, the peer locates the associated (*, G) entry in the mroute table. If the (*, G) entry is found and its outgoing interface list is not null, then there are active receivers in the PIM-SM domain for the source advertised in the SA message.
2. The MSDP peer then creates an (S, G) entry for the advertised source.
3. If the (S, G) entry did not already exist, the MSDP peer immediately triggers an (S, G) join toward the source in order to join the source tree.
4. The peer then floods the SA message to all other MSDP peers with the exception of:
   - The MSDP peer from which the SA message was received.
   - Any MSDP peers that are in the same MSDP mesh group as this router (if the peer is a member of a mesh group).

Note SA messages are stored locally in the router's SA cache.

MSDP Peers

Like BGP, MSDP establishes neighbor relationships with other MSDP peers. MSDP peers connect using TCP port 639. The lower IP address peer takes the active role of opening the TCP connection. The higher IP address peer waits in LISTEN state for the other to make the connection. MSDP peers send keepalive messages every 60 seconds. The arrival of data performs the same function as the keepalive message and keeps the session from timing out. If no keepalive messages or data is received for 75 seconds, the TCP connection is reset.

MSDP MD5 Password Authentication

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

- How MSDP MD5 Password Authentication Works, page 76
- Benefits of MSDP MD5 Password Authentication, page 76

How MSDP MD5 Password Authentication Works

Developed in accordance with RFC 2385, the MSDP MD5 password authentication feature is used to verify each segment sent on the TCP connection between MSDP peers. The **ip msdp password peer** command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and verify the MD5 digest of every segment sent on the TCP connection.

Benefits of MSDP MD5 Password Authentication

- Protects MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.
- Uses the industry-standard MD5 algorithm for improved reliability and security.

SA Message Limits

The **ip msdp sa-limit** command is used to limit the overall number of SA messages that a router can accept from specified MSDP peers. When the **ip msdp sa-limit** command is configured, the router maintains a per-peer count of SA messages stored in the SA cache and will ignore new messages from a peer if the configured SA message limit for that peer has been reached.

The **ip msdp sa-limit** command was introduced as a means to protect an MSDP-enabled router from denial of service (DoS) attacks. We recommended that you configure SA message limits for all MSDP peerings on the router. An appropriately low SA limit should be configured on peerings with a stub MSDP region (for example, a peer that may have some further downstream peers but that will not act as a transit for SA messages across the rest of the Internet). A high SA limit should be configured for all MSDP peerings that act as transits for SA messages across the Internet.

MSDP Keepalive and Hold-Time Intervals

The **ip msdp keepalive** command is used to adjust the interval at which an MSDP peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down.

Once an MSDP peering session is established, each side of the connection sends a keepalive message and sets a keepalive timer. If the keepalive timer expires, the local MSDP peer sends a keepalive message and restarts its keepalive timer; this interval is referred to as the keepalive interval. The *keepalive-interval*argument is used to adjust the interval for which keepalive messages will be sent. The keepalive

timer is set to the value specified for the *keepalive-interval*argument when the peer comes up. The keepalive timer is reset to the value of the *keepalive-interval* argument whenever an MSDP keepalive message is sent to the peer and reset when the timer expires. The keepalive timer is deleted when an MSDP peering session is closed. By default, the keepalive timer is set to 60 seconds.

Note The value specified for the *keepalive-interval* argument must be less than the value specified for the *holdtime-interval*argument and must be at least one second.

The hold-time timer is initialized to the value of the *hold-time-interval* argument whenever an MSDP peering connection is established, and is reset to the value of the *hold-time-interval*argument whenever an MSDP keepalive message is received. The hold-time timer is deleted whenever an MSDP peering connection is closed. By default, the hold-time interval is set to 75 seconds.

Use the *hold-time-interval* argument to adjust the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down.

MSDP Connection-Retry Interval

The **ip msdp timer** command is used to adjust the interval at which all MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. This interval is referred to as the connection-retry interval. By default, MSDP peers will wait 30 seconds after the session is reset before attempting to reestablish sessions with other peers. When the **ip msdp timer** command is configured, the configured connection-retry interval applies to all MSDP peering sessions on the router.

MSDP Compliance with IETF RFC 3618

When the MSDP Compliance with IETF RFC 3618 feature is configured, the peer-RPF forwarding rules defined in IETF RFC 3618 are applied to MSDP peers. IETF RFC 3618 provides peer-RPF forwarding rules that are used for forwarding SA messages throughout an MSDP-enabled internet. Unlike the RPF check used when forwarding data packets, which compares a packet's source address against the interface upon which the packet was received, the peer-RPF check compares the RP address carried in the SA message against the MSDP peer from which the message was received. Except when MSDP mesh groups are being used, SA messages from an RP address are accepted from only one MSDP peer to avoid looping SA messages.

Note For more information about the MSDP peer-forwarding rules defined in RFC 3618, see RFC 3618, Multicast Source Discovery Protocol (MSDP) .

- Benefits of MSDP Compliance with RFC 3618, page 77

Benefits of MSDP Compliance with RFC 3618

- You can use BGP route reflectors (RRs) without running MSDP on them. This capability is useful to service providers that need to reduce the load on RRs.
- You can use an Interior Gateway Protocol (IGP) for the Reverse Path Forwarding (RPF) checks and thereby run peerings without (M)BGP. This capability is useful to enterprise customers that do not run (M)BGP and require larger topologies than mesh groups can provide.

Note IGP peerings must always be between directly connected MSDP peers or else the RPF checks will fail.

- You can have peerings between routers in nondirectly connected autonomous systems (that is, with one or more autonomous systems between them). This capability helps in confederation configurations and for redundancy.

Default MSDP Peers

In most scenarios, an MSDP peer is also a BGP peer. If an autonomous system is a stub or nontransit autonomous system, and particularly if the autonomous system is not multihomed, there is little or no reason to run BGP to its transit autonomous system. A static default route at the stub autonomous system, and a static route pointing to the stub prefixes at the transit autonomous system, is generally sufficient. But if the stub autonomous system is also a multicast domain and its RP must peer with an RP in the neighboring domain, MSDP depends on the BGP next-hop database for its peer-RPF checks. You can disable this dependency on BGP by defining a default peer from which to accept all SA messages without performing the peer-RPF check, using the **ip msdp default-peer** command. A default MSDP peer must be a previously configured MSDP peer.

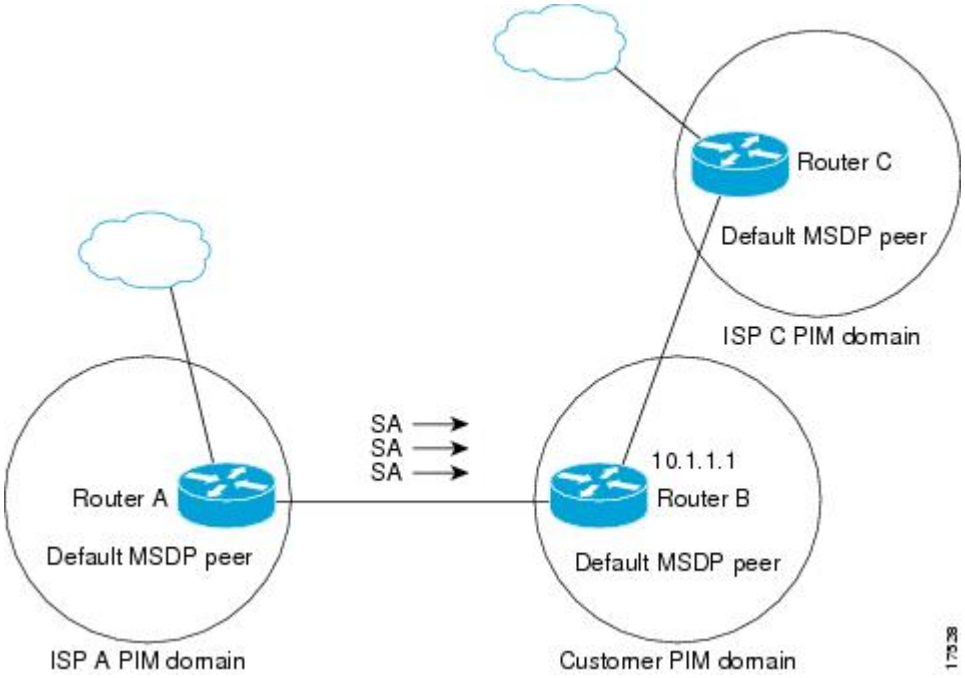
A stub autonomous system also might want to have MSDP peerings with more than one RP for the sake of redundancy. For example, SA messages cannot just be accepted from multiple default peers, because there is no RPF check mechanism. Instead, SA messages are accepted from only one peer. If that peer fails, SA messages are then accepted from the other peer. The underlying assumption here, of course, is that both default peers are sending the same SA messages.

The figure illustrates a scenario where default MSDP peers might be used. In the figure, a customer that owns Router B is connected to the Internet through two Internet service providers (ISPs), one that owns Router A and the other that owns Router C. They are not running BGP or MBGP between them. In order for the customer to learn about sources in the ISP domain or in other domains, Router B identifies Router A as its default MSDP peer. Router B advertises SA messages to both Router A and Router C, but accepts SA messages either from Router A only or Router C only. If Router A is the first default peer in the configuration, it will be used if it is up and running. Only if Router A is not running will Router B accept SA messages from Router C.

The ISP will also likely use a prefix list to define which prefixes it will accept from the customer router. The customer will define multiple default peers, each having one or more prefixes associated with it.

The customer has two ISPs to use. The customer defines both ISPs as default peers. As long as the first default peer identified in the configuration is up and running, it will be the default peer and the customer will accept all SA messages it receives from that peer.

Figure 10 Default MSDP Peer Scenario



Router B advertises SAs to Router A and Router C, but uses only Router A or Router C to accept SA messages. If Router A is first in the configuration, it will be used if it is up and running. Only when Router A is not running will Router B accept SAs from Router C. This is the behavior without a prefix list.

If you specify a prefix list, the peer will be a default peer only for the prefixes in the list. You can have multiple active default peers when you have a prefix list associated with each. When you do not have any prefix lists, you can configure multiple default peers, but only the first one is the active default peer as long as the router has connectivity to this peer and the peer is alive. If the first configured peer goes down or the connectivity to this peer goes down, the second configured peer becomes the active default, and so on.

MSDP Mesh Groups

An MSDP mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity between one another. In other words, each of the MSDP peers in the group must have an MSDP peering relationship (MSDP connection) to every other MSDP peer in the group. When an MSDP mesh group is configured between a group of MSDP peers, SA message flooding is reduced. Because when an MSDP peer in the group receives an SA message from another MSDP peer in the group, it assumes that this SA message was sent to all the other MSDP peers in the group. As a result, it is not necessary for the receiving MSDP peer to flood the SA message to the other MSDP peers in the group.

- Benefits of MSDP Mesh Groups, page 79

Benefits of MSDP Mesh Groups

- Optimizes SA flooding--MSDP mesh groups are particularly useful for optimizing SA flooding when two or more peers are in a group.
- Reduces the amount of SA traffic across the Internet--When MSDP mesh groups are used, SA messages are not flooded to other mesh group peers.
- Eliminates RPF checks on arriving SA messages--When an MSDP mesh group is configured, SA messages are always accepted from mesh group peers.

SA Origination Filters

By default, an RP that is configured to run MSDP will originate SA messages for all local sources for which it is the RP. Local sources that register with an RP, therefore, will be advertised in SA messages, which in some cases is not desirable. For example, if sources inside a PIM-SM domain are using private addresses (for example, network 10.0.0.0/8), you should configure an SA origination filter to restrict those addresses from being advertised to other MSDP peers across the Internet.

To control what sources are advertised in SA messages, you can configure SA origination filters on an RP using the **ip msdp redistribute** command. By creating SA origination filters, you can control the sources advertised in SA messages as follows:

- You can prevent an RP from originating SA messages for local sources by configuring the **ip msdp redistribute** command without any keywords or arguments. Issuing this form of the command effectively prevents the router from advertising local sources in SA messages.

Note When the **ip msdp redistribute** command is entered without any keywords or arguments, the router will still forward SA messages from other MSDP peers in the normal fashion; it will just not originate any SA messages for local sources.

- You can configure the router to originate SA messages only for (S, G) pairs defined in an extended access list by configuring the **ip msdp redistribute** command with the optional **list** keyword and *access-list* argument. Issuing the form of the command effectively configures the router to only originate SA messages for local sources sending to specific groups that match (S, G) pairs defined in the extended access list. All other local sources will not be advertised in SA messages.
- You can configure the router to originate SA messages only for AS paths defined in an AS-path access list by configuring the **ip msdp redistribute** command with the optional **asn** keyword and *as-access-list* argument. Issuing this form of the command effectively configures the router to only originate SA messages for local sources sending to specific groups that the match AS paths defined in an AS-path access list. All other local sources will not be advertised in SA messages.

Note AS-path access lists are configured using the **ip as-path access-list** command.

You can configure the router to originate SA messages only for local sources that match the criteria defined in a route map by configuring the **ip msdp redistribute**command with the optional **route-map** keyword and *map-name* argument. Issuing this form of the command effectively configures the router to only originate SA messages for local sources that match the criteria defined in the route map. All other local sources will not be advertised in SA messages.

Note You can configure an SA origination filter that includes an extended access list, an AS-path access list, and route map (or a combination thereof). In that case, all conditions must be true before any local sources are advertised in SA messages.

Use of Outgoing Filter Lists in MSDP

By default, an MSDP-enabled router forwards all SA messages it receives to all of its MSDP peers. However, you can prevent SA messages from being forwarded to MSDP peers by creating outgoing filter lists using the **ip msdp sa-filter out** command. Outgoing filter lists (configured using the **ip msdp sa-filter out**command) apply to all SA messages, whether locally originated or received from another MSDP peer, whereas SA origination filters (configured using the **ip msdp redistribute** command) apply only to locally originated SA messages. For more information about using the **ip msdp redistribute** command to enable a filter for MSDP SA messages originated by the local router, see the Controlling SA Messages Originated by an RP for Local Sources, page 96 section.

By creating an outgoing filter list, you can control the SA messages that a router forwards to a peer as follows:

- You can filter all outgoing SA messages forwarded to a specified MSDP peer by configuring the **ip msdp filter-sa-request out**command without any keywords or arguments. Issuing this form of the command effectively configures the router to stop forwarding its SA messages to the MSDP peer.
- You can filter a subset of outgoing SA messages forwarded to a specified MSDP peer based on (S, G) pairs defined in an extended access list by configuring the **ip msdp sa-filter out**command with the optional **list** keyword and *access-list* argument. Issuing the form of the command effectively configures the router to only forward SA messages to the MSDP peer that match the (S, G) pairs permitted in an extended access list. The forwarding of all other SA messages to the MSDP peer will be stopped.
- You can filter a subset of outgoing SA messages forwarded to a specified MSDP peer based on match criteria defined in a route map by configuring the **ip msdp sa-filter out**command with the optional **route-map** keyword and *map-name* argument. Issuing this form of the command effectively configures the router to only forward SA messages that match the criteria defined in the route map. The forwarding of all other SA messages to the MSDP peer will be stopped.
- You can filter a subset of outgoing SA messages from a specified peer based on the announcing RP address contained in the SA message by configuring the **ip msdp sa-filter out**command with the optional **rp-list** keyword and *list* argument or with the **rp-route-map** keyword *map-name*argument. This type of outgoing filter list enables the router to filter outgoing SA messages based on their origin, even after an SA message has been transmitted across one or more MSDP peers. The forwarding of all other SA messages to the MSDP peer will be stopped.

Note You can configure an outgoing filter list that includes an extended access list, a route map, and either an RP access list or an RP route map. In that case, all conditions must be true for the MSDP peer to forward the outgoing SA message.

Caution Arbitrary filtering of SA messages can result in downstream MSDP peers being starved of SA messages for legitimate active sources. Care, therefore, should be taken when using these sorts of filters. Normally, outgoing filter lists are used only to reject undesirable sources, such as sources using private addresses.

Use of Incoming Filter Lists in MSDP

By default, an MSDP-enabled router receives all SA messages sent to it from its MSDP peers. However, you can control the source information that a router receives from its MSDP peers by creating incoming filter lists using the **ip msdp sa-filter in** command.

By creating incoming filter lists, you can control the incoming SA messages that a router receives from its peers as follows:

- You can filter all incoming SA messages from a specified MSDP peer by configuring the **ip msdp filter-sa-request in** command without any keywords or arguments. Issuing this form of the command effectively configures the router to ignore all SA messages sent to it from the specified MSDP peer.
- You can filter a subset of incoming SA messages from a specified peer based on (S, G) pairs defined in an extended access list by configuring the **ip msdp sa-filter in** command with the optional **list** keyword and *access-list* argument. Issuing the form of the command effectively configures the router to only receive SA messages from the MSDP peer that match the (S, G) pairs defined in the extended access list. All other incoming SA messages from the MSDP peer will be ignored.
- You can filter a subset of incoming SA request messages from a specified peer based on match criteria defined in a route map by configuring the **ip msdp sa-filter in**command with the optional **route-map** keyword and *map* argument. Issuing this form of the command effectively configures the router to only receive SA messages that match the criteria defined in the route map. All other incoming SA messages from the MSDP peer will be ignored.
- You can filter a subset of incoming SA messages from a specified peer based on both (S, G) pairs defined in an extended access list and on match criteria defined in a route map by configuring the **ip msdp sa-filter in**command with the optional **list** keyword and *access-list* argument and with the optional **route-map** keyword and *map-name* argument. Issuing this form of the command configures the router to only receive incoming SA messages that both match the (S, G) pairs defined in the extended access list and match the criteria defined in the route map. All other incoming SA messages from the MSDP peer will be ignored.
- You can filter a subset of incoming SA messages from a specified peer based on the announcing RP address contained in the SA message by configuring the **ip msdp sa-filter in** command with the optional **rp-list** keyword and *list* argument or with the **rp-route-map** *map-name*. This type of incoming filter list enables the router to filter incoming SA messages based on their origin, even after the SA message may have already been transmitted across one or more MSDP peers.

Note You can configure an incoming filter list that includes an extended access list, a route map, and either an RP access list or an RP route map. In that case, all conditions must be true for the MSDP peer to receive the incoming SA message.

Caution Arbitrary filtering of SA messages can result in downstream MSDP peers being starved of SA messages for legitimate active sources. Care, therefore, should be taken when using these sorts of filters. Normally, incoming filter lists are used only to reject undesirable sources, such as sources using private addresses.

TTL Thresholds in MSDP

The time-to-live (TTL) value provides a means to limit the number of hops a packet can take before being dropped. The **ip multicast ttl-threshold** command is used to specify a TTL for data-encapsulated SA messages sent to specified MSDP peers. By default, multicast data packets in SA messages are sent to an MSDP peer, provided the TTL value of the packet is greater than 0, which is standard TTL behavior.

In general, a TTL-threshold problem can be introduced by the encapsulation of a source's initial multicast packet in an SA message. Because the multicast packet is encapsulated inside of the unicast SA message (whose TTL is 255), its TTL is not decremented as the SA message travels to the MSDP peer. Furthermore, the total number of hops that the SA message traverses can be drastically different than a normal multicast packet because multicast and unicast traffic may follow completely different paths to the MSDP peer and hence the remote PIM-SM domain. As a result, encapsulated packets can end up violating TTL thresholds. The solution to this problem is to configure a TTL threshold that is associated with any multicast packet that is encapsulated in an SA message sent to a particular MSDP peer using the **ip multicast ttl-threshold** command. The **ip msdp ttl-threshold** command prevents any multicast packet whose TTL in the IP header is less than the TTL value specified for the *ttl-value*argument from being encapsulated in SA messages sent to that peer.

SA Request Messages

The **ip msdp sa-request** command is used to enable a noncaching router to send SA request messages to a specified MSDP peer. You can enter this command multiple times to specify that the router send SA request messages to additional MSDP peers.

If an noncaching RP has an MSDP peer that is caching SAs, you can reduce the join latency for a noncaching peer by enabling the noncaching peer to send SA request messages. When a host requests a join to a particular group, the noncaching RP sends an SA request message to its caching peers. If a peer has cached source information for the group in question, it sends the information to the requesting RP with an SA response message. The requesting RP uses the information in the SA response but does not forward the message to any other peers. If a noncaching RP receives an SA request, it sends an error message back to the requestor.

Note In all current and supported Cisco IOS software releases, caching of MSDP SA messages is mandatory and cannot be manually enabled or disabled. By default, when an MSDP peer is configured, the **ip multicast cache-sa-state** command will automatically be added to the running configuration. Prior to Cisco IOS Releases 12.1(7) and 12.0(14)S1, caching of SAs was disabled by default and could be enabled with the **ip msdp cache-sa-state** command.

SA Request Filters

By default, a router honors all outgoing SA request messages from its MSDP peers; that is, it sends cached source information to requesting MSDP peers in SA response messages. You can control the outgoing SA

request messages that a router will honor from specified peers by enabling an SA request filter using the **ip msdp filter-sa-request** command. By creating an SA request filter, you can control the outgoing SA requests that the router will honor from MSDP peers as follows:

- You can filter all SA request messages from a specified peer by configuring the **ip msdp filter-sa-request** command without the optional **list** keyword and *access-list*argument. Issuing this form of the **ip msdp filter-sa request** command effectively configures the router to ignore all SA requests from the specified MSDP peer.
- You can filter a subset of SA request messages from a specified peer based on groups defined in a standard access list by configuring the **ip msdp filter-sa-request**command with the optional **list** keyword and *access-list* argument. Issuing the form of the command effectively configures the router to honor only SA request messages from the MSDP peer that match the groups defined in a standard access list. SA request messages from the specified peer for other groups will be ignored.

MSDP MIB

The MSDP MIB describes managed objects that can be used to remotely monitor MSDP speakers using SNMP. The MSDP MIB module contains four scalar objects and three tables. The tables are the Requests table, the Peer table, and the Source-Active (SA) Cache table. The Cisco implementation supports the Peer table and SA Cache table only. The Requests table contains information used to determine which peer to send SA requests to. However, the MSDP implementation used in Cisco IOS software does not associate sending SA requests to peers with group addresses (or group address masks).

Note The MSDP-MIB.my file can be downloaded from the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

How to Use MSDP to Interconnect Multiple PIM-SM Domains

The first task is required; all other tasks are optional.

- Configuring an MSDP Peer, page 85
- Shutting Down an MSDP Peer, page 86
- Configuring MSDP MD5 Password Authentication Between MSDP Peers, page 87
- Preventing DoS Attacks by Limiting the Number of SA Messages Allowed in the SA Cache from Specified MSDP Peers, page 89
- Adjusting the MSDP Keepalive and Hold-Time Intervals, page 90
- Adjusting the MSDP Connection-Retry Interval, page 92
- Configuring MSDP Compliance with IETF RFC 3618, page 93
- Configuring a Default MSDP Peer, page 94
- Configuring an MSDP Mesh Group, page 95
- Controlling SA Messages Originated by an RP for Local Sources, page 96
- Controlling the Forwarding of SA Messages to MSDP Peers Using Outgoing Filter Lists, page 97
- Controlling the Receipt of SA Messages from MSDP Peers Using Incoming Filter Lists, page 98
- Using TTL Thresholds to Limit the Multicast Data Sent in SA Messages, page 99
- Requesting Source Information from MSDP Peers, page 100
- Controlling the Response to Outgoing SA Request Messages from MSDP Peers Using SA Request Filters, page 102

Configuring an MSDP Peer

Perform this required task to configure an MSDP peer.

- This task assumes that you have enabled IP multicast routing and have configured PIM-SM.
- With the exception of a single MSDP peer, default MSDP peer, and MSDP mesh group scenarios, all MSDP peers must be configured to run BGP prior to being configured for MSDP.

Note By enabling an MSDP peer, you implicitly enable MSDP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*]
4. **ip msdp description** {*peer-name*| *peer-address*} *text*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*] **Example:** `Router(config)# ip msdp peer 192.168.1.2 connect-source loopback0`	Enables MSDP and configures an MSDP peer as specified by the DNS name or IP address. **Note** The router that is selected to be configured as an MSDP peer is also usually a BGP neighbor. If it is not, see the Configuring a Default MSDP Peer, page 94 section or the Configuring an MSDP Mesh Group, page 95 section. • If you specify the **connect-source**keyword, the primary address of the specified local interface *type* and *number* values are used as the source IP address for the TCP connection. The **connect-source**keyword is recommended, especially for MSDP peers on a border that peer with a router inside of a remote domain.
Step 4	**ip msdp description** {*peer-name*| *peer-address*} *text* **Example:** `Router(config)# ip msdp description 192.168.1.2 router at customer a`	(Optional) Configures a description for a specified peer to make it easier to identify in a configuration or in **show** command output.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Shutting Down an MSDP Peer

Perform this optional task to shut down an MSDP peer.

If you are configuring several MSDP peers and you do not want any of the peers to go active until you have finished configuring all of them, you can shut down each peer, configure each peer, and later bring each peer up. You might also want to shut down an MSDP session without losing the configuration for that MSDP peer.

When an MSDP peer is shut down, the TCP connection is terminated and not restarted until the peer is brought back up using the **no** form of the **ip msdp shutdown** command (for the specified peer).

This task assumes that you are running MSDP and have configured MSDP peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp shutdown** {*peer-name* | *peer-address*}
4. Repeat Step 3 to shut down additional MSDP peers.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp shutdown** {*peer-name* | *peer-address*} **Example:** `Router(config)# ip msdp shutdown 192.168.1.3`	Administratively shuts down the specified MSDP peer.
Step 4	Repeat Step 3 to shut down additional MSDP peers.	--
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring MSDP MD5 Password Authentication Between MSDP Peers

Perform this optional task to configure MSDP MD5 password authentication between MSDP peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*
4. **end**
5. **show ip msdp peer** [peer-address | peer-name]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string* **Example:** `Router(config)# ip msdp password peer 10.32.43.144 0 test`	Enables MD5 password encryption for a TCP connection between two MSDP peers. **Note** MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. • If you configure or change the password or key used for MD5 authentication between two MSDP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the keepalive period expires. If the password is not entered or changed on the remote router before the keepalive period expires, the session will time out and the MSDP session will reset.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show ip msdp peer** [peer-address | peer-name] **Example:** `Router# show ip msdp peer`	(Optional) Displays detailed information about MSDP peers. **Note** Use this command to verify whether MD5 password authentication is enabled on an MSDP peer.

• Troubleshooting Tips, page 88

Troubleshooting Tips

If a router has a password configured for an MSDP peer, but the MSDP peer does not, a message such as the following will appear on the console while the routers attempt to establish an MSDP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the console:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

The **debug ip tcp transactions** command is used to display information on significant TCP transactions such as state changes, retransmissions, and duplicate packets. In the context of monitoring or troubleshooting MSDP MD5 password authentication, use the **debug ip tcp transactions** command to verify that the MD5 password is enabled and that the keepalive message is received by the MSDP peer.

Preventing DoS Attacks by Limiting the Number of SA Messages Allowed in the SA Cache from Specified MSDP Peers

Perform this optional (but highly recommended) task to limit the overall number of SA messages that the router can accept from specified MSDP peers. Performing this task protects an MSDP-enabled router from distributed denial-of-service (DoS) attacks.

Note We recommend that you perform this task for all MSDP peerings on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit*
4. Repeat Step 3 to configure SA limits for additional MSDP peers.
5. **end**
6. **show ip msdp count** [*as-number*]
7. **show ip msdp peer** [*peer-address* | *peer-name*]
8. **show ip msdp summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit* **Example:** `Router(config)# ip msdp sa-limit 192.168.10.1 100`	Limits the number of SA messages allowed in the SA cache from the specified MSDP.
Step 4	Repeat Step 3 to configure SA limits for additional MSDP peers.	--
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**show ip msdp count** [*as-number*] **Example:** `Router# show ip msdp count`	(Optional) Displays the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache.
Step 7	**show ip msdp peer** [*peer-address* | *peer-name*] **Example:** `Router# show ip msdp peer`	(Optional) Displays detailed information about MSDP peers. **Note** The output of this command displays the number of SA messages received from MSDP peers that are stored in the cache.
Step 8	**show ip msdp summary** **Example:** `Router# show ip msdp summary`	(Optional) Displays MSDP peer status. **Note** The output of this command displays a per-peer "SA Count" field that displays the number of SAs stored in the cache.

Adjusting the MSDP Keepalive and Hold-Time Intervals

Perform this optional task to adjust the interval at which an MSDP peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down. By default, it may take as long as 75 seconds for an MSDP peer to detect that a peering session with another MSDP peer has gone down. In network environments with redundant MSDP peers, decreasing the hold-time interval (by lowering the value for the *hold-time-interval* argument of the **ip msdp keepalive**

command from the default of 75 seconds) can expedite the reconvergence time of MSDP peers in the event that an MSDP peer fails.

Note We recommend that you do not change the command defaults for the **ip msdp keepalive** command, because the command defaults are in accordance with RFC 3618, *Multicast Source Discovery Protocol* . If your network environment requires that you modify the defaults, you must configure the same time values for the *keepalive-interval* and *hold-time-interval* arguments on both ends of the MSDP peering session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval*
4. Repeat Step 3 to adjust the keepalive message interval for additional MSDP peers.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval* **Example:** `Router(config)# ip msdp keepalive 10.1.1.3 40 55`	Configures the interval at which an MSDP peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down. • By default, an MSDP peer sends keepalive messages at an interval of once every 60 seconds, and the hold-time interval for an MSDP peer is set to 75 seconds. • Use the *keepalive-interval* argument to specify the interval, in seconds, at which the MSDP peer will send keepalive messages. The range is from 1 to 60. • Use the *hold-time-interval*argument to specify the interval, in seconds, at which the MSDP peer will wait for keepalive messages from other peers before declaring them down. The range is from 1 to 75.
Step 4	Repeat Step 3 to adjust the keepalive message interval for additional MSDP peers.	--

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Adjusting the MSDP Connection-Retry Interval

Perform this optional task to adjust the interval at which MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. In network environments where fast recovery of SA messages is required (such as in trading floor network environments), you may want to decrease the connection-retry interval to a time value less than the default value of 30 seconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp timer** *connection-retry-interval*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp timer** *connection-retry-interval* **Example:** `Router# ip msdp timer 45` **Example:**	Configures the interval at which MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. • By default, an MSDP peer will wait 30 seconds after a peering session is reset before attempting to reestablish the peering session with any peer. • Use the *connection-retry-interval* argument to specify the interval, in seconds, at which MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. The range is from 1 to 60.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring MSDP Compliance with IETF RFC 3618

Perform this optional task to configure MSDP peers to be compliant with Internet Engineering Task Force (IETF) RFC 3618 specifications for MSDP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp rpf rfc3618**
4. **end**
5. **show ip msdp rpf-peer** *rp-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp rpf rfc3618** **Example:** `Router(config)# ip msdp rpf rfc3618`	Enables compliance with the peer-RPF forwarding rules specified in IETF RFC 3618.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show ip msdp rpf-peer** *rp-address* **Example:** `Router# show ip msdp rpf-peer 192.168.1.5`	(Optional) Displays the unique MSDP peer information from which a router will accept SA messages originating from the specified RP.

Configuring a Default MSDP Peer

Perform this optional task to configure a default MSDP peer.

An MSDP default peer must be a previously configured MSDP peer. Before configuring a default MSDP peer, you must first configure an MSDP peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*] **Example:** `Router(config)# ip msdp default-peer 192.168.1.3`	Configures a default peer from which to accept all MSDP SA messages
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an MSDP Mesh Group

Perform this optional task to configure an MSDP mesh group.

Note You can configure multiple mesh groups per router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*}
4. Repeat Step 3 to add MSDP peers as members of the mesh group.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*} **Example:** `Router(config)# ip msdp mesh-group peermesh`	Configures an MSDP mesh group and indicates that an MSDP peer belongs to that mesh group. **Note** All MSDP peers on a router that participate in a mesh group must be fully meshed with all other MSDP peers in the group. Each MSDP peer on each router, therefore, must be configured as a peer with **ip msdp peer** and as a member of the mesh group using the **ip msdp mesh-group** command.
Step 4	Repeat Step 3 to add MSDP peers as members of the mesh group.	--
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling SA Messages Originated by an RP for Local Sources

Perform this task to control SA messages originated by an RP by enabling a filter to restrict which registered sources are advertised in SA messages.

Note For best practice information related to configuring MSDP SA message filters, see the Multicast Source Discovery Protocol SA Filter Recommendations tech note.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*] **Example:** `Router(config)# ip msdp redistribute route-map customer-sources`	Enables a filter for MSDP SA messages originated by the local router. **Note** The **ip msdp redistribute** command could also be used to advertise sources that are known to the RP but not registered. However, it is strongly recommended that you not originate advertisements for sources that have not registered with the RP.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling the Forwarding of SA Messages to MSDP Peers Using Outgoing Filter Lists

Perform this optional task to control the forwarding of SA messages to MSDP peers by configuring outgoing filter lists.

Note For best practice information related to configuring MSDP SA message filters, see the Multicast Source Discovery Protocol SA Filter Recommendations tech note.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. Repeat Step 3 to configure outgoing filter lists for additional MSDP peers.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] **Example:** `Router(config)# ip msdp sa-filter out 192.168.1.5 peerone`	Enables a filter for outgoing MSDP messages.
Step 4	Repeat Step 3 to configure outgoing filter lists for additional MSDP peers.	--
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling the Receipt of SA Messages from MSDP Peers Using Incoming Filter Lists

Perform this optional task to control the receipt of incoming SA messages from MSDP peers.

Note For best practice information related to configuring MSDP SA message filters, see the Multicast Source Discovery Protocol SA Filter Recommendations tech note.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. Repeat Step 3 to configure incoming filter lists for additional MSDP peers.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] **Example:** `Router(config)# ip msdp sa-filter in 192.168.1.3`	Enables a filter for incoming MSDP SA messages.
Step 4	Repeat Step 3 to configure incoming filter lists for additional MSDP peers.	--
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Using TTL Thresholds to Limit the Multicast Data Sent in SA Messages

Perform this optional task to establish a time to live (TTL) threshold to limit the multicast data sent in SA messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value* **Example:** **Example:** `Router(config)# ip msdp ttl-threshold 192.168.1.5 8`	Sets a TTL value for MSDP messages originated by the local router. • By default, multicast data packets in SA messages are sent to an MSDP peer, provided the TTL value of the packet is greater than 0, which is standard TTL behavior.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Requesting Source Information from MSDP Peers

Perform this optional task to enable a router to request source information from MSDP peers.

Note Because SA caching is enabled by default and cannot be explicitly enabled or disabled in Cisco IOS Release 12.1(7) and 12.0(14)S1 and later Cisco IOS software releases, performing this task is seldom needed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-request** {*peer-address* | *peer-name*}
4. Repeat Step 3 to specify that the router send SA request messages to additional MSDP caching peers.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-request** {*peer-address* | *peer-name*} **Example:** `Router(config)# ip msdp sa-request 192.168.10.1`	Specifies that the router send SA request messages to the specified MSDP peer.
Step 4	Repeat Step 3 to specify that the router send SA request messages to additional MSDP caching peers.	--
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling the Response to Outgoing SA Request Messages from MSDP Peers Using SA Request Filters

Perform this optional task to control the outgoing SA request messages that the router will honor from MSDP peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]
4. Repeat Step 3 to configure SA request filters for additional MSDP peers.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*] **Example:** `Router(config)# ip msdp filter sa-request 172.31.2.2 list 1`	Enables a filter for outgoing SA request messages. **Note** Only one SA request filter can be configured per MSDP peer.
Step 4	Repeat Step 3 to configure SA request filters for additional MSDP peers.	--
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Including a Bordering PIM Dense Mode Region in MSDP

Perform this optional task to configure a border router to send SA messages for sources active in a PIM dense mode (PIM-DM) region.

You might have a router that borders a PIM-SM region and a PIM-DM region. By default, sources in the PIM-DM domain are not included in MSDP. You could configure this border router to send SA messages for sources active in the PIM-DM domain. If you do so, it is very important to also configure the **ip msdp redistribute** command to control what local sources from the PIM-DM domain are advertised. Not configuring this command can result in the (S, G) state remaining long after a source in the PIM-DM domain has stopped sending.

Note For more information about using the **ip msdp redistribute** command to control the sources advertised in SA messages, see the Controlling SA Messages Originated by an RP for Local Sources, page 96 section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp border sa-address** *type number*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp border sa-address** *type number* **Example:** `Router(config)# ip msdp border sa-address gigabitethernet0/0/0`	Configures the router on the border between a PIM-SM and PIM-DM domain to originate SA messages for active sources in the PIM-DM domain. • The IP address of the interface is used as the originator ID, which is the RP field in the SA message.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an Originating Address Other Than the RP Address

Perform this optional task to allow an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.

The **ip msdp originator-id** command is used to change the default RP address used in MSDP messages. If you need to change the originator ID for any reason, use the **ip msdp originator-id** command. For example, you might change the originator ID in one of these cases:

- If you configure multiple routers in an MSDP mesh group for Anycast RP.
- If you have a router that borders a PIM-SM domain and a PIM-DM domain. If a router borders a PIM-SM domain and a PIM-DM domain and you want to advertise active sources within the PIM-DM domain, use the **ip msdp originator-id** command to configure the RP address in SA messages to be the address of the originating router's interface.

This task assumes that you are running MSDP and have configured MSDP peers. For more information about configuring MSDP peers, see the Configuring an MSDP Peer, page 85 section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp originator-id** *type number*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip msdp originator-id** *type number* **Example:** `Router(config)# ip msdp originator-id ethernet 1`	Configures the RP address in SA messages to be the address of the originating router's interface.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Monitoring MSDP

Perform this optional task to monitor MSDP SA messages, peers, state, and peer status.

SUMMARY STEPS

1. **enable**
2. **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
3. **debug ip msdp resets**
4. **show ip msdp count** [*as-number*]
5. **show ip msdp peer** [*peer-address* | *peer-name*]
6. **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]
7. **show ip msdp summary**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Router# enable
```

Step 2 **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]

Use this command to debug MSDP activity.

Use the optional *peer-address* or *peer-name* argument to specify for which peer debug events are logged.

The following is sample output from the **debug ip msdp** command:

Example:

```
Router# debug ip msdp
MSDP debugging is on
```

```
Router#
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 192.168.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 192.168.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.250: Forward 32-byte SA to peer
```

Step 3 **debug ip msdp resets**

Use this command to debug MSDP peer reset reasons.

Example:

```
Router# debug ip msdp resets
```

Step 4 **show ip msdp count** [*as-number*]

Use this command to display the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache. The **ip msdp cache-sa-state** command must be configured for this command to produce any output.

The following is sample output from the **show ip msdp count**command:

Example:

```
Router# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
    192.168.4.4: 8
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 8
    ?: 8/8
```

Step 5 **show ip msdp peer** [*peer-address* | *peer-name*]

Use this command to display detailed information about MSDP peers.

Use the optional *peer-address* or *peer-name* argument to display information about a particular peer.

The following is sample output from the **show ip msdp peer**command:

Example:

```
Router# show ip msdp peer 192.168.4.4
MSDP Peer 192.168.4.4 (?), AS 64512 (configured AS)
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (2.2.2.2)
    Uptime(Downtime): 00:07:55, Messages sent/received: 8/18
    Output messages discarded: 0
```

```
    Connection and counters cleared 00:08:55 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 8
  Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
```

Step 6 **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]

Use this command to display the (S, G) state learned from MSDP peers.

The following is sample output from the **show ip msdp sa-cache**command:

Example:

```
Router# show ip msdp sa-cache
MSDP Source-Active Cache - 8 entries
(10.44.44.5, 239.232.1.0), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.1), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.2), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.3), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.4), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.5), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.6), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.7), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
```

Step 7 **show ip msdp summary**

Use this command to display MSDP peer status.

The following is sample output from the **show ip msdp summary** command:

Example:

```
Router# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
192.168.4.4      4     Up       00:08:05 0     8     ?
```

Clearing MSDP Connections Statistics and SA Cache Entries

Perform this optional task to clear MSDP connections, statistics, and SA cache entries.

SUMMARY STEPS

1. **enable**
2. **clear ip msdp peer** [*peer-address* | *peer-name*]
3. **clear ip msdp statistics** [*peer-address* | peer-name]
4. **clear ip msdp sa-cache** [*group-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip msdp peer** [*peer-address* | *peer-name*] **Example:** `Router# clear ip msdp peer`	Clears the TCP connection to the specified MSDP peer. • This command resets all MSDP message counters.
Step 3	**clear ip msdp statistics** [*peer-address* | peer-name] **Example:** `Router# clear ip msdp statistics`	Clears the statistics counters for the specified MSDP peer. • This command resets all MSDP message counters.
Step 4	**clear ip msdp sa-cache** [*group-address*] **Example:** `Router# clear ip msdp sa-cache`	Clears SA cache entries. • If the **clear ip msdp sa-cache** is specified with the optional *group-address* argument or *source-address*argument, all SA cache entries are cleared. • Use the optional *group-address* argument to clear all SA cache entries associated with a specific group.

Enabling SNMP Monitoring of MSDP

Perform this optional task to enable Simple Network Management Protocol (SNMP) monitoring of MSDP.

- This task assumes that you have configured SNMP and MSDP on your devices.
- In each PIM-SM domain there should be a device that is configured as the MSDP speaker. This device must have SNMP and the MSDP MIB enabled.

Note

- All MSDP-MIB objects are implemented as read-only.
- The Requests table is not supported in Cisco's implementation of the MSDP MIB.
- The msdpEstablished notification is not supported in Cisco's implementation of the MSDP MIB.

>

SUMMARY STEPS

1. **enable**
2. **snmp-server enable traps msdp**
3. **snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**snmp-server enable traps msdp** **Example:** `Router# snmp-server enable traps msdp`	Enables the sending of MSDP notifications for use with SNMP. **Note** The **snmp-server enable traps msdp** command enables both traps and informs.
Step 3	**snmp-server host** *host* [**traps**	**informs**] [**version** {**1**	**2c**	**3** [**auth**| **priv**	**noauth**]}] *community-string* [**udp-port** *port-number*] **msdp** **Example:** `Router# snmp-server host examplehost msdp`	Specifies the recipient (host) for MSDP traps or informs.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

- Troubleshooting Tips, page 109

Troubleshooting Tips

You can compare the results of MSDP MIB notifications to the output from the software by using the **show ip msdp summary** and **show ip msdp peer** commands on the appropriate router. You can also compare the results of these commands to the results from SNMP Get operations. You can verify SA cache table entries using the **show ip msdp sa-cache** command. Additional troubleshooting information, such as the local address of the connection, the local port, and the remote port, can be obtained using the output from the **debug ip msdp** command.

Configuration Examples for Using MSDP to Interconnect Multiple PIM-SM Domains

Configuring an MSDP Peer Example

The following example shows how to establish MSDP peering connections between three MSDP peers:

Router A

```
!
interface Loopback 0
 ip address 10.220.8.1 255.255.255.255
!
ip msdp peer 10.220.16.1 connect-source Loopback0
ip msdp peer 10.220.32.1 connect-source Loopback0
!
```

Router B

```
!
interface Loopback 0
 ip address 10.220.16.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect connect-source Loopback0
ip msdp peer 10.220.32.1 connect connect-source Loopback0
!
```

Router C

```
!
interface Loopback 0
 ip address 10.220.32.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect 10.220.8.1 connect-source Loopback0
ip msdp peer 10.220.16.1 connect 10.220.16.1 connect-source Loopback0
!
```

Configuring MSDP MD5 Password Authentication Example

The following example shows how to enable MD5 password authentication for TCP connections between two MSDP peers:

Router A

```
!
ip msdp peer 10.3.32.154
```

```
ip msdp password peer 10.3.32.154 0 test
!
```

Router B

```
!
ip msdp peer 10.3.32.153
ip msdp password peer 10.3.32.153 0 test
!
```

Configuring MSDP Compliance with IETF RFC 3618 Example

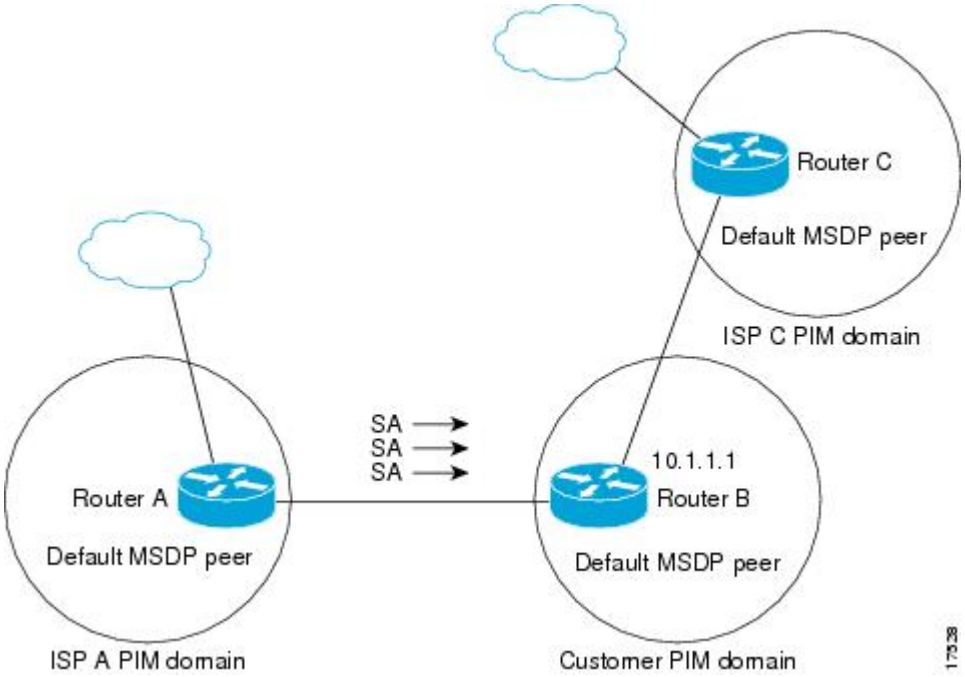
The following example shows how to configure the MSDP peers at 10.10.2.4 and 10.20.1.2 to be compliant with peer-RPF forwarding rules specified in IETF RFC 3618:

```
ip msdp peer 10.10.2.4
ip msdp peer 10.20.1.2
ip msdp rpf rfc3618
```

Configuring a Default MSDP Peer Example

The figure illustrates a scenario where default MSDP peers might be used. In the figure, a customer that owns Router B is connected to the internet through two ISPs, one that owns Router A and the other that owns Router C. They are not running (M)BGP between them. In order for the customer to learn about sources in the ISP domain or in other domains, Router B identifies Router A as its default MSDP peer. Router B advertises SA messages to both Router A and Router C, but accepts SA messages either from Router A only or Router C only. If Router A is the first default peer in the configuration, it will be used if it is up and running. Only if Router A is not running will Router B accept SA messages from Router C.
The ISP will also likely use a prefix list to define which prefixes it will accept from the customer router. The customer will define multiple default peers, each having one or more prefixes associated with it.
The customer has two ISPs to use. The customer defines both ISPs as default peers. As long as the first default peer identified in the configuration is up and running, it will be the default peer and the customer will accept all SA messages it receives from that peer.

Figure 11 Default MSDP Peer Scenario



Router B advertises SAs to Router A and Router C, but uses only Router A or Router C to accept SA messages. If Router A is first in the configuration file, it will be used if it is up and running. Only when Router A is not running will Router B accept SAs from Router C. This is the behavior without a prefix list.

If you specify a prefix list, the peer will be a default peer only for the prefixes in the list. You can have multiple active default peers when you have a prefix list associated with each. When you do not have any prefix lists, you can configure multiple default peers, but only the first one is the active default peer as long as the router has connectivity to this peer and the peer is alive. If the first configured peer goes down or the connectivity to this peer goes down, the second configured peer becomes the active default, and so on.

The following example shows a partial configuration of Router A and Router C in the figure. Each of these ISPs may have more than one customer using default peering, like the customer in the figure. In that case, they may have similar configurations. That is, they will only accept SAs from a default peer if the SA is permitted by the corresponding prefix list.

Router A Configuration

```
ip msdp default-peer 10.1.1.1
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

Router C Configuration

```
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

Configuring MSDP Mesh Groups Example

The following example shows how to configure three routers to be fully meshed members of an MSDP mesh group:

Router A Configuration

```
ip msdp peer 10.2.2.2
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.2.2.2
ip msdp mesh-group test-mesh-group 10.3.3.3
```

Router B Configuration

```
ip msdp peer 10.1.1.1
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.3.3.3
```

Router C Configuration

```
ip msdp peer 10.1.1.1
ip msdp peer 10.2.2.2
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.2.2.2
```

Additional References

Related Documents

Related Topic	Document Title
Multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*
Concepts, tasks and examples for configuring an IP multicast network using PIM	" Configuring Basic IP Multicast " module

Standards

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

MIBs

MIB	MIBs Link
MSDP-MIB.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2858	Multiprotocol Extensions for BGP-4
RFC 3618	Multicast Source Discovery Protocol

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Using MSDP to Interconnect Multiple PIM-SM Domains

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4 Feature Information for Using MSDP to Interconnect Multiple PIM-SM Domains

Feature Name	Releases	Feature Information
MSDP Compliance with IETF RFC 3618	Cisco IOS XE Release 2.1	The MSDP Compliance with IETF RFC 3618 feature enables you to configure MSDP to comply with the peer-RPF forwarding rules defined in the IETF RFC 3618 specifications. Enabling the MSDP Compliance with IETF RFC 3618 feature prevents SA message loops. Additionally, enabling the MSDP Compliance with IETF RFC 3618 feature eliminates the requirement that BGP RRs run MSDP, enables the use of an IGP for the RPF check, and allows MSDP peerings between routers in nondirectly connected autonomous systems. The following commands were introduced or modified by this feature: **ip msdp rpf rfc3618**, **show ip msdp rpf-peer**.
MSDP MD5 Password Authentication	Cisco IOS XE Release 2.5	The MSDP MD5 password authentication feature is an enhancement to support MD5 signature protection on a TCP connection between two MSDP peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream. The following commands were introduced or modified by this feature: **ip msdp password peer**, **show ip msdp peer**.

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

Configuring Source Specific Multicast

This module describes how to configure Source Specific Multicast (SSM). The Source Specific Multicast feature is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Source Specific Multicast

Legacy Applications Within the SSM Range Restrictions

Existing applications in a network predating SSM will not work within the SSM range unless they are modified to support (S, G) channel subscriptions or are enabled through URD. Therefore, enabling SSM in a network may cause problems for existing applications if they use addresses within the designated SSM range.

IGMP v3lite and URD Require a Cisco Last Hop Router

SSM and IGMPv3 are solutions that are being standardized in the IETF. However, IGMP v3lite and URD are Cisco-developed solutions. For IGMP v3lite and URD to operate properly for a host, the last hop router toward that host must be a Cisco router with IGMP v3lite or URD enabled.

Note This limitation does not apply to an application using the HSIL if the host has kernel support for IGMPv3, because then the HSIL will use the kernel IGMPv3 instead of IGMP v3lite.

Address Management Restrictions

Address management is still necessary to some degree when SSM is used with Layer 2 switching mechanisms. Cisco Group Management Protocol (CGMP), IGMP snooping, or Router-Port Group Management Protocol (RGMP) currently support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, then they will not benefit from these existing mechanisms. Instead, both receivers will receive all (S, G) channel traffic (and filter out the unwanted traffic on input). Because of the ability of SSM to reuse the group addresses in the SSM range for many independent applications, this situation can lead to less than expected traffic filtering in a switched network. For this reason it is important to follow the recommendations set forth in the IETF drafts for SSM to use random IP addresses out of the SSM range for an application to minimize the chance for reuse of a single address within the SSM range between different applications. For example, an application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup will guarantee that multiple receivers to different channels within the same application service will never experience traffic aliasing in networks that include Layer 2 switches.

IGMP Snooping and CGMP Limitations

IGMPv3 uses new membership report messages that may not be recognized correctly by older IGMP Snooping switches, in which case hosts will not properly receive traffic. This situation is not an issue if URD or IGMP v3lite is used with hosts where the operating system is not upgraded for IGMPv3, because IGMP v3lite and URD rely only on IGMPv1 or IGMPv2 membership reports.

URD Intercept URL Limitations

A URD intercept URL string must be fewer than 256 bytes in length, starting from the */path* argument. In the HTTP/TCP connection, this string must also be contained within a single TCP/IP packet. For example, for a 256-byte string, a link maximum transmission unit (MTU) of 128 bytes between the host and intercepting router would cause incorrect operation of URD.

State Maintenance Limitations

In PIM-SSM, the last hop router will continue to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source will be maintained, even if the source is not sending traffic for longer periods of time (or even never).

This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S, G) state will be deleted and only reestablished after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

HSIL Limitations

As explained in the IGMP v3lite Host Signalling, page 122 concept, the HSIL tries to determine if the host operating system supports IGMPv3. This check is made so that a single application can be used both

on hosts where the operating system has been upgraded to IGMPv3 and on hosts where the operating system only supports IGMPv1 or IGMPv2.

Checking for the availability of IGMPv3 in the host operating system can only be made by the HSIL if IGMPv3 kernel support exists for at least one version of this operating system at the time when the HSIL was provided. If such an IGMPv3 kernel implementation has become available only recently, then users may need to also upgrade the HSIL on their hosts so that applications compiled with the HSIL will then dynamically bind to the newest version of the HSIL, which should support the check for IGMPv3 in the operating system kernel. Upgrading the HSIL can be done independently of upgrading the application itself.

Information About Source Specific Multicast

SSM Overview

Source Specific Multicast (SSM). SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.

SSM Components

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569. The following two components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

Protocol Independent Multicast (PIM) SSM, or PIM-SSM, is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which is required for SSM. IGMP For SSM to run with IGMPv3, SSM must be supported in the router, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The standard IP multicast infrastructure in the Internet and many enterprise intranets is based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have proved to be reliable,

extensive, and efficient. However, they are bound to the complexity and functionality limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic. With SSM, this information is provided by receivers through the source addresses relayed to the last-hop routers by IGMPv3. SSM is an incremental response to the issues associated with ISM and is intended to coexist in the network with the protocols developed for ISM. In general, SSM provides IP multicast service for applications that utilize SSM.

ISM service is described in RFC 1112. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary 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 host group. Membership in a host group simply requires signaling the host group through IGMP Version 1, 2, or 3.

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. In both SSM and ISM, no signaling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signaling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMP Version 3.

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Internet Assigned Numbers Authority (IANA) has reserved the address range from 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. The software allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 through 239.255.255.255. When an SSM range is defined, an existing IP multicast receiver application will not receive any traffic when it tries to use addresses in the SSM range unless the application is modified to use explicit (S, G) channel subscription or is SSM-enabled through a URL Rendezvous Directory (URD).

SSM Operations

An established network in which IP multicast service is based on PIM-SM can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM. That is, SSM does not require an RP, so there is no need for an RP mechanism such as Auto-RP, MSDP, or bootstrap router (BSR).

If SSM is deployed in a network that is already configured for PIM-SM, then only the last-hop routers must be upgraded to a software image that supports SSM. Routers that are not directly connected to receivers do not have to upgrade to a software image that supports SSM. In general, these non-last-hop routers must only run PIM-SM in the SSM range. They may need additional access control configuration to suppress MSDP signaling, registering, or PIM-SM shared-tree operations from occurring within the SSM range.

The SSM mode of operation is enabled by configuring the SSM range using the **ip pim ssm** global configuration command. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 INCLUDE mode membership reports.
- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-SM. In this mode, only PIM (S, G) Join and Prune messages are generated by the router. Incoming messages related to rendezvous point tree (RPT) operations are ignored or rejected, and incoming PIM register messages are immediately answered with Register-Stop messages. PIM-SSM is backward-

compatible with PIM-SM unless a router is a last-hop router. Therefore, routers that are not last-hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).

- For groups within the SSM range, no MSDP Source-Active (SA) messages within the SSM range will be accepted, generated, or forwarded.

IGMPv3 Host Signaling

IGMPv3 is the third version of the IETF standards track protocol in which hosts signal membership to last-hop routers of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership that allows filtering capabilities with respect to sources. A host can signal either that it wants to receive traffic from all sources sending to a group except for some specific sources (a mode called EXCLUDE) or that it wants to receive traffic only from some specific sources sending to the group (a mode called INCLUDE).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode reports are accepted by the last-hop router. In SSM, only INCLUDE mode reports are accepted by the last-hop router.

Benefits of Source Specific Multicast

IP Multicast Address Management Not Required

In the ISM service, applications must acquire a unique IP multicast group address because traffic distribution is based only on the IP multicast group address used. If two applications with different sources and receivers use the same IP multicast group address, then receivers of both applications will receive traffic from the senders of both applications. Even though the receivers, if programmed appropriately, can filter out the unwanted traffic, this situation would cause generally unacceptable levels of unwanted traffic.

Allocating a unique IP multicast group address for an application is still a problem. Most short-lived applications use mechanisms like Session Description Protocol (SDP) and Session Announcement Protocol (SAP) to get a random address, a solution that does not work well with a rising number of applications in the Internet. The best current solution for long-lived applications is described in RFC 2770, but this solution suffers from the restriction that each autonomous system is limited to only 255 usable IP multicast addresses.

In SSM, traffic from each source is forwarded between routers in the network independent of traffic from other sources. Thus different sources can reuse multicast group addresses in the SSM range.

Denial of Service Attacks from Unwanted Sources Inhibited

In SSM, multicast traffic from each individual source will be transported across the network only if it was requested (through IGMPv3, IGMP v3lite, or URD memberships) from a receiver. In contrast, ISM forwards traffic from any active source sending to a multicast group to all receivers requesting that multicast group. In Internet broadcast applications, this ISM behavior is highly undesirable because it allows unwanted sources to easily disturb the actual Internet broadcast source by simply sending traffic to the same multicast group. This situation depletes bandwidth at the receiver side with unwanted traffic and thus disrupts the undisturbed reception of the Internet broadcast. In SSM, this type of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

Easy to Install and Manage

SSM is easy to install and provision in a network because it does not require the network to maintain which active sources are sending to multicast groups. This requirement exists in ISM (with IGMPv1, IGMPv2, or IGMPv3).

The current standard solutions for ISM service are PIM-SM and MSDP. Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or BSR) and MSDP is required only for the

network to learn about active sources. This management is not necessary in SSM, which makes SSM easier than ISM to install and manage, and therefore easier than ISM to operationally scale in deployment. Another factor that contributes to the ease of installation of SSM is the fact that it can leverage preexisting PIM-SM networks and requires only the upgrade of last hop routers to support IGMPv3, IGMP v3lite, or URD.

Ideal for Internet Broadcast Applications

The three benefits previously described make SSM ideal for Internet broadcast-style applications for the following reasons:

- The ability to provide Internet broadcast services through SSM without the need for unique IP multicast addresses allows content providers to easily offer their service (IP multicast address allocation has been a serious problem for content providers in the past).
- The prevention against DoS attacks is an important factor for Internet broadcast services because, with their exposure to a large number of receivers, they are the most common targets for such attacks.
- The ease of installation and operation of SSM makes it ideal for network operators, especially in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains).

IGMP v3lite Host Signalling

IGMP v3lite is a Cisco-developed transitional solution for application developers to immediately start programming SSM applications. It allows you to write and run SSM applications on hosts that do not yet support IGMPv3 in their operating system kernel.

Applications must be compiled with the Host Side IGMP Library (HSIL) for IGMP v3lite. This software provides applications with a subset of the IGMPv3 applications programming interface (API) that is required to write SSM applications. HSIL was developed for Cisco by Talarian and is available from the following web page:

http://www.talarianmulticast.com/cgi-bin/igmpdownld

One part of the HSIL is a client library linked to the SSM application. It provides the SSM subset of the IGMPv3 API to the SSM application. If possible, the library checks whether the operating system kernel supports IGMPv3. If it does, then the API calls simply are passed through to the kernel. If the kernel does not support IGMPv3, then the library uses the IGMP v3lite mechanism.

When using the IGMP v3lite mechanism, the library tells the operating system kernel to join to the whole multicast group, because joining to the whole group is the only method for the application to receive traffic for that multicast group (if the operating system kernel only supports IGMPv1 or IGMPv2). In addition, the library signals the (S, G) channel subscriptions to an IGMP v3lite server process, which is also part of the HSIL. A server process is needed because multiple SSM applications may be on the same host. This server process will then send IGMP v3lite-specific (S, G) channel subscriptions to the last hop Cisco IOS router, which needs to be enabled for IGMP v3lite. This router will then “see” both the IGMPv1 or IGMPv2 group membership report from the operating system kernel and the (S, G) channel subscription from the HSIL daemon. If the router sees both of these messages, it will interpret them as an SSM (S, G) channel subscription and join to the channel through PIM-SSM. We recommend referring to the documentation accompanying the HSIL software for further information on how to utilize IGMP v3lite with your application.

IGMP v3lite is supported by Cisco only through the API provided by the HSIL, not as a function of the router independent of the HSIL. By default, IGMP v3lite is disabled. When IGMP v3lite is configured through the **ip igmp v3lite** interface configuration command on an interface, it will be active only for IP multicast addresses in the SSM range.

URD Host Signalling

URD is a Cisco-developed transitional solution that allows existing IP multicast receiver applications to be used with SSM without the need to modify the application and change or add any software on the receiver host running the application. URD is a content provider solution in which the receiver applications can be started or controlled through a web browser.

URD operates by passing a special URL from the web browser to the last hop router. This URL is called a URD intercept URL. A URD intercept URL is encoded with the (S, G) channel subscription and has a format that allows the last hop router to easily intercept it.

As soon as the last hop router intercepts both an (S, G) channel subscription encoded in a URD intercept URL and sees an IGMP group membership report for the same multicast group from the receiver application, the last hop router will use PIM-SSM to join toward the (S, G) channel as long as the application maintains the membership for the multicast group G. The URD intercept URL is thus only needed initially to provide the last hop router with the address of the sources to join to.

A URD intercept URL has the following syntax:

```
http://
webserver
:465/
path
?group=
group
&source=
source1
&...source=
sourceN
&
```

The *webserver* string is the name or IP address to which the URL is targeted. This target need not be the IP address of an existing web server, except for situations where the web server wants to recognize that the last hop router failed to support the URD mechanism. The number 465 indicates the URD port. Port 465 is reserved for Cisco by the IANA for the URD mechanism so that no other applications can use this port.

When the browser of a host encounters a URD intercept URL, it will try to open a TCP connection to the web server on port 465. If the last hop router is enabled for URD on the interface where the router receives the TCP packets from the host, it will intercept all packets for TCP connections destined to port 465 independent of the actual destination address of the TCP connection (independent of the address of the web server). Once intercepted, the last hop router will “speak” a very simple subset of HTTP on this TCP connection, emulating a web server. The only HTTP request that the last hop router will understand and reply to is the following GET request:

```
GET
argument
 HTTP/1.0
argument
 = /
path
?group=
group
&source=
source1
&...source=
sourceN
&
```

When it receives a GET command, the router tries to parse the argument according to this syntax to derive one or more (S, G) channel memberships. The *path* string of the argument is anything up to, but not including, the first question mark, and is ignored. The *group* and *source1* through *sourceN* strings are the IP addresses or fully qualified domain names of the channels for which this argument is a subscription

request. If the argument matches the syntax shown, the router interprets the argument to be subscriptions for the channels (*source1* , *group*) through (*sourceN* , *group*).

The router will accept the channel subscriptions if the following conditions are met:

- The IP address of the multicast group is within the SSM range.
- The IP address of the host that originated the TCP connection is directly connected to the router.

If the channel subscription is accepted, the router will respond to the TCP connection with the following HTML page format:

```
HTTP/1.1 200 OK
Server:cisco IOS
Content-Type:text/html
<html>
<body>
Retrieved URL string successfully
</body>
</html>
```

If an error condition occurs, the <body> part of the returned HTML page will carry an appropriate error message. The HTML page is a by-product of the URD mechanism. This returned text may, depending on how the web pages carrying a URD intercept URL are designed, be displayed to the user or be sized so that the actual returned HTML page is invisible.

The primary effect of the URD mechanism is that the router will remember received channel subscriptions and will match them against IGMP group membership reports received by the host. The router will "remember" a URD (S, G) channel subscription for up to 3 minutes without a matching IGMP group membership report. As soon as the router sees that it has received both an IGMP group membership report for a multicast group G and a URD (S, G) channel subscription for the same group G, it will join the (S, G) channel through PIM-SSM. The router will then continue to join to the (S, G) channel based only on the presence of a continuing IGMP membership from the host. Thus, one initial URD channel subscription is all that is needed to be added through a web page to enable SSM with URD.

If the last hop router from the receiver host is not enabled for URD, then it will not intercept the HTTP connection toward the web server on port 465. This situation will result in a TCP connection to port 465 on the web server. If no further provisions on the web server are taken, then the user may see a notice (for example, "Connection refused") in the area of the web page reserved for displaying the URD intercept URL (if the web page was designed to show this output). It is also possible to let the web server "listen" to requests on port 465 and install a Common Gateway Interface (CGI) script that would allow the web server to know if a channel subscription failed (for example, to subsequently return more complex error descriptions to the user).

Because the router returns a Content-Type of text and HTML, the best way to include the URD intercept URL into a web page is to use a frame. By defining the size of the frame, you can also hide the URD intercept URL on the displayed page.

By default, URD is disabled on all interfaces. When URD is configured through the **ip urd** interface configuration command on an interface, it will be active only for IP multicast addresses in the SSM range.

How to Configure Source Specific Multicast

Configuring SSM

To configure SSM, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **ip pim ssm** [**default** | **range***access-list*]
2. Router(config)# **interface** type number
3. Router(config-if)# **ip pim** {**sparse-mode** | **sparse-dense-mode**}
4. Do one of the following:
   - Router(config-if)# **ip igmp version 3**
   -
   -
   -
   - Router(config-if)# **ip igmp v3lite**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **ip pim ssm** [**default** | **range***access-list*]	Defines the SSM range of IP multicast addresses.
Step 2	Router(config)# **interface** type number	Selects an interface that is connected to hosts on which IGMPv3, IGMP v3lite, and URD can be enabled.
Step 3	Router(config-if)# **ip pim** {**sparse-mode** | **sparse-dense-mode**}	Enables PIM on an interface. You must use either sparse mode or sparse-dense mode.

	Command or Action	Purpose
Step 4	Do one of the following: • Router(config-if)# **ip igmp version 3** • • • • Router(config-if)# **ip igmp v3lite** **Example:** **Example:** **Example:** **Example:** `Router(config-if)#` **ip urd**	Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2. or Enables the acceptance and processing of IGMP v3lite membership reports on an interface. or Enables interception of TCP packets sent to the reserved URD port 465 on an interface and processing of URD channel subscription reports.

Monitoring SSM

To monitor SSM, use the following commands in privileged EXEC mode, as needed:

Command	Purpose
`Router#` **show ip igmp groups detail**	Displays the (S, G) channel subscription through IGMPv3, IGMP v3lite, or URD.
`Router#` **show ip mroute**	Displays whether a multicast group supports SSM service or whether a source-specific host report was received.

Configuration Examples of Source Specific Multicast

SSM with IGMPv3 Example

The following example shows how to configure a router (running IGMPv3) for SSM:

```
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
    ip pim sparse-mode
!
interface GigabitEthernet3/2/0
    ip address 131.108.1.2 255.255.255.0
    ip pim sparse-mode
    description ethernet connected to hosts
    ip igmp version 3
!
ip pim ssm default
```

SSM with IGMP v3lite and URD Example

The following example shows how to configure IGMP v3lite and URD on interfaces connected to hosts for SSM. Configuring IGMP v3lite and URD is not required or recommended on backbone interfaces.

```
interface gigabitethernet 3/1/1
 ip address 172.21.200.203 255.255.255.0
 ip pim sparse-dense-mode
 description gigabitethernet connected to hosts
!
interface gigabitethernet 1/1/1
description gigabitethernet connected to hosts
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-dense-mode
 ip urd
 ip igmp v3lite
```

SSM Filtering Example

The following example shows how to configure filtering on legacy RP routers running software releases that do not support SSM routing. This filtering will suppress all unwanted PIM-SM and MSDP traffic in the SSM range. Without this filtering, SSM will still operate, but there may be additional RPT traffic if legacy first hop and last hop routers exist in the network.

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The “ip pim accept-register” command
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. “Filtered on receipt” means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
```

```
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

Additional References

The following sections provide references related to Source Specific Multicast.

Related Documents

Related Topic	Document Title
PIM-SM and SSM concepts and configuration examples	“ Configuring Basic IP Multicast ” module
IP multicast commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Source Specific Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 Feature Information for Source Specific Multicast

Feature Name	Release	Feature Information
Source Specific Multicast	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	Source Specific Multicast is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.

Tunneling to Connect Non-IP Multicast Areas

This module describes how to configure a Generic Route Encapsulation (GRE) tunnel to tunnel IP multicast packets between non-IP multicast areas. The benefit is that IP multicast traffic can be sent from a source to a multicast group, over an area where IP multicast is not supported.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Tunneling to Connect Non-IP Multicast Areas

This module assumes you understand the concepts in the “IP Multicast Technology Overview” module.

Information About Tunneling to Connect Non-IP Multicast Areas

Benefits of Tunneling to Connect Non-IP Multicast Areas

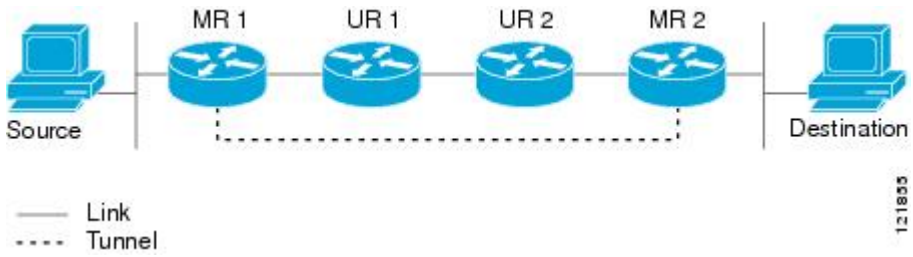
- If the path between a source and a group member (destination) does not support IP multicast, a tunnel between them can transport IP multicast packets.
- Per packet load balancing can be used. Load balancing in IP multicast is normally per (S,G). Therefore, (S1, G) can go over Link X and (S2, G) can go over Link Y, where X and Y are parallel links. If you create a tunnel between the routers, you can get per packet load balancing because the load balancing is done on the tunnel unicast packets.

IP Multicast Static Route

IP multicast static routes (mroutes) allow you to have multicast paths diverge from the unicast paths. When using Protocol Independent Multicast (PIM), the router expects to receive packets on the same interface where it sends unicast packets back to the source. This expectation is beneficial if your multicast and unicast topologies are congruent. However, you might want unicast packets to take one path and multicast packets to take another.

The most common reason for using separate unicast and multicast paths is tunneling. When a path between a source and a destination does not support multicast routing, a solution is to configure two routers with a GRE tunnel between them. In the figure, each unicast router (UR) supports unicast packets only; each multicast router (MR) supports multicast packets.

Figure 12 Tunnel for Multicast Packets



In the figure, Source delivers multicast packets to Destination by using MR 1 and MR 2. MR 2 accepts the multicast packet only if it believes it can reach Source over the tunnel. If this situation is true, when Destination sends unicast packets to Source, MR 2 sends them over the tunnel. The check that MR2 can reach Source over the tunnel is a Reverse Path Forwarding (RPF) check, and the static mroute allows the check to be successful when the interface that the multicast packet arrives on is not the unicast path back to the source. Sending the packet over the tunnel could be slower than natively sending it through UR 2, UR 1, and MR 1.

A multicast static route allows you to use the configuration in the figure by configuring a static multicast source. The system uses the configuration information instead of the unicast routing table to route the traffic. Therefore, multicast packets can use the tunnel without having unicast packets use the tunnel. Static mroutes are local to the router they are configured on and not advertised or redistributed in any way to any other router.

How to Connect Non-IP Multicast Areas

- Configuring a Tunnel to Connect Non-IP Multicast Areas, page 133

Configuring a Tunnel to Connect Non-IP Multicast Areas

Configure a multicast static route if you want your multicast paths to differ from your unicast paths. For example, you might have a tunnel between two routers because the unicast path between a source and destination does not support multicast routing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **ip pim sparse-mode**
6. **tunnel source** {*ip-address* | *type number*}
7. **tunnel destination** {*hostname* | *ip-address*}
8. Repeat Steps 1 through 7 on the router at the opposite end of the tunnel, reversing the tunnel source and destination addresses.
9. **end**
10. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]
11. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]
12. **end**
13. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]
14. **show ip rpf** {*source-address* | *source-name*} [**metric**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 0`	Configures a tunnel interface.
Step 4	**ip unnumbered** *type number* **Example:** `Router(config-if)# ip unnumbered gigabitethernet 0/0/0`	Enables IP processing without assigning an IP address to the interface.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on the tunnel interface.
Step 6	**tunnel source** {*ip-address* | *type number*} **Example:** `Router(config-if)# tunnel source 100.1.1.1`	Configures the tunnel source.
Step 7	**tunnel destination** {*hostname* | *ip-address*} **Example:** `Router(config-if)# tunnel destination 100.1.5.3`	Configures the tunnel destination.
Step 8	Repeat Steps 1 through 7 on the router at the opposite end of the tunnel, reversing the tunnel source and destination addresses.	Router A's tunnel source address will match Router B's tunnel destination address. Router A's tunnel destination address will match Router B's tunnel source address.
Step 9	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 10	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] **Example:** `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	Configures a static multicast route over which to reverse path forward to the other end of the tunnel. • Because the use of the tunnel makes the multicast topology incongruent with the unicast topology, and only multicast traffic traverses the tunnel, you must configure the routers to reverse path forward correctly over the tunnel. • When a source range is specified, the mroute applies only to those sources. • In the example, the *source-address* and *mask* of 0.0.0.0 0.0.0.0 indicate any address. • The shorter distance is preferred. • The default distance is 0.
Step 11	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] **Example:** `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	Configures a static route over which to reverse path forward from the access router to the other end of the tunnel.
Step 12	**end** **Example:** `Router(config)# end`	(Optional) Ends the current configuration session and returns to privileged EXEC mode.
Step 13	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `Router# show ip mroute`	(Optional) Displays the contents of the IP multicast routing (mroute) table.
Step 14	**show ip rpf** {*source-address* | *source-name*} [**metric**] **Example:** `Router# show ip rpf 10.2.3.4`	(Optional) Displays how IP multicast routing does RPF.

Configuration Examples for Tunneling to Connect Non-IP Multicast Areas

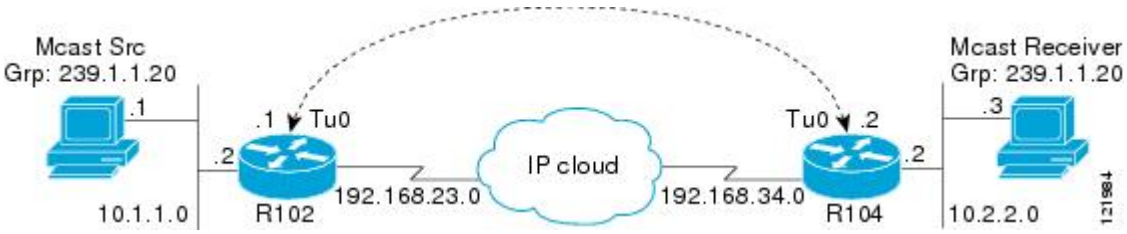
Tunneling to Connect Non-IP Multicast Areas Example

The following example also appears online at:

http://www.cisco.com/en/US/tech/tk828/tk363/technologies_configuration_example09186a00801a5aa2.shtml

In the figure below, the multicast source (10.1.1.1) is connected to R102 and is configured for multicast group 239.1.1.20. The multicast receiver (10.2.2.3) is connected to R104 and is configured to receive multicast packets for group 239.1.1.20. Separating R102 and R104 is an IP cloud, which is not configured for multicast routing.

Figure 13 Tunnel Connecting Non-IP Multicast Areas



A tunnel is configured between R102 to R104 sourced with their loopback interfaces. The **ip pim sparse-dense-mode** command is configured on tunnel interfaces and multicast-routing is enabled on R102 and R104. Sparse-dense mode configuration on the tunnel interfaces allows sparse-mode or dense-mode packets to be forwarded over the tunnel depending on rendezvous point (RP) configuration for the group.

Note For dense mode--With PIM dense mode configured over the tunnel, an **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** command is configured on R104 to ensure a successful RPF for multicast source address 10.1.1.1. Incoming (10.1.1.1, 239.1.1.20) multicast packets over Tunnel0 (Tu0) are checked for Reverse Path Forwarding (RPF) using this mroute statement. After a successful check, the multicast packets are forwarded to outgoing interface list (OIL) interfaces.

Note For sparse mode--With PIM sparse mode configured over the tunnel, ensure that the following points are addressed:

- For a successful RPF verification of multicast traffic flowing over the shared tree (*,G) from RP, an **ip mroute rp-address nexthop** command needs to be configured for the RP address, pointing to the tunnel interface.

Assuming R102 to be the RP (RP address 2.2.2.2) in this case, the mroute would be the **ip mroute 2.2.2.2 255.255.255.255 tunnel 0**command, which ensures a successful RPF check for traffic flowing over the shared tree.

- For a successful RPF verification of multicast (S,G) traffic flowing over the Shortest Path Tree (SPT), an **ip mroute source-address nexthop** command needs to be configured for the multicast source, pointing to the tunnel interface.

In this case, when SPT traffic is flowing over tunnel interface an **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** command is configured on R104 to ensure a successful RPF verification for incoming (10.1.1.1, 239.1.1.20) multicast packets over the Tunnel 0 interface.

R102#

```
version 12.2
hostname r102
ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
!--- Tunnel interface configured for PIM and carrying multicast packets to R104.
 ip address 192.168.24.1 255.255.255.252
 ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 4.4.4.4
!
interface Ethernet0/0
!--- Interface connected to Source.
ip address 10.1.1.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial8/0
 ip address 192.168.23.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
!
ip classless
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R104#

```
version 12.2
!
hostname r104
!
ip subnet-zero
no ip domain-lookup
```

```
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
 ip address 192.168.24.2 255.255.255.252
!--- Tunnel interface configured for PIM and carrying multicast packets.
ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 2.2.2.2
!
interface Ethernet0/0
 ip address 10.2.2.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial9/0
 ip address 192.168.34.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 192.168.34.0 0.0.0.255 area 0
!
ip classless
no ip http server
ip pim bidir-enable
ip mroute 10.1.1.0 255.255.255.0 Tunnel0
!--- This Mroute ensures a successful RPF check for packets flowing from the source.
!--- 10.1.1.1 over Shared tree in case of Dense more and SPT in case of Sparse mode.
!
ip mroute 2.2.2.2 255.255.255.255 tunnel 0
!--- This Mroute is required for RPF check when Sparse mode multicast traffic is
!--- flowing from RP (assuming R102 with 2.2.2.2 as RP)  towards receiver via tunnel
!--- before the SPT switchover.
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Tunneling to Connect Non-IP Multicast Areas

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6 Feature Information for Tunneling to Connect Non-IP Multicast Areas

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS XE Release 2.1 or later. This table will be updated when feature information is added to this module.	--	--

Verifying IP Multicast Operation

This module describes how to verify IP multicast operation in a network after Protocol Independent Multicast (PIM) sparse mode (PIM-SM) or Source Specific Multicast (PIM-SSM) has been implemented. The tasks in this module can be used to test IP multicast reachability and to confirm that receivers and sources are operating as expected in an IP multicast network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Verifying IP Multicast Operation

- Before performing the tasks in this module, you should be familiar with the concepts described in the " IP Multicast Technology Overview " module.
- The tasks in this module assume that IP multicast has been enabled and that PIM-SM or SSM has been configured using the relevant tasks described in the " Configuring Basic IP Multicast " module.

Restrictions for Verifying IP Multicast Operation

- For PIM-SM, this module assumes that the shortest path tree (SPT) threshold for PIM-enabled routers is set to the value of zero (the default) and not infinity. For more information about setting the SPT

threshold, see the **ip pim spt-threshold** command page in the *Cisco IOS IP Multicast Command Reference*.

- Verifying IP multicast operation in a bidirectional PIM (bidir-PIM) network or a PIM-SM network with a finite or infinite SPT threshold is outside the scope of this module.

Information About Verifying IP Multicast Operation

Guidelines for Verifying IP Multicast Operation in a PIM-SM and PIM-SSM Network Environment

When you verify the operation of IP multicast in a PIM-SM network environment or in an PIM-SSM network environment, a useful approach is to begin the verification process on the last hop router, and then continue the verification process on the routers along the SPT until the first hop router has been reached. The goal of the verification is to ensure that IP multicast traffic is being routed properly through an IP multicast network.

Common Commands Used to Verify IP Multicast Operation on the Last Hop Router for PIM-SM and PIM-SSM

The table describes the common commands used to verify IP multicast operation on the last hop router in PIM-SM and PIM-SSM network environments.

Table 7 Common IP Multicast Verification Commands (Last Hop Router)

Command	Description and Purpose
show ip igmp groups	Displays the multicast groups with receivers that are directly connected to the router and that were learned through the Internet Group Management Protocol (IGMP). • Use this command to confirm that the IGMP cache is being properly populated on the last hop router for the groups that receivers on the LAN have joined.

Command	Description and Purpose
show ip pim rp mapping	Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP or BSR). • Use this command to confirm that the group-to-RP mappings are being populated correctly on the last hop router. **Note** The **show ip pim rp mapping**command does not work with routers in a PIM-SSM network because PIM-SSM does not use rendezvous points (RPs).
show ip mroute	Displays the contents of the multicast routing (mroute) table. • Use this command to verify that the mroute table is being populated properly on the last hop router.
show ip interface	Displays information and statistics about configured interfaces. • Use this command to verify that IP multicast fast switching is enabled on the outgoing interface on the last hop router.
show ip mfib	Displays the forwarding entries and interfaces in the IP Multicast Forwarding Information Base (MFIB).
show ip pim interface count	Displays statistics related to the number of multicast packets received by and sent out a PIM-enabled interface. • Use this command on the last hop router to confirm that multicast traffic is being forwarded on the last hop router.
show ip mroute active	Displays the rate that active sources are sending to multicast groups, in kilobits per second (kb/s). • Use this command to display information about the multicast packet rate for active sources sending to groups on the last hop router.

Command	Description and Purpose
show ip mroute count	Displays statistics related to mroutes in the mroute table. • Use this command on the last hop router to confirm that multicast traffic is flowing on the last hop router.

Common Commands Used to Verify IP Multicast Operation on Routers Along the SPT for PIM-SM and PIM-SSM

The table describes the common commands used to verify IP multicast operation on routers along the SPT in PIM-SM and PIM-SSM network environments.

Table 8 Common IP Multicast Verification Commands (Routers Along SPT)

Command	Description and Purpose
show ip mroute	Displays the contents of the mroute table. • Use this command to confirm that the Reverse Path Forwarding (RPF) neighbor toward the source is the expected RPF neighbor for each router along the SPT.
show ip mroute active	Displays the rate that active sources are sending to multicast groups, in kb/s. • Use this command to display information about the multicast packet rate for active sources sending to groups on routers along the SPT.

Common Commands Used to Verify IP Multicast Operation on the First Hop Router for PIM-SM and PIM-SSM

The table describes the common commands used to verify IP multicast operation on the first hop router in PIM-SM and PIM-SSM network environments.

Table 9 Common IP Multicast Verification Commands (First Hop Router)

Command	Description and Purpose
show ip mroute	Displays the contents of the mroute table. • Use this command to confirm that the F flag is set for the mroutes on the first hop router.

Command	Description and Purpose
show ip mroute active	Displays the rate that active sources are sending to multicast groups, in kb/s. • Use this command to display information about the multicast packet rate for active sources sending to groups on the first hop router.

How to Verify IP Multicast Operation

Using PIM-Enabled Routers to Test IP Multicast Reachability

Perform the following tasks to use PIM-enabled routers to test IP multicast reachability.

If all the PIM-enabled routers and access servers that you administer are members of a multicast group, pinging that group causes all routers to respond, which can be a useful administrative and debugging tool.

To use PIM-enabled routers to test IP multicast reachability, perform the following tasks:

Configuring Routers to Respond to Multicast Pings

Perform the following task to configure routers to respond to multicast pings. Performing this task configures interfaces on the router to join a specified group. This task should be performed on each interface on the router participating in the multicast network and on all routers participating in the multicast network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp join-group** *group-address*
5. Repeat Step 3 and Step 4 for each interface on the router participating in the multicast network.
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Enters interface configuration mode. • For the *type* and *number* arguments, specify an interface that is directly connected to hosts or is facing hosts.
Step 4	**ip igmp join-group** *group-address* **Example:** `Router(config-if)# ip igmp join-group 225.2.2.2`	(Optional) Configures an interface on the router to join the specified group. • For the purpose of this task, configure the same group address for the *group-address* argument on all interfaces on the router participating in the multicast network. **Note** With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching.
Step 5	Repeat Step 3 and Step 4 for each interface on the router participating in the multicast network.	--
Step 6	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.

Pinging Routers Configured to Respond to Multicast Pings

Perform the following task on a router to initiate a ping test to the routers configured to respond to multicast pings. This task is used to test IP multicast reachability in a network.

SUMMARY STEPS

1. **enable**
2. **ping** *group-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ping** *group-address* **Example:** `Router# ping 225.2.2.2`	Pings an IP multicast group address. • A successful response indicates that the group address is functioning.

Verifying IP Multicast Operation in a PIM-SM or a PIM-SSM Network

Perform the following optional tasks to verify IP multicast operation in a PIM-SM or a PIM-SSM network. You can perform the steps in these tasks to locate a faulty hop when sources and receivers are not operating as expected.

Note If packets are not reaching their expected destinations, you might want consider disabling IP multicast fast switching, which would place the router in process switching mode. If packets begin reaching their proper destinations after IP multicast fast switching has been disabled, then the issue most likely was related to IP multicast fast switching. See the " Monitoring and Maintaining IP Multicast " module for information on how to disable IP multicast fast switching.

To verify IP multicast operation in a PIM-SM or PIM-SSM multicast network, perform the following verification tasks:

- Verifying IP Multicast Operation on the Last Hop Router, page 147
- Verifying IP Multicast on Routers Along the SPT, page 151
- Verifying IP Multicast on the First Hop Router, page 152

Verifying IP Multicast Operation on the Last Hop Router

Perform the following task to verify the operation of IP multicast on the last hop router.

Note If you are verifying a last hop router in a PIM-SSM network, ignore Step 3.

SUMMARY STEPS

1. **enable**
2. **show ip igmp groups**
3. **show ip pim rp mapping**
4. **show ip mroute**
5. **show ip interface** [*type number*]
6. **show ip mfib**
7. **show ip pim interface count**
8. **show ip mroute count**
9. **show ip mroute active** [*kb/s*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show ip igmp groups**

Use this command to verify IGMP memberships on the last hop router. This information will confirm the multicast groups with receivers that are directly connected to the last hop router and that are learned through IGMP.

The following is sample output from the **show ip igmp groups** command:

Example:

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.1.2.3        GigabitEthernet1/0/0     00:05:14  00:02:14  10.1.0.6
224.0.1.39       GigabitEthernet0/0/0     00:09:11  00:02:08  172.31.100.1
```

Step 3 **show ip pim rp mapping**

Use this command to confirm that the group-to-RP mappings are being populated correctly on the last hop router.

Note Ignore this step if you are verifying a last hop router in a PIM-SSM network. The **show ip pim rp mapping**command does not work with routers in a PIM-SSM network because PIM-SSM does not use RPs. In addition, if configured correctly, PIM-SSM groups should not appear in the output of the **show ip pim rp mapping**command.

The following is sample output from the **show ip pim rp mapping**command:

Example:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 172.16.0.1 (?), v2v1
```

```
    Info source: 172.16.0.1 (?), elected via Auto-RP
         Uptime: 00:09:11, expires: 00:02:47
```

Step 4 **show ip mroute**

Use this command to verify that the mroute table is being populated properly on the last hop router.

The following is sample output from the **show ip mroute** command:

Example:

```
Router# show ip mroute
(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04

(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
  GigabitEthernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04

(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00
    GigabitEthernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00

(172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
```

Step 5 **show ip interface** [*type number*]

Use this command to verify that multicast fast switching is enabled for optimal performance on the outgoing interface on the last hop router.

Note Using the **no ip mroute-cache** interface command disables IP multicast fast-switching. When IP multicast fast switching is disabled, packets are forwarded through the process-switched path.

The following is sample output from the **show ip interface**command for a particular interface:

Example:

```
Router# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.31.100.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13
      224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
```

```
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Step 6 **show ip mfib**

Use this command to display the forwarding entries and interfaces in the IP Multicast Forwarding Information Base (MFIB).

Example:

Step 7 **show ip pim interface count**

Use this command to confirm that multicast traffic is being forwarded on the last hop router.

The following is sample output from the **show ip pim interface** command with the **count** keyword:

Example:

```
Router# show ip pim interface count

State: * - Fast Switched, D - Distributed Fast Switched
       H - Hardware Switching Enabled
Address          Interface              FS Mpackets In/Out
172.31.100.2     GigabitEthernet0/0/0     *   4122/0
10.1.0.1         GigabitEthernet1/0/0     *   0/3193
```

Step 8 **show ip mroute count**

Use this command to confirm that multicast traffic is being forwarded on the last hop router.

The following is sample output from the **show ip mroute**command with the **count** keyword:

Example:

```
Router# show ip mroute count
IP Multicast Statistics
6 routes using 4008 bytes of memory
3 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0

Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120
  Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99

Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10
  Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0
```

Step 9 **show ip mroute active** [*kb/s*]

Use this command on the last hop router to display information about active multicast sources sending traffic to groups on the last hop router. The output of this command provides information about the multicast packet rate for active sources.

Note By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic.

The following is sample output from the **show ip mroute**command with the **active** keyword:

Example:

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)
```

Verifying IP Multicast on Routers Along the SPT

Perform the following task to verify the operation of IP multicast on routers along the SPT in a PIM-SM or PIM-SSM network.

SUMMARY STEPS

1. **enable**
2. **show ip mroute** [*group-address*]
3. **show ip mroute active**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show ip mroute** [*group-address*]
Use this command on routers along the SPT to confirm the RPF neighbor toward the source for a particular group or groups.

The following is sample output from the **show ip mroute**command for a particular group:

Example:

```
Router# show ip mroute 239.1.2.3
```

```
(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:17:56/00:03:02

(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T
  Incoming interface: Serial1/0, RPF nbr 172.31.200.1
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:15:34/00:03:02
```

Step 3 **show ip mroute active**

Use this command on routers along the SPT to display information about active multicast sources sending to groups. The output of this command provides information about the multicast packet rate for active sources.

Note By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic.

The following is sample output from the **show ip mroute** command with the **active** keyword:

Example:

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

Verifying IP Multicast on the First Hop Router

Perform the following task to verify the operation of IP multicast on the first hop router.

SUMMARY STEPS

1. **enable**
2. **show ip mroute** [*group-address*]
3. **show ip mroute active** [*kb/s*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

```
Router> enable
```

Step 2 **show ip mroute** [*group-address*]

Use this command on the first hop router to confirm the F flag has been set for mroutes on the first hop router.

The following is sample output from the **show ip mroute**for a particular group:

Example:

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF
  Incoming interface: Serial1/0, RPF nbr 172.31.200.2
  Outgoing interface list: Null

(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/0, Forward/Sparse-Dense, 00:18:10/00:03:19
```

Step 3 **show ip mroute active** [*kb/s*]

Use this command on the first hop router to display information about active multicast sources sending to groups. The output of this command provides information about the multicast packet rate for active sources.

Note By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic.

The following is sample output from the **show ip mroute** command with the **active** keyword:

Example:

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

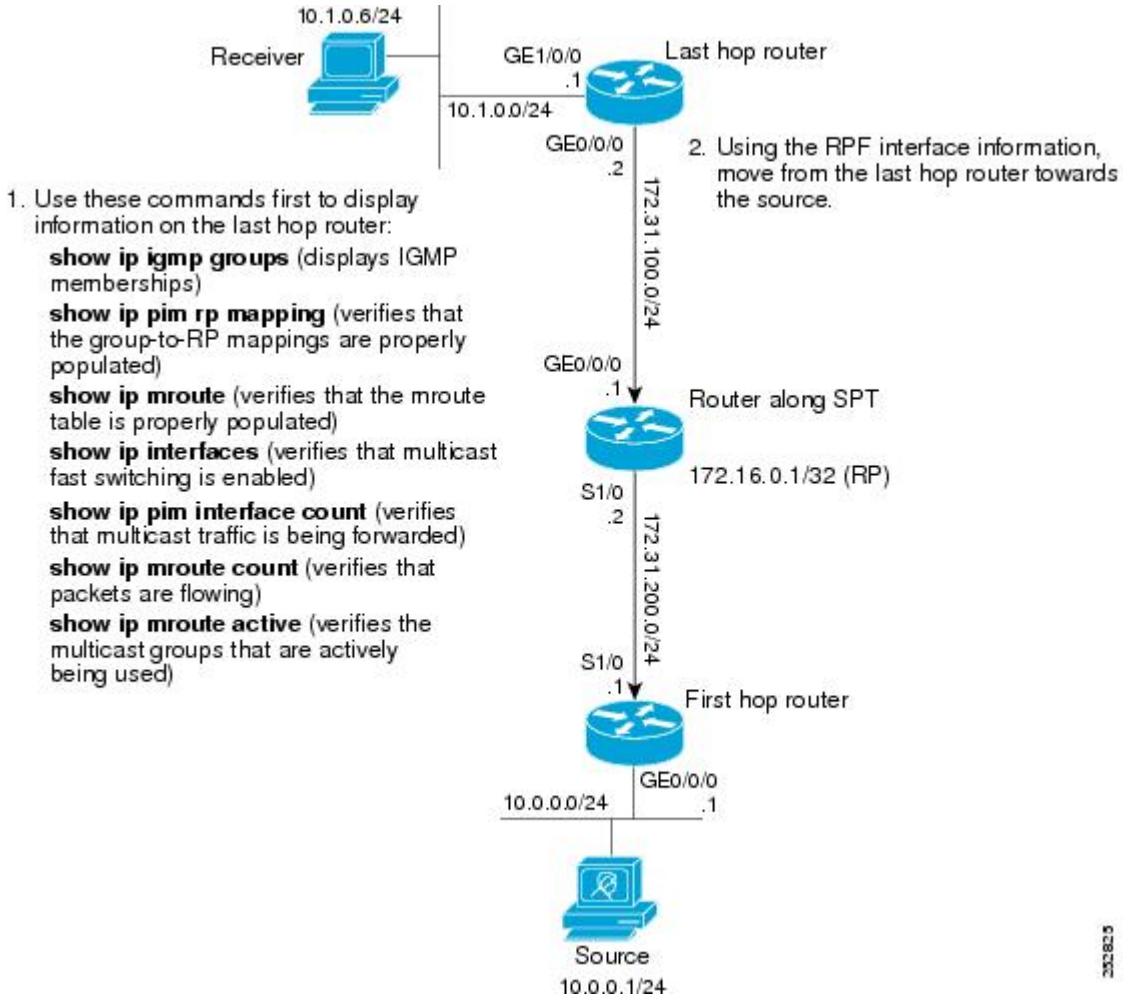
Configuration Examples for Verifying IP Multicast Operation

- Verifying IP Multicast Operation in a PIM-SM or PIM-SSM Network Example, page 154

Verifying IP Multicast Operation in a PIM-SM or PIM-SSM Network Example

The following example shows how to verify IP multicast operation after PIM-SM has been deployed in a network. The example is based on the PIM-SM topology illustrated in the figure.

From the last hop router to the first hop router shown in the figure, this example shows how to verify IP multicast operation for this particular PIM-SM network topology.



- Verifying IP Multicast on the Last Hop Router Example, page 154
- Verifying IP Multicast on Routers Along the SPT Example, page 157
- Verifying IP Multicast on the First Hop Router Example, page 157

Verifying IP Multicast on the Last Hop Router Example

The following is sample output from the **show ip igmp groups** command. The sample output displays the IGMP memberships on the last hop router shown in the figure. This command is used in this example to

confirm that the IGMP cache is being properly populated for the groups that receivers on the LAN have joined.

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.1.2.3        GigabitEthernet1/0/0     00:05:14  00:02:14  10.1.0.6
224.0.1.39       GigabitEthernet0/0/0     00:09:11  00:02:08  172.31.100.1
```

The following is sample output from the **show ip pim rp mapping**command. In the sample output, notice the RP address displayed for the RP field. Use the RP address and group information to verify that the group-to-RP mappings have been properly populated on the last hop router shown in the figure.

Note In the output, the "(?)" indicates that the router is unable to resolve an IP address to a hostname.

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 172.16.0.1 (?), v2v1
    Info source: 172.16.0.1 (?), elected via Auto-RP
         Uptime: 00:09:11, expires: 00:02:47
```

The following is sample output from the **show ip mroute** command. This command is used to verify that the mroute table is being properly populated on the last hop router shown in the figure. In the sample output, notice the T flag for the (10.0.0.1, 239.1.2.3) mroute. The T flag indicates that the SPT-bit has been set, which means a multicast packet was received on the SPT tree for this particular mroute. In addition, the RPF nbr field should point toward the RPF neighbor with the highest IP address determined by unicast routing toward the multicast source.

```
Router# show ip mroute
(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04

(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04

(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00
```

The following is sample output from the **show ip interface** command for the incoming interface. This command is used in this example to confirm that IP multicast fast switching is enabled on the last hop router shown in the figure. When IP multicast fast switching is enabled, the line "IP multicast fast switching is enabled" displays in the output.

```
Router# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 172.31.100.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13
      224.0.0.5 224.0.0.6
  Outgoing access list is not set
```

```
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following is sample output from the **show ip pim interface count** command. This command is used in this example to confirm that multicast traffic is being forwarded to the last hop router shown in the figure. In the sample output, notice the Mpackets In/Out field. This field displays the number of multicast packets received by and sent on each interface listed in the output.

```
Router# show ip pim interface count

State: * - Fast Switched, D - Distributed Fast Switched
       H - Hardware Switching Enabled
Address          Interface                FS Mpackets In/Out
172.31.100.2     GigabitEthernet0/0/0     *   4122/0
10.1.0.1         GigabitEthernet1/0/0     *   0/3193
```

The following is sample output from the **show ip mroute**command with the **count** keyword. This command is used on the last hop router shown in the figure to verify the packets being sent to groups from active sources. In the sample output, notice the packet count displayed for the Forwarding field. This field displays the packet forwarding count for sources sending to groups.

```
Router# show ip mroute count
IP Multicast Statistics
6 routes using 4008 bytes of memory
3 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0

Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120
  Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99

Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10
  Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0
```

The following is sample output from the **show ip mroute**command with the **active** keyword. This command is used on the last hop router shown in the figure to confirm the multicast groups with active sources on the last hop router.

Note In the output, the "(?)" indicates that the router is unable to resolve an IP address to a hostname.

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)
```

Verifying IP Multicast on Routers Along the SPT Example

The following is sample output from the **show ip mroute**for a particular group. This command is used in this example to verify that the RPF neighbor toward the source is the expected RPF neighbor for the router along the SPT shown in the figure.

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:17:56/00:03:02

(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T
  Incoming interface: Serial1/0, RPF nbr 172.31.200.1
  Outgoing interface list:
```

Ethernet0/0, Forward/Sparse-Dense, 00:15:34/00:03:02

The following is sample output from the **show ip mroute** command with the **active** keyword from the router along the SPT shown in the figure. This command is used to confirm the multicast groups with active sources on this router.

Note In the output, the "(?)" indicates that the router is unable to resolve an IP address to a hostname.

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

Verifying IP Multicast on the First Hop Router Example

The following is sample output from the **show ip mroute**for a particular group. This command is used in this example to verify the packets being sent to groups from active sources on the first hop router shown in the figure. In the sample output, notice the packet count displayed for the Forwarding field. This field displays the packet forwarding count for sources sending to groups on the first hop router.

Note The RPF nbr 0.0.0.0 field indicates that the source of an mroute has been reached.

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF
  Incoming interface: Serial1/0, RPF nbr 172.31.200.2
  Outgoing interface list: Null
```

```
(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/0/0, Forward/Sparse-Dense, 00:18:10/00:03:19
```

The following is sample output from the **show ip mroute** command with the **active** keyword from the first hop router shown in the figure:

Note In the output, the "(?)" indicates that the router is unable to resolve an IP address to a host name.

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

Additional References

Related Documents

Related Topic	Document Title
Overview of the IP multicast technology area	" IP Multicast Technology Overview " module
PIM-SM and SSM concepts and configuration examples	" Configuring Basic IP Multicast " module
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Verifying IP Multicast Operation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10 Feature Information for Verifying IP Multicast Operation

Feature Name	Releases	Feature Information
This table is intentionally left blank because no features were introduced or modified in this module since Cisco IOS XE Release 2(1). This table will be updated when feature information is added to this module.	--	--

Monitoring and Maintaining IP Multicast

This module describes many ways to monitor and maintain an IP multicast network, such as

- displaying which neighboring multicast routers are peering with the local router
- displaying multicast packet rates and loss information
- tracing the path from a source to a destination branch for a multicast distribution tree
- displaying the contents of the IP multicast routing table, information about interfaces configured for PIM, the PIM neighbors discovered by the router, and contents of the IP fast-switching cache
- clearing caches, tables, and databases
- monitoring the delivery of IP multicast packets and being alerted if the delivery fails to meet certain parameters (IP multicast heartbeat)
- using session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and communicating the relevant session setup information to prospective participants (SAP listener support)
- storing IP multicast packet headers in a cache and displaying them to find out information such as who is sending IP multicast packets to what groups and any multicast forwarding loops in your network
- using managed objects to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP)
- disabling fast switching of IP multicast in order to log debug messages

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Monitoring and Maintaining IP Multicast

- Before performing the tasks in this module, you should be familiar with the concepts described in the "IP Multicast Technology Overview" module.
- You must also have enabled IP multicast and have Protocol Independent Multicast (PIM) configured and running on your network. Refer to the "Configuring Basic IP Multicast" module.

Information About Monitoring and Maintaining IP Multicast

IP Multicast Heartbeat

The IP Multicast Heartbeat feature enables you to monitor the delivery of IP multicast packets and to be alerted if the delivery fails to meet certain parameters.

Although you could alternatively use MRM to monitor IP multicast, you can perform the following tasks with IP multicast heartbeat that you cannot perform with MRM:

- Generate an SNMP trap
- Monitor a production multicast stream

When IP multicast heartbeat is enabled, the router monitors IP multicast packets destined for a particular multicast group at a particular interval. If the number of packets observed is less than a configured minimum amount, the router sends an SNMP trap to a specified network management station to indicate a loss of heartbeat exception.

The **ip multicast heartbeat** command does not create a heartbeat if there is no existing multicast forwarding state for *group* in the router. This command will not create a multicast forwarding state in the router. Use the **ip igmp static-group**commandon the router or on a downstream router to force forwarding of IP multicast traffic. Use the **snmp-server host ipmulticast** command to enable the sending of IP multicast traps to specific receiver hosts. Use the **debug ip mhbeat**command to debug the Multicast Heartbeat feature.

Session Announcement Protocol (SAP)

Session Announcement Protocol (SAP) listener support is needed to use session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and to communicate the relevant session setup information to prospective participants.

Sessions are described by the Session Description Protocol (SDP), which is defined in RFC 2327. SDP provides a formatted, textual description of session properties (for example, contact information, session lifetime, and the media) being used in the session (for example, audio, video, and whiteboard) with their specific attributes such as time-to-live (TTL) scope, group address, and User Datagram Protocol (UDP) port number.

Many multimedia applications rely on SDP for session descriptions. However, they may use different methods to disseminate these session descriptions. For example, IP/TV relies on the web to disseminate

session descriptions to participants. In this example, participants must know of a web server that provides the session information.

MBONE applications (for example, vic, vat, and wb) and other applications rely on multicast session information sent throughout the network. In these cases, SAP is used to transport the SDP session announcements. SAP Version 2 uses the well-known session directory multicast group 224.2.127.254 to disseminate SDP session descriptions for global scope sessions and group 239.255.255.255 for administrative scope sessions.

Note The Session Directory (SDR) application is commonly used to send and receive SDP/SAP session announcements.

PIM MIB Extensions for SNMP Traps for IP Multicast

Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the PIM MIB for IPv4, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

PIM MIB extensions introduce the following new classes of PIM notifications:

- neighbor-change--This notification results from the following conditions:
  - A router’s PIM interface is disabled or enabled (using the **ip pim** command in interface configuration mode)
  - A router's PIM neighbor adjacency expires (defined in RFC 2934)
- rp-mapping-change--This notification results from a change in the rendezvous point (RP) mapping information due to either Auto-RP messages or bootstrap router (BSR) messages.
- invalid-pim-message--This notification results from the following conditions:
  - An invalid (*, G) Join or Prune message is received by the device (for example, when a router receives a Join or Prune message for which the RP specified in the packet is not the RP for the multicast group)
  - An invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP)

- Benefits of PIM MIB Extensions, page 163

Benefits of PIM MIB Extensions

PIM MIB extensions:

- Allow users to identify changes in the multicast topology of their network by detecting changes in the RP mapping.
- Provide traps to monitor the PIM protocol on PIM-enabled interfaces.
- Help users identify routing issues when multicast neighbor adjacencies expire on a multicast interface.
- Enable users to monitor RP configuration errors (for example, errors due to flapping in dynamic RP allocation protocols like Auto-RP).

How to Monitor and Maintain IP Multicast

Displaying Multicast Peers Packet Rates and Loss Information and Tracing a Path

Monitor IP multicast routing when you want to know which neighboring multicast routers are peering with the local router, what the multicast packet rates and loss information are, or when you want to trace the path from a source to a destination branch for a multicast distribution tree.

SUMMARY STEPS

1. **enable**
2. **mrinfo** [*host-name* | *host-address*] [*source-address* | *interface*]
3. **mstat** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]
4. **mtrace** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**mrinfo** [*host-name*	*host-address*] [*source-address*	*interface*] **Example:** `Router# mrinfo`	(Optional) Queries which neighboring multicast routers are “peering” with the local router.

	Command or Action	Purpose
Step 3	**mstat** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] **Example:** `Router# mstat allsource`	(Optional) Displays IP multicast packet rate and loss information.
Step 4	**mtrace** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] **Example:** `Router# mtrace allsource`	(Optional) Traces the path from a source to a destination branch for a multicast distribution tree.

Displaying IP Multicast System and Network Statistics

Display IP multicast system statistics to show the contents of the IP multicast routing table, information about interfaces configured for PIM, the PIM neighbors discovered by the router, contents of the IP fast-switching cache, and the contents of the circular cache header buffer.

SUMMARY STEPS

1. **enable**
2. **ping** [*group-name* | *group-address*]
3. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active** *kbps*]
4. **show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**]
5. **show ip pim neighbor** [*type number*]
6. **show ip pim rp** [**mapping** | **metric**] [*rp-address*]
7. **show ip rpf** {*source-address* | *source-name*} [**metric**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**ping** [*group-name* | *group-address*] **Example:** `Router# ping cbone-audio`	(Optional) Sends an ICMP echo request message to a multicast group address or group name.
Step 3	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `Router# show ip mroute cbone-audio`	(Optional) Displays the contents of the IP multicast routing table.
Step 4	**show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**] **Example:** `Router# show ip pim interface gigabitethernet1/0/0 detail`	(Optional) Displays information about interfaces configured for PIM.
Step 5	**show ip pim neighbor** [*type number*] **Example:** `Router# show ip pim neighbor`	(Optional) Lists the PIM neighbors discovered by the router.
Step 6	**show ip pim rp** [**mapping** | **metric**] [*rp-address*] **Example:** `Router# show ip pim rp metric`	(Optional) Displays the RP routers associated with a sparse mode multicast group.
Step 7	**show ip rpf** {*source-address* | *source-name*} [**metric**] **Example:** `Router# show ip rpf 172.16.10.13`	(Optional) Displays how the router is doing RPF (that is, from the unicast routing table, DVMRP routing table, or static mroutes). Also displays the unicast routing metric.

Clearing IP Multicast Routing Table or Caches

Clear IP multicast caches and tables to delete entries from the IP multicast routing table, the Auto-RP cache, the IGMP cache, and the caches of Catalyst switches. When these entries are cleared, the information is refreshed by being relearned, thus eliminating any incorrect entries.

SUMMARY STEPS

1. **enable**
2. **clear ip mroute** {***** | *group-name* [*source-name* | *source-address*] | *group-address* [*source-name* | *source-address*]}
3. **clear ip pim auto-rp** *rp-address*
4. **clear ip igmp group** [*group-name* | *group-address* | *interface-type interface-number*]
5. **clear ip cgmp** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip mroute** {*****	*group-name* [*source-name*	*source-address*]	*group-address* [*source-name*	*source-address*]} **Example:** `Router# clear ip mroute 224.2.205.42 228.3.0.0`	(Optional) Deletes entries from the IP multicast routing table.
Step 3	**clear ip pim auto-rp** *rp-address* **Example:** `Router# clear ip pim auto-rp 224.5.6.7`	(Optional) Clears the Auto-RP cache.
Step 4	**clear ip igmp group** [*group-name*	*group-address*	*interface-type interface-number*] **Example:** `Router# clear ip igmp group 224.0.255.1`	(Optional) Deletes entries from the IGMP cache.
Step 5	**clear ip cgmp** [*interface-type interface-number*] **Example:** `Router# clear ip cgmp`	(Optional) Clears all group entries from the caches of Catalyst switches.

Monitoring IP Multicast Delivery Using IP Multicast Heartbeat

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing distributed**
4. **snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*[**udp-port** *port*] [*notification-type*]
5. **snmp-server enable traps ipmulticast**
6. **ip multicast heartbeat** *group-address minimum-number window-size interval*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing distributed** **Example:** `Router(config)# ip multicast-routing distributed`	Enables IP multicast routing.
Step 4	**snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*[**udp-port** *port*] [*notification-type*] **Example:** `Router(config)# snmp-server host 224.1.0.1 traps public`	Specifies the recipient of an SNMP notification operation.

	Command or Action	Purpose
Step 5	**snmp-server enable traps ipmulticast** **Example:** `Router(config)# snmp-server enable traps ipmulticast`	Enables the router to send IP multicast traps.
Step 6	**ip multicast heartbeat** *group-address minimum-number window-size interval* **Example:** `Router(config)# ip multicast heartbeat 224.1.1.1 1 1 10`	Enables the monitoring of the IP multicast packet delivery. • The *interval* should be set to a multiple of 10 seconds on platforms that use Multicast Distributed Fast Switching (MDFS) because on those platforms, the packet counters are only updated once every 10 seconds. Other platforms may have other increments.

Advertising Multicast Multimedia Sessions Using SAP Listener

Enable SAP listener support when you want to use session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and to communicate the relevant session setup information to prospective participants.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sap cache-timeout** *minutes*
4. **interface** *type number*
5. **ip sap listen**
6. **end**
7. **clear ip sap** [*group-address* | **“** *session-name* **”**]
8. **show ip sap** [*group-address* | **“** *session-name* **”**| **detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sap cache-timeout** *minutes* **Example:** `Router(config)# ip sap cache-timeout 600`	(Optional) Limits how long a SAP cache entry stays active in the cache. • By default, SAP cache entries are deleted 24 hours after they are received from the network.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
Step 5	**ip sap listen** **Example:** `Router(config-if)# ip sap listen`	Enables the Cisco IOS XE software to listen to session directory announcements.
Step 6	**end** **Example:** `Router(config-if)# end`	Ends the session and returns to EXEC mode.
Step 7	**clear ip sap** [*group-address* | **"** *session-name* **"**] **Example:** `Router# clear ip sap "Sample Session"`	Deletes a SAP cache entry or the entire SAP cache.
Step 8	**show ip sap** [*group-address* | **"** *session-name* **"**| **detail**] **Example:** `Router# show ip sap 224.2.197.250 detail`	(Optional) Displays the SAP cache.

Disabling Fast Switching of IP Multicast

Disable fast switching if you want to log debug messages, because when fast switching is enabled, debug messages are not logged.

You might also want to disable fast switching, which places the router in process switching, if packets are not reaching their destinations. If fast switching is disabled and packets are reaching their destinations, then switching may be the cause.

Fast switching of IP multicast packets is enabled by default on all interfaces (including generic routing encapsulation [GRE] and DVMRP tunnels), with one exception: It is disabled and not supported over X.25 encapsulated interfaces. The following are properties of fast switching:

- If fast switching is disabled on an *incoming* interface for a multicast routing table entry, the packet is sent at process level for all interfaces in the outgoing interface list.
- If fast switching is disabled on an *outgoing* interface for a multicast routing table entry, the packet is process-level switched for that interface, but may be fast switched for other interfaces in the outgoing interface list.
- When fast switching is enabled, debug messages are not logged.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip mroute-cache**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Specifies an interface.
Step 4	**no ip mroute-cache** **Example:** `Router(config-if)# no ip mroute-cache`	Disables fast switching of IP multicast.

Enabling PIM MIB Extensions for IP Multicast

Perform this task to enable PIM MIB extensions for IP multicast.

Note The following MIB tables are not supported in Cisco IOS and Cisco IOS XE software:

- pimIpMRouteTable
- pimIpMRouteNextHopTable
- The pimInterfaceVersion object was removed from RFC 2934 and, therefore, is no longer supported in software.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]
4. **snmp-server host** *host-address* [**traps** | **informs**] *community-string* **pim**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**snmp-server enable traps pim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**] **Example:** `Router(config)# snmp-server enable traps pim neighbor-change`	Enables a router to send PIM notifications. • **neighbor-change** --This keyword enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires. • **rp-mapping-change** --This keyword enables notifications indicating a change in RP mapping information due to either Auto-RP messages or BSR messages. • **invalid-pim-message** --This keyword enables notifications for monitoring invalid PIM protocol operations (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group or when a router receives a register message from a multicast group for which it is not the RP).
Step 4	**snmp-server host** *host-address* [**traps** | **informs**] *community-string* **pim** **Example:** `Router(config)# snmp-server host 10.10.10.10 traps public pim`	Specifies the recipient of a PIM SNMP notification operation.

Configuration Examples for Monitoring and Maintaining IP Multicast

Displaying IP Multicast System and Network Statistics Example

The following is sample output from the **mrinfo** command:

```
Router# mrinfo

192.31.7.37 (labs-allcompany) [version cisco 12.3] [flags: PMSA]:
192.31.7.37 -> 192.31.7.34 (lab-southwest) [1/0/pim]
192.31.7.37 -> 192.31.7.47 (lab-northwest) [1/0/pim]
192.31.7.37 -> 192.31.7.44 (lab-southeast) [1/0/pim]
131.119.26.10 -> 131.119.26.9 (lab-northeast) [1/32/pim]
```

The following is sample output from the **mstat** command in user EXEC mode:

```
Router> mstat labs-in-china 172.16.0.1 224.0.255.255
```

```
Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 224.0.255.255
>From source (labs-in-china) to destination (labs-in-africa)
Waiting to accumulate statistics......
Results after 10 seconds:
Source Response Dest Packet Statistics For Only For Traffic
172.16.0.0      172.16.0.10 All Multicast Traffic From 172.16.0.0
| __/ rtt 48 ms Lost/Sent = Pct Rate To 224.0.255.255
v / hop 48 ms ---------------------- --------------------
172.16.0.1      labs-in-england
| ^ ttl 1
v | hop 31 ms 0/12 = 0% 1 pps 0/1 = --% 0 pps
172.16.0.2
172.16.0.3      infolabs.com
| ^ ttl 2
v | hop -17 ms -735/12 = --% 1 pps 0/1 = --% 0 pps
172.16.0.4
172.16.0.5      infolabs2.com
| ^ ttl 3
v | hop -21 ms -678/23 = --% 2 pps 0/1 = --% 0 pps
172.16.0.6
172.16.0.7      infolabs3.com
| ^ ttl 4
v | hop 5 ms 605/639 = 95% 63 pps 1/1 = --% 0 pps
172.16.0.8
172.16.0.9      infolabs.cisco.com
| \__ ttl 5
v \ hop 0 ms 4 0 pps 0 0 pps
172.16.0.0      172.16.0.10
Receiver Query Source
```

The following is sample output from the **mtrace** command in user EXEC mode:

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254
Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
0 172.16.0.10
-1 172.16.0.8 PIM thresh^ 0 0 ms
-2 172.16.0.6 PIM thresh^ 0 2 ms
-3 172.16.0.5 PIM thresh^ 0 894 ms
-4 172.16.0.3 PIM thresh^ 0 893 ms
-5 172.16.0.2 PIM thresh^ 0 894 ms
-6 172.16.0.1 PIM thresh^ 0 893 ms
```

Monitoring IP Multicast Delivery Using IP Multicast Heartbeat Example

The following example shows how to monitor IP multicast packets forwarded through this router to group address 244.1.1.1. If no packet for this group is received in a 10-second interval, an SNMP trap will be sent to the SNMP management station with the IP address of 224.1.0.1.

```
!
ip multicast-routing
!
snmp-server host 224.1.0.1 traps public
snmp-server enable traps ipmulticast
ip multicast heartbeat 224.1.1.1 1 1 10
```

Advertising Multicast Multimedia Sessions Using SAP Listener Example

The following example enables a router to listen to session directory announcements and changes the SAP cache timeout to 30 minutes.

```
ip multicast routing
```

```
ip sap cache-timeout 30
interface loopback 0
 ip address 10.0.0.51 255.255.255.0
 ip pim sparse-dense mode
 ip sap listen
```

The following is sample output from the **show ip sap** command for a session using multicast group 224.2.197.250:

```
Router# show ip sap 224.2.197.250
SAP Cache - 198 entries
Session Name: Session1
   Description: This broadcast is brought to you courtesy of Name1.
   Group: 0.0.0.0, ttl: 0, Contiguous allocation: 1
   Lifetime: from 10:00:00 PDT Jul 4 1999 until 10:00:00 PDT Aug 1 1999
   Uptime: 4d05h, Last Heard: 00:01:40
   Announcement source: 128.102.84.134
   Created by: sample 3136541828 3139561476 IN IP4 128.102.84.134
   Phone number: Sample Digital Video Lab (555) 555-5555
   Email: email1 <name@email.com>
   URL: http://url.com/
   Media: audio 20890 RTP/AVP 0
     Media group: 224.2.197.250, ttl: 127
     Attribute: ptime:40
   Media: video 62806 RTP/AVP 31
     Media group: 224.2.190.243, ttl: 127
```

Displaying IP Multicast System and Network Statistics Example

show ip mroute

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    GigabitEthernet0, Forward/Sparse, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    GigabitEthernet0, Forward/Sparse, 5:29:15/0:02:57
```

show ip pim interface

The following is sample output from the **show ip pim interface** command when an interface is specified:

```
Router# show ip pim interface GigabitEthernet1/0/0

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.16.1.4       GigabitEthernet1/0/0     v2/S   1      100 ms 1      172.16.1.4
```

The following is sample output from the **show ip pim rp** command:

```
Router# show ip pim rp
```

```
Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
```

show ip pim rp

The following is sample output from the **show ip pim rp** command when the **mapping** keyword is specified:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?), v2v1, bidir
    Info source:10.10.0.2 (?), via Auto-RP
         Uptime:00:01:42, expires:00:00:32
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?), v2v1, bidir
    Info source:10.10.0.3 (?), via Auto-RP
         Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
Group(s) (-)230.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
```

The following is sample output from the **show ip pim rp** command when the **metric** keyword is specified:

```
Router# show ip pim rp metric

RP Address      Metric Pref    Metric       Flags   RPF Type   Interface
10.10.0.2       0              0              L     unicast    Loopback0
10.10.0.3       90             409600         L     unicast    GigabitEthernet3/3/0
10.10.0.5       90             435200         L     unicast    GigabitEthernet3/3/0
```

show ip rpf

The following is sample output from the **show ip rpf** command:

```
Router# show ip rpf 172.16.10.13

RPF information for host1 (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: sj1.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

The following is sample output from the **show ip rpf**command when the **metric**keyword is specified:

```
Router# show ip rpf 172.16.10.13 metric
RPF information for host1.cisco.com (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: neighbor.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Metric preference: 110
```

Enabling PIM MIB Extensions for IP Multicast Example

The following example shows how to configure a router to generate notifications indicating that a PIM interface of the router has been enabled. The first line configures PIM traps to be sent as SNMP v2c traps to

the host with IP address 10.0.0.1. The second line configures the router to send the neighbor-change class of trap notification to the host.

```
snmp-server host 10.0.0.1 traps version 2c public pim
snmp-server enable traps pim neighbor-change
interface ethernet0/0
 ip pim sparse-dense-mode
```

Additional References

Related Documents

Related Topic	Document Title
IP multicast SNMP notifications	“ Configuring SNMP Support ” module
IP multicast commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

MIBs

MIB	MIBs Link
• CISCO-IPMROUTE-MIB • MSDP-MIB • IGMP-STD-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2934	*Protocol Independent Multicast for IPv4 MIB*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Monitoring and Maintaining IP Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11 Feature Information for Monitoring and Maintaining IP Multicast

Feature Names	Releases	Feature Configuration Information
PIM MIB Extensions	Cisco IOS XE Release 2.1	Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the PIM for IPv4 MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

Feature Names	Releases	Feature Configuration Information
Multicast Heartbeat	Cisco IOS XE Release 2.1	The IP multicast heartbeat feature provides a way to monitor the status of IP multicast delivery and be informed when the delivery fails (via Simple Network Management Protocol [SNMP] traps).