Multicast VPN—IP Multicast Support for MPLS VPNs

The Multicast VPN—IP Multicast Support for MPLS VPNs feature allows a service provider to configure and support multicast traffic in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment. This feature supports routing and forwarding of multicast packets for each individual VPN routing and forwarding (VRF) instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

Feature Specifications for the Multicast VPN—IP Multicast Support for MPLS VPNs Feature

Feature History	
Release	**Modification**
12.0(23)S	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.0(25)S1	Support was added for Cisco 10000 platforms.
12.0(26)S	Support was added for Cisco 12000 platforms.
12.0(32)SY	Support for Engine 5 cards and multiple generic routing encapsulation (GRE) set actions was added to Cisco IOS Release 12.0(32)SY on the Cisco 12000 platforms.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Multicast VPN—IP Multicast Support for MPLS VPNs

Service providers must have a multicast-enabled core in order to use the Cisco Multicast VPN feature. Refer to the "IP Multicast" part of the Release 12.2 *Cisco IOS IP Configuration Guide* for more information.

Restrictions for Multicast VPN—IP Multicast Support for MPLS VPNs

- If the core multicast routing is using Source Specific Multicast (SSM), then the data and default multicast distribution tree (MDT) groups must be configured within the SSM range of IP addresses by default.
- The update source interface for the Border Gateway Protocol (BGP) peerings must be the same for all BGP peerings configured on the router in order for the default MDT to be configured properly. If you use a loopback address for BGP peering, then Protocol Independent Multicast (PIM) sparse mode must be enabled on the loopback address.
- The **ip mroute-cache** command must be enabled on the loopback interface used as the BGP peering interface in order for distributed multicast switching to function on the platforms that support it. The **no ip mroute-cache** command must *not* be present on these interfaces.
- MPLS multicast does not support multiple BGP peering update sources.
- Data MDTs are not created for VRF PIM dense mode multicast streams because of the flood and prune nature of dense mode multicast flows and the resulting periodic bring-up and tear-down of such data MDTs.
- Multiple BGP update sources are not supported and configuring them can break Multicast VPN RPF checking. The source IP address of the Multicast VPN tunnels is determined by the highest IP address used for the BGP peering update source. If this IP address is not the IP address used as the BGP peering address with the remote provider edge (PE) router, Multicast VPN will not function properly.
- Extranet multicast is not supported. Multicast routes cannot be imported or exported between VRFs.
- Multicast VPNs cannot span multiple BGP autonomous systems.
- Cisco 10000 series and Cisco 12000 series routers do not support bidirectional PIM.

Information About Multicast VPN—IP Multicast Support for MPLS VPNs

To configure the Multicast VPN—IP Multicast Support for MPLS VPNs feature, you must understand the following concepts:

IP Multicast VPNs

The Multicast VPN feature in Cisco IOS software provides the ability to support the multicast feature over a Layer 3 VPN. As enterprises extend the reach of their multicast applications, service providers can accommodate these enterprises over their MPLS core network. IP multicast is used to stream video, voice, and data to an MPLS VPN network core.

A VPN is network connectivity across a shared infrastructure, such as an Internet service provider (ISP). Its function is to provide the same policies and performance as a private network, at a reduced cost of ownership, thus creating many opportunities for cost savings through operations and infrastructure.

Historically, IP in IP generic routing encapsulation (GRE) tunnels was the only way to connect through a service provider network. Although such tunneled networks tend to have scalability issues, they represent the only means of passing IP multicast traffic through a VPN.

MPLS was derived from tag switching and various other vendor methods of IP-switching support enhancements in the scalability and performance of IP-routed networks by combining the intelligence of routing with the high performance of switching. MPLS is now used for VPNs, which is an appropriate combination because MPLS decouples information used for forwarding of the IP packet (the label) from the information carried in the IP header.

A Multicast VPN allows an enterprise to transparently interconnect its private network across the network backbone of a service provider. The use of a Multicast VPN to interconnect an enterprise network in this way does not change the way that enterprise network is administered, nor does it change general enterprise connectivity.

Because MPLS VPNs support only unicast traffic connectivity, deploying the Multicast VPN feature in conjunction with MPLS VPN allows service providers to offer both unicast and multicast connectivity to MPLS VPN customers.

Benefits of IP Multicast VPNs

- Provides a scalable solution to dynamically send information to multiple locations.
- Provides high-speed information delivery.
- Provides connectivity through a shared infrastructure.

IP Multicast Functionality for VRFs

IP multicast features are available for VRFs. These features have the same functionality as they do for non-VRF situations. Many command line interface (CLI) commands have been enhanced through addition of the **vrf** *vrf-name* keyword and attribute to include support for VRFs.

Table 1 provides information about Cisco IOS commands that have been enhanced to provide functionality for VRFs. For additional configuration information about the commands described in Table 1, refer to the "Configuring IP Multicast Routing" chapter in the "IP Multicast" part in the *Cisco IOS IP Configuration Guide*, Release 12.2.

For more information about the following commands, see the "Command Reference" section on page 31.

Table 1 IP Multicast Functionality for VRFs—Configuring IP Multicast Routing

Command	Description
clear ip igmp group	Deletes entries from the Internet Group Management Protocol (IGMP) cache.
clear ip mroute	Deletes entries from the IP multicast routing table.
clear ip pim auto-rp	Deletes entries from the Auto-RP cache.
ip multicast cache-headers	Allocates a circular buffer to store IP multicast packet headers that the router receives.
ip multicast multipath	Enables load splitting of IP multicast traffic across multiple equal-cost paths.
ip multicast-routing	Enables IP multicast routing.
ip pim accept-rp	Configures a router to accept join or prune messages destined for a specified RP and for a specific list of groups.
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim register-rate-limit	Sets a limit on the maximum number of PIM Sparse Mode (PIM-SM) register messages sent per second for each (S, G) routing entry.
ip pim register-source	Configures the IP source address of a register message to an interface address other than the outgoing interface address of the designated router (DR) leading toward the RP.
ip pim rp-announce-filter	Filters incoming Auto-RP announcement messages coming from the RP.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
ip pim send-rp-announce	Uses Auto-RP to configure groups for which the router will act as an RP.
ip pim send-rp-discovery	Configures the router to be an RP mapping agent.
ip pim spt-threshold	Configures when a PIM leaf router should join the shortest path source tree for the specified group.
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh control messages on a PIM router.
show ip igmp groups	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays multicast-related information about an interface.

Table 1 IP Multicast Functionality for VRFs—Configuring IP Multicast Routing (continued)

Command	Description
show ip mcache	Displays the contents of the IP fast-switching cache.
show ip mds interface	Displays Multicast distributed switching (MDS) information for all the interfaces on the line card.
show ip mpacket	Displays the contents of the circular cache-header buffer.
show ip mroute	Displays the contents of the IP multicast routing table.
show ip pim bsr	Displays the bootstrap router (BSR) information.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.
show ip pim rp	Displays active rendezvous points (RPs) that are cached with associated multicast routing entries.
show ip pim rp-hash	Displays which RP is being selected for a specified group.
show ip rpf	Displays how IP multicast routing does Reverse Path Forwarding (RPF).

Table 2 provides information about Cisco IOS commands that have been enhanced to provide functionality for VRFs. For additional configuration information about the commands described in Table 2, refer to the "Configuring Multicast Source Discovery Protocol" chapter in the "IP Multicast" part in the *Cisco IOS IP Configuration Guide*, Release 12.2.

For more information about the following commands, see the "Command Reference" section on page 31.

Table 2 IP Multicast Functionality for VRFs—Configuring Multicast Source Discovery Protocol

Command	Description
clear ip msdp peer	Clears the TCP connection to the specified Multicast Source Discovery Protocol (MSDP) peer.
clear ip msdp sa-cache	Clears MSDP Source-Active (SA) cache entries.
clear ip msdp statistics	Clears statistics counters for one or all of the MSDP peers.
debug ip msdp	Debugs MSDP activity.
debug ip msdp resets	Debugs MSDP peer reset reasons.
ip msdp border	Configures a router that borders a PIM sparse mode region and dense mode region to use MSDP.
ip msdp cache-sa-state	Causes the router to create SA state.
ip msdp default-peer	Defines a default peer from which to accept all MSDP SA messages.
ip msdp description	Adds descriptive text to the configuration for an MSDP peer.
ip msdp filter-sa-request.	Configures the router to send SA request messages to an MSDP peer when a new joiner from a group becomes active.
ip msdp mesh-group	Configures an MSDP peer to be a member of a mesh group.
ip msdp originator-id	Allows an MSDP speaker that originates an SA message to use the IP address of the interface as the RP address in the SA message.
ip msdp peer	Configures an MSDP peer.

Table 2 IP Multicast Functionality for VRFs—Configuring Multicast Source Discovery Protocol

ip msdp redistribute	Configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers.
ip msdp sa-filter in	Configures an incoming filter list for SA messages received from the specified MSDP peer.
ip msdp sa-filter out	Configures an outgoing filter list for SA messages sent to the specified MSDP peer.
ip msdp sa-request	Configures the router to send SA request messages to the MSDP peer when a new joiner from the group becomes active.
ip msdp shutdown	Administratively shuts down a configured MSDP peer.
ip msdp ttl-threshold	Limits which multicast data packets are sent in SA messages to an MSDP peer.
show ip msdp count	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.
show ip msdp peer	Displays detailed information about the MSDP peer.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.
show ip msdp summary	Displays MSDP peer status.

Table 3 provides information about Cisco IOS commands that have been enhanced to provide functionality for VRFs. For more information about the following commands see the "Command Reference" section on page 31.

Table 3 IP Multicast Functionality for VRFs—Other IP Multicast Configurations

Command	Description	Section in "IP Multicast" part of *Cisco IOS IP Configuration Guide,* Release 12.2
ip mroute	Configures a multicast static route (mroute).	"Configuring an IP Multicast Static Route" section in "Configuring IP Multicast Routing" chapter.
ip pim accept-register	Configures a candidate RP router to filter PIM register messages.	"Configuring Source Specific Multicast" chapter
ip pim ssm	Defines the SSM range of IP multicast addresses.	"Configuring Source Specific Multicast" chapter
ip pim bidir-enable	Enables bidir-PIM.	"Configuring Bidirectional PIM" chapter

IP Multicast VPN Routing and Forwarding and Multicast Domains

Multicast VPN introduces multicast routing information to the VPN routing and forwarding table. When a PE router receives multicast data or control packets from a customer-edge (CE) router, forwarding is performed according to the information in the Multicast VRF (MVRF).

A set of Multicast VPN Routing and Forwarding instances that can send multicast traffic to each other constitutes a multicast domain. For example, the multicast domain for a customer that wanted to send certain types of multicast traffic to all global employees would consist of all CE routers associated with that enterprise.

Multicast Distribution Trees

Multicast VPN establishes a static default MDT for each multicast domain. The default MDT defines the path used by PE routers to send multicast data and control messages to every other PE router in the multicast domain.

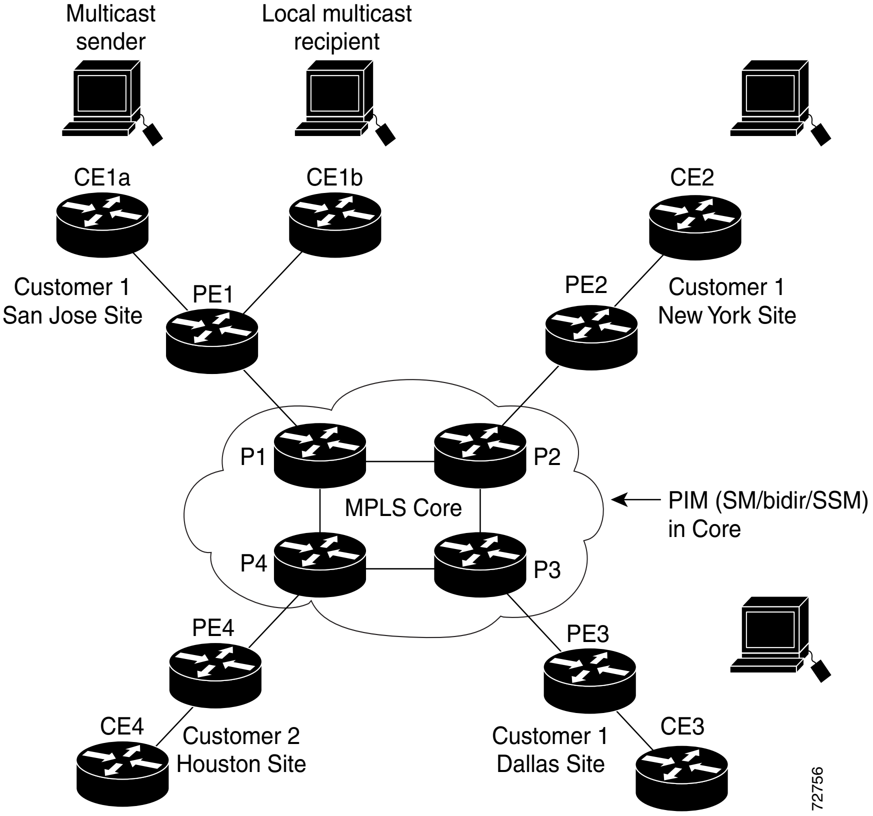
Multicast VPN also supports the dynamic creation of MDTs for high-bandwidth transmission. Data MDTs are a feature unique to Cisco IOS software. Data MDTs are intended for high-bandwidth sources such as full-motion video inside the VPN to ensure optimal traffic forwarding in the MPLS VPN core. The threshold at which the data MDT is created can be configured on a per-router or a per-VRF basis. When the multicast transmission exceeds the defined threshold, the sending PE router creates the data MDT and sends a User Datagram Protocol (UDP) message that contains information about the data MDT to all routers in the default MDT. The statistics to determine whether a multicast stream has exceeded the data MDT threshold are examined once every 10 seconds. If multicast distributed switching is configured, the time period can be up to twice as long.

Data MDTs are created only for (S, G) multicast route entries within the VRF multicast routing table. They are not created for (*, G) entries regardless of the value of the individual source data rate.

In the following example, a service provider has a multicast customer with offices in San Jose, New York, and Dallas. A one-way multicast presentation is occurring in San Jose. The service provider network supports all three sites associated with this customer, in addition to the Houston site of a different enterprise customer.

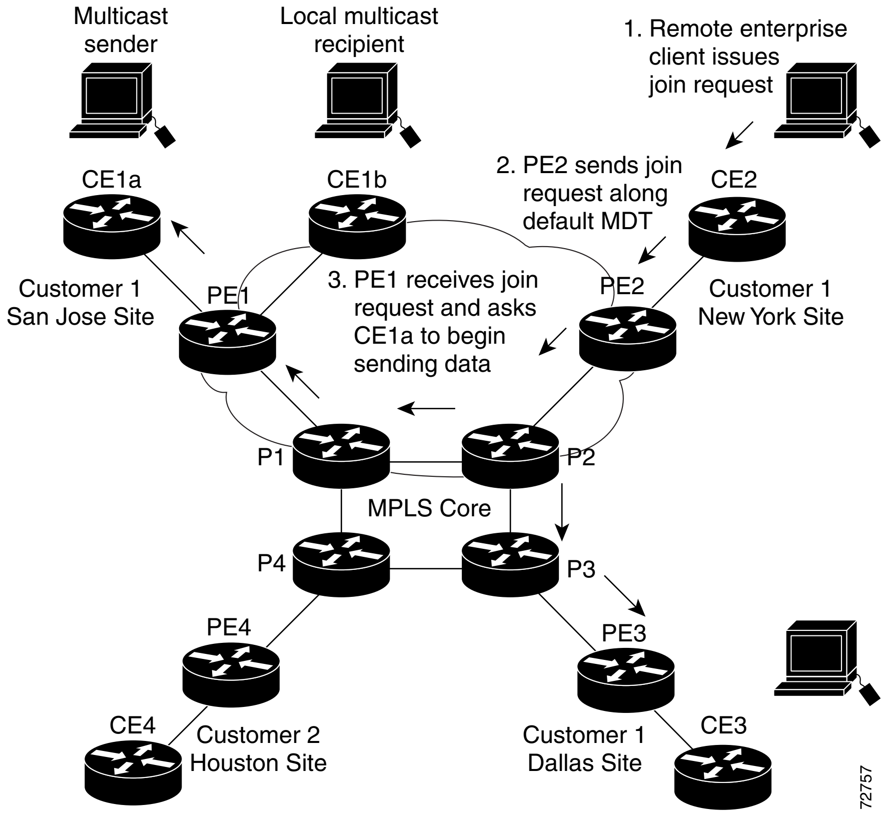
The default MDT for the enterprise customer consists of provider routers P1, P2, and P3 and their associated PE routers. PE4 is not part of the default MDT, because it is associated with a different customer. Figure 1 shows that no data flows along the default MDT, because no one outside of San Jose has joined the multicast.

Figure 1 Default Multicast Distribution Tree Overview



An employee in New York joins the multicast session. The PE router associated with the New York site sends a join request that flows across the default MDT for the multicast domain of the customer whether it is configured to use Sparse Mode, Bidir or SSM within a VRF which contains both the Dallas and the San Jose sites. PE1, the PE router associated with the multicast session source, receives the request. Figure 2 depicts that the PE router forwards the request to the CE router associated with the multicast source (CE1a).

Figure 2 Initializing the Data MDT

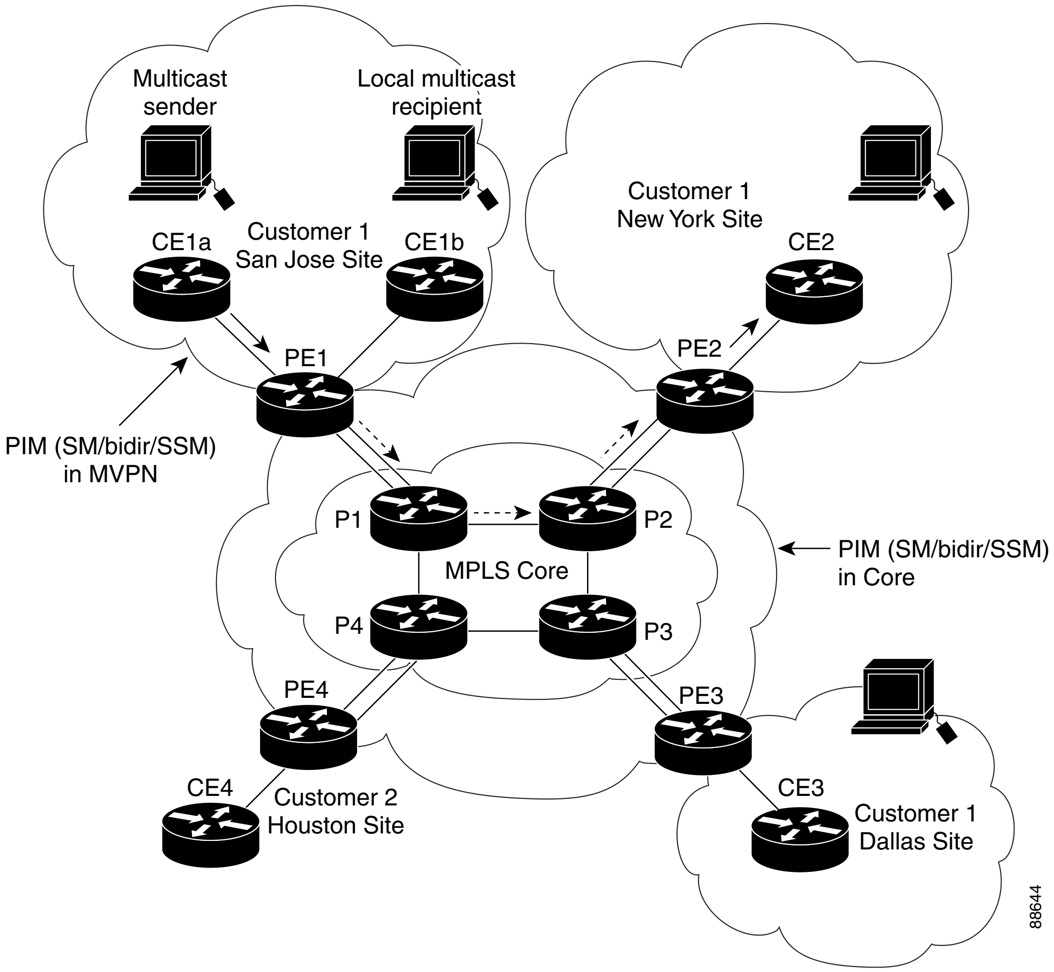

Multicast sender
Local multicast recipient
1. Remote enterprise client issues join request
CE1a
CE1b
2. PE2 sends join request along default MDT
CE2
Customer 1 San Jose Site
PE1
3. PE1 receives join request and asks CE1a to begin sending data
PE2
Customer 1 New York Site
P1
P2
MPLS Core
P4
P3
PE4
PE3
CE4
Customer 2 Houston Site
Customer 1 Dallas Site
CE3
72757

The CE router (CE1a) begins to send the multicast data to the associated PE router (PE1), which sends the multicast data along the default MDT. Immediately after sending the multicast data, PE1 recognizes that the multicast data exceeds the bandwidth threshold at which a data MDT should be created. Therefore, PE1 creates a data MDT, sends a message to all routers using the default MDT that contains information about the data MDT, and, three seconds later, begins sending the multicast data for that particular stream using the data MDT. Only PE2 has interested receivers for this source, so only PE2 will join the data MDT and receive traffic on it.

PE routers maintain a PIM relationship with other PE routers over the default MDT, and a PIM relationship with its directly attached PE routers.

Figure 3 depicts the final flow of multicast data sourced from the multicast sender in San Jose to the multicast client in New York. Multicast data sent from the multicast sender in San Jose is delivered in its original format to its associated PE router (PE1) using either sparse mode, bidir or SSM. PE1 then encapsulates the multicast data and sends it across the data MDT using the configured MDT data groups. The mode used to deliver the multicast data across the data MDT is determined by the service provider and has no direct correlation with the mode used by the customer. The PE router in New York (PE2) receives the data along the data MDT. The PE2 router deencapsulates the packet and forwards it in its original format toward the multicast client using the mode configured by the customer.

Figure 3 Multicast Distribution Tree with VRFs



Multicast Tunnel Interface

For every multicast domain of which an MVRF is a part, the PE router creates a multicast tunnel interface. A multicast tunnel interface is an interface the MVRF uses to access the multicast domain. It can be thought of as a conduit that connects an MVRF and the global MVRF. One tunnel interface is created per multicast VRF.

Multicast Distributed Switching Support

MDS is supported for Multicast VPN on the Cisco 7500 series, Cisco 10000 series, and Cisco 12000 series routers. When MDS is configured, ensure that all interfaces enabled for IP multicast have MDS enabled correctly—verify that no interface has the **no ip mroute-cache** command configured (including loopback interfaces).

Use the following commands to enable MDS for a particular VRF:

- **ip multicast-routing distributed**
- **ip multicast-routing vrf** *vrf-name* **distributed**

How to Configure Multicast VPN—IP Multicast Support for MPLS VPNs

This section contains the following procedures:

Enabling a VPN for Multicast Routing

This task enables a VPN for Multicast Routing.

PIM

PIM can operate in dense mode or sparse mode. It is possible for the router to handle both sparse groups and dense groups at the same time.

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.

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.

Fast-Switching and IP Multicast

Fast switching of IP multicast packets is enabled by default on all interfaces (including GRE and Distance Vector Multicast Routing Protocol [DVMRP] tunnels), with one exception: It is disabled and not supported over X.25 encapsulated interfaces. Note the following 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.

Disable fast switching if you want to log debug messages, because when fast switching is enabled, debug messages are not logged.

Note We recommend that you explicitly enable fast switching if the BGP peering interface (the loopback interface) is a Fast Ethernet interface. If the **no ip mroute-cache** command is configured on the BGP peering interface, fast switching is disabled and distributed multicast switching does not function.

Prerequisites

You must enable PIM sparse mode on the interface that is used for BGP peering. Configure PIM on all interfaces used for IP multicast. We recommend configuring PIM sparse mode on all physical interfaces of PE routers connecting to the backbone. We also recommend configuring PIM sparse mode on all loopback interfaces if they are used for BGP peering or if their IP address is used as an RP address for PIM.

In order to be able to use Auto-RP within a VRF, the interface facing the CE must be configured for PIM sparse-dense mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing vrf** *vrf-name*
4. **interface** *type slot*/*port*
5. **ip pim sparse-mode**

   or

   ip pim sparse-dense-mode
6. **exit**
7. **interface** *type slot*/*port*
8. **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	`ip multicast-routing vrf` *vrf-name* **Example:** `Router(config)# ip multicast-routing vrf vrf1`	Enables IP multicast routing.

	Command or Action	Purpose
Step 4	**interface** *type slot***/***port* **Example:** `Router(config)# interface ethernet1/0`	Selects an interface to configure and enters interface configuration mode.

Step 5	**ip pim sparse-mode**
	or
	ip pim sparse-dense-mode
	Example:
	`Router(config-if)# ip pim sparse-mode`
	or
	Example:
	`Router(config-if)# ip pim sparse-dense-mode`
		Enables PIM sparse mode on the interface.
		or
		Enables PIM sparse-dense mode on the interface

Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	**interface** *type slot***/***port* **Example:** `Router(config)# interface fastethernet 1/0`	(Optional) Selects an interface to configure.
Step 8	**ip-mroute-cache** **Example:** `Router(config-if)# ip-mroute-cache`	(Optional) Enables fast switching of IP multicast.

What to Do Next

Proceed to the section "Configuring an MDT."

Configuring an MDT

This task configures an MDT.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*

6. **mdt default** *group-address*
7. **mdt data** *group-address-range wildcard-bits*
8. **mdt log-reuse**

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 vrf** *vrf-name* **Example:** `Router(config)# ip vrf vrf1`	Enters VRF configuration mode and defines the VPN routing instance by assigning a VRF name.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 55:1111`	(Optional) Creates routing and forwarding tables for a VRF.
Step 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** `Router(config-vrf)# route-target both 55:1111`	(Optional) Creates a route-target extended community for a VRF.
Step 6	**mdt default** *group-address* **Example:** `Router(config-vrf)# mdt default 239.1.1.1`	Configures a default MDT group for a VRF.
Step 7	**mdt data** *group-address-range wildcard-bits* **Example:** `Router(config-vrf)# mdt data 239.1.2.0 0.0.0.3`	(Optional) Configures the multicast group address range for data MDT groups.
Step 8	**mdt log-reuse** **Example:** `Router(config-vrf)# mdt log-reuse`	(Optional) Generates a syslog message when a data MDT has been reused.

What to Do Next

Proceed to the "Configuring the MDT Address Family in BGP for Multicast VPN" task.

Configuring the MDT Address Family in BGP for Multicast VPN

Perform this task to configure an MDT address family session on PE routers to establish MDT peering sessions for MVPN.

The **mdt** keyword has been added to the **address-family ipv4** command to configure an MDT address-family session. MDT address-family sessions are used to pass the source PE address and MDT group address to PIM using Border Gateway Protocol (BGP) MDT Subaddress Family Identifier (SAFI) updates.

BGP Advertisement Methods for Multicast VPN Support

In a single autonomous system, if the default MDT for an MVPN is using PIM sparse mode (PIM-SM) with a rendezvous point (RP), then PIM is able to establish adjacencies over the Multicast Tunnel Interface (MTI) because the source PE and receiver PE discover each other through the RP. In this scenario, the local PE (the source PE) sends register messages to the RP, which then builds a shortest-path tree (SPT) toward the source PE. The remote PE, which acts as a receiver for the MDT multicast group, then sends (*, G) joins toward the RP and joins the distribution tree for that group.

However, if the default MDT group is configured in a PIM Source Specific Multicast (PIM-SSM) environment rather than a PIM-SM environment, the receiver PE needs information about the source PE and the default MDT group. This information is used to send (S, G) joins toward the source PE to build a distribution tree from the source PE (without the need for an RP). The source PE address and default MDT group address are sent using BGP.

Table 4 lists the BGP advertisement methods for sending the source PE address and the default MDT group that are available (by Cisco IOS release).

Table 4 BGP Advertisement Methods for MVPN

Cisco IOS Release	BGP Advertisement Method
• Release 12.0(29)S • Release 12.2(33)SRA1 • Release 12.2(31)SB2 • Release 12.2(33)SXH	Extended Communities
• Release 12.0(29)S and later 12.0S releases • Release 12.2(31)SB2 and later 12.2SB releases • Release 12.2(33)SRA and later 12.2SR releases • Release 12.2(33)SXH and later 12.2SX releases	BGP address family MDT SAFI

BGP Extended Community

When BGP extended communities are used, the PE loopback (source address) information is sent as a VPNv4 prefix using Route Distinguisher (RD) Type 2 (to distinguish it from unicast VPNv4 prefixes). The MDT group address is carried in a BGP extended community. Using a combination of the embedded source in the VPNv4 address and the group in the extended community, PE routers in the same MVRF instance can establish SSM trees to each other.

Note Prior to the introduction of MDT SAFI support, the BGP extended community attribute was used as an interim solution to advertise the IP address of the source PE and default MDT group before IETF standardization. A BGP extended community attribute in an MVPN environment, however, has certain limitations: it cannot be used in inter-AS scenarios (as the attribute is non-transitive), and it uses RD Type 2 (which is not a supported standard).

BGP MDT SAFI

In Cisco IOS Releases that support the MDT SAFI, the source PE address and the MDT group address are passed to PIM using BGP MDT SAFI updates. The RD type has changed to RD type 0 and BGP determines the best path for the MDT updates before passing the information to PIM.

Note To prevent backwards compatibility issues, BGP allows the communication of the older style updates with peers that are unable to understand the MDT SAFI address family.

In Cisco IOS releases that support the MDT SAFI, the MDT SAFI address family needs to be explicitly configured for BGP neighbors using the **address-family ipv4 mdt** command. Neighbors that do not support the MDT SAFI still need to be enabled for the MDT SAFI in the local BGP configuration. Prior to the introduction of the MDT SAFI, additional BGP configuration from the VPNv4 unicast configuration was not needed to support MVPN.

Because the new MDT SAFI does not use BGP route-target extended communities, the regular extended community methods to filter these updates no longer applies. As a result, the **match mdt-group** route-map configuration command has been added to filter on the MDT group address using access control lists (ACLs). These route maps can be applied—inbound or outbound—to the IPv4 MDT address-family neighbor configuration.

Auto-Migration to the MDT SAFI

In Cisco IOS Release 12.0(30)S3, auto-migration to the MDT SAFI functionality was introduced to ease the migration to the MDT SAFI. This functionality was integrated into Cisco IOS Releases 12.2(33)SRA1, 12.2(31)SB2, and 12.2(33)SXH. When migrating a Cisco IOS release to the MDT SAFI, existing VPNv4 neighbors will be automatically configured for the MDT SAFI upon bootup neighbors based on the presence of an existing default MDT configuration (that is, pre-MDT SAFI configurations will be automatically converted to an MDT SAFI configuration upon bootup). In addition, when a default MDT configuration exists and a VPNv4 neighbor in BGP is configured, a similar neighbor in the IPv4 MDT address family will be automatically configured.

Note Because there is no VRF configuration on route reflectors (RRs), auto-migration to the MDT SAFI will not be triggered on RRs. The MDT SAFI configuration, thus, will need to be manually configured on RRs. Having a uniform MDT transmission method will reduce processing time on the routers (as MDT SAFI conversion is not necessary).

Guidelines for Configuring the MDT SAFI

- We recommended that you configure the MDT SAFI on all routers that participate in the MVPN. Even though the benefits of the MDT SAFI are for SSM tree building, the MDT SAFI must also be configured when using MVPN with the default MDT group for PIM-SM. From the multicast point of view, the MDT SAFI is not required for MVPN to work within a PIM-SM core. However, in certain scenarios, the new address family must be configured in order to create the MTI. Without this notification, the MTI would not be created and MVPN would not function (even with PIM-SM).
- For backward compatible sessions, extended communities must be enabled on all MDT SAFI peers. In a pure MDT SAFI environment there is no need to configure extended communities explicitly for MVPN. However, extended communities will be needed for VPNv4 interior BGP (iBGP) sessions to relay the route-target. In a hybrid (MDT SAFI and pre-MDT SAFI) environment, extended communities must be configured to send the embedded source in the VPNv4 address and the MDT group address to MDT SAFI neighbors.

Guidelines for Upgrading a Network to Support the MDT SAFI

When moving from a pre-MDT SAFI to an MDT SAFI environment, upmost care should be taken to minimize the impact to the MVPN service. The unicast service will not be affected, other than the outage due to the reload and recovery. To upgrade a network to support the MDT SAFI, we recommended that you perform the following steps:

1. Upgrade the PEs in the MVPN to a Cisco IOS release that supports the MDT SAFI. Upon bootup, the PE configurations will be auto-migrated to the MDT SAFI. For more information about the auto-migration to the MDT SAFI functionality, see the "Auto-Migration to the MDT SAFI" section.
2. After the PEs have been upgraded, upgrade the RRs and enable the MDT SAFI for all peers providing MVPN service. Enabling or disabling the MDT SAFI will reset the BGP peer relationship for all address families; thus, a loss of routing information may occur.

Note In the case of a multihomed BGP RR scenario, one of the RRs must be upgraded and configured last. The upgraded PEs will use this RR to relay MDT advertisements while the other RRs are being upgraded.

Supported Policy

The following policy configuration parameters are supported under the MDT SAFI:

- Mandatory attributes and well-known attributes, such as the AS-path, multi-exit discriminator MED, BGP local-pref, and next hop attributes.
- Standard communities, community lists, and route maps.

Prerequisites

Before MVPN peering can be established through an MDT address family, MPLS and Cisco Express Forwarding (CEF) must be configured in the BGP network and multiprotocol BGP on PE routers that provide VPN services to CE routers.

Restrictions

The following policy configuration parameters are not supported:

- Route-originator attribute
- Network Layer Reachability Information (NLRI) prefix filtering (prefix lists, distribute lists)
- Extended community attributes (route target and site of origin)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4 mdt**
5. **neighbor** *neighbor-address* **activate**
6. **neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**]
7. **exit**
8. **address-family vpnv4**
9. **neighbor** *neighbor-address* **activate**
10. **neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**]
11. **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	**`router bgp`** *`as-number`*
	Example:
	`Router(config)# router bgp 65535`
		Enters router configuration mode and creates a BGP routing process.

	Command or Action	Purpose
Step 4	**address-family ipv4 mdt** **Example:** `Router(config-router)# address-family ipv4 mdt`	Enters address family configuration to create an IP MDT address family session.
Step 5	**neighbor** *neighbor-address* **activate** **Example:** `Router(config-router-af)# neighbor 192.168.1.1 activate`	Enables the MDT address family for this neighbor.
Step 6	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] **Example:** `Router(config-router-af)# neighbor 192.168.1.1 send-community extended`	Enables community and (or) extended community exchange with the specified neighbor.
Step 7	**exit** **Example:** `Router(config-router-af)# exit`	Exits address family configuration mode and returns to router configuration mode.
Step 8	**address-family vpnv4** **Example:** `Router(config-router)# address-family vpnv4`	Enters address family configuration mode to create a VPNv4 address family session.
Step 9	**neighbor** *neighbor-address* **activate** **Example:** `Router(config-router-af)# neighbor 192.168.1.1 activate`	Enables the VPNv4 address family for this neighbor.
Step 10	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] **Example:** `Router(config-router-af)# neighbor 192.168.1.1 send-community extended`	Enables community and (or) extended community exchange with the specified neighbor.

Step 11	**end**
	Example:
	`Router(config-router-af)# end`
		Exits address-family configuration mode and enters privileged EXEC mode.

What to Do Next

Proceed to the optional "Customizing IP Multicast VPN" task or the optional "Verifying IP Multicast VPN" task.

Customizing IP Multicast VPN

This task configures additional, optional tasks for IP multicast VPN.

Register Messages

Register messages are unicast messages sent by the DR to the RP router when a multicast packet needs to be sent on a rendezvous point tree (RPT). By default, the IP source address of the register message is set to the address of the outgoing interface of the DR leading toward the RP. To configure the IP source address of a register message to an interface address other than the outgoing interface address of the DR leading toward the RP, use the **ip pim register-source** command in global configuration mode. The optional **vrf** *vrf-name* keyword and argument combination has been added to the **ip pim register-source** command to define the VPN routing instance by assigning a VRF name.

IP Multicast Headers Storage

You can store IP multicast packet headers in a cache and then display them to determine any of the following information:

- Who is sending IP multicast packets to what groups
- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- UDP port numbers
- Packet length

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** command in global configuration mode.

Note You should allocate a circular buffer to store IP multicast packet headers for diagnostic purposes only. Configuring the circular buffer can have a performance impact.

The optional **vrf** *vrf-name* keyword and argument combination has been added to the **ip multicast cache-header** command to define the VPN routing instance by assigning a VRF name.

MSDP Peers

MSDP is a mechanism to connect multiple PIM sparse mode (PIM-SM) domains. MSDP allows multicast sources for a group to be known to all 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.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM.

MSDP is also used to announce sources sending to a group. These announcements must originate at the RP of the domain.

MSDP depends heavily on BGP or multiprotocol BGP (MBGP) for interdomain operation. We recommend that you run MSDP in RPs in your domain that are RPs for sources sending to global groups to be announced to the Internet.

For more information about configuring MSDP, refer to the section "Configuring Multicast Source Discover Protocol" in the "IP Multicast" part of the *Cisco IOS IP Configuration Guide*, Release 12.2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip pim** [**vrf** *vrf-name*] **register-source** *type interface-number*
4. **ip multicast** [**vrf** *vrf-name*] **cache-headers** [**rtp**]
5. **ip msdp** [**vrf** *vrf-name*] **peer** {*peer-name* | *peer-address*} [**connect-source** *type number*] [**remote-as** *as-number*]
6. **ip multicast route-limit** *limit* [*threshold*]
7. **ip multicast mrinfo-filter** *acl*

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 pim** [**vrf** *vrf-name*] **register-source** *type interface-number* **Example:** `Router(config)# ip pim vrf vrf1 register-source ethernet 1/0/1`	(Optional) Configures the IP source address of a register message.
Step 4	**ip multicast** [**vrf** *vrf-name*] **cache-headers** [**rtp**] **Example:** `Router(config)# ip multicast vrf vrf1 cache-headers rtp`	(Optional) Allocates a circular buffer to store IP multicast packet headers that the router receives.

	Command or Action	Purpose

Step 5	**`ip msdp`** `[`**`vrf`** *`vrf-name`*`]` **`peer`** `{`*`peer-name`* `|` *`peer-address`*`}` `[`**`connect-source`** *`type number`*`]` `[`**`remote-as`** *`as-number`*`]`
	Example:
	`Router(config)# ip msdp vrf vrf1 peer 10.10.0.1 connect-source ethernet 1/0/1`
		(Optional) Configures an MSDP peer.

Step 6	**`ip multicast route-limit`** *`limit`* `[`*`threshold`*`]`
	Example:
	`Router(config)# ip multicast route-limit 20000 20000`
		(Optional) Sets the multicast static route (mroute) limit and the threshold parameters.

Step 7	**`ip multicast mrinfo-filter`** *`acl`*
	Example:
	`Router(config)# ip multicast mrinfo-filter 4`
		(Optional) Filters the multicast router information request packets for all sources specified in the access list.

What to Do Next

Proceed to the "Verifying IP Multicast VPN" task.

Verifying IP Multicast VPN

The following task verifies the IP multicast VPN configuration, including information about the MSDP peer and MDT default and data groups.

SUMMARY STEPS

1. **enable**
2. **show ip msdp** [**vrf** *vrf-name*] **peer** [*peer-address* | *peer-name*]
3. **show ip msdp** [**vrf** *vrf-name*] **summary**
4. **show ip pim** [**vrf** *vrf-name*] **mdt bgp**
5. **show ip pim** [**vrf** *vrf-name*] **mdt receive** [**detail**]
6. **show ip pim** [**vrf** *vrf-name*] **mdt send**
7. **show ip pim** [**vrf** *vrf-name*] **mdt history** *interval* [*number*]
8. **execute-on slot** *slot-number* **show ip mds mgid-table**
9. **execute-on slot** *slot-number* **show ip hardware-mdfs mgid** *mgid-number* {**both-tables** | **encap-string** | **path-bits**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip msdp** [**vrf** *vrf-name*] **peer** [*peer-address* | *peer-name*] **Example:** `Router# show ip msdp vrf vrf1 peer 224.135.250.116`	(Optional) Displays detailed information about the MSDP peer.
Step 3	**show ip msdp** [**vrf** *vrf-name*] **summary** **Example:** `Router# show ip msdp vrf vrf1 summary`	(Optional) Displays MSDP peer status.
Step 4	**show ip pim** [**vrf** *vrf-name*] **mdt bgp** **Example:** `Router# show ip pim vrf vrf1 mdt bgp`	(Optional) Displays detailed BGP advertisement of the RD for the MDT default group.
Step 5	**show ip pim** [**vrf** *vrf-name*] **mdt receive** [**detail**] **Example:** `Router# show ip pim vrf vrf1 mdt receive`	(Optional) Displays the MDT advertisements received by a specified router.
Step 6	**show ip pim** [**vrf** *vrf-name*] **mdt send** **Example:** `Router# show ip pim vrf vrf1 mdt send`	(Optional) Displays the MDT advertisements that a specified router has made.
Step 7	**show ip pim** [**vrf** *vrf-name*] **mdt history** *interval* [*number*] **Example:** `Router# show ip pim vrf vrf1 mdt history interval 20`	(Optional) Displays information on data MDTs that have been reused.

	Command or Action	Purpose
Step 8	**execute-on slot** *slot-number* **show ip mds mgid-table** **Example:** `Router# execute-on slot 3 show ip mds mgid-table`	(Optional) Displays the information stored in the multicast group ID (MGID) mapping table of a line card. **Note** This command is available only on Cisco 12000 series routers.

Step 9	**execute-on slot** *slot-number* **show ip hardware-mdfs mgid** *mgid-number* {**both-tables** | **encap-string** | **path-bits**}
	Example:
	`Router# execute-on slot 3 show ip hardware-mdfs mgid 125 both-tables`
		(Optional) Displays the mapping between an MGID and the information stored in the line card hardware memory.
		Note This command is available only on Cisco 12000 series routers.

Examples

This section provides the following output examples:

- Sample Output for the show ip msdp peer Command
- Sample Output for the show ip msdp summary Command
- Sample Output for the show ip pim mdt bgp Command
- Sample Output for the show ip pim mdt receive detail Command
- Sample Output for the show ip pim mdt send Command
- Sample Output for the show ip pim mdt history Command
- Sample Output for the show ip hardware-mdfs mgid Command
- Sample Output for the show ip mds mgid-table Command

Sample Output for the show ip msdp peer Command

In the following example, detailed information about MSDP peer for VRF v252 is displayed:

```
Router# show ip msdp vrf v252 peer

MSDP Peer 10.109.3.1 (?), AS ?
Description:
  Connection status:
    State:Up, Resets:0, Connection source:FastEthernet2/0.252
(10.115.3.1)
    Uptime(Downtime):00:00:42, Messages sent/received:1/2
    Output messages discarded:0
    Connection and counters cleared 00:01:00 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
    Sending SA-Requests to peer:disabled
  Peer ttl threshold:0
  SAs learned from this peer:0
  Input queue size:0, Output queue size:0
```

Sample Output for the show ip msdp summary Command

In the following example, summary information about MSDP peer for VRF v252 is displayed:

```
Router# show ip msdp vrf v252 summary

MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
10.109.3.1       ?     Up       00:01:38 0     0     ?
```

Sample Output for the show ip pim mdt bgp Command

In the following example, information about the BGP advertisement of the route distinguisher (RD) for the MDT default group is displayed:

```
Router# show ip pim mdt bgp

MDT-default group 232.2.1.4
 rid:1.1.1.1 next_hop:1.1.1.1
```

Sample Output for the show ip pim mdt receive detail Command

In the following example, detailed information about the data MDT advertisements received by a specified router is displayed:

```
Router# show ip pim vrf vpn8 mdt receive detail

Joined MDT-data groups for VRF:vpn8
group:232.2.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

Sample Output for the show ip pim mdt send Command

In the following example, the MDT advertisements that a specified router has made are displayed:

```
Router# show ip pim mdt send

MDT-data send list for VRF:vpn8
  (source, group)                     MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)            232.2.8.0           1
  (10.100.8.10, 225.1.8.2)            232.2.8.1           1
  (10.100.8.10, 225.1.8.3)            232.2.8.2           1
  (10.100.8.10, 225.1.8.4)            232.2.8.3           1
  (10.100.8.10, 225.1.8.5)            232.2.8.4           1
  (10.100.8.10, 225.1.8.6)            232.2.8.5           1
  (10.100.8.10, 225.1.8.7)            232.2.8.6           1
  (10.100.8.10, 225.1.8.8)            232.2.8.7           1
  (10.100.8.10, 225.1.8.9)            232.2.8.8           1
  (10.100.8.10, 225.1.8.10)           232.2.8.9           1
```

Sample Output for the show ip pim mdt history Command

In the following example, the data MDTs that have been reused during the past configured interval of 20 minutes are displayed:

```
Router# show ip pim vrf vrf1 mdt history interval 20

   MDT-data send history for VRF - vrf1 for the past 20 minutes

MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

Sample Output for the show ip hardware-mdfs mgid Command

The following is sample output from the **show ip hardware-mdfs mgid** command for a line card in slot 2:

```
Router# execute-on slot 2 show ip hardware-mdfs mgid 125 both-tables

========= Line Card (Slot 2) =========
  0x7D:vrf tbl base=0x20030C00, vrfx=y vrf0=n
  0x7D:encap = 00066830000000007819A0C0000000000000007D00000002
```

Sample Output for the show ip mds mgid-table Command

The following is sample output from the **show ip mds mgid-table** command executed on the line card in slot 2:

```
Router# execute-on slot 2 show ip mds mgid-table

========= Line Card (Slot 2) =========

MDFS MGID Table Entries

 MGID    ID  VRFx VRF0 Encap String
 ------- --- ---- ---- ------------
 0x0007C 1   Y    N    45000001 00000000 FF2F0000 02020204 E8000001 00000800
 0x0007D 1   Y    N
 0x0007E 1   Y    N
 0x00080 1   Y    N    42424242 42424242 42424242 42424242 42424242 42424242
```

Configuration Examples for Multicast VPN—IP Multicast Support for MPLS VPNs

This section provides the following configuration examples:

- Enabling a VPN for Multicast Routing Example, page 27
- Configuring the Multicast Group Address Range for Data MDT Groups: Example, page 27
- Configuring the MDT Address Family in BGP for Multicast VPN: Example, page 27
- Configuring the IP Source Address of Register Messages: Example, page 28

- Storing IP Multicast Packet Headers: Example, page 28
- Configuring an MSDP Peer: Example, page 29
- Limiting the Number of Multicast Routes: Example, page 30

Enabling a VPN for Multicast Routing Example

In the following example, multicast routing is enabled for a VPN routing instance named vrf1. Ethernet Interface 1/0/1 is configured for PIM sparse-dense mode and fast switching is explicitly enabled for Fast Ethernet interface1/0/0.

```
ip multicast-routing vrf vrf1
 interface ethernet1/0/1
 ip pim sparse-dense-mode
 exit
interface fastethernet1/0/0
 ip-mroute-cache
```

Configuring the Multicast Group Address Range for Data MDT Groups: Example

In the following example, the VPN routing instance is assigned a VRF name of vrf1. The MDT default group for a VPN VRF is 239.1.1.1, and the multicast group address range for MDT groups is 239.1.2.0 with wildcard bits of 0.0.0.3:

```
ip vrf vrf1
 rd 55:1111
 route-target both 55:1111
 mdt default 239.1.1.1
 mdt data 239.1.2.0 0.0.0.3
 end


Router# show ip vrf vrf1
  Name                             Default RD          Interfaces
  vrf1                             55:1111
```

Configuring the MDT Address Family in BGP for Multicast VPN: Example

In the following example, an MDT address family session is configured on a PE router to establish MDT peering sessions for MVPN.

```
!
ip vrf test
 rd 55:2222
 route-target export 55:2222
 route-target import 55:2222
 mdt default 232.0.0.1
!
ip multicast-routing
ip multicast-routing vrf test
!
router bgp 55
.
.
.
!
 address-family vpnv4
 neighbor 192.168.1.1 activate
 neighbor 192.168.1.1 send-community-both
!
 address-family ipv4 mdt
 neighbor 192.168.1.1 activate
 neighbor 192.168.1.1 send-community-both
!
```

Configuring the IP Source Address of Register Messages: Example

In the following example, the IP source address of the register message is configured to the Ethernet interface 1/0/0 of a DR:

```
ip pim register-source ethernet1/0/1

Router# show running-config | include register

ip pim register-source Ethernet1/0/1
```

Storing IP Multicast Packet Headers: Example

In the following example, a circular buffer is allocated to store IP multicast packet headers that the router receives. The VPN routing instances in this example are named vrf1 and vrf2.

```
ip multicast vrf vrf1 cache-headers
ip multicast vrf vrf2 cache-headers

Router# show running-config

Building configuration...

Current configuration :3552 bytes
!
! Last configuration change at 16:52:30 UTC Fri May 31 2002
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service single-slot-reload-enable
!
hostname Router
!
.
.
.
ip vrf vrf1
 rd 55:111
 route-target export 55:111
 route-target import 55:111
 mdt default 232.1.1.1
!
ip vrf vrf2
 rd 55:112
 route-target export 55:112
 route-target import 55:112
 mdt default 232.2.2.2
!
ip multicast-routing distributed
ip multicast-routing vrf vrf1 distributed
ip multicast-routing vrf vrf2 distributed
ip multicast vrf vrf1 cache-headers
ip multicast vrf vrf2 cache-headers
ip cef distributed
.
.
.
interface Ethernet 1/0/3.1
 encapsulation dot1Q 1 native
 ip vrf forwarding vrf1
 ip address 20.1.1.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 no keepalive
 no cdp enable
!
interface Ethernet 1/0/3.2
 encapsulation dot1Q 2
 ip vrf forwarding vrf2
 ip address 20.1.1.2 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 no keepalive
 no cdp enable
.
.
.
address-family ipv4 vrf vrf2
 redistribute connected
 redistribute static
 redistribute rip metric 50
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vrf1
 redistribute connected
 redistribute static
 redistribute rip metric 50
 no auto-summary
 no synchronization
 exit-address-family
.
.
.
end
```

Configuring an MSDP Peer: Example

In the following example, an MSDP peer is configured with a VPN routing instance named vrf1 and a source of 10.10.0.1 from Ethernet interface 1/0/1:

```
ip msdp vrf vrf1 peer 10.10.0.1 connect-source ethernet 1/0/1
```

Limiting the Number of Multicast Routes: Example

In the following example, the number of multicast routes that can be added in to a multicast routing table is set to 200,000 and the threshold value of the number of mroutes that will cause a warning message to occur is set to 20,000:

```
Router# show running-config

ip multicast-routing distributed
ip multicast-routing vrf cisco distributed
ip multicast cache-headers
ip multicast route-limit 200000 20000
ip multicast vrf cisco route-limit 200000 20000
no mpls traffic-eng auto-bw timers frequency 0
!
.
.
.
```

Where to Go Next

If you want to configure other IP multicast features for a VRF, see the "IP Multicast Functionality for VRFs" section on page 4 for more information.

Additional References

For additional information related to Multicast VPN—IP Multicast Support for MPLS VPNs, see the following sections:

- Related Documents, page 30
- Standards, page 31
- MIBs, page 31
- RFCs, page 31
- Technical Assistance, page 31

Related Documents

Related Topic	Document Title
Cisco IP configuration	*Cisco IOS IP Configuration Guide*, Release 12.2
Cisco IP multicast commands	*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*, Release 12.2
Multicast VPN for MPLS	*Multicast VPN for MPLS*

Standards

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

MIBs

MIBs	MIBs Link
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 IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

- **clear ip igmp group**
- **clear ip mroute**

- **clear ip msdp peer**
- **clear ip msdp sa-cache**
- **clear ip msdp statistics**
- **clear ip pim auto-rp**
- **debug ip igmp**
- **debug ip mcache**
- **debug ip mpacket**
- **debug ip mrouting**
- **debug ip msdp**
- **debug ip msdp resets**
- **debug ip pim**
- **debug ip pim auto-rp**
- **ip mroute**
- **ip msdp border**
- **ip msdp cache-sa-state**
- **ip msdp default-peer**
- **ip msdp description**
- **ip msdp filter-sa-request**
- **ip msdp mesh-group**
- **ip msdp originator-id**
- **ip msdp peer**
- **ip msdp redistribute**
- **ip msdp sa-filter in**
- **ip msdp sa-filter out**
- **ip msdp sa-request**
- **ip msdp shutdown**
- **ip msdp ttl-threshold**
- **ip multicast cache-headers**
- **ip multicast mrinfo-filter**
- **ip multicast multipath**
- **ip multicast route-limit**
- **ip multicast-routing**
- **ip pim accept-register**
- **ip pim accept-rp**
- **ip pim bidir-enable**
- **ip pim bsr-candidate**
- **ip pim register-rate-limit**
- **ip pim register-source**

- ip pim rp-announce-filter
- ip pim rp-candidate
- ip pim send-rp-announce
- ip pim send-rp-discovery
- ip pim spt-threshold
- ip pim ssm
- ip pim state-refresh disable
- mdt data
- mdt default
- mdt log-reuse
- show ip hardware-mdfs mgid
- show ip igmp groups
- show ip igmp interface
- show ip mcache
- show ip mds interface
- show ip mds mgid-table
- show ip mpacket
- show ip mroute
- show ip msdp count
- show ip msdp peer
- show ip msdp sa-cache
- show ip msdp summary
- show ip pim mdt bgp
- show ip pim mdt history
- show ip pim mdt receive
- show ip pim mdt send
- show ip pim bsr
- show ip pim interface
- show ip pim neighbor
- show ip pim rp
- show ip pim rp-hash (BSR)
- show ip rpf

clear ip igmp group

To delete entries from the Internet Group Management Protocol (IGMP) cache, use the **clear ip igmp group** command in EXEC mode.

clear ip igmp [**vrf** *vrf-name*] **group** [*group-name* | *group-address* | *interface-type interface-number*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-name	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the **ip host** command.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
interface-type interface-number	(Optional) Interface type and number.

Defaults

When this command is used with no arguments, all entries are deleted from the IGMP cache.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The IGMP cache contains a list of the multicast groups of which hosts on the directly connected LAN are members. If the router has joined a group, that group is also listed in the cache.

To delete all entries from the IGMP cache, specify the **clear ip igmp group** command with no arguments.

Examples

The following example clears entries for the multicast group 224.0.255.1 from the IGMP cache:

```
Router# clear ip igmp group 224.0.255.1
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays multicast-related information about an interface.

clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** command in EXEC mode.

clear ip mroute [**vrf** *vrf-name*] {* | *group*} [*source*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
*	Deletes all entries from the IP multicast routing table.
group	Either of the following: • Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the **ip host** command. • IP address of the multicast group. This is a multicast IP address in four-part, dotted notation.
source	(Optional) If you specify a group name or address, you can also specify a name or address of a multicast source that is sending to the group. A source need not be a member of the group.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using this command now clears both the multicast routing table on the Multicast Multilayer Switching (MMLS) RP and all multicast MLS cache entries for all MMLS-SEs that are performing multicast MLS for the MMLS-RP. That is, the original clearing occurs, and the derived hardware switching table is also cleared.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following example deletes all entries from the IP multicast routing table:

```
Router# clear ip mroute *
```

The following example deletes from the IP multicast routing table all sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42. Note that this example deletes all sources on network 228.3, not individual sources.

```
Router# clear ip mroute 224.2.205.42 228.3.0.0
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.
show ip mroute	Displays the contents of the IP multicast routing table.

clear ip msdp peer

To clear the TCP connection to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **clear ip msdp peer** command in EXEC mode.

clear ip msdp [**vrf** *vrf-name*] **peer** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to which the TCP connection is cleared.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command closes the TCP connection to the peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

Examples

The following example clears the TCP connection to the MSDP peer at 224.15.9.8:

```
Router# clear ip msdp peer 224.15.9.8
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

clear ip msdp sa-cache

To clear Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache entries, use the clear **ip msdp sa-cache** command in EXEC mode.

clear ip msdp [**vrf** *vrf-name*] **sa-cache** [*group-address* | *group-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	(Optional) Multicast group address or name for which SA entries are cleared from the SA cache.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

In order to have any SA entries in the cache to clear, SA caching must have been enabled with the **ip msdp cache-sa-state** command.

If no multicast group is identified by group address or name, all SA cache entries are cleared.

Examples

The following example clears the SA entries for the multicast group 224.5.6.7 from the cache:

```
Router# clear ip msdp sa-cache 224.5.6.7
```

Related Commands

Command	Description
ip msdp cache-sa-state	Enables the router to create SA state.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

clear ip msdp statistics

To clear statistics counters for one or all of the Multicast Source Discovery Protocol (MSDP) peers without resetting the sessions, use the **clear ip msdp statistics** command in EXEC mode.

clear ip msdp [**vrf** *vrf-name*] **statistics** [*peer-address* | *peer-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	(Optional) Address or name of the MSDP peers whose statistics counters, reset count, and input/output count are cleared.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following example clears the counters for the peer named sanjose:

```
Router# clear ip msdp statistics sanjose
```

clear ip pim auto-rp

To delete entries from the Auto-RP cache, use the **clear ip pim auto-rp** command in EXEC mode.

clear ip pim [**vrf** *vrf-name*] **auto-rp** *rp-address*

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rp-address	Clears only the entries related to the rendezvous point (RP) at this address. If this argument is omitted, the entire Auto-RP cache is cleared.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following example deletes all entries from the Auto-RP cache:

```
Router# clear ip pim auto-rp 224.5.6.7
```

debug ip igmp

To display Internet Group Management Protocol (IGMP) packets received and sent, and IGMP-host related events, use the **debug ip igmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip igmp [**vrf** *vrf-name*]

no debug ip igmp [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.1(3)T	Additional fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command helps discover whether the IGMP processes are functioning. In general, if IGMP is not working, the router process never discovers that another host is on the network that is configured to receive multicast packets. In dense mode, this situation will result in packets being delivered intermittently (a few every 3 minutes). In sparse mode, packets will never be delivered.

Use this command in conjunction with the **debug ip pim** and **debug ip mrouting** commands to observe additional multicast activity and to learn the status of the multicast routing process, or why packets are forwarded out of particular interfaces.

Examples

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

```
Router# debug ip igmp

IGMP: Received Host-Query from 172.16.37.33 (Ethernet1)
IGMP: Received Host-Report from 172.16.37.192 (Ethernet1) for 224.0.255.1
IGMP: Received Host-Report from 172.16.37.57 (Ethernet1) for 224.2.127.255
IGMP: Received Host-Report from 172.16.37.33 (Ethernet1) for 225.2.2.2
```

The messages displayed by the **debug ip igmp** command show query and report activity received from other routers and multicast group addresses.

The following is sample output from the **debug ip igmp** command when SSM is enabled. Because IGMP Version 3 lite (IGMP v3lite) requires the host to send IGMP Version 2 (IGMPv2) packets, IGMPv2 host reports also will be displayed in response to the router IGMPv2 queries. If SSM is disabled, the word "ignored" will be displayed in the **debug ip igmp** command output.

```
IGMP:Received v3-lite Report from 10.0.119.142 (Ethernet3/3), group count 1
IGMP:Received v3 Group Record from 10.0.119.142 (Ethernet3/3) for 232.10.10.10
IGMP:Update source 224.1.1.1
IGMP:Send v2 Query on Ethernet3/3 to 224.0.0.1
IGMP:Received v2 Report from 10.0.119.142 (Ethernet3/3) for 232.10.10.10
IGMP:Update source 224.1.1.1
```

Related Commands

Command	Description
debug ip mrm	Displays MRM control packet activity.
debug ip pim	Displays PIM packets received and sent, and PIM-related events.

debug ip mcache

To display IP multicast fast-switching events, use the **debug ip mcache** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip mcache [**vrf** *vrf-name*] [*hostname* | *group-address*]

no debug ip mcache [**vrf** *vrf-name*] [*hostname* | *group-address*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
hostname	(Optional) The host name.
group-address	(Optional) The group address.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use this command when multicast fast switching appears not to be functioning.

Examples

The following is sample output from the **debug ip mcache** command when an IP multicast static route (mroute) is cleared:

```
Router# debug ip mcache

IP multicast fast-switching debugging is on

Router# clear ip mroute *

MRC: Build MAC header for (172.31.60.185/32, 224.2.231.173), Ethernet0
MRC: Fast-switch flag for (172.31.60.185/32, 224.2.231.173), off -> on, caller
ip_mroute_replicate-1
MRC: Build MAC header for (172.31.191.10/32, 224.2.127.255), Ethernet0
MRC: Build MAC header for (172.31.60.152/32, 224.2.231.173), Ethernet0
```

Table 5 describes the significant fields shown in the display.

Table 5 debug ip mcache Field Descriptions

Field	Description
MRC	Multicast route cache.
Fast-switch flag	Route is fast switched.
(172.31.60.185/32)	Host route with 32 bits of mask.
off -> on	State has changed.
caller ...	The code function that activated the state change.

Related Commands

Command	Description
debug ip dvmrp	Displays information on DVMRP packets received and sent.
debug ip igmp	Displays IGMP packets received and sent, and IGMP-host related events.
debug ip igrp transactions	Displays transaction information on IGRP routing transactions.
debug ip mrm	Displays MRM control packet activity.
debug ip sd	Displays all SD announcements received.

debug ip mpacket

To display IP multicast packets received and sent, use the **debug ip mpacket** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

debug ip mpacket [**vrf** *vrf-name*] [**detail** | **fastswitch**] [*access-list*] [*group*]

no debug ip mpacket [**vrf** *vrf-name*] [**detail** | **fastswitch**] [*access-list*] [*group*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
detail	(Optional) Causes the **debug ip mpacket** command to display IP header information and MAC address information.
fastswitch	(Optional) Displays IP packet information in the fast path.
access-list	(Optional) The access list number.
group	(Optional) The group name or address.

Defaults

The **debug ip mpacket** command displays all IP multicast packets switched at the process level.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.1(2)T	The **fastswitch** keyword was added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command displays information for multicast IP packets that are forwarded from this router. Use the *access-list* or *group* argument to limit the display to multicast packets from sources described by the access list or a specific multicast group.

Use this command with the **debug ip packet** command to display additional packet information.

Note The **debug ip mpacket** command generates many messages. Use this command with care so that performance on the network is not affected by the debug message traffic.

Examples

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

```
Router# debug ip mpacket 224.2.0.1

IP: s=10.188.34.54 (Ethernet1), d=224.2.0.1 (Tunnel0), len 88, mforward
IP: s=10.188.34.54 (Ethernet1), d=224.2.0.1 (Tunnel0), len 88, mforward
```

```
IP: s=10.188.34.54 (Ethernet1), d=224.2.0.1 (Tunnel0), len 88, mforward
IP: s=10.162.3.27 (Ethernet1), d=224.2.0.1 (Tunnel0), len 68, mforward
```

Table 6 describes the significant fields shown in the display.

Table 6 debug ip mpacket Field Descriptions

Field	Description
IP	IP packet.
s=10.188.34.54	Source address of the packet.
(Ethernet1)	Name of the interface that received the packet.
d=224.2.0.1	Multicast group address that is the destination for this packet.
(Tunnel0)	Outgoing interface for the packet.
len 88	Number of bytes in the packet. This value will vary depending on the application and the media.
mforward	Packet has been forwarded.

Related Commands

Command	Description
debug ip dvmrp	Displays information on DVMRP packets received and sent.
debug ip igmp	Displays IGMP packets received and sent, and IGMP host-related events.
debug ip mrm	Displays MRM control packet activity.
debug ip packet	Displays general IP debugging information and IPSO security transactions.
debug ip sd	Displays all SD announcements received.

debug ip mrouting

To display changes to the IP multicast routing table, use the **debug ip mrouting** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip mrouting [**vrf** *vrf-name*] [*group*]

no debug ip mrouting [**vrf** *vrf-name*] [*group*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group	(Optional) Group name or address to monitor packet activity of a single group.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command indicates when the router has made changes to the multicast static route (mroute) table. Use the **debug ip pim** and **debug ip mrouting** commands consecutively to obtain additional multicast routing information. In addition, use the **debug ip igmp** command to learn why an mroute message is being displayed.

This command generates a substantial amount of output. Use the optional *group* argument to limit the output to a single multicast group.

Examples

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

```
Router# debug ip mrouting 224.2.0.1

MRT: Delete (10.0.0.0/8, 224.2.0.1)
MRT: Delete (10.4.0.0/16, 224.2.0.1)
MRT: Delete (10.6.0.0/16, 224.2.0.1)
MRT: Delete (10.9.0.0/16, 224.2.0.1)
MRT: Delete (10.16.0.0/16, 224.2.0.1)
MRT: Create (*, 224.2.0.1), if_input NULL
MRT: Create (224.69.15.0/24, 225.2.2.4), if_input Ethernet0, RPF nbr 224.69.61.15
MRT: Create (224.69.39.0/24, 225.2.2.4), if_input Ethernet1, RPF nbr 0.0.0.0
MRT: Create (10.0.0.0/8, 224.2.0.1), if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create (10.4.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create (10.6.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 224.0.0.0
```

```
MRT: Create (10.9.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create (10.16.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 224.0.0.0
```

The following lines show that multicast IP routes were deleted from the routing table:

```
MRT: Delete (10.0.0.0/8, 224.2.0.1)
MRT: Delete (10.4.0.0/16, 224.2.0.1)
MRT: Delete (10.6.0.0/16, 224.2.0.1)
```

The (*, G) entries are generally created by receipt of an IGMP host report from a group member on the directly connected LAN or by a Protocol Independent Multicast (PIM) join message (in sparse mode) that this router receives from a router that is sending joins toward the RP. This router will in turn send a join toward the route processor (RP) that creates the shared tree (or RP tree).

```
MRT: Create (*, 224.2.0.1), if_input NULL
```

The following lines are an example of creating an (S, G) entry that shows that an mpacket was received on Ethernet interface 0. The second line shows a route being created for a source that is on a directly connected LAN. The RPF means "reverse path forwarding," whereby the router looks up the source address of the multicast packet in the unicast routing table and asks which interface will be used to send a packet to that source.

```
MRT: Create (224.69.15.0/24, 225.2.2.4), if_input Ethernet0, RPF nbr 224.69.61.15
MRT: Create (224.69.39.0/24, 225.2.2.4), if_input Ethernet1, RPF nbr 224.0.0.0
```

The following lines show that multicast IP routes were added to the routing table. Note the 224.0.0.0 as the RPF, which means the route was created by a source that is directly connected to this router.

```
MRT: Create (10.9.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create (10.16.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 224.0.0.0
```

If the source is not directly connected, the neighbor address shown in these lines will be the address of the router that forwarded the packet to this router.

The shortest path tree state maintained in routers consists of source (S), multicast address (G), outgoing interface (OIF), and incoming interface (IIF). The forwarding information is referred to as the multicast forwarding entry for (S, G).

An entry for a shared tree can match packets from any source for its associated group if the packets come through the proper incoming interface as determined by the Reverse Path Forwarding (RPF) lookup. Such an entry is denoted as (*, G). A (*, G) entry keeps the same information a (S, G) entry keeps, except that it saves the rendezvous point (RP) address in place of the source address in sparse mode or 24.0.0.0 in dense mode.

Related Commands

Command	Description
debug ip dvmrp	Displays information on DVMRP packets received and sent.
debug ip igmp	Displays IGMP packets received and sent, and IGMP host-related events.
debug ip packet	Displays general IP debugging information and IPSO security transactions.
debug ip pim	Displays all SD announcements received.
debug ip sd	Displays all SD announcements received.

debug ip msdp

To debug Multicast Source Discovery Protocol (MSDP) activity, use the **debug ip msdp** command in privileged EXEC mode. To disable debugging activity, use the **no** form of this command.

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

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *name*	(Optional) The peer for which debug events are logged.
detail	(Optional) Provides more detailed debugging information.
routes	(Optional) Displays the contents of Source-Active messages.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

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

```
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: 205.167.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 205.167.76.241, 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
```

Table 7 describes the significant fields shown in the display.

Table 7 debug ip msdp Field Descriptions

Field	Description
MSDP	Protocol being debugged.
224.150.44.254:	IP address of the MSDP peer.
Received 1388-byte message from peer	MSDP event.

debug ip msdp resets

To debug Multicast Source Discovery Protocol (MSDP) peer reset reasons, use the **debug ip msdp resets** command in privileged EXEC mode.

debug ip msdp [**vrf** *vrf-name*] **resets**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

debug ip pim

To display Protocol Independent Multicast (PIM) packets received and sent, and to display PIM-related events, use the **debug ip pim** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip pim [**vrf** *vrf-name*] [*group* | **df** [*rp-address*]]

no debug ip pim [**vrf** *vrf-name*] [*group* | **df** [*rp-address*]]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group	(Optional) The group name or address to monitor the packet activity of a single group.
df	(Optional) When bidirectional PIM is used, displays all designated forwarder (DF) election messages.
rp-address	(Optional) The rendezvous point (RP) IP address.

Defaults

All PIM packets are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.1(2)T	The **df** keyword was added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

PIM uses Internet Group Management Protocol (IGMP) packets to communicate with routers and advertise reachability information.

Use this command with the **debug ip igmp** and **debug ip mrouting** commands to display additional multicast routing information.

Examples

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

```
Router# debug ip pim 224.2.0.1

PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
```

```
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1
PIM: Received Join/Prune on Ethernet1 from 172.16.37.6
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Join-list: (10.0.0.0/8, 224.2.0.1)
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
PIM: Join-list: (10.4.0.0/16, 224.2.0.1)
PIM: Prune-list (172.16.84.16/28, 224.2.0.1) RP-bit set RP 172.16.84.16
PIM: Send Prune on Ethernet1 to 172.16.37.6 for (172.16.84.16/28, 224.2.0.1), RP
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16
PIM: For RP, Prune-list: 10.84.0.0/16
PIM: For RP, Prune-list: 10.146.0.0/16
PIM: For 10.3.84.1, Join-list: 172.16.84.16/28
PIM: Send periodic Join/Prune to RP via 172.16.37.6 (Ethernet1)
```

The following lines appear periodically when PIM is running in sparse mode and indicate to this router the multicast groups and multicast sources in which other routers are interested:

```
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
```

The following lines appear when an RP message is received and the RP timer is reset. The expiration timer sets a checkpoint to make sure the RP still exists. Otherwise, a new RP must be discovered.

```
PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
```

The prune message in the following line states that this router is not interested in the SA information. This message tells an upstream router to stop forwarding multicast packets from this source.

```
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
```

In the following line, a second router on the network wants to override the prune message that the upstream router just received. The timer is set at a random value so that if additional routers on the network still want to receive multicast packets for the group, only one will actually send the message. The other routers will receive the join message and then suppress sending their own message.

```
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1
```

In the following line, a join message is sent toward the RP for all sources:

```
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
```

In the following lines, the interface is being added to the outgoing interface (OIF) of the (*, G) and (S, G) multicast static route (mroute) table entry so that packets from the source will be forwarded out that particular interface:

```
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
```

The following line appears in sparse mode only. There are two trees on which data may be received: the RP tree and the source tree. In dense mode there is no RP. After the source and the receiver have discovered one another at the RP, the first hop router for the receiver will usually join to the source tree rather than the RP tree.

```
PIM: Prune-list (172.16.84.16/28, 224.2.0.1) RP-bit set RP 172.16.84.16
```

The send prune message in the next line shows that a router is sending a message to a second router saying that the first router should no longer receive multicast packets for the (S, G). The RP at the end of the message indicates that the router is pruning the RP tree and is most likely joining the source tree, although the router may not have downstream members for the group or downstream routers with members of the group. The output shows the specific sources from which this router no longer wants to receive multicast messages.

```
PIM: Send Prune on Ethernet1 to 172.16.37.6 for (172.16.84.16/28, 224.2.0.1), RP
```

The following lines indicate that a prune message is sent toward the RP so that the router can join the source tree rather than the RP tree:

```
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16

In the following line, a periodic message is sent toward the RP. The default period is
once per minute. Prune and join messages are sent toward the RP or source
rather than directly to the RP or source. It is the responsibility of the next hop router
to take proper action with this message, such as continuing to forward it to the
next router in the tree.

PIM: Send periodic Join/Prune to RP via 172.16.37.6 (Ethernet1)
```

Related Commands

Command	Description
debug ip dvmrp	Displays information on DVMRP packets received and sent.
debug ip igmp	Displays IGMP packets received and sent, and displays IGMP host-related events.
debug ip igrp transactions	Displays transaction information on IGRP routing transactions.
debug ip mrouting	Displays changes to the IP multicast routing table.
debug ip sd	Displays all SD announcements received.

debug ip pim auto-rp

To display the contents of each Protocol Independent Multicast (PIM) packet used in the automatic discovery of group-to-rendezvous point (RP) mapping and the actions taken on the address-to-RP mapping database, use the **debug ip pim auto-rp** command in privileged EXEC. To disable debugging output, use the **no** form of this command.

debug ip pim auto-rp [**vrf** *vrf-name*]

no debug ip pim auto-rp [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following is sample output from the **debug ip pim auto-rp** command:

```
Router# debug ip pim auto-rp

Auto-RP: Received RP-announce, from 172.16.214.66, RP_cnt 1, holdtime 180 secs
Auto-RP:  update (192.168.248.0/24, RP:172.16.214.66)
Auto-RP: Build RP-Discovery packet
Auto-RP:  Build mapping (192.168.248.0/24, RP:172.16.214.66),
Auto-RP:  Build mapping (192.168.250.0/24, RP:172.16.214.26).
Auto-RP:  Build mapping (192.168.254.0/24, RP:172.16.214.2).
Auto-RP: Send RP-discovery packet (3 RP entries)
Auto-RP: Build RP-Announce packet for 172.16.214.2
Auto-RP:  Build announce entry for (192.168.254.0/24)
Auto-RP: Send RP-Announce packet, IP source 172.16.214.2, ttl 8
```

The first two lines show a packet received from 172.16.214.66 announcing that it is the RP for the groups in 192.168.248.0/24. This announcement contains one RP address and is valid for 180 seconds. The RP-mapping agent then updates its mapping database to include the new information.

```
Auto-RP: Received RP-announce, from 172.16.214.66, RP_cnt 1, holdtime 180 secs
Auto-RP:  update (192.168.248.0/24, RP:172.16.214.66)
```

In the next five lines, the router creates an RP-discovery packet containing three RP mapping entries. The packet is sent to the well-known CISCO-RP-DISCOVERY group address (224.0.1.40).

```
Auto-RP: Build RP-Discovery packet
Auto-RP:  Build mapping (192.168.248.0/24, RP:172.16.214.66),
Auto-RP:  Build mapping (192.168.250.0/24, RP:172.16.214.26).
Auto-RP:  Build mapping (192.168.254.0/24, RP:172.16.214.2).
Auto-RP: Send RP-discovery packet (3 RP entries)
```

The final three lines show the router announcing that it intends to be an RP for the groups in 192.168.254.0/24. Only routers inside the scope ttl 8 receive the advertisement and use the RP for these groups.

```
Auto-RP: Build RP-Announce packet for 172.16.214.2
Auto-RP:  Build announce entry for (192.168.254.0/24)
Auto-RP: Send RP-Announce packet, IP source 172.16.214.2, ttl 8
```

The following is sample output from the **debug ip pim auto-rp** command when a router receives an update. In this example, the packet contains three group-to-RP mappings, which are valid for 180 seconds. The RP-mapping agent then updates its mapping database to include the new information.

```
Router# debug ip pim auto-rp

Auto-RP: Received RP-discovery, from 172.16.214.17, RP_cnt 3, holdtime 180 secs
Auto-RP:  update (192.168.248.0/24, RP:172.16.214.66)
Auto-RP:  update (192.168.250.0/24, RP:172.16.214.26)
Auto-RP:  update (192.168.254.0/24, RP:172.16.214.2)
```

ip mroute

To configure a multicast static route (mroute), use the **ip mroute** command in global configuration mode. To remove the route, use the **no** form of this command.

ip mroute [**vrf** *vrf-name*] *source-address mask* [*protocol as-number*] {*rpf-address* | *interface-type interface-number*} [*distance*]

no ip mroute [**vrf** *vrf-name*] *source mask* [*protocol as-number*] {*rpf-address* | *interface-type interface-number*} [*distance*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
source-address	IP address of the multicast source.
mask	Mask on the IP address of the multicast source.
protocol	(Optional) Unicast routing protocol that you are using.
as-number	(Optional) Autonomous system number of the routing protocol you are using, if applicable.
rpf-address	Incoming interface for the mroute. If the Reverse Path Forwarding (RPF) address *rpf-address* is a Protocol Independent Multicast (PIM) neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-address* argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system. If the *rpf-address* argument is not specified, the interface *interface-type interface-number* value is used as the incoming interface.
interface-type interface-number	Interface type and number for the mroute.
distance	(Optional) Determines whether a unicast route, a Distance Vector Multicast Routing Protocol (DVMRP) route, or a static mroute should be used for the RPF lookup. The lower distances have better preference. If the static mroute has the same distance as the other two RPF sources, the static mroute will take precedence. The default is 0.

Defaults

distance: 0

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command allows you to statically configure where multicast sources are located (even though the unicast routing table shows something different).

When a source range is specified, the *rpf-address* argument applies only to those sources.

Examples

The following example configures all sources via a single interface (in this case, a tunnel):

```
ip mroute 224.0.0.0 255.255.255.255 tunnel0
```

The following example configures all specific sources within a network number to be reachable through 172.30.10.13:

```
ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
```

The following example causes this multicast static route to take effect if the unicast routes for any given destination go away:

```
ip mroute 224.0.0.0 255.255.255.255 serial0 200
```

ip msdp border

To configure a router that borders a Protocol Independent Multicast (PIM) sparse mode region and dense mode region to use Multicast Source Discovery Protocol (MSDP), use the **ip msdp border** command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **border sa-address** *internet-type internet-number*

no ip msdp [**vrf** *vrf-name*] **border sa-address** *internet-type internet-number*

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
sa-address	Active source IP address.
internet-type internet-number	Interface type and number from which the IP address is derived and used as the rendezvous point (RP) address in Source-Active (SA) messages. Thus, MSDP peers can forward SA messages away from this border. The IP address of the interface is used as the originator ID, which is the RP field in the MSDP SA message.

Defaults

The active sources in the dense mode region will not participate in MSDP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use this command if you want the router to send SA messages for sources active in the PIM dense mode region to MSDP peers.

Note We recommend configuring the border router in the sparse mode domain to proxy-register sources in the dense mode domain, and have the sparse mode domain use standard MSDP procedures to advertise these sources.

Note If you use this command, you must constrain the sources advertised by using the **ip msdp redistribute** command. Configure the **ip msdp redistribute** command to apply to only local sources. Be aware that this configuration can result in (S, G) state remaining long after a source in the dense mode domain has stopped sending.

Note The **ip msdp originator-id** command also identifies an interface type and number to be used as the RP address. If both the **ip msdp border** and **ip msdp originator-id** commands are configured, the latter command prevails. That is, the address derived from the **ip msdp originator-id** command determines the address of the RP.

Examples

In the following example, the local router is not an RP. It borders a PIM sparse mode region with a dense mode region. It uses the IP address of Ethernet interface 0 as the "RP" address in SA messages.

```
ip msdp border sa-address ethernet0
```

Related Commands

Command	Description
ip msdp originator-id	Allows an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.
ip msdp redistribute	Configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers.

ip msdp cache-sa-state

To have the router create Source-Active (SA) state, use the **ip msdp cache-sa-state** command in global configuration mode.

ip msdp cache-sa-state [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

The router creates SA state for all Multicast Source Discovery Protocol (MSDP) SA messages it receives.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified such that it is enabled by default and cannot be disabled.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command is automatically configured if at least one MSDP peer is configured. It cannot be disabled.

If you are running a version of Cisco IOS software prior to Release 12.1(7), we recommend enabling the **ip msdp cache-sa-state** command.

Examples

The following example shows how the **ip msdp cache-sa-state** command is enabled when an MSDP peer is configured. For more MSDP configuration examples, refer to the “Configuring Multicast Source Discovery Protocol” chapter in the Release 12.2 *Cisco IOS IP Configuration Guide*.

```
.
.
.
ip classless
ip msdp peer 224.168.1.2 connect-source Loopback0
ip msdp peer 224.169.1.7
ip msdp mesh-group outside-test 192.168.1.2
ip msdp cache-sa-state
ip msdp originator-id Loopback0
.
.
.
```

Related Commands

Command	Description
clear ip msdp sa-cache	Clears MSDP SA cache entries.
ip msdp sa-request	Configures the router to send SA request messages to the MSDP peer when a new joiner from the group becomes active.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

ip msdp default-peer

To define a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages, use the **ip msdp default-peer** command in global configuration mode. To remove the default peer, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]

no ip msdp [**vrf** *vrf-name*] **default-peer**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP default peer.
prefix-list *list*	(Optional) Border Gateway Protocol (BGP) prefix list that specifies that the peer will be a default peer only for the prefixes listed in the list specified by the *list* argument. A BGP prefix list must be configured for this **prefix-list** *list* keyword and argument to have any effect.

Defaults

No default MSDP peer exists.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use the **ip msdp default-peer** command if you do not want to configure your MSDP peer to be a BGP peer also.

If only one MSDP peer is configured (with the **ip msdp peer** command), it will be used as a default peer. Therefore, you need not configure a default peer with this command.

If the **prefix-list** *list* keyword and argument are not specified, all SA messages received from the configured default peer are accepted.

Remember to configure a BGP prefix list if you intend to configure the **prefix-list** *list* keyword and argument with the **ip msdp default-peer** command.

If the **prefix-list** *list* keyword and argument are specified, SA messages originated from rendezvous points (RPs) covered by the **prefix-list** *list* keyword and argument will be accepted from the configured default peer. If the **prefix-list** *list* keyword and argument are specified but no prefix list is configured, the default peer will be used for all prefixes.

You can enter multiple **ip msdp default-peer** commands, with or without the **prefix-list** keyword, as follows. However, all commands must either have the keyword or all must not have the keyword.

- When you use multiple **ip msdp default-peer** commands with the **prefix-list** keyword, you use all the default peers at the same time for different RP prefixes. This syntax is typically used in a service provider cloud that connects stub site clouds.
- When you use multiple **ip msdp default-peer** commands without the **prefix-list** keyword, you use a single active peer to accept all SA messages. If that peer goes down, then you move to the next configured default peer to accept all SA messages. This syntax is typically used at a stub site.

Examples

The following example configures the router named router.cisco.com as the default peer to the local router:

```
ip msdp peer 224.12.2.3
ip msdp peer 224.13.4.5
ip msdp default-peer router.cisco.com    !At a stub site
```

The following example configures two default peers:

```
ip msdp peer 224.12.2.3
ip msdp peer 224.13.4.5
ip msdp default-peer 224.12.2.3 prefix-list site-c
ip prefix-list site-a permit 224.12.0.0/16
ip msdp default-peer 224.13.4.5 prefix-list site-a
ip prefix-list site-a permit 224.13.0.0/16
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip prefix-list	Creates a prefix list.

ip msdp description

To add descriptive text to the configuration for a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp description** command in global configuration mode. To remove the description, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **description** {*peer-name* | *peer-address*} *text*

no ip msdp [**vrf** *vrf-name*] **description** {*peer-name* | *peer-address*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name | *peer-address*	Peer name or address to which this description applies.
text	Description of the MSDP peer.

Defaults

No description is associated with an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Configure a description to make the MSDP peer easier to identify. This description is displayed in the output of the **show ip msdp peer** command.

Examples

The following example configures the router at the IP address 224.107.5.4 with a description indicating it is a router at customer A:

```
ip msdp description 224.107.5.4 router at customer a
```

ip msdp filter-sa-request

To configure the router to send Source-Active (SA) request messages to the Multicast Source Discovery Protocol (MSDP) peer when a new joiner from a group becomes active, use the **ip msdp filter-sa-request** command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]

no ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.
list *access-list*	(Optional) Standard IP access list number or name that describes a multicast group address. If no access list is specified, all SA request messages are ignored.

Defaults

If this command is not configured, all SA request messages are honored. If this command is configured but no access list is specified, all SA request messages are ignored.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

By default, the router honors all SA request messages from peers. Use this command if you want to control exactly which SA request messages the router will honor.

If no access list is specified, all SA request messages are ignored. If an access list is specified, only SA request messages from those groups permitted will be honored, and all others will be ignored.

Examples

The following example configures the router to filter SA request messages from the MSDP peer at 172.16.2.2. SA request messages from sources on the network 192.168.22.0 pass access list 1 and will be honored; all others will be ignored.

```
ip msdp filter sa-request 224.69.2.2 list 1
access-list 1 permit 228.4.22.0 0.0.0.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp mesh-group

To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the **ip msdp mesh-group** command in global configuration mode. To remove an MSDP peer from a mesh group, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
mesh-name	Name of the mesh group.
peer-address | *peer-name*	IP address or name of the MSDP peer to be a member of the mesh group.

Defaults

The MSDP peers do not belong to a mesh group.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. Source-Active (SA) messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group.

Mesh groups can be used to achieve two goals:

- To reduce SA message flooding
- To simplify peer-Reverse Path Forwarding (RPF) flooding (no need to run Border Gateway Protocol [BGP] or multiprotocol BGP among MSDP peers)

Examples

The following example configures the MSDP peer at address 224.1.1.1 to be a member of the mesh group named internal:

```
ip msdp mesh-group internal 224.1.1.1
```

ip msdp originator-id

To allow a Multicast Source Discovery Protocol (MSDP) speaker that originates a Source-Active (SA) message to use the IP address of the interface as the rendezvous point (RP) address in the SA message, use the **ip msdp originator-id** command in global configuration mode. To prevent the RP address from being derived in this way, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

no ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type *interface-number*	Interface type and number on the local router, whose IP address is used as the RP address in SA messages.

Defaults

The RP address is used as the originator ID.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **ip msdp originator-id** command identifies an interface type and number to be used as the RP address in an SA message.

Use this command if you want to configure a logical RP. Because only RPs and MSDP border routers originate SAs, there are times when it is necessary to change the ID used for this purpose.

If both the **ip msdp border sa-address** and **ip msdp originator-id** commands are configured, the latter command prevails. That is, the address derived from the **ip msdp originator-id** command determines the address of the RP to be used in the SA message.

Examples

The following example configures the IP address of Ethernet interface 1 as the RP address in SA messages:

```
ip msdp originator-id ethernet1
```

Related Commands

Command	Description
ip msdp border	Configures a router that borders a PIM sparse mode region and dense mode region to use MSDP.

ip msdp peer

To configure a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp peer** command in global configuration mode. To remove the peer relationship, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*]

no ip msdp [**vrf** *vrf-name*] **peer** {*peer-name* | *peer-address*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name | *peer-address*	Domain Name System (DNS) name or IP address of the router that is to be the MSDP peer.
connect-source *interface-type interface-number*	(Optional) Interface type and number whose primary address becomes the source IP address for the TCP connection. This interface is on the router being configured.
remote-as *as-number*	(Optional) Autonomous system number of the MSDP peer. This is used for display purposes only. There are cases where a peer might appear to be in another autonomous system (other than the one it really resides in) when you have an MSDP peering session but do not have a BGP peer session with that peer. In this case, if the prefix of the peer is injected by another autonomous system, it is displayed as the autonomous system number of the peer (and is misleading).

Defaults

No MSDP peer is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The router specified should also be configured as a BGP neighbor.

If you are also BGP peering with this MSDP peer, you should use the same IP address for MSDP as you do for BGP. However, you are not required to run BGP or multiprotocol BGP with the MSDP peer, as long as there is a BGP or MBGP path between the MSDP peers. If there is no path, you must configure the **ip msdp default-peer** command.

Examples

The following example configures the router at the IP address 224.108.1.2 as an MSDP peer to the local router. The neighbor belongs to autonomous system 109.

```
ip msdp peer 224.108.1.2 connect-source ethernet 0
router bgp 110
 network 224.108.0.0
 neighbor 224.108.1.2 remote-as 109
 neighbor 224.108.1.2 update-source ethernet 0
```

The following example configures the router named router.cisco.com as an MSDP peer to the local router:

```
ip msdp peer router.cisco.com
```

The following example configures the router named router.cisco.com to be an MSDP peer in autonomous system 109. The primary address of Ethernet interface 0 is used as the source address for the TCP connection.

```
ip msdp peer router.cisco.com connect-source ethernet0 remote-as 109
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP neighbor table.

ip msdp redistribute

To configure which (S, G) entries from the multicast routing table are advertised in Source-Active (SA) messages originated to Multicast Source Discovery Protocol (MSDP) peers, use the **ip msdp redistribute** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **redistribute** [**list** *access-list-name*] [**asn** *as-access-list-number*] [**route-map** *map-name*]

no ip msdp [**vrf** *vrf-name*] **redistribute**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
list *access-list-name*	(Optional) Standard or extended IP access list number or name that controls which local sources are advertised and to which groups they send.
asn *as-access-list-number*	(Optional) Standard or extended IP access list number in the range from 1 to 199. This access list number must also be configured in the **ip as-path** command.
route-map *map-name*	(Optional) Defines the route map.

Defaults

If no portion of this command is configured, only local sources are advertised, provided they send to groups for which the router is a rendezvous point (RP).

If no portion of this command is configured and if the **ip msdp border sa-address** command is configured, all local sources are advertised.

If the **ip msdp redistribute** command is configured with no keywords, no multicast sources are advertised.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command affects SA message origination, not SA message forwarding. If you want to filter which SA messages are forwarded to MSDP peers, use the **ip msdp sa-filter in** or **ip msdp sa-filter out** command.

The **ip msdp redistribute** command controls which (S, G) pairs the router advertises from the multicast routing table. By default, only sources within the local domain are advertised. Use the following guidelines for the **ip msdp redistribute** command:

- If you specify the **list** *access-list-name* keyword and argument only, you filter which local sources are advertised and to which groups they send. The access list specifies a source address, source mask, group address, and group mask.
- If you specify the **asn** *as-access-list-number* keyword and argument only, you advertise all sources sending to any group that pass through the autonomous system path access list. The autonomous system path access list number refers to the **ip as-path** command, which specifies an access list. If the **asn 0** keywords are specified, sources from all autonomous systems are advertised. The **asn 0** keywords are useful when connecting dense mode domains to a sparse mode domain running MSDP, or when using MSDP in a router that is not configured with Border Gateway Protocol (BGP). In these cases, you do not know if a source is local.
- If you specify the **route-map** *map-name* keyword and argument only, you advertise all sources that satisfy the match criteria in the route map *map-name* argument.
- If you specify all three keywords (**list**, **asn**, and **route-map**), all conditions must be true before any multicast source is advertised in an SA message.
- If you specify the **ip multicast redistribute** command with no other keywords or arguments, no multicast sources are advertised.

Examples

The following example configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers:

```
ip msdp redistribute route-map customer-sources

route-map customer-sources permit
match as-path customer-as

ip as-path access-list ^109$
```

Related Commands

Command	Description
ip as-path	Defines a BGP-related access list.
ip msdp border	Configures a router that borders a PIM sparse mode region and dense mode region to use MSDP.

ip msdp sa-filter in

To configure an incoming filter list for Source-Active (SA) messages received from the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter in** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

no ip msdp [**vrf** *vrf-name*] **sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the SA messages are filtered.
list *access-list-name*	(Optional) IP access list number or name. If no access list is specified, all source/group pairs from the peer are filtered.
route-map *map-name*	(Optional) Route map name. From the specified MSDP peer, passes only those SA messages that meet the match criteria in the route map *map-name* argument. If all match criteria are true, a **permit** keyword from the route map will pass routes through the filter. A **deny** keyword will filter routes.

Defaults

If this command is not configured, no incoming messages are filtered; all SA messages are accepted from the peer.

If the command is configured, but no access list or route map is specified, all source/group pairs from the peer are filtered.

If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S, G) pair in incoming SA messages.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following example configures the router to filter all SA messages from the peer named router.cisco.com:

```
ip msdp peer router.cisco.com connect-source ethernet 0
ip msdp sa-filter in router.cisco.com
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter out	Configures an outgoing filter list for SA messages sent to the specified MSDP peer.

ip msdp sa-filter out

To configure an outgoing filter list for Source-Active (SA) messages sent to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter out** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

no ip msdp [**vrf** *vrf-name*] **sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer to which the SA messages are filtered.
list *access-list*	(Optional) Extended IP access list number or name. If no access list is specified, all source/group pairs are filtered. To the specified MSDP peer, passes only those SA messages that pass the extended access list. If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S, G) pairs in outgoing SA messages.
route-map *map-name*	(Optional) Route map name. To the specified MSDP peer, passes only those SA messages that meet the match criteria in the route map *map-name* argument. If all match criteria are true, a **permit** keyword from the route map will pass routes through the filter. A **deny** keyword will filter routes.

Defaults

If this command is not configured, no outgoing messages are filtered; all SA messages received are forwarded to the peer.

If the command is configured, but no access list or route map is specified, all source/group pairs are filtered.

If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S, G) pairs in outgoing SA messages.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following example allows only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer named router.cisco.com:

```
ip msdp peer router.cisco.com connect-source ethernet 0
ip msdp sa-filter out router.cisco.com list 100
access-list 100 permit ip 224.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter in	Configures an incoming filter list for SA messages received from the specified MSDP peer.

ip msdp sa-request

To configure the router to send Source-Active (SA) request messages to the Multicast Source Discovery Protocol (MSDP) peer when a new joiner from the group becomes active, use the **ip msdp sa-request** command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.

Defaults

The router does not send SA request messages to the MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

By default, the router does not send any SA request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive any SA messages that eventually arrive.

Use this command if you want a new member of a group to learn the current, active multicast sources in a connected Protocol Independent Multicast sparse mode (PIM-SM) domain that are sending to a group. The router will send SA request messages to the specified MSDP peer when a new member joins a group. The peer replies with the information in its SA cache. If the peer does not have a cache configured, this command provides nothing.

An alternative to this command is using the **ip msdp cache-sa-state** command to have the router cache messages.

Examples

The following example configures the router to send SA request messages to the MSDP peer at 224.69.1.1:

```
ip msdp sa-request 224.69.1.1
```

Related Commands

Command	Description
ip mdsp cache-sa-state	Enables the router to create SA state.
ip msdp peer	Configures an MSDP peer.

ip msdp shutdown

To administratively shut down a configured Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp shutdown** command in global configuration mode. To bring the peer back up, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to shut down.

Defaults

No action is taken to shut down an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following example shuts down the MSDP peer at IP address 224.5.7.20:

```
ip msdp shutdown 224.5.7.20
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp ttl-threshold

To limit which multicast data packets are sent in Source-Active (SA) messages to a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp ttl-threshold** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*

no ip msdp [**vrf** *vrf-name*] **ttl-threshold** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to which the *ttl-value* argument applies.
ttl-value	Time-to-live (TTL) value. The default value of the *ttl-value* argument is 0, meaning all multicast data packets are forwarded to the peer until the TTL is exhausted.

Defaults

ttl-value: 0

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command limits which multicast data packets are sent in data-encapsulated SA messages. Only multicast packets with an IP header TTL greater than or equal to the *ttl-value* argument are sent to the MSDP peer specified by the IP address or name.

Use this command if you want to use TTL to scope your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you would need to send those packets with a TTL greater than 8.

Examples

The following example configures a TTL threshold of 8 hops:

```
ip msdp ttl-threshold 224.5.7.20 8
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip multicast cache-headers

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** command in global configuration mode. To remove the buffer, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **cache-headers** [**rtp**]

no ip multicast [**vrf** *vrf-name*] **cache-headers**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rtp	(Optional) Caches Real-Time Transport Protocol (RTP) headers.

Defaults

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1	The **rtp** keyword was added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

You can store IP multicast packet headers in a cache and then display them to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- UDP port numbers
- Packet length

Note This command allocates a circular buffer of approximately 32 KB. Do not configure this command if you are low on memory.

Use the **show ip mpacket** command to display the buffer.

Examples

The following example allocates a buffer to store IP multicast packet headers:

```
ip multicast cache-headers
```

Related Commands

Command	Description
show ip mpacket	Displays the contents of the circular cache-header buffer.

ip multicast mrinfo-filter

To filter multicast router information request packets, use the **ip multicast mrinfo-filter** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip multicast mrinfo-filter *access-list*

no ip multicast mrinfo-filter *access-list*

Syntax Description

access-list	Access list of the source IP address to be filtered.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

The **ip multicast mrinfo-filter** command filters the mrinfo request packets for all of the sources listed in the specified access list.

Examples

The following example specifies that mrinfo request packets be filtered for all sources listed in access list number 4.

```
ip multicast mrinfo-filter 4
```

ip multicast multipath

To enable load splitting of IP multicast traffic across multiple equal-cost paths, use the **ip multicast multipath** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **multipath**

no ip multicast [**vrf** *vrf-name*] **multipath**

SyntaDescription

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

By default, if multiple equal-cost paths exist, multicast traffic will not be load split across these paths.

Command Modes

Global configuration

Command History

Release	Modification
12.0(8)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

If the **ip multicast multipath** command is configured and multiple equal-cost paths exist, load splitting will occur across the equal-cost paths for multicast traffic from different sources to the same multicast group, but not for traffic from the same source to different multicast groups. Because this command changes the way a Reverse Path Forwarding (RPF) neighbor is selected, it must be configured consistently on all routers in a redundant topology to avoid looping.

Examples

The following example shows how to configure the **ip multicast multipath** command:

```
ip multicast multipath
```

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

ip multicast route-limit

To limit the number of multicast routes that can be added to a multicast routing table, use the **ip multicast route-limit** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

no ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
limit	The number of mroutes that can be added. The range is from 1 to 2147483647.
threshold	(Optional) The number of mroutes that cause a warning message to occur. The threshold value must not exceed the limit value.

Defaults

Limit = 2147483647

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

The **ip multicast route-limit** command limits the number of multicast routes that can be added to a router and generates an error message when the limit is exceeded. If the user sets the *threshold* argument, a threshold error message is generated when the threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the *limit* argument.

The mroute warning threshold must not exceed the mroute limit.

Examples

The following example sets the mroute limit at 200,000 and the threshold at 20,000 for a VRF instance named cisco:

```
ip multicast vrf cisco route-limit 200000 20000
```

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing [**vrf** *vrf-name*] [**distributed**]

no ip multicast-routing [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
distributed	(Optional) Enables Multicast Distributed Switching (MDS).

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the **no** form of this command now disables IP multicast routing on the Multicast Multilayer Switching (MMLS) route processor (RP) and purges all multicast MLS cache entries on the MMLS-SE.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.

Examples

The following example enables IP multicast routing:

```
ip multicast-routing
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim accept-register

To configure a candidate rendezvous point (RP) router to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

no ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
list *access-list*	Defines the extended access list number or name.
route-map *map-name*	Defines the route map.

Defaults

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

Examples

The following example shows how to restrict the RP from allowing sources in the Source Specific Multicast (SSM) range of addresses to register with the RP. These statements need to be configured only on the RP.

```
ip pim accept-register list no-ssm-range

ip access-list extended no-ssm-range
 deny ip any 232.0.0.0 0.255.255.255
 permit ip any any
```

ip pim accept-rp

To configure a router to accept join or prune messages destined for a specified rendezvous point (RP) and for a specific list of groups, use the **ip pim accept-rp** command in global configuration mode. To remove that check, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address* | **auto-rp**} [*access-list*]

no ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address* | **auto-rp**} [*access-list*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rp-address	RP address of the RP allowed to send join messages to groups in the range specified by the group access list.
auto-rp	Join and register messages are accepted only for RPs that are in the Auto-RP cache.
access-list	(Optional) Access list number or name that defines which groups are subject to the check.

Defaults

Command is disabled, so all join messages and prune messages are processed.

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command causes the router to accept only (*, G) join messages destined for the specified RP address. Additionally, the group address must be in the range specified by the access list.

When the *rp-address* argument is one of the addresses of the system, the system will be the RP only for the specified group range specified by the access list. When the group address is not in the group range, the RP will not accept join or register messages and will respond immediately to register messages with register-stop messages.

Examples

The following example states that the router will accept join or prune messages destined for the RP at address 172.17.1.1 for the multicast group 224.2.2.2:

```
ip pim accept-rp 172.17.1.1 3
access-list 3 permit 224.2.2.2
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

ip pim bidir-enable

To enable bidirectional Protocol Independent Multicast (bidir-PIM), use the **ip pim bidir-enable** command in global configuration mode. To disable bidir-PIM, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bidir-enable**

no ip pim [**vrf** *vrf-name*] **bidir-enable**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

Command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Bidir-PIM is disabled by default to ensure complete backward compatibility when upgrading a router to Cisco IOS Release 12.0(18)ST or a later release.

When bidir-PIM is disabled, the router will behave similarly to a router without bidir-PIM support. The following conditions will apply:

- PIM hello messages sent by the router will not contain the bidirectional mode option.
- The router will not send designated forwarder (DF) election messages and will ignore DF election messages it receives.
- The **ip pim rp-address**, **ip pim send-rp-announce**, and **ip pim rp-candidate** global configuration commands will be treated as follows:
  - If these commands are configured when bidir-PIM is disabled, bidirectional mode will not be a configuration option.
  - If these commands are configured with the bidirectional mode option when bidir-PIM is enabled and then bidir-PIM is disabled, these commands will be removed from the command-line interface (CLI). In this situation, these commands must be configured again with the bidirectional mode option when bidir-PIM is reenabled.
- The **df** keyword for the **show ip pim interface** EXEC command and **debug ip pim** privileged EXEC command is not supported.

Examples

The following example shows how to configure a rendezvous point (RP) for both sparse mode and bidirectional mode groups: 224/8 and 227/8 are bidirectional groups, 226/8 is sparse mode, and 225/8 is dense mode. 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 such that the other routers in the PIM domain can receive Auto-RP announcements and communicate with the RP.

```
ip multicast-routing !Enable IP multicast routing
ip pim bidir-enable  !Enable bidir-PIM
!
interface loopback 0
description One Loopback adddress for this routers Bidir Mode RP function
ip address 10.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface loopback 1
 description One Loopback adddress for this routers Sparse Mode RP function
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-dense-mode

ip pim send-rp-announce Loopback0 scope 10 group-list 45 bidir
ip pim send-rp-announce Loopback1 scope 10 group-list 46
ip pim send-rp-discovery scope 10

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 45 deny   225.0.0.0 0.255.255.255

access-list 46 permit 226.0.0.0 0.255.255.255
```

Related Commands

Command	Description
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
ip pm send-rp-announce	Uses Auto-RP to configure for which groups the router is willing to act as RP.

ip pim bsr-candidate

To configure the router to announce its candidacy as a bootstrap router (BSR), use the **ip pim bsr-candidate** command in global configuration mode. To remove this router as a candidate for being a bootstrap router, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority*]

no ip pim [**vrf** *vrf-name*] **bsr-candidate**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type *interface-number*	Interface type and number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with Protocol Independent Multicast (PIM).
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the 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. This fact allows you to get one RP for multiple groups.
priority	(Optional) Integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

Defaults

Command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command causes the router to send bootstrap messages to all its PIM neighbors, with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is the same or higher address, it caches the current address and forwards the bootstrap message. Otherwise, it drops the bootstrap message.

This router continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good candidate BSR.

Examples

The following example configures the IP address of the router on Ethernet interface 0 to be a candidate BSR with priority of 10:

```
ip pim bsr-candidate ethernet 0 10
```

Related Commands

Command	Description
ip pim border	Configures the interface to be the PIM domain border.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
ip pim send-rp-discovery	Configures the router to be an RP-mapping agent.
show ip pim bsr	Displays the BSR information.
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.

ip pim register-rate-limit

To set a limit on the maximum number of Protocol Independent Multicast sparse mode (PIM-SM) register messages sent per second for each (S, G) routing entry, use the **ip pim register-rate-limit** command in global configuration mode. To disable this limit, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **register-rate-limit** *rate*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rate	Maximum number of register messages sent per second by the router. If no limit is defined, the router will not limit the rate of register messages sent.

Defaults

No limit is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use this command to limit the number of register messages that the designated router (DR) will allow for each (S, G) entry. Enabling this command will limit the load on the DR and RP at the expense of dropping those register messages that exceed the set limit. Receivers may experience data packet loss within the first second in which register messages are sent from bursty sources.

If the **ip pim dense-mode proxy-register** command is configured, then the **ip pim register-rate-limit** command must be configured because of the potentially large number of sources from the dense mode area that may send data into the sparse mode region (and thus need registering in the border router).

This command applies only to sparse mode (S, G) multicast routing entries.

Examples

The following example shows how to configure the **ip pim register-rate-limit** command with a maximum rate of two register messages per second:

```
ip pim register-rate-limit 2
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim register-source

To configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP), use the **ip pim register-source** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **register-source** *interface-type interface-number*

no ip pim [**vrf** *vrf-name*] **register-source**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and interface number that identify the IP source address of a register message.

Defaults

By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message.

Command Modes

Global configuration

Command History

Release	Modification
12.0(8)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command is required only when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation may occur if the source address is filtered such that packets sent to it will not be forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address will fail to reach the DR, resulting in Protocol Independent Multicast sparse mode (PIM-SM) protocol failures.

If no IP source address is configured or if the configured source address is not in service, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of the register message. Therefore, we recommend using a loopback interface with an IP address that is uniquely routed throughout the PIM-SM domain.

Examples

The following example shows how to configure the IP source address of the register message to the loopback 3 interface of a DR:

```
ip pim register-source loopback 3
```

ip pim rp-announce-filter

To filter incoming Auto-RP announcement messages coming from the rendezvous point (RP), use the **ip pim rp-announce-filter** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-announce-filter rp-list** *access-list* **group-list** *access-list*

no ip pim [**vrf** *vrf-name*] **rp-announce-filter rp-list** *access-list* **group-list** *access-list*

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rp-list *access-list*	Number or name of a standard access list of RP addresses that are allowable for the group ranges supplied in the **group-list** *access-list* combination.
group-list *access-list*	Number or name of a standard access list that describes the multicast groups the RPs serve.

Defaults

All RP announcements are accepted.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Configure this command on the Protocol Independent Multicast (PIM) RP mapping agent. We recommend that if you use more than one RP mapping agent, make the filters among them consistent so that there are no conflicts in mapping state when the announcing agent goes down.

Examples

The following example configures the router to accept RP announcements from RPs in access list 1 for group ranges described in access list 2:

```
ip pim rp-announce-filter rp-list 1 group-list 2
access-list 1 permit 10.0.0.1
access-list 1 permit 10.0.0.2
access-list 2 permit 224.0.0.0 192.168.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

ip pim rp-candidate

To configure the router to advertise itself as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP) to the bootstrap router (BSR), use the **ip pim rp-candidate** command in global configuration mode. To remove this router as an RP candidate, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-type interface-number* [**group-list** *access-list*] [**bidir**]

no ip pim [**vrf** *vrf-name*] **rp-candidate**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	IP address associated with this interface type and number is advertised as a candidate RP address.
group-list *access-list*	(Optional) Standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
bidir	(Optional) Indicates that the multicast groups specified by the *access-list* argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in PIM sparse mode.

Defaults

Command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(2)T	The **bidir** keyword was added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command causes the router to send a PIM Version 2 message advertising itself as a candidate RP to the BSR. The addresses allowed by the access list, together with the router identified by the type and number, constitute the RP and its range of addresses for which it is responsible.

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good candidate RP.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using the PIM Version 2 BSR mechanism to distribute group-to-RP mappings. Other options are as follows:

- If you are using Auto-RP to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim send-rp-announce** command.
- If you are not distributing group-to-RP mappings using either Auto-RP or the PIM Version 2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

Examples

The following example configures the router to advertise itself as a candidate RP to the BSR in its PIM domain. Standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Ethernet interface 2. That RP is responsible for the groups with the prefix 239.

```
ip pim rp-candidate 192.168.37.33 ethernet 2 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
```

Related Commands

Command	Description
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-announce-filter	Filters incoming Auto-RP announcement messages coming from the RP.
ip pim send-rp-announce	Uses Auto-RP to configure for which groups the router is willing to act as RP.

ip pim send-rp-announce

To use Auto-RP to configure groups for which the router will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To deconfigure this router as an RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-type interface-number* **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]

no ip pim [**vrf** *vrf-name*] **send-rp-announce**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and number that is used to define the RP address.
scope *ttl-value*	Time-to-live (TTL) value that limits the number of Auto-RP announcements.
group-list *access-list*	(Optional) Standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
interval *seconds*	(Optional) Specifies the interval between RP announcements in seconds. The total holdtime of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds.
bidir	(Optional) Indicates that the multicast groups specified by the *access-list* argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in Protocol Independent Multicast sparse mode (PIM-SM).

Defaults

Auto-RP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(2)T	The following keywords and argument were added: • **interval** *seconds* • **bidir**
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use this command in the router you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using Auto-RP to distribute group-to-RP mappings. Other options are as follows:

- If you are using the PIM Version 2 bootstrap router (PIMv2 BSR) mechanism to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim rp-candidate** command.
- If you are not distributing group-to-RP mappings using either Auto-RP or the PIMv2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

Examples

The following example sends RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as RP is the IP address associated with Ethernet interface 0. Access list 5 describes the groups for which this router serves as RP.

```
ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.

ip pim send-rp-discovery

To configure the router to be an rendezvous point (RP) mapping agent, use the **ip pim send-rp-discovery** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value*

no ip pim [**vrf** *vrf-name*] **send-rp-discovery**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	(Optional) Interface type and number that is used to define the RP mapping agent address.
scope *ttl-value*	Time-to-live (TTL) value in the IP header that keeps the discovery messages within this number of hops.

Defaults

The router is not an RP mapping agent.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Configure this command on the router designated as an RP mapping agent. Specify a TTL large enough to cover your Protocol Independent Multicast (PIM) domain.

When Auto-RP is used, the following steps occur:

1. The RP mapping agent listens on well-known group address CISCO-RP-ANNOUNCE (224.0.1.39), which candidate RPs send to.
2. The RP mapping agent sends RP-to-group mappings in an Auto-RP RP discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40). The TTL value limits how many hops the message can take.
3. PIM designated routers listen to this group and use the RPs they learn about from the discovery message.

Examples

The following example limits Auto-RP RP discovery messages to 20 hops:

```
ip pim send-rp-discovery scope 20
```

ip pim spt-threshold

To configure when a Protocol Independent Multicast (PIM) leaf router should join the shortest path source tree for the specified group, use the **ip pim spt-threshold** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
kbps	Traffic rate (in kbps).
infinity	Causes all sources for the specified group to use the shared tree.
group-list *access-list*	(Optional) Indicates which groups the threshold applies to. Must be an IP standard access list number or name. If the value is 0 or is omitted, the threshold applies to all groups.

Defaults

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

If a source sends at a rate greater than or equal to traffic rate (the *kbps* value), a PIM join message is triggered toward the source to construct a source tree.

If the **infinity** keyword is specified, all sources for the specified group will use the shared tree. Specifying a group list access list indicates the groups to which the threshold applies.

If the traffic rate from the source drops below the threshold traffic rate, the leaf router will, after some amount of time, switch back to the shared tree and send a prune message toward the source.

Examples

The following example sets a threshold of 4 kbps, above which traffic to a group from a source will cause the router to switch to the shortest path tree to that source:

```
ip pim spt-threshold 4
```

ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **ssm** {**default** | **range** *access-list*}

no ip pim [**vrf** *vrf-name*] **ssm**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
default	Defines the SSM range access list to 232/8.
range *access-list*	Standard IP access list number or name defining the SSM range.

Defaults

Command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.

Examples

The following example shows how to configure SSM service for the IP address range defined by access list 4:

```
access-list 4 permit 224.2.151.141
ip pim ssm range 4
```

Related Commands

Command	Description
ip igmp v3lite	Enables the acceptance and processing of IGMP v3lite membership reports on an interface.
ip urd	Enables interception of TCP packets sent to the reserved URD port 659 on an interface and processing of URD channel subscription reports.

ip pim state-refresh disable

To disable the processing and forwarding of PIM dense mode state refresh control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh disable** command in global configuration mode. To reenable the processing and forwarding of PIM dense mode state refresh control messages, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **state-refresh disable**

no ip pim [**vrf** *vrf-name*] **state-refresh disable**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

The processing and forwarding of PIM dense mode state refresh control messages is enabled on PIM routers that are running a Cisco IOS software release that supports the PIM dense mode state refresh feature.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Configuring this command removes PIM dense mode state refresh information from PIM hello messages.

Examples

The following example disables the periodic forwarding of the PIM dense mode state refresh control message down a source-based IP multicast distribution tree:

```
ip pim state-refresh disable
```

Related Commands

Command	Description
ip pim state-refresh origination-interval	Configures the origination of and the interval for the PIM dense mode state refresh control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

mdt data

To configure the multicast group address range for data multicast distribution tree (MDT) groups, use the **mdt data** command in VRF configuration mode. To disable this function, use the **no** form of this command.

mdt data *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

no mdt data *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

Syntax Description

group-address-range	Multicast group address range. The range is from 224.0.0.1 to 239.255.255.255.
wildcard-bits	Wildcard bits to be applied to the multicast group address range.
threshold *threshold-value*	(Optional) Defines the bandwidth threshold value. The range is from 1 through 4294967.
list *access-list*	(Optional) Defines the access list name or number.

Defaults

Disabled

Command Modes

VRF configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

A data MDT group can include a maximum of 256 multicast groups per VPN. Multicast groups used to create the data MDT group are dynamically chosen from a pool of configured IP addresses.

This command configures a range of alternative multicast destination addresses for the tunnel header. The destination address chosen depends on the traffic profile (that is, the source and destination match the specified access list and the rate of the traffic has exceeded the bandwidth threshhold value).

Examples

In the following example, Protocol Independent Multicast (PIM) source-specific mode (SSM) is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only the Auto-RP announcements are accepted.

```
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
ip pim ssm default
ip pim vrf red accept-rp auto-rp
```

Related Commands

Command	Description
mdt default	Configures a default MDT group for a VPN VRF.

mdt default

To configure a default multicast distribution tree (MDT) group for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **mdt default** command in VRF configuration mode. To disable this function, use the **no** form of this command.

mdt default *group-address*

no mdt default *group-address*

Syntax Description

group-address	IP address of the default MDT group. This address serves as an identifier for the community in that provider-edge (PE) routers configured with the same group address become members of the group, allowing them to receive packets sent by each other.

Defaults

Disabled

Command Modes

VRF configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

The default MDT group must be the same group configured on all PE routers that belong to the same VPN.

If Source Specific Multicast (SSM) is used as the protocol for the default MDT, the source IP address will be the address used to source the Border Gateway Protocol (BGP) sessions.

A tunnel interface is created as a result of this command. By default, the destination address of the tunnel header is the *group-address* argument.

Examples

In the following example, Protocol Independent Multicast (PIM) source-specific mode (SSM) is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only the Auto-RP announcements are accepted.

```
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
ip pim ssm default
ip pim vrf red accept-rp auto-rp
```

Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.

mdt log-reuse

To enable the recording of data MDT reuse, use the **mdt log-reuse** command in VRF configuration mode. To disable this function, use the **no** form of this command.

mdt log-reuse

no mdt log-reuse

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VRF configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

The **mdt log-reuse** command generates a syslog message whenever a data MDT is reused.

Examples

In the following example, the MDT log reuse function is enabled.

```
mdt log-resue
```

Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.
mdt default	Configures a default MDT group for a VPN VRF.

show ip hardware-mdfs mgid

To display the mapping between a multicast group ID (MGID) and the information stored in the line card hardware memory, use the **show ip hardware-mdfs mgid** command in user EXEC or privileged EXEC mode.

execute-on slot *slot-number* **show ip hardware-mdfs mgid** *mgid-number* {**both-tables** | **encap-string** | **path-bits**}

Syntax Description

execute-on slot	Executes this **show** command on a particular line card.
slot-number	Slot number of the line card on which to execute this command.
mgid-number	MGID number about which to display mapping information. **Note** Use the **show ip mds mgid-table** command to display the MGID numbers for a line card.
both-tables	Displays the mapping between the MGID and the VPN routing amd forwarding instance (VRF) decapsulation and encapsulation information.
encap-string	Displays the mapping between the MGID and the encapsulation string stored in the line card hardware memory.
path-bits	Displays the VRF information required for forwarding multicast packets in a VRF that is mapped to a particular MGID and stored in the line card hardware memory.

Defaults

No default behaviors or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.

Usage Guidelines

Use this command with the **show ip mds mgid-table** command to verify that all entries in the Cisco IOS software table have corresponding entries in the line card hardware table.

You can execute this command on Engine 3 and Engine 5 line cards, because FastPath forwarding of multicast VPN (MVPN) packets upon encapsulation and decapsulation is supported on Engine 3 and Engine 5. Use this command to display information about the hardware memory used for MVPN.

Note This command is available only on Cisco 12000 series routers.

Examples

The following is sample output from the **show ip hardware-mdfs mgid** command for a line card in slot 2:

```
Router# execute-on slot 2 show ip hardware-mdfs mgid 125 both-tables

========= Line Card (Slot 2) =========
  0x7D:vrf tbl base=0x20030C00, vrfx=y vrf0=n
  0x7D:encap = 00066830000000007819A0C0000000000000007D00000002
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip hardware-mdfs mgid Field Descriptions

Field	Description
vrf tbl base	Memory location of the Mtrie base in the hardware corresponding to the VRF that maps to the MGID. This information is used by the provider edge (PE) router during decapsulation.
vrfx	Boolean indicator that a core-facing interface of the VRF, mapped by the MGID provided, is present on the line card. The VRFx indicator is used by the PE router performing decapsulation.
vrf0	Boolean indicator that a customer-facing interface on the VRF, mapped by the MGID, is present on the line card. This information is used by the PE router during decapsulation.
encap	Generic routing encapsulation (GRE) header to be prepended to the packet header. The encapsulation string is used by the PE router performing encapsulation.

Related Commands

Command	Description
show ip mds mgid-table	Displays the information stored in the MGID mapping table of a line card.

show ip igmp groups

To display the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show ip igmp groups** command in EXEC mode.

show ip igmp [**vrf** *vrf-name*] **groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-name	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted-decimal notation.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
detail	(Optional) Provides a detailed description of the sources known through IGMP Version 3 (IGMPv3), IGMP v3lite, or URL Rendezvous Directory (URD).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	Fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.
12.1(5)T	The **detail** keyword was added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip igmp groups** command displays by group address, interface type, and interface number all directly connected multicast groups.

Examples

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

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface         Uptime      Expires     Last Reporter
239.255.255.254  Ethernet3/1       1w0d        00:02:19    172.21.200.159
224.0.1.40       Ethernet3/1       1w0d        00:02:15    172.21.200.1
224.0.1.40       Ethernet3/3       1w0d        never       172.16.214.251
224.0.1.1        Ethernet3/1       1w0d        00:02:11    172.21.200.11
```

```
224.9.9.2          Ethernet3/1        1w0d         00:02:10     172.21.200.155
232.1.1.1          Ethernet3/1        5d21h        stopped      172.21.200.206
```

The following is sample output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword:

```
Router# show ip igmp groups 232.1.1.1 detail

Interface:       Ethernet3/2
Group:           232.1.1.1
Uptime:          01:58:28
Group mode:      INCLUDE
Last reporter:   10.0.119.133
CSR Grp Exp:     00:02:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote)
  Source Address   Uptime    v3 Exp    CSR Exp   Fwd  Flags
  172.16.214.1     01:58:28  stopped   00:02:31  Yes  C
```

Table 9 describes the significant fields shown in the displays.

Table 9 show ip igmp groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long (in weeks, days, hours, minutes, and seconds) this multicast group has been known.
Expires	How long (in hours, minutes, and seconds) until the entry expires. If an entry expires, then the entry will (for a short period) show the word “now” before it is removed. The word “never” indicates that the entry will not time out, because a local receiver is on this router for this entry. The word “stopped” indicates that timing out of this entry is not determined by this expire timer. If the router is in INCLUDE mode for a group, then the whole group entry will time out after the last source entry has timed out (unless the mode is changed to EXCLUDE mode before it times out).
Last Reporter	Last host to report being a member of the multicast group. Both IGMP v3lite and URD require a v2-report.
Group mode:	Can be either INCLUDE or EXCLUDE. The group mode is based on the type of membership reports received on the interface for the group. In the output for the **show ip igmp groups detail** command, the EXCLUDE mode also shows the “Expires:” field for the group entry (not shown in the output).
CSR Grp Exp	This field is shown for multicast groups in the Source Specific Multicast (SSM) range. It indicates the time (in hours, minutes, and seconds) since the last received group membership report was received. Cisco IOS software needs to use these reports for the operation of URD and IGMP v3lite, but they do not indicate group membership by themselves.
Group source list:	Provides details of which sources have been requested by the multicast group.

Table 9 show ip igmp groups Field Descriptions (continued)

Field	Description
Source Address	IP address of the source.
Uptime	Indicates the time since the source state was created.
v3 Exp	Indicates the time (in hours, minutes, and seconds) until the membership for the source will time out according to IGMP operations. The word “stopped” is shown if no member uses IGMPv3 (but only IGMP v3lite or URD).
CSR Exp	Indicates the time (in hours, minutes, and seconds) until the membership for the source will time out according to IGMP v3lite or URD reports. The word “stopped” is shown if members use only IGMPv3.
Fwd	Indicates whether the router is forwarding multicast traffic due to this entry.
Flags	Information about the entry. The Remote flag indicates that an IGMPv3 report has been received by this source. The C flag indicates that an IGMP v3lite or URD report was received by this source. The U flag indicates that a URD report was received for this source.

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.

show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface** command in EXEC mode.

show ip igmp [**vrf** *vrf-name*] **interface** [*type number*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
type	(Optional) Interface type.
number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

If you omit the optional arguments, the **show ip igmp interface** command displays information about all interfaces.

This command also displays information about dynamically learned Distance Vector Multicast Routing Protocol (DVMRP) routers on the interface.

Examples

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

```
Router# show ip igmp interface

Ethernet0 is up, line protocol is up
  Internet address is 192.168.37.6, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 192.168.37.33
  No multicast groups joined
Ethernet1 is up, line protocol is up
  Internet address is 192.168.36.129, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 192.168.36.131
  Multicast groups joined: 225.2.2.2 226.2.2.2
```

```
Tunnel0 is up, line protocol is up
  Internet address is 10.1.37.2, subnet mask is 255.255.0.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  No multicast groups joined
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip igmp interface Field Descriptions

Field	Description
Ethernet0 is up, line protocol is up	Interface type, number, and status.
Internet address is..., subnet mask is...	Internet address of the interface and subnet mask being applied to the interface, as specified with the **ip address** command.
IGMP is enabled on interface	Indicates whether IGMP has been enabled on the interface with the **ip pim** command.
IGMP query interval is 60 seconds	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages, as specified with the **ip igmp query-interval** command.
Inbound IGMP access group is not set	Indicates whether an IGMP access group has been configured with the **ip igmp access-group** command.
Multicast routing is enabled on interface	Indicates whether multicast routing has been enabled on the interface with the **ip pim** command.
Multicast TTL threshold is 0	Packet time-to-threshold, as specified with the **ip multicast ttl-threshold** command.
Multicast designated router (DR) is...	IP address of the designated router for this LAN segment (subnet).
No multicast groups joined	Indicates whether this interface is a member of any multicast groups and, if so, lists the IP addresses of the groups.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip igmp access-group	Controls the multicast groups that hosts on the subnet serviced by an interface can join.
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.
ip multicast ttl-threshold	Configures the TTL threshold of packets being forwarded out an interface.
ip pim	Enables PIM on an interface.

show ip mcache

To display the contents of the IP fast-switching cache, use the **show ip mcache** command in EXEC mode.

show ip mcache [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	(Optional) Displays the fast-switching cache for the single group. Can be either a Class D IP address or a Domain Name System (DNS) name.
source-address | *source-name*	(Optional) If the source address or name is also specified, displays a single multicast cache entry. Can be either a unicast IP address or a DNS name.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following is sample output from the **show ip mcache** command. This entry shows a specific source (wrn-source 226.62.246.73) sending to the World Radio Network group (224.2.143.24).

```
Router> show ip mcache wrn wrn-source

IP Multicast Fast-Switching Cache
(226.62.246.73/32, 224.2.143.24), Fddi0, Last used: 00:00:00
  Ethernet0       MAC Header: 01005E028F1800000C1883D30800
  Ethernet1       MAC Header: 01005E028F1800000C1883D60800
  Ethernet2       MAC Header: 01005E028F1800000C1883D40800
  Ethernet3       MAC Header: 01005E028F1800000C1883D70800
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip mcache Field Descriptions

Field	Description
226.62.246.73	Source address.
224.2.143.24	Destination address.
Fddi0	Incoming or expected interface on which the packet should be received.

Table 11 show ip mcache Field Descriptions (continued)

Field	Description
Last used:	Latest time the entry was accessed for a packet that was successfully fast switched. The word "Semi-fast" indicates that the first part of the outgoing interface list is fast switched and the rest of the list is process level switched.
Ethernet0 MAC Header:	Outgoing interface list and respective MAC header that is used when rewriting the packet for output. If the interface is a tunnel, the MAC header will show the real next hop MAC header and then, in parentheses, the real interface name.

show ip mds interface

To display Multicast Distributed Switching (MDS) information for all the interfaces on the line card, use the **show ip mds interface** command in EXEC mode.

show ip mds interface [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

The following is sample output from the **show ip mds interface** command.

```
Router# show ip mds interface

Interface                SW-Index  HW-Index  HW IDB      FS Vector   VRF
Ethernet1/0/0            2         1         0x60C2DB40  0x602FB7A4 default
Ethernet1/0/1            3         2         0x60C32280  0x603D52B8 default
Ethernet1/0/2            4         3         0x60C35E40  0x602FB7A4 default
Ethernet1/0/3            5         4         0x60C39E60  0x603D52B8 default
Ethernet1/0/4            6         5         0x60C3D780  0x602FB7A4 default
Ethernet1/0/5            7         6         0x60C41140  0x602FB7A4 default
Ethernet1/0/6            8         7         0x60C453A0  0x602FB7A4 default
Ethernet1/0/7            9         8         0x60C48DC0  0x602FB7A4 default
POS2/0/0                 10        9         0x0                    default
POS3/0/0                 11        10        0x0                    default
Virtual-Access1          13        11        0x0                    default
Loopback0                14        12        0x0                    default
Tunnel0                  15        23        0x61C2E480  0x603D52B8  vrf1
Tunnel1                  16        24        0x61C267E0  0x603D52B8  vrf2
Ethernet1/0/3.1          17        4         0x60C39E60  0x603D52B8  vrf1
Ethernet1/0/3.2          18        4         0x60C39E60  0x603D52B8  vrf2
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip mds interface Field Descriptions

Field	Description
Interface	The specified interface.
SW-Index	Software index.
HW-Index	Hardware index.

Table 12 show ip mds interface Field Descriptions (continued)

Field	Description
HW IDB	Hardware interface description block.
VRF	VPN routing/forwarding instance.

show ip mds mgid-table

To display the information stored in the multicast group ID (MGID) mapping table of a line card, use the **show ip mds mgid-table** command in user EXEC or privileged EXEC mode.

execute-on slot *slot-number* **show ip mds mgid-table**

Syntax Description

execute-on slot	Executes this **show** command on a particular line card.
slot-number	Slot number of the line card on which to execute this command.

Defaults

No default behaviors or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.

Usage Guidelines

Use this command to display the mapping table stored in the line card CPU memory. This table displays, for each global MGID, the VPN routing and forwarding instance (VRF), used for the decapsulation of the generic routing encapsulation (GRE) header, and the encapsulation string, used for encapsulation of the GRE header.

Note This command is available only on Cisco 12000 series routers.

Examples

The following is sample output from the **show ip mds mgid-table** command executed on the line card in slot 2:

```
Router# execute-on slot 2 show ip mds mgid-table

========= Line Card (Slot 2) =========

MDFS MGID Table Entries

 MGID    ID  VRFx VRF0 Encap String
 ------- --- ---- ---- ------------
 0x0007C 1   Y    N    45000001 00000000 FF2F0000 02020204 E8000001 00000800
 0x0007D 1   Y    N
 0x0007E 1   Y    N
 0x00080 1   Y    N    42424242 42424242 42424242 42424242 42424242 42424242
```

Table 13 describes the significant fields shown in the display.

Table 13 show ip mds mgid-table Field Descriptions

Field	Description
MGID	Unique multicast group identifier displayed in hexadecimal format. The MGID is used by the provider edge (PE) router performing decapsulation.
ID	Table identifier corresponding to the VRF to which the MGID maps in order to perform the second multicast lookup. The ID is used by the PE router performing decapsulation.
VRFx	Boolean indicator that a customer-facing interface of the VRF, mapped by the MGID provided, is present on the line card. The VRFx indicator is used by the PE router performing decapsulation.
VRF0	Boolean indicator that a core-facing interface is present on this line card. The VRF0 indicator is used by the PE router performing decapsulation.
Encap String	GRE header to be prepended to the packet header. The encapsulation string is used by the PE router performing encapsulation.

Related Commands

Command	Description
show ip hardware-mdfs mgid	Displays the mapping between an MGID and the information stored in the line card hardware memory.

show ip mpacket

To display the contents of the circular cache-header buffer, use the **show ip mpacket** command in EXEC mode.

show ip mpacket [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*] [**detail**]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	(Optional) Displays cache headers matching the specified group address or group name.
source-address | *source-name*	(Optional) Displays cache headers matching the specified source address or source name.
detail	(Optional) In addition to the summary information, displays the rest of the IP header fields on an additional line, plus the first 8 bytes after the IP header (usually the User Datagram Protocol [UDP] port numbers).

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command is applicable only when the **ip multicast cache-headers** command is in effect.

Each time this command is entered, a new buffer is allocated. The summary display (when the **detail** keyword is omitted) shows the IP packet identifier, time-to-live (TTL) value, source and destination IP addresses, and a local time stamp when the packet was received.

The two arguments and one keyword can be used in the same command in any combination.

Examples

The following is sample output from the **show ip mpacket** command with the *group-name* argument:

```
Router # show ip mpacket smallgroup

IP Multicast Header Cache - entry count:6, next index: 7
Key: id/ttl timestamp (name) source group

D782/117 206416.908 (ABC-xy.company.com) 192.168.228.10 224.5.6.7
7302/113 206417.908 (school.edu) 147.12.2.17 224.5.6.7
6CB2/114 206417.412 (MSSRS.company.com) 154.2.19.40 224.5.6.7
D782/117 206417.868 (ABC-xy.company.com) 192.168.228.10 224.5.6.7
E2E9/123 206418.488 (Newman.com) 211.1.8.10 224.5.6.7
1CA7/127 206418.544 (teller.company.com) 192.168.6.10 224.5.6.7
```

Table 14 describes the significant fields shown in the display.

Table 14 show ip mpacket Field Descriptions

Field	Description
entry count	Number of packets cached (one packet for each line in the display). The cache has lines numbered from 0 to 1024.
next index	The index for the next element in the cache.
id	Identification number of the IP packet.
ttl	Current TTL of the packet.
timestamp	Time-stamp sequence number of the packet.
(name)	Domain Name System (DNS) name of the source sending to the group. Name appears in parentheses.
source	IP address of the source sending to the group.
group	Multicast group address to which the packet is sent. In this example, the group address is the group name smallgroup.

Related Commands

Command	Description
ip multicast cache-headers	Allocates a circular buffer to store IP multicast packet headers that the router receives.

show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** command in EXEC mode.

show ip mroute [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	(Optional) IP address or name multicast group as defined in the Domain Name System (DNS) hosts table.
source-address | *source-name*	(Optional) IP address or name of a multicast source.
interface-type interface-number	(Optional) Interface type and number.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bytes per second.
active *kbps*	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at the *kbps* value or higher. The *kbps* argument defaults to 4 kbps.

Defaults

The **show ip mroute** command displays all groups and sources.

The **show ip mroute active** command displays all sources sending at a rate greater than or equal to 4 kbps.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	The U, s, and I flags for Source Specific Multicast (SSM) were introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP multicast routing table.

The Cisco IOS software populates the multicast routing table by creating (S, G) entries from (*, G) entries. The asterisk (*) refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Examples

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This output displays the contents of the IP multicast routing table for the multicast group named cbone-audio.

```
Router# show ip mroute cbone-audio

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 224.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 224.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(192.168.37.100/32, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

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, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set
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:
    Ethernet0, 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:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

The following is sample output from the **show ip mroute** command that shows the virtual circuit descriptor (VCD) value, because an ATM interface with Protocol Independent Multicast (PIM) multipoint signaling is enabled:

```
Router# show ip mroute 224.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(*, 224.1.1.1), 00:03:57/00:02:54, RP 130.4.101.1, flags: SJ
  Incoming interface: Null, RPF nbr 224.0.0.0224.0.0.0
  Outgoing interface list:
    ATM0/0, VCD 14, Forward/Sparse, 00:03:57/00:02:53
```

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

```
Router# show ip mroute summary

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.255.255.255), 2d16h/00:02:30, RP 172.16.10.13, flags: SJPC

(*, 224.2.127.253), 00:58:18/00:02:00, RP 172.16.10.13, flags: SJC

(*, 224.1.127.255), 00:58:21/00:02:03, RP 172.16.10.13, flags: SJC

(*, 224.2.127.254), 2d16h/00:00:00, RP 172.16.10.13, flags: SJCL
  (172.16.160.67/32, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
  (172.16.244.217/32, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
  (172.16.8.33/32, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
  (172.16.2.62/32, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
  (172.16.8.3/32, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
  (172.16.60.189/32, 224.2.127.254), 00:03:47/00:00:46, flags: CLJT
```

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

```
Router# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

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

```
Router# show ip mroute count

IP Multicast Statistics - Group count: 8, Average sources per group: 9.87
Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Group: 224.255.255.255, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.2.127.253, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.1.127.255, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.2.127.254, Source count: 9, Group pkt count: 14
```

```
  RP-tree: 0/0/0/0
  Source: 172.16.6.9/32, 2/0/796/0
  Source: 172.16.131.87/32, 1/0/616/0
  Source: 172.16.51.58/32, 1/0/412/0
  Source: 172.16.8.33/32, 1/0/936/0
  Source: 172.16.2.62/32, 1/0/750/0
  Source: 172.16.8.3/32, 1/0/660/0
  Source: 192.168.28.69/32, 1/0/584/0
  Source: 172.16.60.189/32, 4/0/447/0
  Source: 192.162.119.8/32, 2/0/834/0

Group: 224.0.1.40, Source count: 1, Group pkt count: 3606
  RP-tree: 0/0/0/0
  Source: 172.16.214.50/32, 3606/0/48/0, RPF Failed: 1203

Group: 224.2.201.241, Source count: 36, Group pkt count: 54152
  RP-tree: 7/0/108/0
  Source: 10.242.36.83/32, 99/0/123/0
  Source: 10.29.1.3/32, 71/0/110/0
  Source: 172.17.160.96/32, 505/1/106/0
  Source: 172.17.163.170/32, 661/1/88/0
  Source: 172.17.31.26/32, 192/0/118/0
  Source: 172.17.111.45/32, 500/0/87/0
  Source: 172.17.33.134/32, 248/0/119/0
  Source: 172.17.7.62/32, 527/0/118/0
  Source: 172.17.32.25/32, 554/0/105/0
  Source: 172.17.32.151/32, 551/1/125/0
  Source: 172.17.156.117/32, 535/1/114/0
  Source: 172.17.225.21/32, 582/0/114/0
  Source: 172.17.142.50/32, 78/0/127/0
  Source: 172.17.50.14/32, 526/0/118/0
  Source: 172.18.0.13/32, 522/0/95/0
  Source: 172.18.52.160/32, 40839/16/920/161
  Source: 172.18.52.161/32, 476/0/97/0
  Source: 172.18.224.10/32, 456/0/113/0
  Source: 172.18.32.108/32, 9/1/112/0
```

The following is sample output from the **show ip mroute** command for a router supporting SSM services:

```
Router# show ip mroute 232.6.6.6

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 - Advertised via MSDP, U
- URD, I - Received Source Specific Host Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 232.6.6.6), 00:01:20/00:02:59, RP 224.0.0.0, flags:sSJP
  Incoming interface:Null, RPF nbr 224.0.0.0
  Outgoing interface list:Null

(10.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags:CTI
  Incoming interface:Ethernet3/3, RPF nbr 224.0.0.0
  Outgoing interface list:
    Ethernet3/1, Forward/Sparse-Dense, 00:00:36/00:02:35
```

Table 15 describes the significant fields shown in the display.

Table 15 show ip mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
B - Bidir Group	Indicates that a multicast group is operating in bidirectional mode.
s - SSM Group	Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
C - Connected	A member of the multicast group is present on the directly connected interface.
L - Local	The router itself is a member of the multicast group. Groups are joined locally by the **ip igmp join-group** command (for the configured group), the **ip sap listen** command (for the well-known session directory groups), and rendezvous point (RP) mapping (for the well-known groups 224.0.1.39 and 224.0.1.40). Locally joined groups are not fast switched.
P - Pruned	Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source.
R - RP-bit set	Indicates that the (S, G) entry is pointing toward the RP. This is typically prune state along the shared tree for a particular source.
F - Register flag	Indicates that the software is registering for a multicast source.
T - SPT-bit set	Indicates that packets have been received on the shortest path source tree.

Table 15 show ip mroute Field Descriptions (continued)

Field	Description
J - Join SPT	For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute. **Note** The router measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started. If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest path source tree when traffic from a new source is received.
M - MSDP created entry	Indicates that a (*, G) entry was learned through a Multicast Source Discovery Protocol (MSDP) peer. This flag is applicable only for an RP running MSDP.
X - Proxy Join Timer Running	Indicates that the proxy join timer is running. This flag is set only for (S, G) entries of an RP or “turnaround” router. A “turnaround” router is located at the intersection of a shared path (*, G) tree and the shortest path from the source to the RP.
A - Advertised via MSDP	Indicates that an (S, G) entry was advertised through an MSDP peer. This flag is applicable only for an RP running MSDP.
U - URD	Indicates that a URL Rendezvous Directory (URD) channel subscription report was received for the (S, G) entry.
I - Received Source Specific Host Report	Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by Internet Group Management Protocol Version 3 (IGMPv3), URD, or IGMP v3lite. This flag is set only on the designated router (DR).
Outgoing interface flags:	Provides information about the entry.
H - Hardware switched	Indicates that a Multicast Multilayer Switching (MMLS) forwarding path has been established for this entry.

Table 15 show ip mroute Field Descriptions (continued)

Field	Description
Timers:Uptime/Expires	"Uptime" indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. "Expires" indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
Interface state:	Indicates the state of the incoming or outgoing interface.
Interface	Indicates the type and number of the interface listed in the incoming or outgoing interface list.
Next-Hop or VCD	"Next-hop" specifies the IP address of the downstream neighbor. "VCD" specifies the virtual circuit descriptor number. "VCD0" means the group is using the static map virtual circuit.
State/Mode	"State" indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time to live (TTL) threshold. "Mode" indicates whether the interface is operating in dense, sparse, or sparse-dense mode.
(*, 224.0.255.1) and (192.168.37.100/32, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S, G) or "S comma G" entries. (*, G) entries are used to build (S, G) entries.
RP	Address of the RP router. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.
flags:	Information about the entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor or RPF nbr	IP address of the upstream router to the source. Tunneling indicates that this router is sending data to the RP encapsulated in register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used.
Outgoing interface list:	Interfaces through which packets will be forwarded. When the **ip pim nbma-mode** command is enabled on the interface, the IP address of the Protocol Independent Multicast (PIM) neighbor is also displayed.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip pim	Enables PIM on an interface.
ip pim ssm	Defines the SSM range of IP multicast addresses.

show ip msdp count

To display the number of sources and groups originated in Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages and the number of SA messages from an MSDP peer in the SA cache, use the **show ip msdp count** command in EXEC mode.

show ip msdp [**vrf** *vrf-name*] **count** [*as-number*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
as-number	(Optional) Displays the number of sources and groups originated in SA messages from the specified autonomous system number.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the number of SA messages from each MSDP peer in the SA cache.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The **ip msdp cache-sa-state** command must be configured for this command to have any output.

Examples

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

```
Router# show ip msdp count

SA State per Peer Counters, <Peer>: <# SA learned>
 224.135.250.116: 24
 172.16.240.253: 3964
 172.16.253.19: 10
 172.16.170.110: 11

SA State per ASN Counters, <asn>: <# sources>/<# groups>
 Total entries: 4009
 ?: 192/98, 9: 1/1, 14: 107/57, 17: 7/5
 18: 4/3, 25: 23/17, 26: 39/27, 27: 2/2
 32: 19/7, 38: 2/1, 52: 4/4, 57: 1/1
 68: 4/4, 73: 12/8, 81: 19/1, 87: 9/6
  .
  .
  .
```

Table 16 describes the significant fields shown in the display.

Table 16 show ip msdp count Field Descriptions

Field	Description
224.135.250.116: 24	MSDP peer with IP address 224.135.250.116: 24 SA messages from the MSDP peer in the SA cache.
Total entries	Total number of SA entries in the SA cache.
9: 1/1	Autonomous system 9: 1 source/1 group.

Related Commands

Command	Description
ip msdp cache-sa-state	Enables the router to create SA state.

show ip msdp peer

To display detailed information about the Multicast Source Discovery Protocol (MSDP) peer, use the **show ip msdp peer** command in EXEC mode.

show ip msdp [**vrf** *vrf-name*] **peer** [*peer-address* | *peer-name*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	(Optional) Domain Name System (DNS) name or IP address of the MSDP peer for which information is displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the source address (SA) message limit configured using the **ip msdp sa-limit** command.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

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

```
Router# show ip msdp peer 224.135.250.116

MSDP Peer 224.135.250.116 (rtp5-rp1.cisco.com), AS 109 (configured AS)
Description:
 Connection status:
   State: Up, Resets: 9, Connection source: Loopback2 (228.69.199.17)
   Uptime(Downtime): 1d10h, Messages sent/received: 436765/429062
   Output messages discarded: 0
   Connection and counters cleared 1w2d     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
   Sending SA-Requests to peer: disabled
 Peer ttl threshold: 0
 SAs learned from this peer: 32, SAs limit: 500
 Input queue size: 0, Output queue size: 0
```

Table 17 describes the significant fields shown in the display.

Table 17 show ip msdp peer Field Descriptions

Field	Description
MSDP Peer	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the IP address for the TCP local connection address.
Uptime(Downtime):	Days and hours the MSDP peer is up or down. If the time is less than 24 hours, it is shown in terms of hours:minutes:seconds.
Messages sent/received:	Number of SA messages sent to the MSDP peer/number of SA messages received from the MSDP peer.
SA Filtering:	Information regarding access list filtering of SA input and output, if any.
SA-Requests:	Information regarding access list filtering of SA requests, if any.
SAs learned from this peer:	Number of SA messages from the MSDP peer in the SA cache.
SAs limit:	SA message limit for this MSDP peer.

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

show ip msdp sa-cache

To display (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp sa-cache** command in EXEC mode.

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

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *source-address* | *group-name* | *source-name*	(Optional) Group address, source address, group name, or source name of the group or source about which (S, G) information is displayed. If two address or names are specified, an (S, G) entry corresponding to those addresses is displayed. If only one group address is specified, all sources for that group are displayed. If no options are specified, the entire Source-Active (SA) cache is displayed.
as-number	(Optional) Only state originated by the autonomous system number specified is displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

State is cached only if the **ip msdp cache-sa-state** command is configured.

Examples

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

```
Router# show ip msdp sa-cache

MSDP Source-Active Cache - 2398 entries
(172.16.41.33, 238.105.148.0), RP 172.16.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.16.112.8, 224.2.0.1), RP 192.168.200.65, MBGP/AS 10888, 00:03:21/00:02:38
(172.16.10.13, 227.37.32.1), RP 192.168.3.92, MBGP/AS 704, 05:22:20/00:03:32
(172.16.66.18, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.66.148, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.10.13, 227.37.32.2), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:01:31
(172.16.70.203, 224.2.236.2), RP 192.168.253.7, MBGP/AS 3582, 02:34:16/00:05:49
(172.18.42.104, 236.195.56.2), RP 192.168.3.92, MBGP/AS 704, 04:21:13/00:05:22
(172.16.10.13, 227.37.32.3), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:02:31
(172.18.15.43, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 6d09h/00:05:35
(172.18.15.111, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.21.45, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
```

```
(172.18.15.75, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.18.15.100, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.16.10.13, 227.37.32.6), RP 192.168.3.92, MBGP/AS 704, 00:45:30/00:05:31
(172.18.41.33, 224.247.228.10), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.18.222.210, 224.2.224.13), RP 192.168.3.92, MBGP/AS 704, 01:51:53/00:05:22
(172.18.41.33, 229.231.124.13), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.18.32.138, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
(172.18.75.244, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
```

Table 18 describes the significant fields shown in the display.

Table 18 show ip msdp sa-cache Field Descriptions

Field	Description
(172.16.41.33, 238.105.148.0)	The first address (source) is sending to the second address (group).
RP 172.16.3.111	Rendezvous point (RP) address in the originating domain where the SA messages started.
MBGP/AS 704	RP is in autonomous system 704 according to multiprotocol Border Gateway Protocol (BGP).
2d10h/00:05:33	The route has been cached for 2 days and 10 hours. If no SA message is received in 5 minutes and 33 seconds, the route will be removed from the SA cache.

Related Commands

Command	Description
clear ip msdp sa-cache	Clears MSDP SA cache entries.
ip msdp cache-sa-state	Enables the router to create SA state.

show ip msdp summary

To display Multicast Source Discovery Protocol (MSDP) peer status, use the **show ip msdp summary** command in EXEC mode.

show ip msdp [**vrf** *vrf-name*] **summary**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the number of SA messages from each MSDP peer in the SA cache.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Examples

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

```
Router# show ip msdp summary

MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
224.135.250.116  109   Up       1d10h    9     111   rtp5-rp1
*172.20.240.253 1239  Up       14:24:00 5     4010  sl-rp-stk
172.16.253.19    109   Up       12:36:17 5     10    shinjuku-rp1
172.16.170.110   109   Up       1d11h    9     12    ams-rp1
```

Table 19 describes the significant fields shown in the display.

Table 19 show ip msdp summary Field Descriptions

Field	Description
Peer Address	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State	State of the MSDP peer.
Uptime/Downtime	Days and hours the MSDP peer is up or down, per state shown in the previous column. If the time is less than 24 hours, it is shown in terms of hours:minutes:seconds.
SA Count	Number of SA messages from this MSDP peer in the SA cache.
Peer Name	Name of the MSDP peer.

show ip pim mdt bgp

To show detailed Border Gateway Protocol (BGP) advertisement of the route distinguisher (RD) for the multicast distribution tree (MDT) default group, use the **show ip pim mdt bgp** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **mdt bgp**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

Use this command to show detailed BGP advertisement of the RD for the MDT default group.

Examples

The following is sample output from the **show ip pim mdt bgp** command:

```
Router# show ip pim mdt bgp

MDT-default group 232.2.1.4
 rid:1.1.1.1 next_hop:1.1.1.1
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip pim mdt bgp Field Descriptions

Field	Description
MDT-default group	The MDT default groups that have been advertised to this router.
rid:10.1.1.1	The BGP router ID of the advertising router.
next_hop:10.1.1.1	The BGP next-hop address that was contained in the advertisement.

show ip pim mdt history

To provide information on data MDTs that have been reused, use the **show ip pim mdt history** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **mdt history** *interval* {*number*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interval	Interval during which data MDTs have been reused.
minutes	Length of time, in minutes, for which the interval can be configured.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

The **show ip pim mdt history** command displays the data MDTs that have been reused during the past configured interval.

Examples

The following is sample output from the **show ip pim mdt history** command with the interval configured to be 20 minutes:

```
Router# show ip pim vrf blue mdt history interval 20

   MDT-data send history for VRF - blue for the past 20 minutes

MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

Table 21 describes the significant fields shown in the display.

Table 21 show ip pim mdt history Field Descriptions

Field	Description
MDT-data group	The MDT data group for which information is being shown.
Number of reuse	The number of data MDTs that have been reused in this group.

show ip pim mdt receive

To show the data multicast distribution tree (MDT) advertisements received by a specified router, use the **show ip pim mdt receive** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **mdt receive** [**detail**]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
detail	(Optional) Provides a detailed description of the data MDT advertisements received.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

When a router wants to switch over from the default MDT to a data MDT, it advertises the VRF source, the group pair, and the global multicast address over which the traffic will be sent. If the remote router wants to receive this data, then it will join this global address multicast group.

Examples

The following is sample output from the **show ip pim mdt receive** command using the **detail** keyword for further information:

```
Router# show ip pim vrf vpn8 mdt receive detail

Joined MDT-data groups for VRF:vpn8
group:232.2.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

Table 22 describes the significant fields shown in the display.

Table 22 show ip pim mdt receive Field Descriptions

Field	Description
group:172.16.8.0	Group that caused the data MDT to be built.
source:10.0.0.100	VRF source that caused the data MDT to be built.
ref_count:13	Number of source, group pairs that are reusing this data MDT.

Table 22 show ip pim mdt receive Field Descriptions (continued)

Field	Description
OIF count:1	Number of interfaces out of which this multicast data is being forwarded.
flags:	Information about the entry. A - Candidate MSDP advertisement B - Bidir Group D - Dense C - Connected F - Register flag I - Received source-specific host report J - Join SPT L - Local M - MSDP created entry P - Pruned R - RP bit set S - Sparse s - SSM group T - SPT bit set X - Proxy join timer running U -URD Y - Joined MDT data group y - Sending to MDT data group Z - Multicast tunnel

show ip pim mdt send

To show the data multicast distribution tree (MDT) advertisements that a specified router has made, use the **show ip pim mdt send** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **mdt send**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)S	This command was introduced.

Usage Guidelines

Use this command to show the data MDT advertisements that a specified router has made.

Examples

The following is sample output from the **show ip pim mdt send** command:

```
Router# show ip pim mdt send

MDT-data send list for VRF:vpn8
  (source, group)                     MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)            232.2.8.0           1
  (10.100.8.10, 225.1.8.2)            232.2.8.1           1
  (10.100.8.10, 225.1.8.3)            232.2.8.2           1
  (10.100.8.10, 225.1.8.4)            232.2.8.3           1
  (10.100.8.10, 225.1.8.5)            232.2.8.4           1
  (10.100.8.10, 225.1.8.6)            232.2.8.5           1
  (10.100.8.10, 225.1.8.7)            232.2.8.6           1
  (10.100.8.10, 225.1.8.8)            232.2.8.7           1
  (10.100.8.10, 225.1.8.9)            232.2.8.8           1
  (10.100.8.10, 225.1.8.10)           232.2.8.9           1
```

Table 23 describes the significant fields shown in the display.

Table 23 show ip pim mdt send Field Descriptions

Field	Description
source, group	Source and group addresses that this router has switched over to data MDTs.
MDT-data group	Multicast address over which these data MDTs are being sent.
ref_count	Number of source, group pairs that are reusing this data MDT.

show ip pim bsr

To display the bootstrap router (BSR) information, use the **show ip pim bsr** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **bsr**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Examples

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

```
Router# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

Table 24 describes the significant fields shown in the display.

Table 24 show ip pim bsr Field Descriptions

Field	Description
BSR address	IP address of the BSR.
Uptime	Length of time that this router has been up, in hours, minutes, and seconds.
BSR Priority	Priority as configured in the **ip pim bsr-candidate** command.
Hash mask length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured in the **ip pim bsr-candidate** command.

Table 24 show ip pim bsr Field Descriptions (continued)

Field	Description
Next bootstrap message in	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Cand_RP_advertisement in	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.
RP	List of IP addresses of RPs.
Group acl	Standard IP access list number that defines the group prefixes that are advertised in association with the RP address. This value is configured in the **ip pim rp-candidate** command.

Related Commands

Command	Description
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.
show ip pim rp-hash	Displays which RP is being selected for a specified group.

show ip pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
type number	(Optional) Interface type and number.
df	(Optional) When bidirectional PIM (bidir-PIM) is used, displays the IP address of the elected designated forwarder (DF) for each rendezvous point (RP) of an interface.
count	(Optional) Number of packets received and sent out the interface.
rp-address	(Optional) RP IP address.
detail	(Optional) PIM details of each interface.

Defaults

If no interface is specified, all interfaces are displayed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	This command was integrated into Cisco IOS Release 11.2(11)GS.
12.0(5)T	The flag "H" was added in the output display to indicate that an outgoing interface is hardware-switched in the case of IP multicast Multilayer Switching (MLS).
12.1(2)T	The **df** keyword and *rp-address* argument were added.
12.1(5)T	The **detail** keyword was added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command works only on interfaces that are configured for PIM.

Use the **show ip pim interface count** command to display switching counts for Multicast Distributed Switching (MDS) and other fast-switching statistics. For more information on MDS, refer to the "Configuring Multicast Distributed Switching" chapter in the *Cisco IOS Switching Services Configuration Guide*.

Examples

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

```
Router# show ip pim interface

Address          Interface          Mode    Neighbor  Query     DR
                                            Count     Interval
192.168.37.6      Ethernet0          Dense   2         30        192.168.37.33
192.168.36.129    Ethernet1          Dense   2         30        192.168.36.131
10.1.37.2        Tunnel0            Dense   1         30        224.0.0.0
```

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

```
Router# show ip pim interface count

Address          Interface          FS  Mpackets In/Out
172.16.121.35    Ethernet0          *   548305239/13744856
172.16.121.35    Serial0.33         *   8256/67052912
192.168.12.73     Serial0.1719       *   219444/862191
```

The following is sample output from the **show ip pim interface** command when the **count** keyword is specified and IP multicast MLS is enabled. The example lists the PIM interfaces that are fast switched and process switched, and the packet counts for these interfaces. The flag “H” is added to interfaces where IP multicast MLS is enabled.

```
Router# show ip pim interface count

States: FS - Fast Switched, H - Hardware Switched
Address          Interface          FS  Mpackets In/Out
192.168.10.2       Vlan10             * H 40886/0
192.168.11.2       Vlan11             * H 0/40554
192.168.12.2       Vlan12             * H 0/40554
192.168.23.2       Vlan23             *   0/0
192.168.24.2       Vlan24             *   0/0
```

The following are two sample outputs from the **show ip pim interface** command when the **df** keyword is specified:

```
Router# show ip pim interface df

Interface          RP               DF Winner        Metric          Uptime
Ethernet3/3        10.10.0.2        10.4.0.2         0               00:03:49
                   10.10.0.3        10.4.0.3         0               00:01:49
                   10.10.0.5        10.4.0.4         409600          00:01:49
Ethernet3/4        10.10.0.2        10.5.0.2         0               00:03:49
                   10.10.0.3        10.5.0.2         409600          00:02:32
                   10.10.0.5        10.5.0.2         435200          00:02:16
Loopback0          10.10.0.2        10.10.0.2        0               00:03:49
                   10.10.0.3        10.10.0.2        409600          00:02:32
                   10.10.0.5        10.10.0.2        435200          00:02:16

Router# show ip pim interface Ethernet3/3 df 10.10.0.3

Designated Forwarder election for Ethernet3/3, 10.4.0.2, RP 10.10.0.3
  State                           Non-DF
  Offer count is                  0
  Current DF ip address           10.4.0.3
  DF winner up time               00:02:33
  Last winner metric preference   0
  Last winner metric              0
```

Table 25 describes the significant fields shown in the displays.

Table 25 show ip pim interface Field Descriptions

Field	Description
Address	Interface IP address of the next hop router.
Interface	Interface type and number that is configured to run PIM.
Mode	Multicast mode in which the Cisco IOS software is operating. This can be dense mode or sparse mode. "DVMRP" indicates that a Distance Vector Multicast Routing Protocol tunnel is configured.
Neighbor Count	Number of PIM neighbors that have been discovered through this interface. If the Neighbor Count is 1 for a DVMRP tunnel, the neighbor is active (receiving probes and reports).
Query Interval	Frequency, in seconds, of PIM router query messages, as set by the **ip pim query-interval** interface configuration command. The default is 30 seconds.
DR	IP address of the designated router (DR) on a network. Note that serial lines do not have designated routers, so the IP address would be shown as 224.0.0.0.
FS	An asterisk (*) in this column indicates that fast switching is enabled.
Mpackets In/Out	Number of packets into and out of the interface since the router has been up.
RP	IP address of the RP.
DF Winner	IP address of the elected DF.
Metric	Unicast routing metric to the RP announced by the DF.
Uptime	Length of time the RP has been up, in days and hours. If less than 1 day, time is expressed in hours, minutes, and seconds.
State	Indicates whether the specified interface is an elected DF.
Offer count is	Number of PIM DF election offer messages that the router has sent out the interface during the current election interval.
Current DF ip address	IP address of the current DF.
DF winner up time	Length of time the current DF has been up, in days and hours. If less than 1 day, time is expressed in hours, minutes, and seconds.
Last winner metric preference	The preference value used for selecting the unicast routing metric to the RP announced by the DF.
Last winner metric	Unicast routing metric to the RP announced by the DF.

The following is sample output from the **show ip pim interface** command with the **detail** keyword for Fast Ethernet interface 0/1:

```
Router# show ip pim interface fastethernet 0/1 detail

FastEthernet0/1 is up, line protocol is up
  Internet address is 172.16.8.1/24
  Multicast switching:process
  Multicast packets in/out:0/0
  Multicast boundary:not set
  Multicast TTL threshold:0
  PIM:enabled
    PIM version:2, mode:dense
    PIM DR:172.16.8.1 (this system)
    PIM neighbor count:0
    PIM Hello/Query interval:30 seconds
    PIM State-Refresh processing:enabled
    PIM State-Refresh origination:enabled, interval:60 seconds
    PIM NBMA mode:disabled
    PIM ATM multipoint signalling:disabled
    PIM domain border:disabled
  Multicast Tagswitching:disabled
```

Table 26 describes the significant fields shown in the display.

Table 26 show ip pim interface detail Field Descriptions

Field	Description
Internet address	IP address of the specified interface.
Multicast switching:	The type of multicast switching enabled on the interface: process, fast, or distributed.
Multicast boundary:	Indicates whether an administratively scoped boundary is configured.
Multicast TTL threshold:	The time-to-live (TTL) threshold of multicast packets being forwarded out the interface.
PIM:	Indicates whether PIM is enabled or disabled.
PIM version:	Indicates whether PIM version 1 or version 2 is configured.
PIM mode:	Indicates whether PIM sparse mode, dense mode, or sparse-dense mode is configured.
PIM DR:	The IP address of the DR.
PIM State-Refresh processing:	Indicates whether the processing of PIM state refresh control messages is enabled.
PIM State-Refresh origination:	Indicates whether the origination of the PIM state refresh control messages is enabled.
interval:	Indicates the configured interval for the origination of the PIM state refresh control messages. The available interval range is from 4 to 100 seconds.
PIM NBMA mode:	Indicates whether the interface is enabled for nonbroadcast multiaccess (NBMA) mode.
PIM ATM multipoint signalling:	Indicates whether the interface is enabled for ATM multipoint signaling.
PIM domain border:	Indicates whether the interface is enabled as a PIM domain border.
Multicast Tagswitching:	Indicates whether multicast tag switching is enabled.

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim query-interval	Configures the frequency of PIM router query messages.
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh control messages on a PIM router.

Command	Description
ip pim state-refresh origination-interval	Configures the origination of and the interval for PIM dense mode state refresh control messages on a PIM router.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

show ip pim neighbor

To list the Protocol Independent Multicast (PIM) neighbors discovered by the Cisco IOS software, use the **show ip pim neighbor** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **neighbor** [*interface-type interface-number*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use this command to determine which routers on the LAN are configured for PIM.

Examples

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

```
Router# show ip pim neighbor

PIM Neighbor Table
Neighbor Address  Interface          Uptime    Expires   Mode
192.168.37.2       Ethernet0          17:38:16  0:01:25   Dense
192.168.37.33      Ethernet0          17:33:20  0:01:05   Dense (DR)
192.168.36.131     Ethernet1          17:33:20  0:01:08   Dense (DR)
192.168.36.130     Ethernet1          18:56:06  0:01:04   Dense
10.1.22.9         Tunnel0            19:14:59  0:01:09   Dense
```

Table 27 describes the significant fields shown in the display.

Table 27 show ip pim neighbor Field Descriptions

Field	Description
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table.
Expires	How long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.

Table 27 show ip pim neighbor Field Descriptions (continued)

Field	Description
Mode	Mode in which the interface is operating.
(DR)	Indicates that this neighbor is a designated router on the LAN.

Related Commands

Command	Description
ip pim state-refresh disable	Disables the processing and forwarding of PIM Dense Mode State Refresh feature control messages on a PIM router.
ip pim state-refresh origination-interval	Configures the origination of and the interval for the PIM Dense Mode State Refresh feature control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.

show ip pim rp

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ip pim rp** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp** [**mapping** | **metric**] [*rp-address*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
mapping	(Optional) Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP).
metric	(Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap router (BSR).
rp-address	(Optional) RP IP address.

Defaults

If no RP is specified, all active RPs are displayed.

Command Modes

EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.1(2)T	The **metric** keyword and *rp-address* argument were added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The Protocol Independent Multicast (PIM) version known for an RP influences the type of PIM register messages (version 1 or version 2) that the router sends when acting as the designated router (DR) for an active source. If an RP is statically configured, the PIM version of the RP is not set and the router, if required to send register packets, first tries to send PIM version 2 register packets. If that fails, the router sends PIM version 1 register packets.

The version of the RP displayed in the **show ip pim rp** command output can change according to the operations of the router. When the group is created, the version shown is for the RP in the RP mapping cache. Later, the version displayed by this command may change. If this router is acting as a DR for an active source, the router sends PIM register messages. The PIM register messages are answered by the RP with PIM register stop messages. The router learns from these PIM register stop messages the actual PIM version of the RP. Once the actual PIM version of the RP is learned, this command displays only this version. If the router is not acting as a DR for active sources on this group, then the version shown for the RP of the group does not change. In this case, the PIM version of the RP is irrelevant to the router because the version of the RP influences only the PIM register messages that this router must send.

When you enter the **show ip pim rp mapping** command, the version of the RP displayed in the output is determined only by the method through which an RP is learned. If the RP is learned from Auto-RP then the RP displayed is either "v1" or "v2, v1." If the RP is learned from a static RP definition, the RP version is undetermined and no RP version is displayed in the output. If the RP is learned from the BSR, the RP version displayed is "v2."

Examples

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
```

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    Ethernet3/3
10.10.0.5        90             435200         L     unicast    Ethernet3/3
```

Table 28 describes the significant fields shown in the displays.

Table 28 show ip pim rp Field Descriptions

Field	Description
Group	Address of the multicast group about which to display RP information.
RP	Address of the RP for that group.
v2	Indicates that the RP is running Protocol Independent Multicast (PIM) version 2.
v1	Indicates that the RP is running PIM version 1.

Table 28 show ip pim rp Field Descriptions (continued)

Field	Description
bidir	Indicates that the RP is operating in bidirectional mode.
Info source	RP mapping agent that advertised the mapping.
(?)	Indicates that no Domain Name System (DNS) name has been specified.
via Auto-RP	Indicates that RP was learned via Auto-RP.
Uptime	Length of time the RP has been up (in days and hours). If less than 1 day, time is expressed in hours, minutes, and seconds.
expires	Time in (hours, minutes, and seconds) in which the entry will expire.
Metric Pref	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.
Flags	Indicates the flags set for the specified RP. The following are descriptions of possible flags: C—RP is configured. L—RP learned via Auto-RP or the BSR.
RPF Type	Routing table from which this route was obtained, either unicast, Distance Vector Multicast Routing Protocol (DVMRP), or static mroute.
Interface	Interface type and number that is configured to run PIM.

show ip pim rp-hash (BSR)

To display which rendezvous point (RP) is being selected for a specified group, use the **show ip pim rp-hash** command in EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp-hash** {*group-address* | *group-name*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	Displays the RP information for the specified group address or name as defined in the Domain Name System (DNS) hosts table.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command displays which RP was selected for the group specified. It also shows whether this RP was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

Examples

The following is sample output from the **show ip pim rp-hash** command with the group address 239.1.1.1 specified:

```
Router# show ip pim rp-hash 239.1.1.1

RP 172.16.24.12 (mt1-47a.cisco.com), v2
    Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap
         Uptime: 05:15:33, expires: 00:02:01
```

Table 29 describes the significant fields shown in the display.

Table 29 show ip pim rp-hash Field Descriptions

Field	Description
RP 172.16.24.12 (mt1-47a.cisco.com), v2	Address of the RP for the group specified (239.1.1.1). Within parentheses is the DNS name of the RP. If the address of the RP is not registered in the DNS, a question mark (?) is displayed. PIM Version 2 configured.
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	Indicates from which system the router learned this RP information, along with the DNS name of the source. RP was selected by the bootstrap mechanism. In this case, the BSR is also the RP.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this RP.
expires	Time (in hours, minutes, and seconds) after which the information about this RP expires. If the router does not receive any refresh messages in this time, it will discard information about this RP.

show ip rpf

To display how IP multicast routing does Reverse Path Forwarding (RPF), use the **show ip rpf** command in EXEC mode.

show ip rpf [**vrf** *vrf-name*] {*source-address* | *source-name*} [**metric**]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
source-address | *source-name*	Displays the RPF information for the specified source address or name.
metric	(Optional) Displays the unicast routing metric.

Defaults

If no source is specified, all sources are displayed.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.1(2)T	The **metric** keyword was added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The router can reverse path forward from multiple routing tables (that is, the unicast routing table, Distance Vector Multicast Routing Protocol (DVMRP) routing table, or static mroutes). This command tells you from where the information is retrieved.

Examples

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

```
Router# show ip rpf 172.16.10.13

RPF information for sj.cisco.com (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 of the **show ip rpf** command when the **metric** keyword is specified:

```
Router# show ip rpf 172.16.10.13 metric

RPF information for sj.cisco.com (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
  Metric preference: 110
  Metric: 11
```

Table 30 describes the significant fields shown in the display.

Table 30 show ip rpf Field Descriptions

Field	Description
RPF information for <host name (source address)>	Host name and source address that this information concerns.
RPF interface	For the given source, the interface from which the router expects to get packets.
RPF neighbor	For given source, the neighbor from which the router expects to get packets.
RPF route/mask	Route number and mask that matched against this source.
RPF type	Routing table from which this route was obtained, either unicast, DVMRP, or static mroutes.
RPF recursion count	Indicates the number of times the route is recursively resolved.
Doing distance-preferred...	Indicates whether RPF was determined based on distance or length of mask.
Metric preference	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.

Glossary

BSR—bootstrap router. A router that provides a fault-tolerant, automated rendezvous point (RP) discovery and distribution mechanism. Thus, routers dynamically learn the group-to-RP mappings.

IGMP—Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

multicast distribution tree (MDT)—Defines the path used by PE routers to send multicast data and control messages to every other PE router in the multicast domain.

multicast router—Router used to send IGMP query messages on their attached local networks. Host members of a multicast group respond to a query by sending IGMP reports noting the multicast groups to which they belong. The multicast router takes responsibility for forwarding multicast datagrams from one multicast group to all other networks that have members in the group.

PE—provider edge. Router that is part of a service provider's network and is connected to a customer edge (CE) router.

PIM—Protocol Independent Multicast. An IP multicast routing protocol used for routing multicast data packets to multicast groups. PIM is unicast routing protocol-independent and can operate in different modes such as sparse mode and dense mode.

PIM dense mode—One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

PIM sparse mode—One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM.

Protocol Independent Multicast—See PIM.

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

RPF—Reverse Path Forwarding. Multicasting technique in which a multicast datagram is forwarded out of all but the receiving interface if the receiving interface is the one used to forward unicast datagrams to the source of the multicast datagram.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.

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