Chapter 3

Configuring PIM for IPv4 Multicast

The Protocol Independent Multicast (PIM) protocol is a collection of multicast routing protocols that enables multicast routers to identify other multicast routers to receive packets.

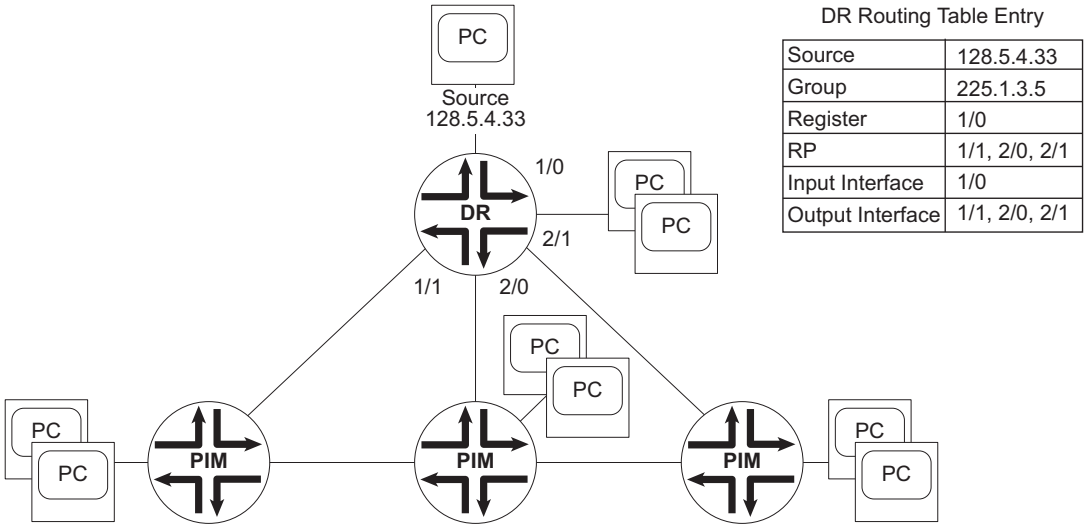
This chapter describes how to configure PIM for IPv4 on E-series routers; it contains the following sections:

Overview

The IPv4 implementation of PIM supports PIM dense mode, PIM sparse mode, PIM sparse-dense mode, and PIM source-specific multicast (PIM SSM).

Figure 7 represents how PIM builds a source, group (S,G) entry in a source-rooted tree (SRT). When multiple routers are connected to a multiaccess network, one router becomes the designated router. The designated router receives data from the source on interface 1/0 and multicasts the data to its downstream neighbors on interfaces 1/1, 2/0, and 2/1. In the designated router routing table, the entry for this operation lists the source as the IP address of the source and the group as the IP address of the multicast group.

Figure 7: Source-Rooted Tree



Neighbors exchange hello messages periodically to determine the designated router. The router with the highest network layer address becomes the designated router. If the designated router subsequently receives a hello message from a neighbor with a higher network layer address, that neighbor becomes the designated router.

PIM Dense Mode

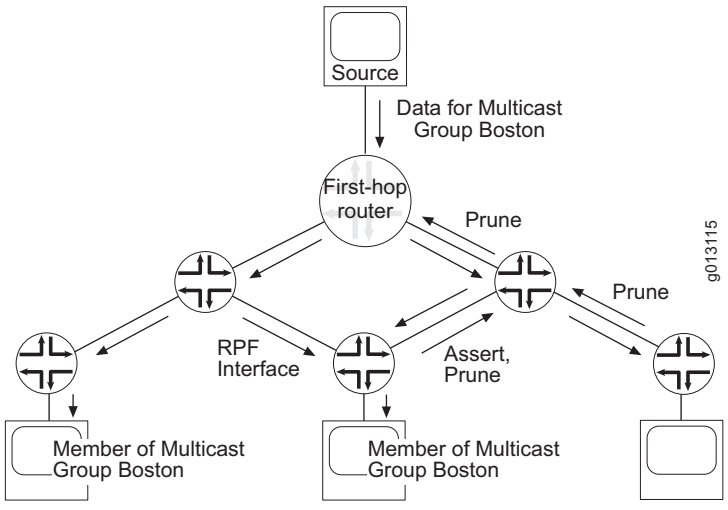
PIM dense mode uses a reverse-path multicast, flood-and-prune mechanism. The protocol was developed for situations that meet one or more of the following criteria:

- Sources and receivers are close together, and there are many more receivers than sources.
- There is a constant stream of multicast data.
- There is a lot of multicast data.

Dense-mode routing protocols use *SRT algorithms*. An SRT algorithm establishes a tree that connects each source in a multicast group to the members of the group. All traffic for the multicast group passes along this tree.

Figure 8 illustrates how PIM dense mode works. When a source sends a multicast packet to a first-hop router, the first-hop router multicasts that packet to its neighbors. Those neighbors in turn forward the packet to their neighbors and their hosts that belong to the multicast group. If a neighbor has no hosts that belong to the multicast group and has no other PIM neighbors, it returns a prune message to the first-hop router. The first-hop router does not multicast subsequent packets for that group to neighbors who respond with prune messages.

Figure 8: PIM Dense Mode Operation



Overriding Prunes

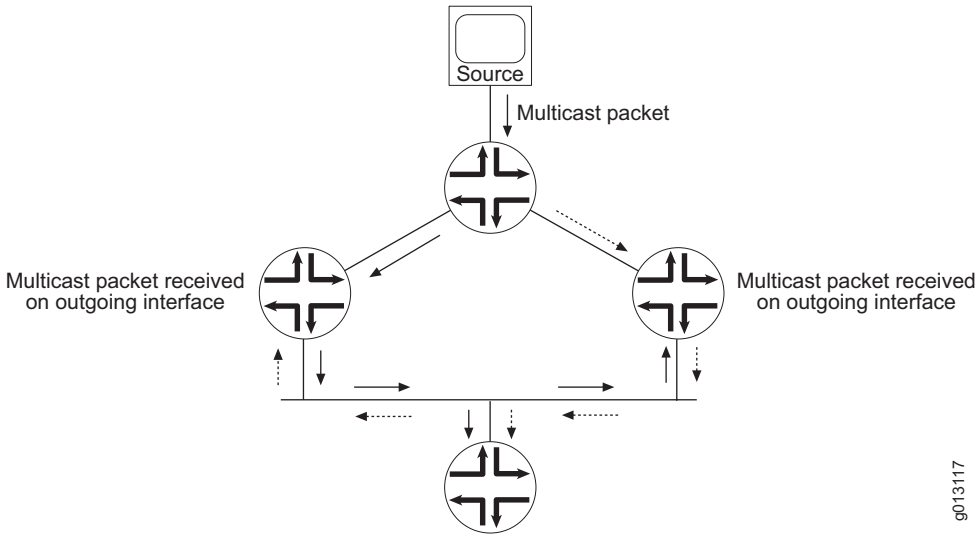
If a host on a previously pruned branch requests to join a multicast group, it sends an IGMP message to its first-hop router. The first-hop router then sends a graft message upstream.

PIM routers send join messages on multiaccess interfaces to override prune messages. For example, if a PIM router sent a prune message to indicate that it had no hosts for a multicast group, and one of its hosts subsequently requests to send a packet to that group, the router sends a join message to the first-hop router.

Preventing Duplication

If there are parallel paths to a source, duplicate packets can travel downstream through different routers to the network. If a forwarding router receives a multicast packet on its outgoing interface, the router identifies that the packet is a duplicate and notifies the upstream routers. See Figure 9.

Figure 9: Detecting Duplication



The upstream routers responsible for the duplication send assert messages to determine which router becomes the forwarder. Downstream routers listen to the assert messages to discover which router becomes the forwarder.

PIM Sparse Mode

This implementation of PIM sparse mode supports the following features:

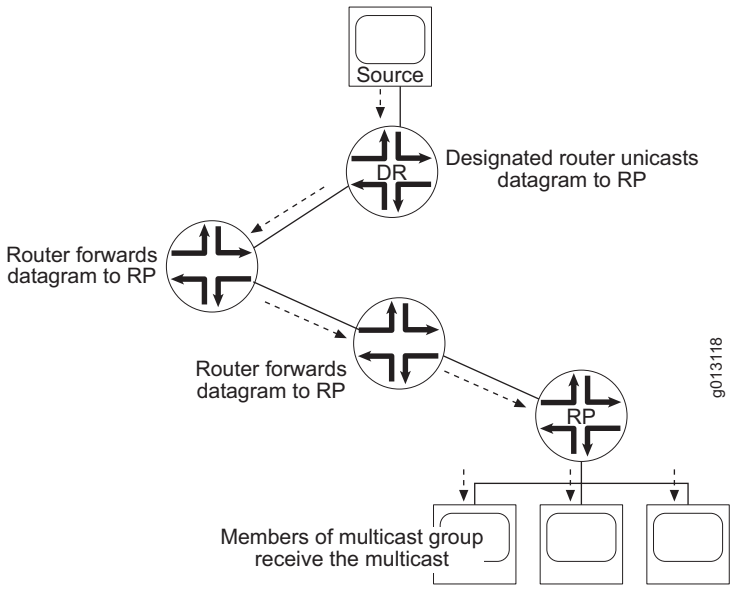
- Rendezvous point (RP) routers
- Designated routers and designated router election
- Join/prune messages, hello messages, assert messages, and register messages
- Switching from a shared tree to a shortest path tree (SPT)
- (*,*,RP) support for interoperation with dense-mode protocols
- RPF checks of multicast entries when unicast routing configuration changes
- Timers for tree maintenance
- Border, null, Rendezvous Point Tree (RPT), SPT, and wildcard flags

PIM sparse mode resolves situations that meet one or more of the following criteria:

- The multicast group contains few receivers.
- Multicast traffic is infrequent.
- Wide area networks (WANs) separate sources and receivers.

Sparse-mode routing protocols use *shared trees*. In a shared tree, sources forward multicast datagrams to a directly connected router, the designated router. The designated router encapsulates the datagram and unicasts it to an assigned RP router, which then forwards the datagram to members of multicast groups. See Figure 10.

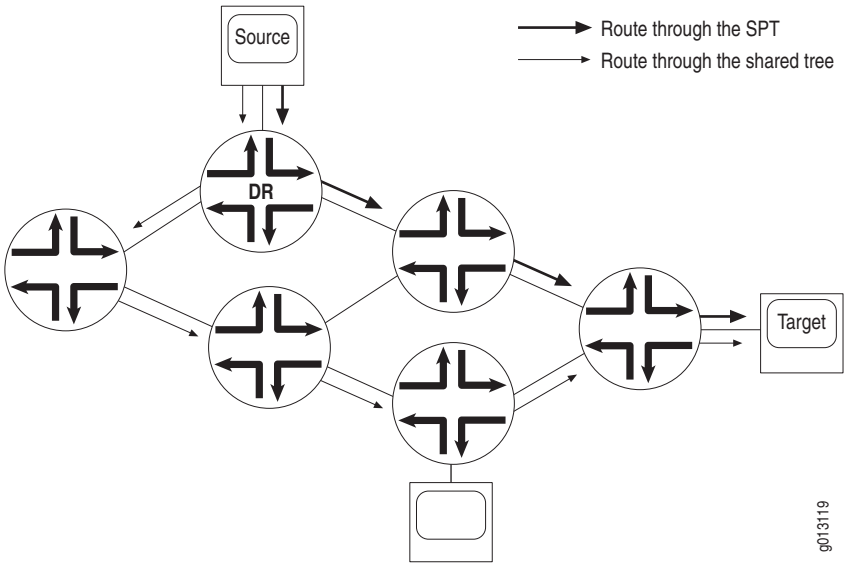
Figure 10: PIM Sparse Mode Operation



In PIM sparse mode, an RP announces a source and establishes paths from the source to members of a multicast group before multicasting any datagrams. RPs transmit join messages to become part of the shared tree that enables distribution of packets to the multicast group.

However, when a source starts multicasting datagrams, PIM sparse mode can switch to an SRT—known in PIM sparse mode as an SPT—to improve the network's efficiency. Although shared trees minimize the traffic in the network and the costs associated with unnecessary transmission of data, the routes in a shared tree might be longer than those in an SPT. See Figure 11.

Figure 11: Shared Tree Versus SPT



The designated routers on the network determine when the source switches from a shared tree to an SPT. A designated router switches to the SPT when it receives a certain number of packets which you can configure.

When all designated routers associated with a specific RP router have switched to the SPT, the RP router sends a join/prune message toward the multicast source. When the multicast source receives this message, it stops sending multicast data through the SPT.

Joining Groups

A host's designated router (DR) sends join messages to the RP when that host wants to join a group. When a host wants to leave a group, it communicates with its designated router through IGMP. When the designated router no longer has any hosts that belong to a particular group, it sends a prune message to the RP.

Timers

PIM sparse mode uses timers to maintain the networking trees.

NOTE: PIM sparse mode routers poll their neighbors and hosts for various pieces of information at set intervals.

If a PIM sparse mode router does not receive information from a neighbor or host within a specific time, known as the *hold time*, it removes the associated information from its routing tables.

You can configure how often an interface sends hello messages (hello interval) and how often routers send RP announce messages (RP announce interval). The hold-time associated with hello messages is 3.5 times the hello interval, and the holdtime associated with RP announce messages is 2.5 times the RP announce interval.

All other timers are fixed and take the default values recommended in RFC 2934—Protocol Independent Multicast MIB for IPv4 (October 2000).

PIM Sparse Mode Bootstrap Router

PIM sparse mode routers need the address of the rendezvous point (RP) for each group for which they have (*,G) state. They obtain this address either through a bootstrap mechanism or through static configuration. PIM sparse mode routers commonly use one of two bootstrap mechanisms: bootstrap router (BSR) or auto-RP. Auto-RP is standards based, but is not used in IPv6 implementations, so BSR configuration has become more popular.

When implemented, BSR operates as follows:

1. One router in each PIM domain is elected the BSR.
2. All the routers in the domain that are configured to be RP candidates periodically unicast their candidacy to the BSR.
3. The BSR picks an RP set from the available candidates and periodically announces this set in a bootstrap message.
4. Bootstrap messages are flooded hop by hop throughout the domain until all routers in the domain learn the RP set.

NOTE: A PIM router can receive group-to-RP mappings from either BSR or auto-RP, but not from both. Because BSR and auto-RP use different mapping algorithms, the mechanisms cannot coexist.

PIM Sparse-Dense Mode

In PIM sparse-dense mode, if an RP is not known for a group, the router sends data using PIM dense mode. However, if the router discovers an RP or you configure an RP statically, PIM sparse mode takes over.

You can configure both PIM dense mode and PIM sparse mode commands in PIM sparse-dense mode.

PIM Source-Specific Multicast

PIM SSM is an extension of the PIM protocol. Using SSM, a client can receive multicast traffic directly from the source. PIM SSM uses PIM sparse mode functionality to create an SPT between the client and the source, but builds the SPT without using an RP.

By default, the SSM group multicast address is limited to the IP address range 232.0.0.0 to 232.255.255.255. You can use the **ip pim ssm** command to extend SSM operations into another Class D range. (See *Configuring PIM SSM* on page 102.)

An SSM-configured network has the following advantages over a traditionally configured PIM sparse mode network include the following:

- No need for shared trees or RP mapping (no RP is required).
- No need for RP-to-RP source discovery through Multicast Source Discovery Protocol (MSDP).
- Simplified administrative deployment; you need only configure PIM sparse mode on all router interfaces and issue the necessary SSM commands (including specifying IGMPv3 on the receiver local area network).
- Support for source lists; you can use source lists, supported in IGMPv3, where only specified sources send traffic to the SSM group.

In a PIM SSM–configured network, an E-series router subscribes to an SSM channel (by means of IGMPv3 or by means of IGMP ssm-mapping for IGMPv2/v1 joins), requesting to join group G and source S. The directly connected PIM sparse mode router, the designated router of the receiver, sends an (S,G) join message to its RPF neighbor for the source. For PIM SSM, the RP is not contacted in this process by the receiver (as happens in normal PIM sparse mode operations).

Platform Considerations

For information about modules that support PIM on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support PIM.

For information about modules that support PIM on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support PIM.

References

For more information about PIM, see the following resources:

- Protocol Independent Multicast MIB for IPv4—draft-ietf-idmr-pim-mib-10.txt (July 2000 expiration)
- RFC 2362—Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (June 1998)
- RFC 3569—An Overview of Source-Specific Multicast (SSM) (July 2003)
- Source-Specific Multicast for IP—draft-ietf-ssm-arch-06.txt (March 2005 expiration)
- Source-Specific Protocol Independent Multicast in 232/8—draft-ietf-mboned-ssm232-08.txt (September 2004 expiration)
- Multicast in MPLS/BGP VPNs—draft-rosen-vpn-mcast-06.txt (April 2004 expiration)
- Multicast in MPLS/BGP IP VPNs—draft-rosen-vpn-mcast-08.txt (June 2005 expiration)

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

Before You Begin

You can configure PIM on IPv4 and IPv6 interfaces. However, IPv6 does not support all PIM configuration options. For information about configuring PIM on IPv6 interfaces, see *Chapter 7, Configuring PIM for IPv6 Multicast*.

Enabling PIM on a VR

By default, PIM is disabled. To enable PIM on a VR:

1. Enable multicast routing. (See *Enabling IP Multicast* on page 7.)
2. Create a VR, or access an existing VR context.

   host1(config)#**virtual-router boston**

3. Create and enable PIM processing.

   host1:boston(config**)#router pim**

router pim

- Use to create and enable PIM processing on a VR or to access Router Configuration mode.
- Example

  host1:boston(config)#**router pim**

- Use the **no** version to remove PIM from the VR.

Disabling PIM on a VR

To disable PIM processing on a router, use the **pim disable** command.

pim disable

- Use to disable PIM processing. By default, PIM processing is enabled.
- Example

  host1:boston(config-router)#**pim disable**

- Use the **no** version to reenable PIM processing.

Enabling PIM on an Interface

You can enable PIM on an interface in one of the PIM modes (dense, sparse, or sparse-dense) and specify how often the interface sends hello messages to neighbors.

You can configure PIM and IGMP on the same interface. If you configure IGMP and PIM on an interface, the router determines that PIM owns the interface.

NOTE: You cannot configure DVMRP and PIM on the same interface.

ip pim

- Use to enable PIM on an interface; dense mode is the default.
- Example

  host1(config-if)#**ip pim sparse-dense-mode**

- Use the **no** version to disable PIM on an interface.

ip pim query-interval

- Use to specify the interval, in seconds, at which the router sends hello messages to neighbors.
- Example

  host1(config-if)#**ip pim query-interval 100**

- Use the **no** version to restore the default setting, 30 seconds.

ip pim sparse-mode graceful-restart-duration

- Use to set the graceful restart duration for IP PIM sparse mode.
- Example

  host1(config-if)#**ip pim sparse-mode graceful-restart-duration 10**

- Use the **no** version to return to the default duration of 30 seconds.

Setting a Priority to Determine the Designated Router

You can influence whether a particular router is selected as the designated router with the **ip pim dr-priority** command. A higher priority value increases the likelihood that a router is selected as the designated router, while a lower value decreases the likelihood.

ip pim dr-priority

- Use to set a priority value, in the range 1–254, by which a router is likely to be selected as the designated router.
- Example

  host1(config-if)#**ip pim dr-priority 24**

- Use the **no** version to restore the default value, 1.

Configuring an RP Router for PIM Sparse Mode and PIM Sparse-Dense Mode

When you use the router for PIM sparse mode or PIM sparse-dense mode, some VRs must act as RP routers. You can configure static RP routers or configure the router to assign RP routers automatically.

To configure the router to assign RP routers automatically, you must define several VRs as RP routers and one VR as an RP mapping agent. RP routers send their announcement messages to the RP mapping agent, which assigns groups to RP routers and resolves any conflicts. The RP mapping agent notifies neighbors of the RP assigned to each group.

Configuring a Static RP Router

If you want to control PIM more tightly, you can configure a static RP router. To do so:

1. Configure an access list that specifies the multicast groups that can use the static RP router.

   host1(config)#**access-list boston permit 228.0.0.0 15.255.255.255**

2. Specify a static RP router.

   host1(config)#**ip pim rp-address 122.0.0.1 1 boston**

Configuring an Auto-RP Router for PIM Sparse Mode

Two multicast groups, 224.0.1.39 and 224.0.1.40, are reserved for forwarding auto-RP messages through the network. When you configure an auto-RP router for PIM sparse mode, you must assign a static RP router to these two groups. You can then specify an RP mapping agent for other multicast groups.

To configure an auto-RP router for PIM sparse mode:

1. Configure a static RP to have priority over the auto-RP for the groups that send auto-RP multicast messages.

   host1(config)#**access-list 11 permit 224.0.1.39 0.0.0.0**
   host1(config)#**access-list 11 permit 224.0.1.40 0.0.0.0**
   host1(config)#**ip pim rp-address 192.48.1.22 11 override**

2. Assign an RP mapping agent.

   host1(config)#**ip pim send-rp-discovery scope 23 loopback 1**

3. Configure routers to send auto-RP announcement messages to the mapping agent.

   host1(config)#**ip pim send-rp-announce loopback 2 scope 16 group-list 1**

Configuring an Auto-RP Router for PIM Sparse-Dense Mode

In PIM sparse-dense mode, you must prevent routers from advertising auto-RP messages to the multicast groups 224.0.1.39 and 224.0.1.40, which are reserved for forwarding auto-RP messages through the network. To configure an auto-RP router for PIM sparse-dense mode:

1. Assign an RP mapping agent.

   host1(config)#**ip pim send-rp-discovery scope 23 loopback 1**

2. Configure an access list that details the multicast groups that can use the static RP router.

   host1(config)**access-list boston permit 224.0.0.0 15.255.255.255**

3. Prevent routers from advertising auto-RP messages to the multicast groups that are reserved for forwarding auto-RP messages through the network.

   host1(config)#**access-list 1 deny 224.0.1.39**
   host1(config)#**access-list 1 deny 224.0.1.40**

4. Configure routers to send auto-RP announcement messages to the mapping agent.

   host1(config)#**ip pim send-rp-announce loopback 2 scope 23 group-list boston interval 200**

ip pim rp-address

- Use to specify a static PIM RP router.
- Specify a standard IP access list of multicast groups to control which multicast groups can use this RP router.
- Specify the **override** keyword if you want this static RP router to have priority over auto-RP routers.
- Example

  host1(config)#**ip pim rp-address 192.48.1.22 11 override**

- Use the **no** version to clear the filter from this interface.

ip pim send-rp-announce

- Use to send auto-RP announcement messages from a router you configured as an RP.
- Specify an interface type and specifier, such as atm 3/0. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- The auto-RP announcement messages contain the IP address for the interface that you specify.
- Specify the number of hops for which the announcement is valid; default value is 64.
- Specify an access list that details which multicast groups the RP can include in announcement messages.
- Specify a time interval in the range 1–65535 seconds to control how often the router sends announcements. The default is 60 seconds.
- Example

  host1(config)#**ip pim send-rp-announce loopback 2 scope 23 group-list boston interval 200**

- Use the **no** version to clear filters from this interface.

ip pim send-rp-discovery scope

- Use to configure the router as an RP mapping agent, which records group-to-RP mappings and notifies PIM designated routers about the mappings.
- Specify the number of hops for which the RP discovery message is valid; default value is 64.
- To assign an interface from which the router sends auto-RP discovery messages, specify an interface type and specifier, such as atm 3/0. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Example

  host1(config)#**ip pim send-rp-discovery scope 23 loopback 1**

- Use the **no** version to stop the router from acting as an RP mapping agent.

Configuring BSR and RP Candidates for PIM Sparse Mode

When choosing candidate BSRs, select well-connected routers in the core of the network. Typically, candidate BSRs are a subset of the candidate RPs. A single BSR is elected for the domain of candidate BSRs. The elected BSR floods bootstrap messages (BSMs) containing their group-to-RP mappings to all PIM routers. PIM routers use the group-to-RP mappings supplied by the elected (or preferred) BSR.

ip pim bsr-candidate

- Use to define a router as a BSR candidate.
- To assign an interface from which the router sends messages, specify an interface type and specifier, such as atm 3/0. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Specify a length (up to 32 bits) for the hash mask length field sent in BSMs that the router originates. This mask is combined with the group address before the router calls the hash function. For example, specifying a value of 24 limits the group address to the first 24 bits. The default hash mask length is 30 bits.
- Use the **priority** keyword to specify a value for the BSR-priority field of BSMs that the router originates. In the BSR election process, the BSR with the higher priority is preferred. If the priority values are equal, the router with the higher IP address becomes the BSR. The default value is 0 (address comparison only).
- Use the **period** keyword to specify the interval, in the range 1–65535 seconds, at which the BSR sends bootstrap messages. The default value is 60 seconds.
- Example

  host1(config)#**ip pim bsr-candidate loopback 1 30 10**

- Use the **no** version to stop the router from acting as a BSR candidate.

ip pim rp-candidate

- Use to define a router as an RP candidate.
- To assign an interface from which the router sends messages, specify an interface type and specifier, such as atm 3/0. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Use the **group-list** keyword to specify an access-list that contains the set of group prefixes supported by this candidate RP (C-RP). If you do not specify a group-list, the default is the entire multicast address range.

NOTE: Because BSR has no mechanism for distributing negative entries, you should not configure negative access-list entries (also called deny access-list entries).

- Use the **hold-time** keyword to specify the amount of time the BSR keeps an RP in its C-RP list if the BSR does not receive a C-RP advertisement message. The default value is 150 seconds.
- Use the **priority** keyword to specify a priority field value that the C-RP sends to the BSR in C-RP advertisement messages. In the RP election process, the RP with the lower priority value is preferred. The default value is 192.
- Use the **interval** keyword to specify an interval, in the range 1–65535 seconds, at which the C-RP sends advertisement messages to the BSR. The default value is 60 seconds.
- Example

  host1(config)#**access-list 1 permit 227.0.0.0 15.255.255.255**
  host1(config)#**access-list 1 permit 228.0.0.0 15.255.255.255**
  host1(config)#**ip pim rp-candidate loopback 1 group-list 1**

- Use the **no** version to stop the router from acting as an RP candidate

Migrating to BSR from Auto-RP

Migrating to BSR from auto-RP requires that you upgrade all PIM routers in the domain to support BSR. However, until all routers are BSR-capable, continue to use auto-RP.

After all routers are BSR-capable, switch from auto-RP to BSR as follows:

1. Use the **no ip pim send-rp-discovery scope** command to stop PIM in the network by disabling all auto-RP mapping agents. This results in flooding to an empty map.

2. Reconfigure auto-RP mapping agents as candidate BSRs by using the **ip pim bsr-candidate** command.

3. Reconfigure auto-RP candidate RPs as BSR candidate RPs by issuing the **no ip pim send-rp-announce** command and then issuing the **ip pim rp-candidate** command.

Switching to an SPT for PIM Sparse Mode

PIM sparse mode initiates multicasting using a shared tree. You can configure PIM sparse mode to switch to an SPT when a source starts sending multicast messages, or you can prevent PIM sparse mode from switching to an SPT. Multicasting over an SPT might be more efficient than multicasting over a shared tree. (See *PIM Sparse Mode*, earlier in this chapter.)

ip pim spt-threshold

- Use to specify when PIM sparse mode switches from a shared tree to an SPT.
- Specify a nonzero integer or the keyword **infinity** to prevent PIM sparse mode from switching to an SPT.
- Specify a value of 0 (default) to configure PIM to switch to an SPT when a source starts sending multicast messages.
- Example

  host1(config)#**ip pim spt-threshold 4**

- Use the **no** version to restore the default value, 0.

Creating Multicast VPNs

JUNOSe router software provides the ability to create multicast VPNs by using GRE tunnels. This implementation is based on *Multicast in MPLS/BGP VPNs* (draft-rosen-vpn-mcast-06.txt and draft-rosen-vpn-mcast-08.txt) and further defined by *Base Specification for Multicast in MPLS/BGP VPNs* (draft-raggarwa-13vpn-2547-mvpn-00.txt).

NOTE: Although you can configure PIM sparse mode remote neighbors, you can no longer use these remote neighbors for BGP/MPLS VPNs. For multicast VPNs, use the functionality described in this section.

The JUNOSe software supports default Multicast Distribution Trees (MDTs) and data MDTs.

Creating Multicast VPNs Using the Default MDT

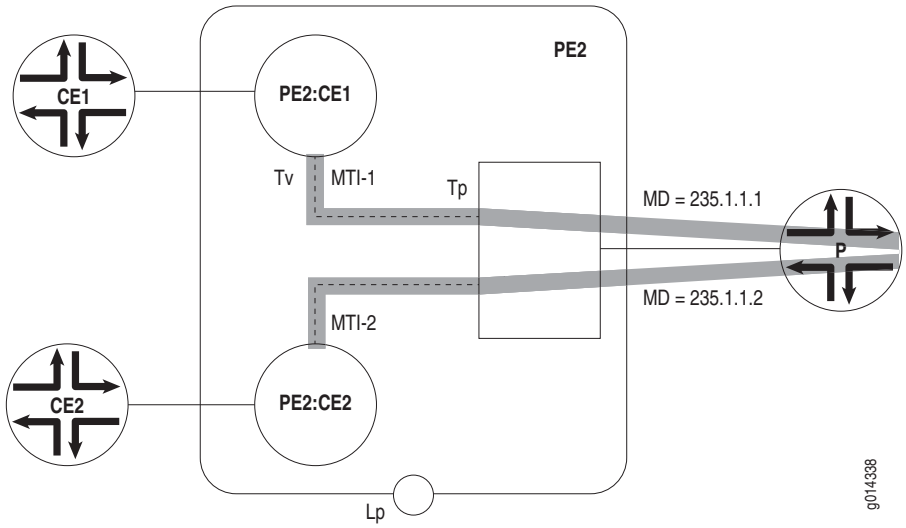
The JUNOSe software does not support a single MDT command. Instead, you must configure the multicast tunnel interfaces (MTIs) explicitly. The MTI is an IP interface that is stacked on a GRE tunnel interface. The destination address of the GRE tunnel is the multicast VPN (MVPN) group address of the MDT.

A **tunnel mdt** command specifies that the tunnel is the MTI for the default MDT, enabling the creation of a second, layer 2 interface (interface tunnel gre:*name*.mdt) on which an unnumbered IP interface (tied to the provider edge loopback interface) is stacked in the context of the parent virtual router.

Multicast VPN Configuration Example

In the following example (Figure 12), customer edge router 1 (CE1) and customer edge router 2 (CE2) exist in two separate VPNs. Each VPN is configured with its assigned Multicast Domain (235.1.1.1 and 235.1.1.2, respectively).

Figure 12: Multicast VPNs



To better understand the example, keep the following in mind:

- Lp is a loopback interface in the parent router. This address is the loopback interface used as the BGP peer address of the provider edge router (PE). Its address is advertised in the provider address space.

- Tv is the MTI in the VRF. This interface is typically configured as a PIM sparse-mode interface (though you can configure it for dense-mode or sparse-dense-mode). Any packets that originate in the VRF are sent using the address of this interface as the source address. You must set this interface address to be identical to loopback interface of the parent router (Lp).

CAUTION: Defining the Tv interface with an address other than the loopback interface of the parent router might restrict operation with non-Juniper Networks routers.

- Tp is an unnumbered IP interface that is tied to the loopback interface of the provider edge router (PE).

To configure the example, use the following general procedures:

NOTE: This example provides general information for configuring a simple Multicast VPN network. For detailed information about creating GRE tunnels, see *JUNOSe IP Services Configuration Guide, Chapter 10, Configuring IP Tunnels*. For detailed information about PIM sparse-mode configuration, see *PIM Sparse Mode* on page 80.

1. Configure BGP/MPLS VPN.

   ```
   host1:PE2(config-router)#router bgp 100
   host1:PE2(config-router)#address-family vpnv4 unicast
   host1:PE2(config-router-af)#neighbor 1.1.1.1 activate
   host1:PE2(config-router-af)#neighbor 1.1.1.1 next-hop-self
   host1:PE2(config-router-af)#neighbor 3.3.3.3 activate
   host1:PE2(config-router-af)#neighbor 3.3.3.3 next-hop-self
   host1:PE2(config-router-af)#exit-address-family
   ```

   See *JUNOSe BGP and MPLS Configuration Guide, Chapter 3, Configuring BGP-MPLS Applications* for details.

2. Configure PIM sparse mode in the core and RP for MVPN group addresses.

NOTE: For MVPN, it is a typical practice to use shared trees.

```
host1:PE1(config-router)#virtual-router PE2
host1:PE2(config)#ip multicast-routing
host1:PE2(config)#
host1:PE2(config)#! MDT RP is 72.72.72.72 (P1)
host1:PE2(config)#access-list 1 permit ip 235.0.0.0 0.255.255.255 any
host1:PE2(config)#ip pim rp-address 72.72.72.72 1
host1:PE2(config)#
host1:PE2(config)#! Do not switch from RPT for MDTs
host1:PE2(config)#ip pim spt-threshold infinity group-list 1
host1:PE2(config)#
```

3. Configure the loopback interface, Lp, in parent router PE2.

   ```
   host1:PE2(config)#interface loopback 0
   host1:PE2(config-if)#ip address 2.2.2.2 255.255.255.255
   host1:PE2(config-if)#ip pim sparse-mode
   host1:PE2(config-if)
   ```

NOTE: You must configure the loopback interface for PIM sparse mode to support unnumbered MDTs.

4. Add PIM-SM to core-facing interfaces.

   ```
   host1:PE2(config)#interface atm2/1.20
   host1:PE2(config-subif)#ip pim sparse-mode
   host1:PE2(config-subif)#
   ```

5. Extend the BGP router configuration to contribute VPN routes into the multicast router table of the VRF using the **ip route-type both** command.

```
host1:PE2(config)#router bgp 100
host1:PE2(config-router)#address-family ipv4 unicast vrf PE21
host1:PE2(config-router-af)#ip route-type both
host1:PE2(config-router-af)#exit
host1:PE2(config-router)#
```

6. Configure the GRE tunnel for VPN1.

```
host1(config)#interface tunnel gre:MTI-21 transport-virtual-router PE2
host1(config-if)#tunnel source 2.2.2.2
host1(config-if)#tunnel destination 235.1.1.1
host1(config-if)#tunnel mdt
host1(config-if)#exit
host1(config)#
```

7. Configure the GRE tunnel for VPN2

```
host1(config)#interface tunnel gre:MTI-22 transport-virtual-router PE2
thost1(config-if)#tunnel source 2.2.2.2
host1(config-if)#tunnel destination 235.1.1.2
host1(config-if)#tunnel mdt
host1(config-if)#exit
host1(config)#
```

8. Configure the IP interface (Tv) in PE2:CE1 as a PIM sparse-mode interface with the address of the loopback interface.

```
host1(config)#virtual-router PE2:CE21
host1:PE2:CE21(config)#interface tunnel gre:MTI-21
host1:PE2:CE21(config)#ip address 2.2.2.2 255.255.255.255
host1:PE2:CE21(config)#ip pim sparse-mode
host1:PE2:CE21(config)#exit
host1:PE2:CE21#
```

9. Configure the IP interface (Tv) in PE2:CE2 as a PIM sparse-mode interface with the address of the loopback interface (same as the loopback 0 address for PE2).

```
host1:PE2:CE21(config)#interface loopback 0
host1:PE2:CE21(config-if)#ip address 2.2.2.2 255.255.255.255
host1:PE2:CE21(config-if)#exit
host1:PE2:CE21(config)#exit
host1:PE2:CE21#virtual-router PE2:CE22
host1:PE2:CE22#configuration terminal
host1:PE2:CE22(config)#interface tunnel gre:MTI-22
host1:PE2:CE22(config)#ip unnumbered loopback 0
host1:PE2:CE22(config)#ip pim sparse-mode
host1:PE2:CE22(config)#exit
host1:PE2:CE22#
```

10. Configure the Tp interfaces as unnumbered IP interfaces.

```
host1(config)#interface tunnel gre:MTI-21.mdt
host1(config-if)#ip unnumbered loopback 0
host1(config-if)#ip pim sparse-mode
```

```
host1(config-if)#exit
host1(config)#

host1(config)#interface tunnel gre:MTI-22.mdt
host1(configif)#ip unnumbered loopback 0
host1(config-if)#ip pim sparse-mode
host1(config-if)#exit
host1(config)#
```

tunnel mdt

- Use to enable multicast distribution tree operation so the IP tunnel component can create an MDT interface. This command functions for GRE interfaces only.
- Example

  ```
  host1(config-if)#tunnel mdt
  ```

- The **no** version disables MDT on the interface.

Creating Multicast VPNs Using the Data MDT

A data multicast distribution tree (MDT), based on section 8 of Internet draft draft-rosen-vpn-mcast-08.txt, *Multicast in MPLS/BGP IP VPNs*, solves the problem of P routers flooding unnecessary multicast information to PE routers that have no interested receivers for a particular VPN multicast group. The data MDT solution requires the creation of a new tunnel by the PE router if the source exceeds a configured rate threshold parameter. All other PE routers join the new tunnel only if the PE router has receivers in the VPN for that multicast group.

The JUNOSe software uses dynamic point-to-multipoint GRE tunnels to configure data MDTs. In the current release, IPv6 transport over GRE (unicast or multicast) is not supported. For more information, see *JUNOSe IP Services Configuration Guide, Chapter 11, Configuring Dynamic IP Tunnels*.

Data MDTs are established using PIM-SM (shared RP Trees) and PIM-SSM (Source Trees). Profiles for dynamic interfaces in the VRF are restricted to sparse-mode only.

Data MDT Sources

A C-SG flow arriving in the source VRF is a candidate for a data MDT if the system matches the C-SG in the route map that you specify for the data MDT using the **ip pim data-mdt** command. The C-SG flow is initially forwarded on the default MDT. The system creates the data MDT when the flow rate exceeds a value you configure in the route map using the **set threshold** command.

When the Source C-PIM-SM first creates a data MDT for a C-SG flow, it sends a <C-SG, P-G> MDT join message with type, length, value (TLV) format to the default MDT. This message invites peer PE routers to join the new data MDT. It starts a timer that you can configure using the **mdt-data-delay** command to track the number of seconds before switching to the data MDT. When that timer expires, C-PIM-SM switches from sending C-SG data on the default MDT to sending data on the data MDT.

When the C-SG flow is switched to the data MDT, the Source C-PIM-SM starts a timer that you can configure using the **mdt-data-holddown** command to track the number of seconds before switching to the default MDT. When the timer expires, the data MDT is deleted and the C-SG flow switched back to the default MDT if the flow rate drops back below the threshold. If the flow rate exceeds the threshold, the timer restarts. If the timer expires and the flow rate is below the threshold, the data MDT is removed.

The Source C-PIM-SM maintains sent MDT Join TLV messages in its database as long as they are active. While the data MDT is active, C-PIM-SM resends that MLD Join TLV message using a setting that you can configure using the **mdt-interval** command to measure time in seconds between successive MLD join TLV messages.

Data MDT Receivers

When the Receiver C-PIM-SM receives a < C-SG, P-G > MDT Join TLV message from the default MDT, it extracts the C-SG and the data MDT P-Group address from the TLV and queries the route map that you specified for the data MDT to determine whether the C-SG is a candidate for a data MDT. If it matches, the C-PIM-SM adds the MDT Join TLV to its database and records the time.

If the Receiver C-PIM-SM does not receive an MDT Join TLV < C-SG, P-G > to refresh its database within the amount of time specified for the timeout in the **mdt-data-timeou**t command, the MDT Join TLV < C-SG > is removed from the database and the associated data MDT is removed.

When a new MDT Join TLV < C-SG, P-G > is added to the database, the Receiver C-PIM-SM determines whether it has an SG, SPT state. If it has an SG state, and the incoming interface (IIF) is the default MDT, then C-PIM-SM creates the data MDT and deletes the corresponding forwarding entry. C-PIM-SM waits for the source to transmit data on the data MDT. During this period, data can continue to be received on the default MDT. C-PIM-SM fails the reverse-path forwarding (RPF) check, which results in a forwarding entry with a discarded IIF.

If the C-SG,SPT state is created (either as a result of a C-SSM join or switch from RPT to SPT), and it is the default MDT, the Receiver C-PIM-SM determines whether an MDT Join TLV < C-SG > is active. If it is, C-PIM-SM creates the data MDT.

Establishing a Data MDT Using ASM or SSM

A data MDT carries one C-SG flow. If the data MDTs are established using any-source multicast (ASM), then the P-Group address selected by a PE for the data MDT must be unique to that PE in the MDT (that is, the range of MDT P-Group addresses available in the core must be administratively divided among all the PEs that will source VPN multicasts). The VRFs in a PE must share the P-Group addresses in the assigned range for the PE.

If the data MDTs are established using single-source multicast (SSM), you must configure VRFs to transmit on a tunnel using the same MDT P-Group address. Each VRF transmits using a unique P-Source address; however, each data MDT created by the VRF must use a different P-Group address. There might be one sender data MDT and possibly many receiver data MDTs sharing an IP tunnel. Each PE can assign MDT P-Groups from the same range, but the P-Group addresses must be administratively divided among the VPNs.

For a receiver on the data MDT, P-PIM-SM joins the data MDT by propagating join state into the core. The P-Group for that join is extracted from the MDT Join TLV. If SSM is not activated or the P-Group is not in the SSM group range, P-PIM-SM performs a <*, G> join towards the RP for that P-Group.

If SSM is activated and the P-Group is in the SSM group range, P-PIM-SM performs an <S, G> join towards the P-Source, where the P-Source address is the SA of the MDT Join TLV.

Configuring Data MDTs

To configure data MDTs:

1. Configure a dynamic interface profile to specify the PIM configuration of the IP/MTI interface in the VRF.

   ```
   host1(config)#profile pe13DataMdtMti
   host1(config-profile)#ip virtual-router "pe1:pe13"
   host1(config-profile)#ip unnumbered loopback 0
   host1(config-profile)#ip pim sparse-mode
   ```

2. Configure a dynamic interface profile to specify the IP/MDT interface in the parent.

   ```
   host1(config-profile)#profile pe1DataMdtMdt
   host1(config-profile)#ip virtual-router pe1
   host1(config-profile)#ip unnumbered loopback 0
   host1(config-profile)#ip pim sparse-mode
   ```

3. Configure the destination profile for dynamic IP tunnel creation.

   ```
   host1(config-profile)#gre destination profile pe13DataMdtProfile
   virtual-router pe1
   host1(config-dest-profile)#tunnel destination subnet 233.3.0.0 255.255.0.0
   host1(config-dest-profile)#tunnel source 1.1.1.1
   host1(config-dest-profile)#tunnel mdt profile pe1DataMdtMdt
   host1(config-dest-profile)#profile pe13DataMdtMti
   host1(config-dest-profile)#virtual-router pe1
   ```

   For more information about creating dynamic IP tunnels, see *JUNOSe IP Services Configuration Guide, Chapter 11, Configuring Dynamic IP Tunnels*.

4. Configure the VRF, including an access list to match <S,G> and <*,G> entries.

   ```
   host1:pe1(config)#ip vrf pe13
   host1:pe1(config-vrf)#rd 100:13
   host1:pe1(config-vrf)#route-target both 100:3
   host1:pe1(config-vrf)#interface tunnel gre:MTI-13.mdt
   host1:pe1(config-if)# ip unnumbered loopback 0
   host1:pe1(config-if)# ip pim sparse-mode
   host1:pe1(config-if)#access-list pe13DataMdt permit ip any 225.1.0.0
   0.0.255.255
   ```

5. Specify a route map to configure the set of (S, G) for which data MDTs can be created, and the threshold to be applied for each SG.

   host1:pe1(config)#**route-map pe13MdtThresholds permit 10**
   host1:pe1(config-route-map)#**match ip address pe13DataMdtSend**
   host1:pe1(config-route-map)#**set threshold 0**
   host1:pe1(config-route-map)#**route-map pe13MdtThresholds permit 20**
   host1:pe1(config-route-map)#**match ip address pe13DataMdt**

6. Configure the group address pools in the route map.

   host1:pe1(config-route-map)#**ip pim group-address-pool pe13DataMdtGroups 233.3.1.0 233.3.1.255**

   If the data MDTs are established using ASM, you must divide the range of available MDT P-Group addresses so that PEs source VPN multicasts. All VRFs in a PE draw from a single address pool that contains the range of group addresses assigned to that PE.

   If the data MDTs are established using SSM, you can configure VRFs to transmit on a tunnel using the same MDT P-Group address. Each VRF transmits using a unique P-Source address; however, each data MDT created by the VRF must use a different P-Group address. There might be one sender data MDT and possibly many receiver data MDTs sharing an IP tunnel.

   For SSM, each PE can assign MDT P-Groups from the same range, but the P-Group addresses must be administratively divided among the VPNs.

7. Configure the tunnel for the VRF.

   host1:pe1(config)#**virtual-router pe1:pe13**
   host1:pe1:pe13(config)#**interface tunnel gre:MTI-13 transport-virtual-router pe1**
   host1:pe1:pe13(config)#**tunnel source 1.1.1.1**
   host1:pe1:pe13(config)#**tunnel destination 235.3.3.3**
   host1:pe1:pe13(config)#**tunnel mdt**
   host1:pe1:pe13(config)#**ip unnumbered loopback 0**
   host1:pe1:pe13(config)#**ip pim sparse-mode**

8. Configure the data MDT.

   host1:pe1:pe13(config)#**ip pim data-mdt**
   host1:pe1:pe13(config-ip-pim-data-mdt)#**tunnel source 1.1.1.1**
   host1:pe1:pe13(config-ip-pim-data-mdt)#**tunnel group-address-pool pe13DataMdtG$**
   host1:pe1:pe13(config-ip-pim-data-mdt)#**route-map pe13MdtThresholds**

ip pim

- Use to enable PIM on an interface.
- Example

  host1(config-if)#**ip pim sparse-dense-mode**

- Use the **no** version to disable PIM on an interface.

ip pim data-mdt

- Use to activate data MDTs and enter IP PIM Data MDT Configuration mode.
- Example

  host1(config)#**ip pim data-mdt**

- Use the **no** version to deactivate data MDTs.

ip pim group-address-pool

- Use to configure PIM group address pools from which data MDT group addresses are allocated.
- Example

  host1(config)#**ip pim group-address-pool pe21DataMDT 232.1.0.0 232.2.255.255**

- There is no **no** version.

mdt-data-delay

- Use to configure a delay before switching to data MDT.
- The delay is measured by 0.1 seconds; the default is 30.
- Example

  host1(ip-pim-data-mdt-config)#**mdt-data-delay 20**

- Use the **no** version to return to the default.

mdt-data-holddown

- Use to configure the time in seconds before switching to the default MDT group from the data MDT group.
- The default is 60.
- Example

  host1(ip-pim-data-mdt-config)#**mdt-data-holddown 200**

- Use the **no** version to return to the default.

mdt-data-timeout

- Use to configure the time in seconds before the flow leaves the data MDT group.
- The default is 180.
- Example

  host1(ip-pim-data-mdt-config)#**mdt-data-timeout 160**

- Use the **no** version to return to the default.

mdt-interval

- Use to configure the time in seconds between successive MLD join TLV messages.
- The default is 60.
- Example

  host1(ip-pim-data-mdt-config)#**mdt-interval 80**

- Use the **no** version to return to the default.

set threshold

- Use to configure a threshold value for multicast VPN applications, including default MDT and data MDT.
- Example

  host1(config)#**set threshold 30**

- Use the **no** version to remove the threshold.

tunnel group-address-pool

- Use to configure a group address pool for a data MDT tunnel.
- Example

  host1(ip-pim-data-mdt-config)#**tunnel group-address-pool dataMDT1**

- Use the **no** version to delete the group address pool.

Using PIM Sparse Mode Join Filters

You can use PIM sparse mode join filters to prevent multicast state from being created in the PIM sparse mode router. The filters are applied to join entries in PIM join/prune messages that are received from PIM sparse mode neighbors.

By denying joins at the edge of a network, you can limit the multicast state and traffic in the network. By accepting only certain joins, you can control which multicast services an end user can receive. PIM join filters also reduce the potential for denial of service (DoS) attacks where large numbers of joins forwarded to each router on the RPT can result in a PIM state explosion and very high memory consumption.

For information about how to create access lists, see *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

ip pim join-filter

- Use to specify an extended access list that you want this PIM interface to use as a join filter.
- You can apply the join filter at the global level or at the interface level.
- If an interface-level filter exists, it takes precedence over the global-level filter.

- Example 1

  host1(config)#**ip pim join-filter gold**

- Example 2

  host1(config-interface)#**ip pim join-filter gold**

- Use the **no** version to remove the filter association.

Configuring PIM SSM

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is networking technology that targets audio and video broadcast application environments.

To configure PIM SSM, you enable PIM SSM on the router and define the SSM range of IP multicast addresses.

To use PIM SSM, IGMPv3 must be configured on customer premise equipment (CPE)–facing interfaces to receivers, and PIM sparse mode must be configured on CPE-facing interfaces to sources and on core-facing interfaces. After configuring SSM, you can use the **show ip pim sparse-mode sg-state** command to display SSM group membership information.

To configure PIM SSM:

1. Enable PIM SSM on the E-series router. The IANA SSM range is configured by default. You can modify the SSM address range by using the access list.

   host1(config)#**access-list 15 permit ip any host 239.0.0.2**
   host1(config)#**access-list 15 permit ip any 232.0.0.0 0.225.225.225**
   host1(config)#**ip pim ssm range 15**

2. Enable PIM sparse mode on the CPE-facing interface towards the source or core.

3. Enable IGMPv3 on the CPE-facing interface towards the receiver. PIM SSM also works with IGMPv2 if you configure the ssm-map in IGMP as in the following example:

PIM SSM also works with IGMPv2 if you configure the ssm-map in IGMP as in the following example:

host1(config)#**ip pim ssm**
host1(config)#**access-list ssm_map1 permit 232.0.0.1 255.255.255.255**
host1(config)#**ip igmp ssm-map enable**
host1(config)#**ip igmp ssm-map static ssm_map1 51.0.0.1**

The **no** version disables ssm-map:

host1(config)#**no ip igmp ssm-map static ssm_map1 51.0.0.1**

ip pim ssm

- Use to enable PIM SSM and define the SSM range for IPv4 multicast addresses.
- Use the **range** keyword to define the SSM range of IP multicast addresses.
- Example 1—Enables SSM with addresses in the IANA range. The SSM address range is set as the default and by default, the SSM group multicast address is limited to the IPv4 address range 232.0.0.0/6.

  host1(config)#**ip pim ssm**

- Example 2—Configures Class D addresses outside of the default SSM range.

  host1(config)#**access-list alist permit any 223.0.0.0 0.255.255.255**
  host1(config)#**ip pim ssm range alist**

- Example 3—Resets the SSM address range to the default.

  host1(config)#**ip pim ssm default**

- Use the **no** version to disable SSM.

Configuring the BFD Protocol for PIM

The **ip pim bfd-liveness-detection** command configures the Bidirectional Forwarding Detection (BFD) protocol for PIM. The BFD protocol uses control packets and shorter detection time limits to more rapidly detect failures in a network. Also, because they are adjustable, you can modify the BFD timers for more or less aggressive failure detection.

PIM routers send periodic hello messages from each PIM-enabled interface. You can configure this interval using the **ip pim query-interval** command. By default, the PIM router sends a hello message every 30 seconds (with an interval range of 0–210 seconds). If it receives no response from a neighbor within 3.5 times the interval value (a minimum of 3.5 seconds), the PIM router drops the neighbor.

In contrast, when a BFD session exists between neighbors, a PIM neighbor that goes down is detected quickly (in milliseconds rather than in seconds).

When you issue the **ip pim bfd-liveness-detection** command on a PIM router, the router establishes BFD liveness detection with all BFD-enabled PIM neighbors. When the local router receives an update from a remote PIM neighbor—if BFD is enabled and if the session is not already present—the local router attempts to create a BFD session to the remote neighbor.

Each adjacent pair of neighbors negotiates an acceptable transmit interval for BFD packets. The negotiated value can be different on each neighbor. Each neighbor then calculates a BFD liveness detection interval. When a neighbor does not receive a BFD packet within the detection interval, it declares the BFD session to be down.

NOTE: Before the router can use the **ip pim bfd-liveness-detection** command, you must specify a BFD license key. To view an already configured license, use the **show license bfd** command.

For general information about configuring and monitoring the BFD protocol, see *JUNOSe IP Services Configuration Guide, Chapter 5, Configuring BFD*.

ip pim bfd-liveness-detection

- Use to enable BFD (bidirectional forwarding detection) and define BFD values to more quickly detect PIM data path failures.
- The neighbors in a PIM network use the configured values to negotiate the actual transmit intervals for BFD packets.
  - You can use the **minimum-transmit-interval** keyword to specify the interval at which the local router proposes to transmit BFD control packets to its neighbors. The default value is 300 milliseconds.
  - You can use the **minimum-receive-interval** keyword to specify the minimum interval at which the local router must receive BFD control packets from its neighbors. The default value is 300 milliseconds.
  - You can use the **minimum-interval** keyword to specify the same value for both of those intervals. Configuring a minimum interval has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value. The default value is 300 milliseconds.
- You can use the **multiplier** keyword to specify the detection multiplier value. The calculated BFD liveness detection interval can be different on each neighbor. The multiplier value is roughly equivalent to the number of packets that can be missed before the BFD session is declared to be down. The default value is 3.
- For details on liveness detection negotiation, see *Negotiation of the BFD Liveness Detection Interval* section in *JUNOSe IP Services Configuration Guide, Chapter 5, Configuring BFD*.
- You can change the BFD liveness detection parameters at any time without stopping or restarting the existing session; BFD automatically adjusts to the new parameter value. However, no changes to BFD parameters take place until the values resynchronize with each neighbor.
- Example

  host1(configif)#**ip pim bfd-liveness-detection minimum-interval 800**

- Use the **no** version to disable BFD on the PIM interface.

Removing PIM

To remove PIM from a VR, use the **no router pim** command.

router pim

- Use to create and enable PIM processing on a VR or to access Router Configuration mode.
- Example

  host1:boston(config)#**router pim**

- Use the **no** version to remove PIM from the VR.

Resetting PIM Counters and Mappings

You can use the **clear ip pim** commands to reset PIM counters and mappings.

clear ip pim auto-rp

- Use to clear the group-to-RP router mappings that the router learned through auto-RP.
- Specify the IP address of an RP to clear the group-to-RP mappings for a particular RP. If you do not specify an IP address, the router clears the group-to-RP mappings on all RP routers learned through auto-RP.
- Example

  host1#**clear ip pim auto-rp 192.34.56.7**

- There is no **no** version.

clear ip pim interface count

- Use to clear the counters for multicast packet statistics on all interfaces or a specified interface.
- Specify an interface type and specifier, such as atm 3/0, to clear the counters on that interface. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- If you do not specify an interface, the router clears the counters on all interfaces.
- Example

  host1#**clear ip pim interface atm 3/0.5 count**

- There is no **no** version.

Monitoring PIM

You can display information about PIM events and parameters.

Monitoring PIM Events

You can use the debug PIM commands to view information about PIM events.

debug ip pim

- Use to show information about the selected event.
- To control the type of events displayed, specify a severity level.
- To control how much information to display, specify a verbosity level.
- Example

  host1#**debug ip pim events severity 1 verbosity low**

- Use the **no** version to disable the display.

undebug ip pim

- Use to turn off the display of information previously enabled with the **debug ip pim** command.
- Example

  host1#**undebug ip pim events**

- There is no **no** version.

Monitoring PIM Settings

You can use the **show ip pim** commands to display information about PIM settings.

show ip pim

- Use to view general PIM router-level information.
- Field descriptions
  - Default PIM Version—Default PIM version number (always 2)
  - Default Domain Id—Default Domain Id (always 0)
  - Default Hello period—Default interval (in minutes) at which the router sends hello messages to neighbors
  - Default Hello Hold Time—Default time (in minutes) for which the router keeps the neighbor state alive
  - Default J / P Hold Time—Hold time value (in seconds) set in Join/Prune messages originated by this PIM router
  - Keepalive Period—Time SG join state is maintained in the absence of SG Join message
  - Assert Time—Period after last assert before assert state is timed out
  - Register Suppression Time—Period during which a designated router stops sending registers to the RP

- Register Probe Time—Time before register suppression time (RST) expires when a designated router might send a NULL-Register to the RP
- Register TTL—TTL value (in PIM register packets) originated by this PIM router
- SSM—State of SSM on this PIM router (enabled or disabled)
- range—Default SSM group range or name of the access list specifying the range
- Sparse-Mode Graceful Restart Duration—Restart interval in seconds
- Join filter—Name of the join filter access-list (if configured) for this PIM router

- Example

```
host1:1#show ip pim
Default PIM Version: 2
Default Domain Id: 0
Default Hello Period: 30
Default Hello HoldTime: 105
Default J/P HoldTime: 210
Keepalive Period: 210
Assert Time: 210
Register Suppression Time: 60
Register Probe Time: 5
Register TTL: 64
SSM enabled, range default
Sparse-Mode Graceful Restart Duration: 30
Graceful restart is complete (timer 0 seconds)
Join filter, access-list bronze
```

show ip pim auto-rp

- Use to display information about RP routers and the RP mapping agent in a PIM sparse mode environment.
- Field descriptions
  - Configured with ttl—Number of hops for which the RP discovery message is valid
  - Using interface addr—IP address of the interface from which the router sends RP discovery messages
  - interval—Time interval, in seconds, at which the router sends RP discovery messages
  - PIM AutoRP candidate RP mapping(s)—Routers that the RP mapping agent is evaluating to determine an RP router for this interface
- Example 1

```
host1:1#show ip pim auto-rp
This PIM router is an Auto RP mapping agent.
  Configured with ttl 64
  [ Using interface addr 121.0.0.1, interval 60 ].
PIM AutoRP candidate RP mapping(s)
```

- Example 2

```
host1:1#show ip pim auto-rp
This PIM router is _not_ an Auto RP mapping agent.
PIM AutoRP candidate RP mapping(s)
Candidate RP 122.0.0.1
  Group(s) 224.0.0.0/4, AutoRP, ttl 64, interval 60, from access List 1
Candidate RP 122.0.0.1
  Group(s) 224.0.1.39/32 (negative), AutoRP, ttl 64, interval 60, from access List 1
Candidate RP 122.0.0.1
  Group(s) 224.0.1.40/32 (negative), AutoRP, ttl 64, interval 60, from access List 1
```

show ip pim bsr

- Use to display BSR information and the group prefixes for which the local router is a candidate RP in a PIM sparse mode environment.
- Field descriptions
  - Candidacy—Whether the router is a candidate BSR
  - Configured on—Interface on which the router is configured
  - address—Address of the router
  - hashMaskLen—Hash mask length
  - priority—Priority of the router
  - period—Time between bootstrap messages, in seconds
  - Elected BSR—This router or IP address of the elected bootstrap router
  - next BSM—If BSR is this router, time until the next bootstrap message is sent, in seconds
  - expires in—If BSR is not this router, time until the elected BSR expires if no bootstrap messages are received
  - Local candidate RP mapping(s)—Routers that the mapping agent is evaluating to determine an RP router for this interface
- Example 1—On a router that is the elected BSR

```
host1:1#show ip pim bsr

This PIM router is a Candidate BSR.
  Configured on intf ATM3/0.101, address: 101.0.0.1
  hashMaskLen 30, priority 2, period 60 seconds.
Elected BSR is this router, next BSM in 3 seconds.

Local candidate RP mapping(s):
Candidate RP 101.0.0.1
  224.0.0.0/4, BSR, hold-time 150, interval 60, priority 192
  228.0.0.0/24, BSR, hold-time 150, interval 60, priority 192, from
access-list acl
  230.0.0.0/24, BSR, hold-time 150, interval 60, priority 192, from
access-list acl
```

- Example 2—On a router that is a candidate BSR

```
host1:1#show ip pim bsr
This PIM router is a Candidate BSR.
  Configured on intf ATM3/0.100, address: 100.0.0.1
  hashMaskLen 30, priority 2, period 60 seconds.
Elected BSR is 101.0.0.1 (priority 0), expires in 73 seconds.
```

- Example 3—On a router that is not a candidate BSR

```
host1:1#show ip pim bsr
This PIM router is not a Candidate BSR.
Elected BSR is 101.0.0.1 (priority 0), expires in 73 seconds.
```

show ip pim data-mdt

- Use to display information about active data MDTs.
- To display information about data MDTs on which the provider edge transmits data, use the **sender** keyword.
- To display information about data MDTs on which the provider edge receives data, use the **receiver** keyword.
- To display information about an IP PIM group address pool, use the **group** keyword.
- To display a summary of configuration for each data MDT, use the **summary** keyword.
- To display the number of data MDTs, use the **count** keyword.
- Field descriptions
  - PE *Name*—Name of the PE
  - C-SG—Address of the C-SG
  - P-SG—Address of the P-SG
  - MTI—Name of the dynamic IP tunnel on which the data MDT was created
  - Data rate/Threshold—Rate and threshold of multicast data
  - Time until next MDT Join TLV—Configured delay until next MDT Join TLV
  - Time until MDT Join TLV expires—Configured delay until MDT Join TLV expires
  - Time until switchover from default-MDT—Configured delay until the data MDT switches over to the default MDT
- Example 1—Displays information about a data MDT sender

```
host1:PE1#show ip pim data-mdt 225.1.1.1
PE11 - Sender
  C-SG: 10.11.0.100, 225.1.1.1
  P-SG: 1.1.1.1, 235.0.1.1
  MTI: TUNNEL gre:mvpn-dynamic-1
    Data rate/Threshold: 10012/500 Kbps
    Time until next MDT Join TLV: 25 seconds
```

- Example 2—Displays information about a data MDT receiver

```
host1:PE1#show ip pim data-mdt 225.2.2.2
PE31 - Receiver
  C-SG: 10.13.0.100, 225.2.2.2
  P-SG: 3.3.3.3, 235.0.1.1
  MTI: TUNNEL gre:mvpn-dynamic-3
    Time until MDT Join TLV expires: 29 seconds
```

- Example 3—Displays a summary of data MDT senders

```
host1:PE1#show ip pim data-mdt senders summary

VRF   S/R      C-Group    C-Source     P-Group   P-Source         MTI
----   -------   ---------   -----------   ---------  --------
---------------
PE11   Sender   225.1.1.1   10.11.0.100    235.0.1.1  1.1.1.1    TUNNEL
gre:mvpn-dynamic-1
PE12   Sender   225.1.1.1   10.12.0.100    235.0.1.2  1.1.1.1    TUNNEL
gre:mvpn-dynamic-2

Counts: 2 senders, 0 receivers, total 3.
```

- Example 4—Displays the number of data MDT senders and receivers

```
host1:PE1#show ip pim data-mdt count
Counts: 2 senders, 1 receivers, total 3.
```

show ip pim dense-mode sg-state

- Use to display information for each (Source, Group) pair for PIM dense mode.
- Field descriptions
  - (Source, Group) pair—IP addresses of multicast source and group
  - EntryExpires—Time until the (S,G) pair entry expires
  - RPF Route—Reverse-path forwarding route
  - IIF—IP address of incoming interface
  - UpNbr—IP address of upstream neighbor
  - Pruned Oifs—Outgoing interfaces that have been pruned
    - Address—IP address of outgoing interface
    - IfId—Index of the interface
    - Pruned due to—Reason for prune: assert or explicit prune
    - Pruned time remaining—Time in seconds until the prune expires
- Example

```
host1:8#show ip pim dense-mode sg-state
PIM DM route table and pruned oif information
<122.0.0.1, 224.0.1.39>   EntryExpires: 99
  RPF Route: 122.0.0.0/255.0.0.0   IIF: 107.0.8.4   UpNbr: 107.0.4.8
  Pruned Oifs:
   Address: 108.0.8.5   IfId: 95
    Pruned due to assert
    Pruned time remaining 129
<130.0.0.2, 224.0.1.39>   EntryExpires: 100
  RPF Route: 130.0.0.0/255.0.0.0   IIF: 107.0.8.4   UpNbr: 107.0.4.8
```

```
  Pruned Oifs:
   Address: 108.0.8.5   IfId: 95
    Pruned due to assert
    Pruned time remaining 130
<121.0.0.1, 224.0.1.40>   EntryExpires: 102
  RPF Route: 121.0.0.0/255.0.0.0   IIF: 107.0.8.4   UpNbr: 107.0.4.8
  Pruned Oifs:
   Address: 108.0.8.5   IfId: 95
    Pruned due to assert
    Pruned time remaining 133
```

show ip pim interface

- Use to display information about PIM interfaces.
- Specify no keywords or variables to view information about all PIM interfaces.
- Provide an interface type and specifier (such as atm 3/0) to display information about that interface only. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Specify the **summary** keyword to view the number of configured, enabled, and disabled PIM dense mode, PIM sparse mode, and PIM sparse-dense mode interfaces.
- Specify the **count** keyword to view the number of multicast packets that the interface has sent and received.
- Field descriptions
  - Interface Addr—IP address of the interface
  - Interface Name—Type and specifier of the interface. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
  - Ver—Version of PIM running on this interface
  - Mode—PIM mode running on this interface: Sparse, Dense, or SparseDense
  - Nbr Count—Number of neighbors connected to this interface
  - Hello Intvl—Time interval, in seconds, at which the interface sends hello messages to neighbors
  - DR Addr—Address of the designated router
  - SM—Number of PIM sparse mode interfaces
  - DM—Number of PIM dense mode interfaces
  - SM/DM—Number of PIM sparse-dense mode interfaces
    - enabled—Number of interfaces administratively enabled
    - disabled—Number of interfaces administratively disabled
  - ControlPktCount In|Out—PIM messages received on and sent from this interface
    - Hello—Total number of hello messages
    - JoinPrune—Total number of join and prune messages
    - Assert—Total number of assert messages

- Example 1

```
host1#show ip pim interface
Interface                                          Nbr    Hello                          BFD
  Addr         Interface      State   Ver    Mode    count   Intvl   DR Addr   JoinFilter Enabled
---------   ---------------   -----   ---   ------   -----   -----   -------   ----------   -----
1.1.1.2     FastEthernet1/1   up      2     Sparse   1       30      1.1.1.2   ---          yes


Interface                                          Nbr    Hello                          BFD
  Addr         Interface      State   Ver    Mode    count   Intvl   DR Addr  JoinFilter  Enabled
---------   ---------------   -----   ---   ------   -----   -----   -------  ----------   ------
1.1.1.2     FastEthernet1/1   up      2     Sparse   1       30      1.1.1.2   ---          no
```

- Example 2

```
host1#show ip pim interface summary
PIM Interface Summary
  SM:    0, 0 enabled, 0 disabled
  DM:    0, 0 enabled, 0 disabled
  SM/DM: 1, 0 enabled, 1 disabled
```

- Example 3

```
host1#show ip pim interface count
PIM Interface Count
Interface Addr  Interface Name       ControlPktCount In|Out
                                     Hello     JoinPrune  Assert
192.32.10.20    ATM3/0.20             0         0          0
                                      0         0          0
```

show ip pim neighbor

- Use to display information about PIM neighbors that the router discovered.
- Provide an interface type and specifier (such as atm 3/0) to display information about that interface only. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Field descriptions
  - Neighbor Addr—IP address of the neighbor
  - Interface Name—Type and specifier of the interface to which the neighbor connects. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
  - Uptime—Time since the router discovered this neighbor in *days hours:minutes:seconds* format
  - Expires—Time available for the neighbor to send a hello message to the interface. If the neighbor does not send a hello message during this time, it no longer is a neighbor.
  - Ver—Version of PIM that the neighbor is running
  - Mode—PIM mode that the neighbor is using: Sparse, Dense, or SparseDense
  - BFD—BFD status: up or down

- Example

```
host1#show ip pim neighbor
Neighbor
  Addr     Interface Name     Uptime    Expires    Ver    Mode    BFD
--------   ---------------   --------   --------   ---   ------   ---
1.1.1.1    FastEthernet1/1   00:02:49   00:01:27   2     Sparse

Neighbor
  Addr     Interface Name     Uptime    Expires    Ver    Mode    BFD
--------   ---------------   --------   --------   ---   ------   ---
1.1.1.1    FastEthernet1/1   00:03:16   00:01:30   2     Sparse   up

Neighbor
  Addr     Interface Name     Uptime    Expires    Ver    Mode    BFD
--------   ---------------   --------   --------   ---   ------   ----
1.1.1.1    FastEthernet1/1   00:00:07   00:01:39   2     Sparse   down
```

show ip pim rp

- Use to display information about PIM group-to-RP mappings.
- Specify the address of a group to view PIM group-to-RP mappings for a particular group.
- Specify the mapping keyword to display all group-to-RP mappings that the router has recorded.
- Field descriptions
  - Group(s)—Prefix of the multicast group
  - RP—IP address of RP router for the multicast group
  - priority—Priority of the router
  - via—Method by which the RP router was assigned: AutoRP, Static RP, or BSR
  - expiryTime—Time in seconds at which the RP mapping becomes invalid, unless the mapping agent (access list) reassigns the RP router to this group
- Example 1

```
host1:8#show ip pim rp mapping
PIM Group-to-RP mapping(s)
Group(s) 224.0.0.0/4
  RP 122.0.0.1,  priority 0,  via  AutoRP, expiryTime 88
Group(s) 224.0.1.39/32 (negative)
  RP 122.0.0.1,  priority 0,  via  AutoRP (Negative), expiryTime 88
Group(s) 224.0.1.40/32 (negative)
  RP 122.0.0.1,  priority 0,  via  AutoRP (Negative), expiryTime 88
```

- Example 2

```
host1:8#show ip pim rp mapping
PIM Group-to-RP mapping(s)
Group(s) 224.0.0.0/4
  RP 134.0.0.1, priority 0, via Static, from access-list 1
Group(s) 232.0.0.0/16
  RP 134.0.0.1, priority 0, via BSR, expires in 121 seconds
```

show ip pim rp-hash

- Use to show which RP router that a multicast group is using.
- Field descriptions
  - Group(s)—Multicast group or groups
  - RP—RP router for the multicast group
  - priority—Priority of the router
  - via—Method by which the RP router was assigned: AutoRP, Static RP, or BSR
  - expiryTime—Time in seconds at which the RP mapping becomes invalid, unless it is renewed by the mapping agent
- Example 1

```
host1:2#show ip pim rp-hash 232.1.1.1
Group(s) 224.0.0.0/4
  RP 122.0.0.1,  priority 0,  via  AutoRP, expiryTime 128
```

- Example 2

```
host1:2#show ip pim rp-hash 226.0.0.1
Group(s) 226.0.0.0/24
  RP 101.0.0.1, priority 192, via BSR, expires in 145 seconds
 *RP 145.0.0.3, priority 192, via BSR, expires in 145 seconds
```

show ip pim sparse-mode sg-state

- Use to display information for each (S,G) pair for PIM sparse mode and PIM SSM.
- Field descriptions
  - (S, G) pair—Source, Group pair for which information is provided
  - Group-to-RP mapping—IP addresses and network mask of the multicast group
  - RP—IP address of RP router
  - SSM group—Indicator that this is an SSM group
  - RPF Route—IP address and network mask of the RPF route
  - IIF—IP address of the incoming interface for the RPF route
  - UpNbr—IP address of the upstream neighbor
  - Oifs—Outgoing interface
  - Auto RP Discovery SELF oif—Indicates that RP router for this group was assigned through auto-RP
  - Register Oif to RP—IP address of RP router for the outgoing interface; suppressed for SSM
  - Address—IP address of outgoing interface
  - Interface—Type and specifier of the interface. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.

- Joined as—Type of mapping
  - (S, G)—Mapping from a specific source to a specific group
  - (*, G)—Mapping from any source to a specific group
  - (*, * , RP)—Mapping from any source to any group
- Join expires—Number of seconds before the (S,G) membership expires
- Count of entries—Total counts of (S,G) pair mappings

- Example

```
host1:2#show ip pim sparse-mode sg-state
PIM SM route table and oif information
<*, 224.0.1.40>
  Group-to-RP mapping: 224.0.0.0/240.0.0.0   RP: 123.0.0.1
  RPF Route: 123.0.0.0/255.0.0.0   IIF: 106.0.7.3   UpNbr: 106.0.3.7
  Oifs:
   Auto RP Discovery SELF oif.
    Joined as <*, G>

<*, 225.1.2.3>
  Group-to-RP mapping: 224.0.0.0/240.0.0.0   RP: 123.0.0.1
  RPF Route: 123.0.0.0/255.0.0.0   IIF: 106.0.7.3   UpNbr: 106.0.3.7
  Oifs:
   Address: 78.7.7.7   Interface: loopback7
    Local group membership present.
<*, 235.1.1.1>
  Group-to-RP mapping: 224.0.0.0/240.0.0.0   RP: 123.0.0.1
  RPF Route: 123.0.0.0/255.0.0.0   IIF: 106.0.7.3   UpNbr: 106.0.3.7
  Oifs:
   Address: 78.7.7.7   Interface: loopback7
    Local group membership present.

<118.1.33.34, 232.0.0.1>
  SSM Group
  RPF Route: 118.1.0.0/255.255.0.0   IIF: 118.1.0.1 (Directly attached)
  Oifs:
   Register Oif to RP: 141.0.0.2 suppressed for SSM Group.
   Address: 134.0.0.1   Interface: ATM3/0.104
    Joined as <S, G>   Join Expires: 161

<118.1.33.35, 232.0.0.1>
  SSM Group
  RPF Route: 118.1.0.0/255.255.0.0   IIF: 118.1.0.1 (Directly attached)
  Oifs:
   Register Oif to RP: 141.0.0.2 suppressed for SSM Group.
   Address: 134.0.0.1   Interface: ATM3/0.104
    Joined as <S, G>   Join Expires: 161

<10.0.1.8, 235.1.1.1>      EntryExpires: 143
  Group-to-RP mapping: 224.0.0.0/240.0.0.0   RP: 123.0.0.1
  RPF Route: 10.0.0.0/255.0.0.0   IIF: 106.0.7.3   UpNbr: 106.0.3.7
  Oifs:
   Address: 78.7.7.7   Interface: loopback7
    Joined as <*, G>

Count of entries - <S, G>    : 3
                   <*, G>    : 3
                   <*, *, RP>: 0
```

show ip pim sparse-mode unicast-route

- Use to display the unicast routes that PIM sparse mode is using.
- Field descriptions
  - Route—IP address and network mask for the unicast route
  - RpfNbr—RPF neighbor
  - Iif—Incoming interface for the unicast route
  - Pref—Preference value for the unicast route
  - Metric—Value of metric for the unicast route (type of metric varies with the unicast protocol)
  - Count of entries—Number of unicast routes that PIM sparse mode is using
- Example

```
host1:2#show ip pim sparse-mode unicast-route
PIM SM unicast route table information
Route                          RpfNbr          Iif             Pref  Metric
------------------------------------------------------------------------------
122.0.0.0      /255.0.0.0                       122.0.0.1       255   1
Count of entries: 1
```

show ip pim spt-threshold

- Use to display the threshold for switching to the shortest path tree at a PIM designated router.
- Field descriptions
  - Access List Name—Name of the IP access list that specifies the groups to which the threshold applies
  - SptThreshold (in kbps)—Value at which PIM sparse mode switches from a shared tree to an SPT. A value of infinity indicates that PIM sparse mode never switches to an SPT.
- Example

```
host1:2#show ip pim spt-threshold
Access List Name                SptThreshold(in kbps)
------------------------------------------------------
1                               infinity
```