Chapter 7

Configuring PIM for IPv6 Multicast

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

This chapter describes how to configure PIM for IPv6 multicast on the E-series router; it contains the following sections:

- Overview on page 206
- Platform Considerations on page 208
- References on page 209
- Before You Begin on page 209
- Enabling and Disabling PIM on a VR on page 209
- Enabling PIM on an Interface on page 210
- Configuring an RP Router for PIM Sparse Mode on page 210
- Configuring BSR and RP Candidates for PIM Sparse Mode on page 211
- Switching to an SPT for PIM Sparse Mode on page 212
- Configuring PIM Sparse Mode Remote Neighbors on page 213
- Using PIM Sparse Mode Join Filters on page 215
- Configuring PIM SSM on page 215
- Configuring the BFD Protocol for PIM on page 217
- Removing PIM on page 218
- Resetting PIM Counters and Mappings on page 218
- Monitoring PIM on page 219

Overview

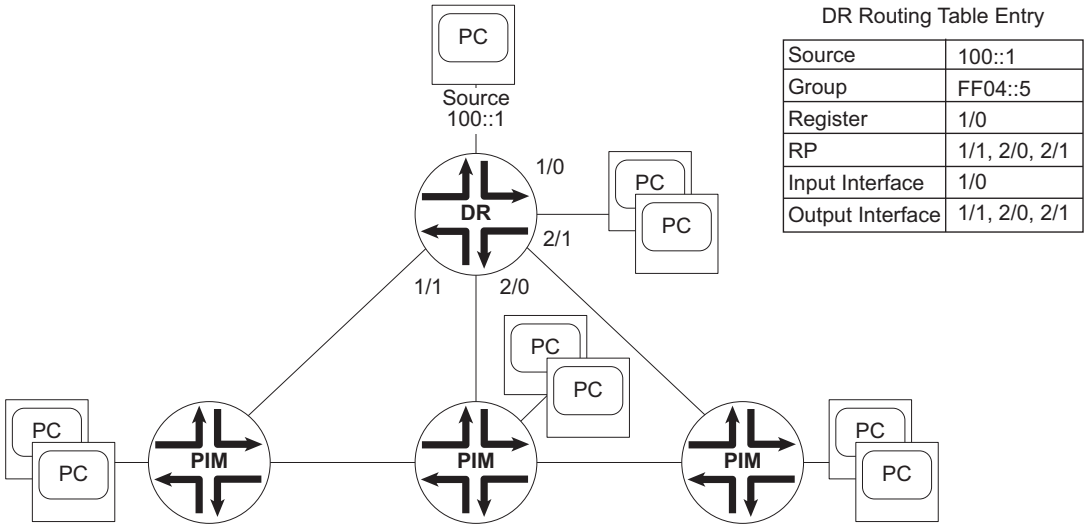
This implementation of PIM supports PIM sparse mode and PIM source-specific multicast (PIM SSM) for IPv6 multicast.

SSM is an extension to the Any Source Multicast (ASM) service model and facilitates the deployment of broadcast (one-to-many) applications, such as Internet TV and radio where large receiver audiences require traffic from a few well-known sources.

Figure 19 represents how PIM builds an (S,G) entry in an SRT. When multiple routers are connected to a multiaccess network, one router is assigned the role of 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.

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.

Figure 19: Source-Rooted Tree



PIM Sparse Mode

In addition to the features PIM sparse mode supports for IPv4, this IPv6 implementation of PIM sparse mode also supports remote neighbors.

For a description of PIM sparse mode, see *Chapter 3, Configuring PIM for IPv4 Multicast*.

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 MLD. 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. Two bootstrap mechanisms exist—bootstrap router (BSR) or auto-RP. Auto-RP is not used in IPv6 implementations.

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.

PIM Source-Specific Multicast

PIM source-specific multicast (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 IPv6 address range FF3x::/96 where x represents any valid scope. You can use the **ipv6 pim ssm range** command to change the SSM group address range.

Advantages that an SSM-configured network has 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 MLDv2 on the receiver local area network).
- Support for source lists; you can use source lists, supported in MLDv2, where only specified sources send traffic to the SSM group.

In a PIM SSM–configured network, the E-series router subscribes to an SSM channel (by means of MLDv2), announcing a desire 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 for IPv6 multicasting 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 IPv6 multicasting.

For information about modules that support PIM for IPv6 multicasting 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 for IPv6 multicasting.

References

For more information about IPv6 multicast, see the following resources:

- 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)

Before You Begin

You can configure multicast on IPv4 and IPv6 interfaces.

For information about configuring IP interfaces, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*. For information about configuring IPv6 interfaces, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 2, Configuring IPv6*.

For information about configuring PIM on IPv4 interfaces, see *Chapter 3, Configuring PIM for IPv4 Multicast*.

Enabling and Disabling PIM on a VR

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

1. Enable multicast routing.
2. Create a VR, or access the VR context.
3. Create and enable PIM processing.

```
host1(config)#virtual-router boston
host1:boston(config)#ipv6 router pim
```

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

ipv6 router pim

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

  ```
  host1:boston(config)#ipv6 router pim
  ```

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

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 allowed modes and specify how often the interface sends hello messages to neighbors.

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

ipv6 pim query-interval

- Use to specify how often the router sends hello messages to neighbors.
- Example

  host1(config-if)#**ipv6 pim query-interval**

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

ipv6 pim sparse-mode

- Use to enable PIM in sparse mode on an interface.
- Example

  host1(config-if)#**ipv6 pim sparse-mode**

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

Configuring an RP Router for PIM Sparse Mode

When you use the router for PIM sparse mode, some VRs must act as RP routers. If you want to control PIM more tightly, you can configure a static RP router. To do so:

1. Configure an access list that details the multicast groups that can use the static RP router (in this case, all globally scoped multicast groups).

   host1(config)#**ipv6 access-list boston permit ff0e::/16 any**

2. Specify a static RP router.

   host1(config)#**ipv6 pim rp-address ::122:1 boston**

ipv6 pim rp-address

- Use to specify a static PIM RP router.
- Specify a standard IPv6 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)#**ipv6 pim rp-address 2001::1 76 override**

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

Configuring BSR and RP Candidates for PIM Sparse Mode

When choosing candidate BSRs or candidate RPs, 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 the set 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.

Candidate RPs are routers that are capable of performing as a rendezvous point router for one or more multicast groups. Candidate RPs periodically advertise the set of groups they support to BSRs. A candidate RP may support all the multicast group address range or any subset thereof. You can achieve redundancy by configuring more than one candidate RP for a group or range of groups.

ipv6 pim bsr-candidate

- Use to define a router as a BSR candidate.
- To assign an interface from which the router should send 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 a 128 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 32 limits the group address to the first 32 bits. The default and maximum hash mask length is 126 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 (from 1 to 65535 seconds) at which the BSR sends bootstrap messages. The default value is 60 seconds.
- Example

  host1(config)#**ipv6 pim bsr-candidate loopback 1 30 10**

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

ipv6 pim rp-candidate

- Use to define a router as an RP router candidate.
- To assign an interface from which the router should send 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. If you do not specify a group list, the default is the entire multicast address range.

NOTE: You should not configure negative (that is, deny) access-list entries. BSR has no mechanism for distributing negative entries.

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

  host1(config)#**access-list 1 permit 1001::1**
  host1(config)#**access-list 1 permit 1002::1**
  host1(config)#**ipv6 pim rp-candidate loopback 1 group-list 1**

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

Switching to an SPT for PIM Sparse Mode

PIM sparse mode initiates multicast 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 can be more efficient than multicasting over a shared tree (see *PIM Sparse Mode* on page 80).

ipv6 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 to configure PIM to switch to an SPT when a source starts sending multicast messages.
- Example

  host1(config)#**ipv6 pim spt-threshold 4**

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

Configuring PIM Sparse Mode Remote Neighbors

You must use PIM sparse mode remote neighbors to run multicast services over BGP/MPLS VPNs.

NOTE: Although you can configure PIM sparse mode remote neighbors, you can not use these remote neighbors for BGP/MPLS VPNs.

To configure a pair of E-series routers to act as PIM remote neighbors:

1. On one router, specify the other router to be a remote neighbor, and identify the IP address of the interface on the other router that is used for the connection to this router.

   host1(config-router):boston#**remote-neighbor 1001::1 sparse-mode**

2. Specify the location of the local interface whose address is used as the source address for the PIM connection to a remote neighbor.

   host1(config-router-rn):boston#**update-source atm 2/1.108**

3. (Optional) Specify how often the router sends hello messages to the remote neighbor.

   host1(config-router-rn):boston#**query-interval 40**

4. Repeat Steps 2 to 3 for the other router.

query-interval

- Use to specify how often the router sends hello messages to remote neighbors.
- Example

  host1(config-router-rn)#**query-interval 40**

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

remote-neighbor

- Use to specify a remote neighbor for PIM sparse mode.
- Specify the IP address of the interface on the remote neighbor that PIM uses as the source address for the connection to this router.
- Example

  host1(config-router)#**remote-neighbor 1001::1 sparse-mode**

- Use the **no** version to remove the remote neighbor and any attributes configured for the remote neighbor.

update-source

- Use to specify the PIM interface whose local address is used as the source address for the PIM connection to a remote neighbor.
- You can use the same source address to form neighbor adjacencies with more than one PIM remote neighbor.
- You must use the IPv6 address of this interface when issuing the **remote-neighbor** command on the remote neighbor.
- Example

  host1(config-router-rn)#**update-source loopback 5**

- Use the **no** version to delete the source address from the connection to the remote neighbor.

Configuration Example

This example uses the configuration shown in Figure 19 on page 206. Two E-series routers called router Boston and router Chicago are running PIM and are connected by MPLS tunnels. To configure the routers as PIM remote neighbors:

1. Specify that router Chicago will be a remote neighbor of router Boston, and identify the IP address on router Chicago that will transmit datagrams to router Boston.

   boston(config-router)#**remote-neighbor 1001::1 sparse-mode**

2. Specify the location of the interface that will transmit datagrams from router Boston to router Chicago.

   boston(config-router-rn)#**update-source atm 2/1.108**

3. Specify that router Boston will send hello messages to router Chicago every 40 seconds.

   boston(config-if)#**ipv6 pim query-interval 40**

4. Specify that router Boston will be a remote neighbor of router Chicago, and identify the IP address on router Boston that will transmit datagrams to router Chicago.

   chicago(config-router)#**remote-neighbor 2001::1 sparse-mode**

5. Specify the location of the interface that will transmit datagrams from router Chicago to router Boston.

   chicago(config-router-rn)#**update-source atm 2/1.95**

6. Specify that router Chicago will send hello messages to router Boston every 40 seconds.

   chicago(config-if)#**ipv6 pim query-interval 40**

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*.

ipv6 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)#**ipv6 pim join-filter gold**

- Example 2

  host1(config-interface)#**ipv6 pim join-filter gold**

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

Configuring PIM SSM

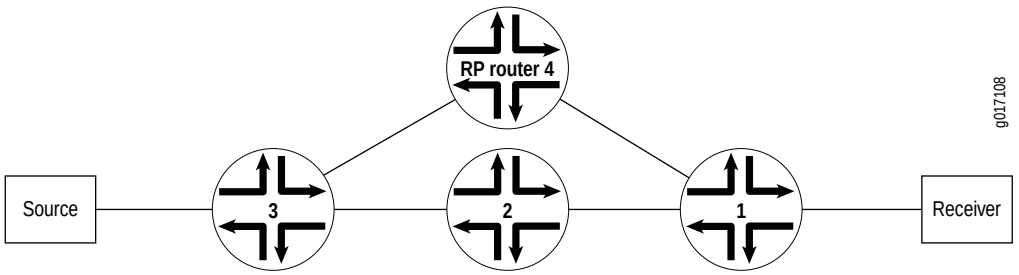
Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is networking technology that targets audio and video broadcast application environments.

To use PIM SSM, MLDv2 must be configured on customer premises 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 ipv6 pim sparse-mode sg-state** command to display SSM group membership information.

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

Figure 20 shows how PIM SSM is configured between a receiver and a source in the network. Interface 1 has MLDv2 enabled and all other interfaces towards the core or source have PIM SSM enabled.

Figure 20: Network on Which to Configure PIM SSM



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)#**ipv6 pim ssm range 15**

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

3. Enable MLDv2 on the CPE-facing interface towards the receiver.

PIM SSM also works with MLDv1 if you configure the ssm-map in MLD as in the following example:

host1(config)#**ipv6 pim ssm**
host1(config)#**ipv6 access-list ssm_map1 permit any host ff3e::1**
host1(config)#**ipv6 mld ssm-map enable**
host1(config)#**ipv6 mld ssm-map static ssm_map1 51::1**

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

host1(config)#**no ipv6 mld ssm-map static ssm_map1 51::1**

ipv6 pim ssm

- Use to enable PIM SSM and define the SSM range of IPv6 multicast addresses.
- Example 1—Enables SSM with addresses in the IANA range. The SSM address range is set as the default, which is limited to the IPv6 address range, and where *x* represents any valid scope.

  host1(config)#**ipv6 pim ssm FF3x::/96**

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

  host1(config)#**ipv6 access-list alist permit any ff3e::1:0:0/96**
  host1(config)#**ipv6 pim ssm range alist**

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

  host1(config)#**ipv6 pim ssm default**

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

Configuring the BFD Protocol for PIM

The **ipv6 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 **ipv6 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 **ipv6 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 **ipv6 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*.

ipv6 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)#**ipv6 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 ipv6 router pim** command.

ipv6 router pim

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

  host1:boston(config)#**no ipv6 router pim**

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

Resetting PIM Counters and Mappings

You can use the **clear ipv6 pim** commands to reset PIM counters and mappings.

clear ipv6 pim interface

- Use to clear the counters for multicast packet statistics on all interfaces or a specified interface.
- Specify an interface type and identifier, 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 ipv6 pim interface atm 3/0.5 count**

- There is no **no** version.

clear ipv6 pim remote-neighbor

- Use to clear the counters for remote neighbor statistics on all interfaces or the specified interface.
- Specify the IP address of an interface to clear the counters for that interface.
- If you do not specify an interface, the router clears the counters on all interfaces.
- Example

  host1#**clear ipv6 pim remote-neighbor 1001::1 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 ipv6 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 ipv6 pim events severity 1 verbosity low**

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

undebug ipv6 pim

- Use to turn off the display of information previously enabled with the **debug ipv6 pim** command.
- Example

  host1#**undebug ipv6 pim events**

- There is no **no** version.

Monitoring PIM Settings

You can use the **show ipv6 pim** commands to display information about PIM settings.

show ipv6 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
  - Join filter—Name of the join filter access-list (if configured) for this PIM router
- Example

```
host1:1#show ipv6 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
Join filter, access-list bronze
```

show ipv6 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 or not 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
  - 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
  - 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 ipv6 pim bsr

This PIM router is a Candidate BSR.
  Configured on intf ATM3/0.101, address: ::107:9
  hashMaskLen 30, priority 2, period 60 seconds.
Elected BSR is this router, next BSM in 3 seconds.

Local candidate RP mapping(s):
Candidate RP ::107:9
::108:86, BSR, hold-time 150, interval 60, priority 192
::108:87, BSR, hold-time 150, interval 60, priority 192, from access-list acl
::108:88, 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 ipv6 pim bsr
This PIM router is a Candidate BSR.
  Configured on intf ATM3/0.100, address: ::107:9
  hashMaskLen 30, priority 2, period 60 seconds.
Elected BSR is ::107:8 (priority 0), expires in 73 seconds.
```

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

```
host1:1#show ipv6 pim bsr
This PIM router is not a Candidate BSR.
Elected BSR is ::107:9 (priority 0), expires in 73 seconds.
```

show ipv6 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 **detail** keyword to view detailed information for all PIM interfaces or for a specified PIM interface.
- Specify the **summary** keyword to view the number of configured, enabled, and disabled PIM sparse-mode interfaces.
- Specify the **count** keyword to view the number of multicast packets that the interface has sent and received.
- Field descriptions
  - Interface Addr—IPv6 address of the interface
  - Interface Name—Type and identifier 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
  - Nbr Count—Number of neighbors connected to this interface
  - Hello Intvl—Time interval at which the interface sends hello messages to neighbors
  - DR Address—Address of the designated router
  - SM—Number of PIM sparse mode interfaces
    - enabled—Number of interfaces administratively enabled
    - disabled—Number of interfaces administratively disabled
  - ControlPkt Count In | Out—PIM messages received on and sent from this interface
    - Hello—Number of hello messages
    - JoinPrune—Number of join and prune messages
    - Assert—Number of assert messages
- Example 1

```
host1#show ipv6 pim interface
PIM Interface Table
Interface Addr  Interface Name        Ver Mode        Nbr   Hello  DR Addr
                                                      Count Intvl
::108:85        atm2/1.108            2   Sparse      1     30     ::108:85
::107:84        atm2/1.109            2   Sparse      1     30     ::107:84
::111:89        atm2/0.110            2   Sparse      1     30     ::111:89
::110:8c        loopback8             2   Sparse      0     30     ::110:8c
```

- Example 2

```
host1#show ipv6 pim interface summary
PIM Interface Summary
  SM:    0, 0 enabled, 0 disabled
```

- Example 3

```
host1#show ipv6 pim interface count
PIM Interface Count
Interface Addr  Interface Name       ControlPktCount In|Out
                                     Hello     JoinPrune  Assert
::107:84        ATM3/0.20             0         0          0
                                      0         0          0
```

show ipv6 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*.
- Specify the **detail** keyword to view detailed information for all PIM neighbors or for a specified PIM neighbor.
- Field descriptions
  - Neighbor Addr—IPv6 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
  - 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 will no longer be a neighbor.
  - Ver—Version of PIM that the neighbor is running
  - Mode—PIM mode that the neighbor is using: sparse
- Example

```
host1#show ipv6 pim neighbor
PIM Neighbor Table
Neighbor Addr   Interface Name        Uptime         Expires  Ver Mode
::107:48        atm2/1.109            1d15:47:35     00:01:41 2   Sparse
::108:58        atm2/1.108            1d15:47:34     00:01:42 2   Sparse
::111:98        atm2/0.110            1d15:48:02     00:01:44 2   Sparse
```

show ipv6 pim remote-neighbor

- Use to view information about PIM remote neighbors.
- Field descriptions
  - Remote Nbr Addr—IPv6 address of remote neighbor
  - OurEnd Addr—IPv6 address of local interface, such as the local endpoint of a tunnel, that transmits data to remote neighbor
  - Ver—Version of PIM running on the local interface
  - Mode—PIM mode running on the local interface; always PIM sparse mode
  - Nbr Count—Number of remote neighbors detected: 0 or 1
  - Hello Intvl—Time interval at which the interface sends hello messages to neighbors
  - DR Addr—Address of designated router
  - In interface—Type and identifier of the interface on which PIM router receives packets from remote neighbor. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
  - Out interface—Type and identifier of the interface on which PIM router sends packets to remote neighbor. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Example

```
host1:boston#show ipv6 pim remote-neighbor
PIM RemoteNbr Table
RemoteNbr Addr  OurEnd Addr     Ver Mode        Nbr   Hello  DR Addr
                                                Count Intvl
1001::1         2001::1         2   Sparse      1     30     ::107:84
      In interface : atm2/1.109
      Out interface: atm2/1.108
```

show ipv6 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.
- To display all group-to-RP mappings that the router has recorded, specify the **mapping** keyword.
- Field descriptions
  - Group—Prefix of the multicast group
  - RP—IP address of RP router for the multicast group
  - priority—This field is not functional
  - via—Method by which the RP router was assigned (static, BSR)
- Example

```
host1:8#show ipv6 pim rp mapping
PIM Group-to-RP mapping(s)
Group(s) ff00::/12
  RP ::122:1,  priority 0,  via  static
Group(s) ff0e::1:0/96
  RP ::120:1,  priority 0,  via  static
```

show ipv6 pim rp-hash

- Use to show which RP router a multicast group is using.
- Field descriptions
  - Group—Multicast group
  - RP—RP router for the multicast group
  - priority—This field is not functional
  - via—Method by which the RP router was assigned (static, BSR)
- Example

```
host1:2#show ipv6 pim rp-hash 232.1.1.1
Group(s) ff00::/12
  RP ::122:1,  priority 0,  via  static
```

show ipv6 pim sparse-mode sg-state

- Use to display information for each (S,G) entry for PIM sparse mode and PIM SSM.
- Field descriptions
  - Group-to-RP mapping—IPv6 addresses and network mask of the multicast group
  - RP—IPv6 address of RP router
  - SSM group—Indicates that this is an SSM group
  - RPF route—IPv6 address and network mask of the RPF route
  - IIF—IPv6 address of the incoming interface for the RPF route
  - UpNbr—IPv6 address of the upstream neighbor
  - Oifs—Outgoing interface
  - Register Oif to RP—IP address of RP router for the outgoing interface; suppressed for SSM
  - Address—IPv6 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 count of (S,G) pair mappings
- Example

```
host1:2#show ipv6 pim sparse-mode sg-state
PIM SM route table and oif information
<*, ff0e::1:3>
  Group-to-RP mapping: ff00::/12 RP: ::123:1
  RPF Route: ::123:1/96 IIF: :106:73 UpNbr: ::106:37
```

```
  Oifs:
   Address: ::78:7:7 Interface: loopback7
    Local group membership present.
<*, ff0e::a:1>
  Group-to-RP mapping: ff001:/12 RP: ::123:1
  RPF Route: :123:1/96 IIF: :106:73 UpNbr: :106:37
  Oifs:
   Address: ::78:7:7 Interface: loopback7
    Local group membership present.

<::118:34, ff3e::1>
  SSM Group
  RPF Route: ::118:0/96 IIF: :118:1 (Directly attached)
  Oifs:
   Register Oif to RP: ::141:2 suppressed for SSM Group.
   Address: ::134:1 Interface: ATM3/0.104
    Joined as <S, G>   Join Expires: 161

<::118:35, ff3e::1>
  SSM Group
  RPF Route: ::118:0/96 IIF: ::118:1 (Directly attached)
  Oifs:
   Register Oif to RP: ::141:2 suppressed for SSM Group.
   Address: ::134:1 Interface: ATM3/0.104
    Joined as <S, G>   Join Expires: 161

<::10:8, ff0e::5:1>      EntryExpires: 143
  Group-to-RP mapping: ff00::/12 RP: ::123:1
  RPF Route: ::10:0/96 IIF: ::106:73 UpNbr: ::106:37
  Oifs:
   Address: ::78:7:7 Interface: loopback7
    Joined as <*, G>

Count of entries - <S, G>    : 3
                   <*, G>    : 2
                   <*, *, RP>: 0
```

show ipv6 pim sparse-mode unicast-route

- Use to display the unicast routes that PIM sparse mode is using.
- Field descriptions
  - Route—IPv6 address and network mask for the unicast route
  - RpfNbr—RPF neighbor
  - Iif—Incoming interface for the unicast route
  - Pref—Preference 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 ipv6 pim sparse-mode unicast-route
PIM SM unicast route table information
Route                          RpfNbr          Iif             Pref  Metric
------------------------------------------------------------------------------
::122:0       /96                              ::122:1         255   1
Count of entries: 1
```

show ipv6 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 IPv6 access list that specifies the groups to which the threshold applies
  - SptThreshold (in kbps)—Value at which PIM sparse mode should switch from a shared tree to an SPT. A value of infinity indicates that PIM sparse mode should never switch to an SPT.
- Example

```
host1:2#show ipv6 pim spt-threshold
Access List Name                 SptThreshold(in kbps)
-------------------------------------------------------
1                                infinity
```