Chapter 17

Multicast over Layer 3 VPNs

The JUNOS software provides support for IP version 4 (IPv4) multicast over Layer 3 virtual private networks (VPNs), as described in RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*. The implementation is based on Section Two of the IETF Internet draft draft-rosen-vpn-mcast-06.txt, *Multicast in MPLS/BGP VPNs* (expires April 2004*)* and uses Protocol Independent Multicast (PIM) and generic routing encapsulation (GRE) tunneling. Initially, only PIM sparse mode was supported. However, Layer 3 VPN multicast support now also includes PIM dense mode and the Multicast Source Discovery Protocol (MSDP).

This document assumes the reader is familiar with Layer 3 VPN operation on Juniper Networks routers, as well as standard PIM configurations. For more information on PIM and MSDP and their usage in a Layer 3 VPN, see the *JUNOS Multicast Protocols Configuration Guide*. For more information on Layer 3 VPN configuration, see the *JUNOS VPNs Configuration Guide*. Both manuals are located at http://www.juniper.net/techpubs/software/index.html.

This feature guide covers these topics:

Overview

In a unicast environment for Layer 3 VPNs, all VPN states are contained within the provider edge (PE) routers. With multicast over Layer 3 VPNs, two PIM adjacencies are established: one between the customer edge (CE) and PE routers through a VPN routing and forwarding (VRF) routing instance, the second between the main PE routers and their service provider core neighbors. You can establish a PIM adjacency in a routing instance with the pim statement at the [edit routing-instances *instance-name* protocols] hierarchy level. For the main PIM adjacency (sometimes referred to as the *master instance*), include the pim statement at the [edit protocols] hierarchy level.

The set of master PIM adjacencies throughout the service provider's network makes up the forwarding path, and eventually forms a rendezvous point (RP) multicast distribution tree. The tree is rooted at the RP contained within the service provider's network. Because of this, core provider transit routers within the service provider's network must maintain multicast state information for the VPNs.

For multicast in Layer 3 VPNs to work correctly, there must be two types of rendezvous points. The VPN customer rendezvous point (VPN C-RP) is an RP that resides within a VPN that connects the segments of a customer network. The service provider rendezvous point (SP-RP) resides within the service provider network itself. Because a PE router connects to both the customer network and the service provider network, a PE router can act as an SP-RP, a VPN C-RP, or both.

NOTE: If you configure auto-RP or bootstrap router (BSR) on a PE router, the PE router cannot act as a VPN C-RP in a routing instance, but can learn about another router acting as the VPN C-RP.

The operation of multicast within a Layer 3 VPN domain occurs in multiple stages, which are shown in Figure 70 on page 849 and described on the following pages.

Figure 70: Multicast over Layer 3 VPNs Operation

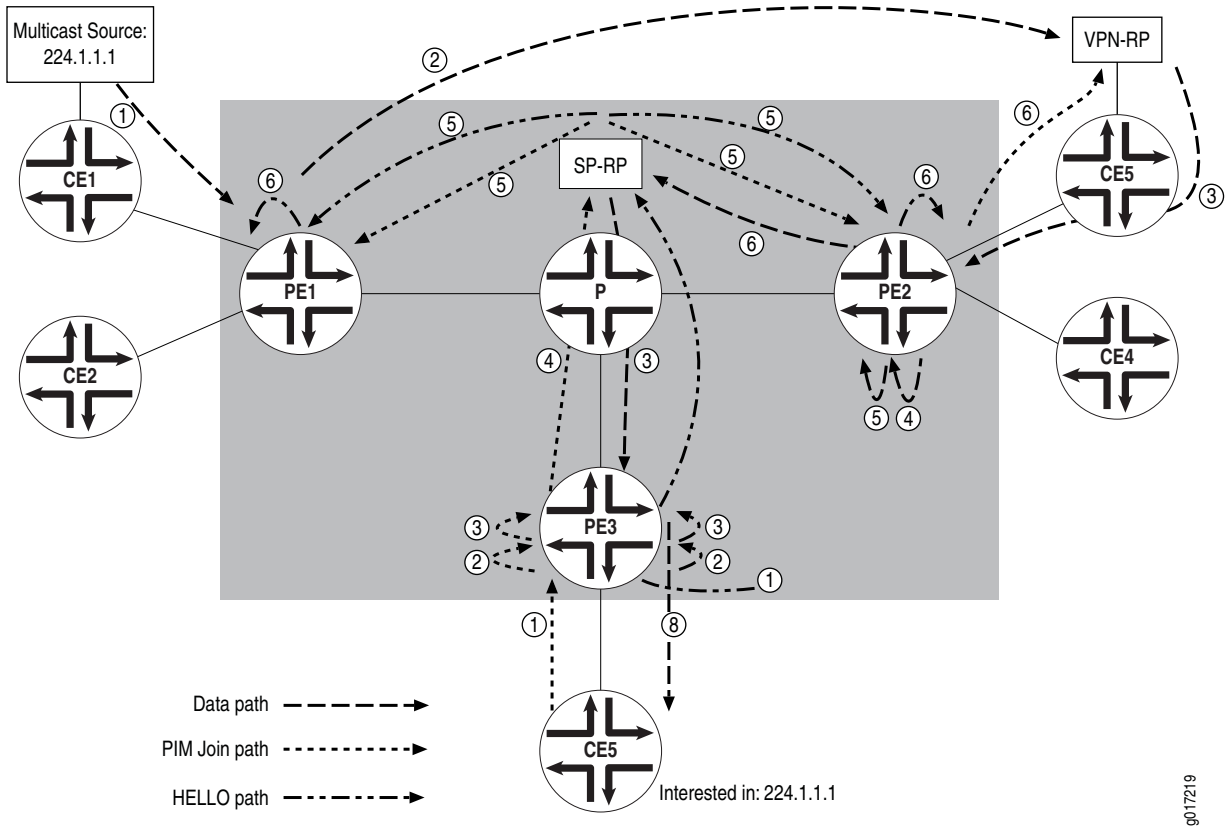


Figure 70 shows the various stages that multicast packets pass through in a Layer 3 VPN environment.

- Stage 1: PIM HELLO

  1. PIM is configured as part of a VPN routing instance and the configuration is committed. For M-series and T-series routing platforms, a virtual multicast tunnel interface (mt-*fpc/pic/port.abcde*) is created if a Tunnel Services Physical Interface Card (PIC) is installed on the router. On MX960 Ethernet Services Routers, you can create a virtual multicast tunnel interface by including the tunnel-services statement at the [edit chassis fpc *slot-number* pic *number*] hierarchy level. For more information about configuring tunnel interfaces on MX960 routers, see the *JUNOS System Basics Configuration Guide*. The virtual multicast tunnel interface is used to communicate between the PIM instance within the VRF and the master PIM instance.

  2. A PIM HELLO is sent from the VRF across the mt interface. When this happens, a GRE header is prepended to the PIM HELLO with fields containing the VPN group address and the loopback address of the PE router.

  3. A PIM register header is prepended to the HELLO as the packet is looped through the pe (PIM encapsulation) interface. This header contains the destination address of the SP-RP and the loopback address of the PE router.

4. The packet is sent to the SP-RP.

5. The SP-RP de-encapsulates the top header off the packet as it travels through the pd (PIM de-encapsulation) interface and sends the remaining GRE encapsulated HELLO to all of the PE routers.

6. The master PIM instance on the PE router handles the GRE encapsulated packet. Because the VPN group address is contained in the packet, the master PIM instance de-encapsulates the packet and sends the HELLO over the mt interface to reach the desired VPN group address within the VRF.

- Stage 2: PIM Join message

  1. Router CE5 is interested in receiving from multicast source 224.1.1.1, so a PIM Join message is sent from Router CE5 to Router PE3.

  2. The PIM Join message is sent through the mt interface and a GRE header is prepended to it. The GRE header contains the VPN group ID and the loopback address of Router PE3.

  3. The PIM Join message is then sent through the pe interface and a register header is prepended to the packet. The data contained within the register header is the IP address of the SP-RP and the loopback address of Router PE3.

  4. The PIM Join message is sent to the SP-RP using unicast routing.

  5. Upon arrival at the SP-RP, the register header is stripped off and the packet is sent (with the GRE header intact) to all the PE routers.

  6. Router PE2 receives the packet. Because the VPN C-RP is behind Router PE2, Router PE2 sends the packet through the mt interface, which strips off the GRE header.

  7. The PIM Join message is now sent to the VPN C-RP.

- Stage 3: Multicast forwarding

  1. The source behind Router CE1 is sending to group 224.1.1.1. The designated router (DR) behind the CE router encapsulates this packet into a PIM register.

  2. Because the packet already has the PIM register header, it is forwarded to the VPN C-RP by unicast routing over the Layer 3 VPN.

  3. The VPN C-RP de-encapsulates the data packet and sends it out the downstream interfaces (which include the return path interface leading to Router CE3). Router CE3 also forwards the packet to Router PE3.

  4. The data packet is sent through the mt interface on Router PE2. In the process, the GRE header is prepended to the packet.

  5. The packet is next sent through the pe interface where the register header is prepended to the data packet.

6. The packet is forwarded to the SP-RP, which removes the register from the packet.

7. The packet is sent to the PE routers with GRE header intact.

8. The "interested" PE routers strip the GRE header off the packet and forward it to the CE routers that requested the PIM join. If there are no PIM-join messages for this group at this site, the PE router drops the packet.

When PIM is configured within a routing instance, two mt interfaces are created:

- mt-[*xxxxx*] (*xxxxx* range is 32768 through 49151) for mt-encap
- mt-[*yyyyy*] (*yyyyy* range is 49152 through 65535) for mt-decap

PIM is run only on the mt-encap interface. The mt-decap interface is used to populate downstream interface information.

System Requirements

To implement IPv4 multicast over Layer 3 VPNs, your system must meet these minimum requirements:

- JUNOS Release 8.2 or later for support on MX-series routing platforms
- JUNOS Release 7.2 or later for MSDP in a Layer 3 VPN
- JUNOS Release 7.1 or later for multicast distribution trees for data
- JUNOS Release 6.4 or later for PIM sparse mode graceful restart and configuring a PE router as the VPN C-RP
- JUNOS Release 5.5 or later for PIM dense mode and logical loopback interfaces
- JUNOS Release 5.3 or later for PIM sparse mode
- Any hardware needed in your network to enable your Juniper Networks routers to act as PE routers
- On M-series and T-series routers, a Tunnel Services PIC or for any provider core router acting as an SP-RP
- On M-series and T-series routers, a Tunnel Services PIC for any PE router where GRE tunneling is needed
- On M-series and T-series routers, a Tunnel Services PIC for any CE or PE router acting as a DR or VPN C-RP
- On M-series and T-series routers, a Tunnel Services PIC is required for GRE tunneling, as specified in Section Two of the IETF Internet draft *Multicast in MPLS/BGP VPNs*.

Terms and Acronyms

- **master PIM instance**—The global instance of PIM that is configured at the [edit protocols pim] hierarchy level.
- **multicast domain**—The set of VPN routing and forwarding (VRF) instances associated with interfaces that can send multicast traffic to one another.
- **SP-RP**—The rendezvous point (RP) for the service provider (this RP is not contained within the VPN).
- **VPN C-RP**—The customer RP for the VPN (this RP is contained within the VPN).

Configuring IPv4 Multicast for Layer 3 VPNs

To implement IPv4 multicast for a Layer 3 VPN, you must configure the following:

- Configuring BGP, MPLS, RSVP, and an IGP on the PE and Core Routers on page 853
- Creating a Unique Logical Loopback Interface for the Routing Instance on page 853
- Configuring the Master PIM Instance on the PE Router on page 853
- Configuring PIM and the VPN Group Address in a Routing Instance on page 854
- Option: Configuring PIM Sparse Mode Graceful Restart for a Layer 3 VPN on page 855
- Option: Configuring Multicast Distribution Trees for Data on page 856
- Option: Configuring MSDP Within a Layer 3 VPN on page 857

To apply your knowledge, visit these sections:

- Example: Basic IPv4 Multicast over a Layer 3 VPN Configuration on page 858
- Checking Your Work on page 863
- Example: IPv4 Multicast with Interprovider VPNs Configuration on page 875
- Checking Your Work on page 880

Configuring BGP, MPLS, RSVP, and an IGP on the PE and Core Routers

To send multicast traffic across a Layer 3 VPN, you must configure network protocols to handle *intradomain routing* (an interior gateway protocol [IGP], such as Open Shortest Path First [OSPF] or Intermediate System-to-Intermediate System [IS-IS]), *interdomain routing* (Border Gateway Protocol [BGP]), *label switching* (Multiprotocol Label Switching [MPLS]), and *path signaling* (Resource Reservation Protocol [RSVP]). For more information about these protocols and examples of how to configure these protocols to support a Layer 3 VPN, see the *JUNOS VPNs Configuration Guide*.

NOTE: In multicast Layer 3 VPNs, the multicast PE routers must use the primary loopback address (or router ID) for sessions with their internal BGP peers. If the PE routers use a route reflector with next-hop self configured, Layer 3 multicast over VPN does not work because PIM cannot transmit upstream interface information for multicast sources behind remote PE routers into the network core. Multicast Layer 3 VPNs require the BGP next-hop address of the VPN route to match the BGP next-hop address of the loopback VRF instance address.

Creating a Unique Logical Loopback Interface for the Routing Instance

To facilitate the PIM protocol within a Layer 3 VPN, configure a unique loopback interface for the routing instance at the [edit interfaces lo0 unit] hierarchy level:

```
[edit interfaces]
lo0 {
    unit 1 {
        family inet {
            address ip-address;
        }
    }
}
```

Configuring the Master PIM Instance on the PE Router

To configure the master PIM instance that communicates with other PIM neighbors and the SP-RP within the service provider network, include the pim statement at the [edit protocols] hierarchy level. The example shown enables PIM sparse mode.

```
[edit protocols]
pim {
    rp {
        static {
            address ip-address;
        }
    }
    interface all {
        mode sparse;
        version 2;
    }
}
```

Configuring PIM and the VPN Group Address in a Routing Instance

The configuration syntax for PIM in a Layer 3 instance is available at the [edit routing-instances protocols pim] hierarchy level. It is similar to the global PIM configuration syntax found at the [edit protocols pim] hierarchy level.

In JUNOS Release 5.3 and later, you can include the vpn-group-address statement at the [edit routing-instances *instance-name* protocols pim] hierarchy level. You include this statement within the routing instance and specify the multicast group address for a particular VPN. Only one vpn-group-address statement can be configured per VPN, and this address should be unique on a per-VPN basis. To review how the VPN group address is used within GRE packet headers, see "Stage 2: PIM Join message" on page 850.

Keep in mind that each PE router will contain two entries of PIM: one for the master instance of PIM that connects through the service provider network and a second for the routing instance that connects to the CE router. The RP listed within the routing instance is the VPN C-RP, while the RP in the master PIM instance is an SP-RP. The following sample configuration shows a PE router with PIM enabled for sparse-dense mode in the VPN instance.

```
[edit]
routing-instances {
    instance-name {
        .....
        protocols {
            .....
            pim {
                vpn-group-address group-address;
                rp {
                    static {
                        address ip-address;
                    }
                }
                interface interface-name {
                    mode sparse-dense;
                    version 2;
                }
                interface lo0.1 {
                    mode sparse-dense;
                    version 2;
                }
            }
        }
    }
}
```

NOTE: In JUNOS Release 5.5 and later, you can configure PIM dense mode with the dense statement at the [edit routing-instances pim mode] hierarchy level. Sparse mode is available at this same hierarchy level in JUNOS Release 5.3 and later.

Option: Configuring PIM Sparse Mode Graceful Restart for a Layer 3 VPN

Graceful restart permits a routing platform to continue forwarding multicast traffic to neighbors while the routing protocol process restarts. To enable graceful restart for PIM sparse mode in a Layer 3 VPN, include the graceful-restart statement at both the [edit routing-options] and [edit routing-instances *instance-name* routing-options] hierarchy levels. To disable graceful restart in a Layer 3 VPN, include the disable statement at the [edit routing-instances *instance-name* protocols pim graceful-restart] hierarchy level.

```
[edit]
routing-options {
    graceful-restart {
        disable;
        restart-duration seconds;
    }
}
routing-instances {
    instance-name {
        .....
        protocols {
            pim {
                graceful-restart {
                    disable;
                    restart-duration seconds;
                }
            }
        }
        routing-options {
            graceful-restart {
                disable;
                restart-duration seconds;
            }
        }
    }
}
```

For more information about PIM sparse mode graceful restart in a Layer 3 VPN, see "Configuring Graceful Restart Options for PIM Sparse Mode" on page 424 and "Enabling Graceful Restart in the Routing Instance" on page 428, or the *JUNOS Multicast Protocols Configuration Guide*.

Option: Configuring Multicast Distribution Trees for Data

By using multicast distribution trees (MDTs) for data in a Layer 3 VPN, you can prevent multicast packets from being flooded unnecessarily to specified provider edge (PE) routers within a VPN group. This option is primarily useful for PE routers in your Layer 3 VPN multicast network that have no receivers for the multicast traffic from a particular source.

When a PE router directly connected to the multicast source receives Layer 3 VPN multicast traffic exceeding a configured threshold, a new data-MDT tunnel is established between the source PE router and its remote PE router neighbors. Neighbors that do not have receivers for the multicast traffic ignore the new tunnel. Conversely, neighbors that do have receivers for the multicast traffic link to the data-MDT tunnel, which is created based on the multicast data in the VPN. If the multicast traffic level drops back below the threshold, the data-MDT tunnel is torn down automatically and traffic flows back across the original Layer 3 VPN PIM tunnel.

To specify when the PE router directly connected to the multicast source should create a new data-MDT tunnel, you must configure the maximum threshold value by including the rate statement at the [edit routing-instances *instance-name* protocols pim mdt threshold group *group-address* source *source-address*] hierarchy level. The data rate is specified in kilobits per second (kbps). To specify the maximum number of data-MDT tunnels that can be created for a single routing instance, include the tunnel-limit statement at the [edit routing-instances *instance-name* protocols pim mdt] hierarchy level. To specify the IP group range used when a new data-MDT tunnel needs to be initiated on the PE router, include the group-range statement at the [edit routing-instances *instance-name* protocols pim mdt] hierarchy level.

```
[edit routing-instances instance-name protocols pim]
mdt {
    group-range multicast-prefix;
    threshold {
        group group-address {
            source source-address {
                rate threshold-rate;
            }
        }
    }
    tunnel-limit limit;
}
```

NOTE: Because MDT applies to VPNs and VRF routing instances, you cannot configure MDT statements in the master routing instance. If you configure MDT in the master routing instance, the configuration commit will fail.

For more information about MDT, see the *JUNOS Multicast Protocols Configuration Guide*.

Option: Configuring MSDP Within a Layer 3 VPN

MSDP, defined in RFC 3618, allows a PIM-enabled network to connect multicast routing domains. It typically runs on the same router as a PIM sparse-mode rendezvous point (RP). Each MSDP router establishes adjacencies with internal and external MSDP peers similar to adjacency establishment for BGP peers. MSDP peer routers inform each other about active sources within the domain. When the peers detect active sources, they send explicit Join messages to the active source.

You can configure MSDP in the master instance of a routing platform, or in the following types of routing instances:

- Forwarding
- No forwarding
- Virtual router
- VPLS
- VRF

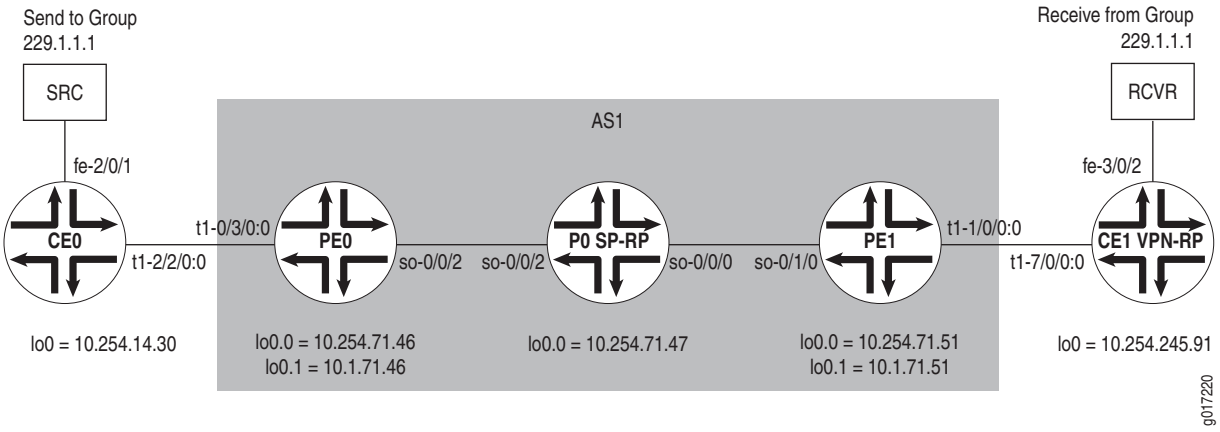
To configure MSDP in a Layer 3 VPN, include the msdp statement at the [edit routing-instances *instance-name* protocols] hierarchy level and specify local and peer addresses. You must also configure PIM sparse mode in the routing instance and specify a rendezvous point.

```
[edit routing-instances instance-name protocols]
pim {
    rp {
        local {
            address ip-address;
        }
    }
    interface interface-name;
}
msdp {
    local-address local-ip-address;
    peer peer-ip-address;
}
```

To view information about the operation of MSDP within a Layer 3 VPN instance, issue the show msdp instance, show msdp statistics instance, show msdp source instance, and show msdp source-active instance commands. For more information about MSDP, see the *JUNOS Multicast Protocols Configuration Guide*.

Example: Basic IPv4 Multicast over a Layer 3 VPN Configuration

Figure 71: Basic IPv4 Multicast over a Layer 3 VPN Topology Diagram



In Figure 71, the multicast source sends to group 229.1.1.1, and the receiver listens to the same group address. The VPN C-RP is located at Router CE1, while the SP-RP is located at Router P0. The routing instances are named VPN-A on both routers PE0 and PE1.

Router CE0

```
[edit]
protocols {
    pim {
        rp {
            dense-groups {
                229.0.0.0/8;
            }
            static {
                address 10.254.245.91;
            }
        }
        interface all {
            mode sparse-dense;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

In this example, the statement interface all is configured. If the topology requires only a few interfaces to be configured for PIM, then loopback interface lo0 must also be one of the configured interfaces.

Router PE0

```
[edit]
protocols {
    pim {
        rp {
            static {
                address 10.254.71.47;
            }
        }
        interface all {
            mode sparse;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

Router PE0 also requires a standard VPN configuration, along with the PIM instance configuration. The vpn-group-address command is the only new PIM statement with PIM used exclusively with a routing instance multicast configuration.

```
[edit]
routing-instances {
    VPN-A {
        instance-type vrf;
        interface t1-0/3/0:0.0;
        interface lo0.1
        route-distinguisher 10.254.71.46:100;
        vrf-import VPNA-import;
        vrf-export VPNA-export;
        protocols {
            ospf {
                export bgp-to-ospf;
                area 0.0.0.0 {
                    interface t1-0/3/0:0.0;
                    interface lo0.1;
                }
            }
            pim {
                dense-groups {
                    229.0.0.0/8;
                }
                vpn-group-address 239.1.1.1;
                rp {
                    static {
                        address 10.254.245.91;
                    }
                }
                interface t1-0/3/0:0.0 {
                    mode sparse-dense;
                    version 2;
                }
                interface lo0.1 {
                    mode sparse-dense;
                    version 2;
                }
            }
        }
    }
}
```

Router P0

```
[edit]
protocols {
    pim {
        rp {
            local {
                address 10.254.71.47;
            }
        }
        interface all {
            mode sparse;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

Again, if the configuration calls for specific interfaces to be configured for PIM, loopback interface lo0 must be included as one of the interfaces running PIM.

Router PE1

```
[edit]
protocols {
    pim {
        rp {
            static {
                address 10.254.71.47;
            }
        }
        interface all {
            mode sparse;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

```
routing-instances {
    VPN-A {
        instance-type vrf;
        interface t1-1/0/0:0.0;
        interface lo0.1;
        route-distinguisher 10.254.71.51:100;
        vrf-import VPNA-import;
        vrf-export VPNA-export;
        protocols {
            ospf {
                export bgp-to-ospf;
                area 0.0.0.0 {
                    interface t1-1/0/0:0.0;
                    interface lo0.1;
                }
            }
            pim {
                dense-groups {
                    229.0.0.0/8;
                }
                vpn-group-address 239.1.1.1;
                rp {
                    static {
                        address 10.254.245.91;
                    }
                }
                interface t1-1/0/0:0.0 {
                    mode sparse-dense;
                    version 2;
                }
                interface lo0.1 {
                    mode sparse-dense;
                    version 2;
                }
            }
        }
    }
}
```

Router CE1

```
[edit]
protocols {
    pim {
        dense-groups {
            229.0.0.0/8;
        }
        rp {
            local {
                address 10.254.245.91;
            }
        }
        interface all {
            mode sparse-dense;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

Checking Your Work

To verify correct operation of basic IPv4 multicast over a Layer 3 VPN, use the following commands:

- show pim
- show pim rps
- show pim rps instance *instance-name*
- show pim join
- show pim join extensive
- show pim join extensive instance *instance-name*
- show multicast route extensive
- show multicast next-hops
- show interfaces mt-*fpc/pic/port* extensive

The following sections show the output of these commands used with the configuration example:

- RP Information on page 864
- PIM Information Prior to Multicast Transmission on page 865
- Successful PIM Join Verification on page 868

RP Information

You can view PIM information for the master instance with the show pim command. You can see information on the PIM routing instance with the show pim (rps | join extensive) instance *instance-name* command. Output verifying the SP-RP (10.254.71.47) as well as the VPN C-RP (10.254.245.91) follows.

```
user@PE0> show pim rps
Instance: PIM.master

Family: INET
RP address      Type      Holdtime Timeout Active groups Group prefixes
10.254.71.47    static           0    None             1 224.0.0.0/4

Family: INET6
RP address      Type      Holdtime Timeout Active groups Group prefixes

user@PE0> show pim rps instance VPN-A
Instance: PIM.VPN-A

Family: INET
RP address      Type      Holdtime Timeout Active groups Group prefixes
10.254.245.91   static           0    None             0 224.0.0.0/4

Family: INET6
RP address      Type      Holdtime Timeout Active groups Group prefixes
```

PIM Information Prior to Multicast Transmission

With the configuration properly set, the backbone PIM sessions should be established before any traffic is forwarded. In the output below, the routers were configured, but the traffic source was not transmitting and the receiver was not requesting to be part of a group. Notice that there is no PIM join information for the routing instances yet.

Router PE0

```
user@PE0> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.47
    Flags: sparse,rptree,wildcard
    Upstream interface: so-0/0/2.0
    Upstream State: Join to RP
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: SRW  Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.46
    Flags: sparse
    Upstream interface: local
    Upstream State: Local Source, Prune to RP
    Keepalive timeout: 166
    Downstream Neighbors:
        Interface: so-0/0/2.0
            192.168.296.70 State: Join   Flags: S    Timeout: 204

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse,spt-pending
    Upstream interface: so-0/0/2.0
    Upstream State: Join to Source
    Keepalive timeout: 166
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: S    Timeout: Infinity

user@PE0> show pim join extensive instance VPN-A
Instance: PIM.VPN-A Family: INET
```

Router P0

```
user@P0> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.47
    Flags: sparse,rptree,wildcard
    Upstream interface: local
    Upstream State: Local RP
    Downstream Neighbors:
        Interface: so-0/0/0.0
            192.168.296.34 State: Join   Flags: SRW  Timeout: 186
        Interface: so-0/0/2.0
            192.168.296.69 State: Join   Flags: SRW  Timeout: 198

Group: 239.1.1.1
    Source: 10.254.71.46
    Flags: sparse,spt
    Upstream interface: so-0/0/2.0
    Upstream State: Local RP, Join to Source
    Keepalive timeout: 170
    Downstream Neighbors:
        Interface: so-0/0/0.0
            192.168.296.34 State: Join   Flags: S    Timeout: 186
        Interface: so-0/0/2.0             (pruned)
            192.168.296.69 State: Prune  Flags: SR   Timeout: 198

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse,spt
    Upstream interface: so-0/0/0.0
    Upstream State: Local RP, Join to Source
    Keepalive timeout: 170
    Downstream Neighbors:
        Interface: so-0/0/0.0             (pruned)
            192.168.296.34 State: Prune  Flags: SR   Timeout: 186
        Interface: so-0/0/2.0
            192.168.296.69 State: Join   Flags: S    Timeout: 198
```

Router PE1

```
user@PE1> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.47
    Flags: sparse,rptree,wildcard
    Upstream interface: so-0/1/0.0
    Upstream State: Join to RP
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: SRW  Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.46
    Flags: sparse,spt-pending
    Upstream interface: so-0/1/0.0
    Upstream State: Join to Source
    Keepalive timeout: 180
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: S    Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse
    Upstream interface: local
    Upstream State: Local Source, Prune to RP
    Keepalive timeout: 180
    Downstream Neighbors:
        Interface: so-0/1/0.0
            192.168.296.33 State: Join   Flags: S    Timeout: 168
```

Successful PIM Join Verification

In the remaining output for this example, the show pim join output shows group participation. Also displayed is the output from the show multicast route extensive and show multicast next-hop commands. The join output for PIM within a VPN will reference the group 229.1.1.1, while the service provider side of the network will reference the join information for group 239.1.1.1 (which is the VPN group ID). In the show multicast route extensive output, you can view the group, sender, and upstream interface toward the sender.

Router CE0

```
user@CE0> show pim join
Instance: PIM.master Family: INET
Group: 229.1.1.1
    Source: 192.168.295.34
    Flags: dense
    Upstream interface: fe-2/0/1.0
Instance: PIM.master Family: INET6

user@CE0> show multicast route extensive

Family: INET
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
229.1.1.1       192.168.295.34 /32 A   F  120   8010       0          360
    Upstream interface: fe-2/0/1.0
    Session name: Unknown
    Forwarding rate: 1 kBps (10 pps)

Family: INET6
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout

user@CE0> show multicast next-hops
Family: INET
ID      Refcount  KRefcount Downstream interface
120            2          1 t1-2/2/0:0.0
```

Router PE0

```
user@PE0> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.47
    Flags: sparse,rptree,wildcard
    Upstream interface: so-0/0/2.0
    Upstream State: Join to RP
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            10.1.71.46 State: Join   Flags: SRW  Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.46
    Flags: sparse
    Upstream interface: local
    Upstream State: Local Source, Prune to RP
    Keepalive timeout: 188
    Downstream Neighbors:
        Interface: so-0/0/2.0
            192.168.296.70 State: Join   Flags: S    Timeout: 180

Instance: PIM.master Family: INET6
```

```
user@PE0> show interfaces mt-1/1/0 extensive
Physical interface: mt-1/1/0, Enabled, Physical link is Up
  Interface index: 37, SNMP ifIndex: 45, Generation: 36
  Type: Multicast-GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
  Hold-times     : Up 0 ms, Down 0 ms
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :              2887970                    0 bps
   Output bytes  :                    0                    0 bps
   Input  packets:                31896                    0 pps
   Output packets:                    0                    0 pps

  Logical interface mt-1/1/0.32769 (Index 43) (SNMP ifIndex 0) (Generation 46)
    Flags: Point-To-Point SNMP-Traps
    IP-Header 239.1.1.1:10.254.71.46:47:df:64:0000000800000000
    Encapsulation: GRE-NULL
    Traffic statistics:
     Input  bytes  :                    0
     Output bytes  :                 2396
     Input  packets:                    0
     Output packets:                   34
    Local statistics:
     Input  bytes  :                    0
     Output bytes  :                 2396
     Input  packets:                    0
     Output packets:                   34
    Transit statistics:
     Input  bytes  :                    0                    0 bps
     Output bytes  :                    0                    0 bps
     Input  packets:                    0                    0 pps
     Output packets:                    0                    0 pps
    Protocol inet, MTU: 4446, Generation: 79, Route table: 3
      Flags: None

  Logical interface mt-1/1/0.49154 (Index 44) (SNMP ifIndex 0) (Generation 47)
    Flags: Point-To-Point SNMP-Traps Encapsulation: GRE-NULL
    Traffic statistics:
     Input  bytes  :                 1550
     Output bytes  :                    0
     Input  packets:                   33
     Output packets:                    0
    Local statistics:
     Input  bytes  :                 1550
     Output bytes  :                    0
     Input  packets:                   33
     Output packets:                    0
    Transit statistics:
     Input  bytes  :                    0                    0 bps
     Output bytes  :                    0                    0 bps
     Input  packets:                    0                    0 pps
     Output packets:                    0                    0 pps
    Protocol inet, MTU: Unlimited, Generation: 80, Route table: 3
      Flags: None
```

```
user@PE0> show pim join extensive instance VPN-A
Instance: PIM.VPN-A Family: INET
Group: 229.1.1.1
    Source: 192.168.295.34
    Flags: dense
    Upstream interface: t1-0/3/0:0.0
    Downstream interfaces:
        mt-1/1/0.32769

Instance: PIM.VPN-A Family: INET6
user@PE0> show pim join
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.47
    Flags: sparse,rptree,wildcard
    Upstream interface: so-0/0/2.0

Group: 239.1.1.1
    Source: 10.254.71.46
    Flags: sparse
    Upstream interface: local

Instance: PIM.master Family: INET6

user@PE0> show pim join instance VPN-A
Instance: PIM.VPN-A Family: INET
Group: 229.1.1.1
    Source: 192.168.295.34
    Flags: dense
    Upstream interface: t1-0/3/0:0.0
Instance: PIM.VPN-A Family: INET6

user@PE0> show multicast route extensive

Family: INET
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
239.1.1.1       10.254.71.46   /32 A   F  86    9174       0          360
    Upstream interface: local
    Session name: Administratively Scoped
    Forwarding rate: 1 kBps (10 pps)
239.1.1.1       10.254.71.51   /32 A   F  96    36         0          360
    Upstream interface: so-0/0/2.0
    Session name: Administratively Scoped
    Forwarding rate: 0 kBps (0 pps)

Family: INET6
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout

user@PE0> show multicast route extensive instance VPN-A

Family: INET
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
229.1.1.1       192.168.295.34 /32 A   F  85    9408       0          360
    Upstream interface: t1-0/3/0:0.0
    Session name: Unknown
    Forwarding rate: 1 kBps (10 pps)

Family: INET6
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
```

```
user@PE0> show multicast next-hops
Family: INET
ID      Refcount  KRefcount Downstream interface
86             2          1 so-0/0/2.0

85             2          1 mt-1/1/0.32769

96             2          1 mt-1/1/0.49154

Family: INET6
```

Router P0

```
user@P0> show pim join
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.47
    Flags: sparse,rptree,wildcard
    Upstream interface: local

Group: 239.1.1.1
    Source: 10.254.71.46
    Flags: sparse,spt
    Upstream interface: so-0/0/2.0

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse,spt
    Upstream interface: so-0/0/0.0

Instance: PIM.master Family: INET6

user@P0> show multicast route extensive

Family: INET
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
239.1.1.1       10.254.71.46   /32 A   F  127   9906       195        360
    Upstream interface: so-0/0/2.0
    Session name: Administratively Scoped
    Forwarding rate: 1 kBps (10 pps)
239.1.1.1       10.254.71.51   /32 A   F  126   135        23         359
    Upstream interface: so-0/0/0.0
    Session name: Administratively Scoped
    Forwarding rate: 0 kBps (0 pps)

Family: INET6
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout

user@P0> show multicast next-hops
Family: INET
ID      Refcount  KRefcount Downstream interface
127            2          1 so-0/0/0.0

126            2          1 so-0/0/2.0

Family: INET6
```

Router PE1

```
user@PE1> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.47
    Flags: sparse,rptree,wildcard
    Upstream interface: so-0/1/0.0
    Upstream State: Join to RP
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            10.1.71.51 State: Join   Flags: SRW  Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.46
    Flags: sparse,spt-pending
    Upstream interface: so-0/1/0.0
    Upstream State: Join to Source
    Keepalive timeout: 199
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            10.1.71.51 State: Join   Flags: S    Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse
    Upstream interface: local
    Upstream State: Local Source, Prune to RP
    Keepalive timeout: 79
    Downstream Neighbors:
        Interface: so-0/1/0.0
            192.168.296.33 State: Join   Flags: S    Timeout: 174
        Interface: register to RP 10.254.71.47 on pe-1/1/0.32769

Instance: PIM.master Family: INET6

user@PE1> show pim join extensive instance VPN-A
Instance: PIM.VPN-A Family: INET
Group: 229.1.1.1
    Source: 192.168.295.34
    Flags: dense
    Upstream interface: mt-1/1/0.32769
    Downstream interfaces:
        t1-1/0/0:0.0

Instance: PIM.VPN-A Family: INET6
```

```
user@PE1> show interfaces mt-1/1/0 extensive
Physical interface: mt-1/1/0, Enabled, Physical link is Up
  Interface index: 38, SNMP ifIndex: 45, Generation: 37
  Type: Multicast-GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
  Hold-times     : Up 0 ms, Down 0 ms
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :              2265256                 7568 bps
   Output bytes  :                    0                    0 bps
   Input  packets:                24981                   10 pps
   Output packets:                    0                    0 pps

  Logical interface mt-1/1/0.32769 (Index 45) (SNMP ifIndex 0) (Generation 46)
    Flags: Point-To-Point SNMP-Traps
    IP-Header 239.1.1.1:10.254.71.51:47:df:64:0000000800000000
    Encapsulation: GRE-NULL
    Traffic statistics:
     Input  bytes  :                    0
     Output bytes  :                10934
     Input  packets:                    0
     Output packets:                  153
    Local statistics:
     Input  bytes  :                    0
     Output bytes  :                10934
     Input  packets:                    0
     Output packets:                  153
    Transit statistics:
     Input  bytes  :                    0                    0 bps
     Output bytes  :                    0                    0 bps
     Input  packets:                    0                    0 pps
     Output packets:                    0                    0 pps
    Protocol inet, MTU: 4418, Generation: 77, Route table: 1
      Flags: None

  Logical interface mt-1/1/0.49154 (Index 46) (SNMP ifIndex 0) (Generation 47)
    Flags: Point-To-Point SNMP-Traps Encapsulation: GRE-NULL
    Traffic statistics:
     Input  bytes  :              1820512
     Output bytes  :                    0
     Input  packets:                19848
     Output packets:                    0
    Local statistics:
     Input  bytes  :                 5536
     Output bytes  :                    0
     Input  packets:                  120
     Output packets:                    0
    Transit statistics:
     Input  bytes  :              1814976                 7568 bps
     Output bytes  :                    0                    0 bps
     Input  packets:                19728                   10 pps
     Output packets:                    0                    0 pps
    Protocol inet, MTU: Unlimited, Generation: 78, Route table: 1
      Flags: None
```

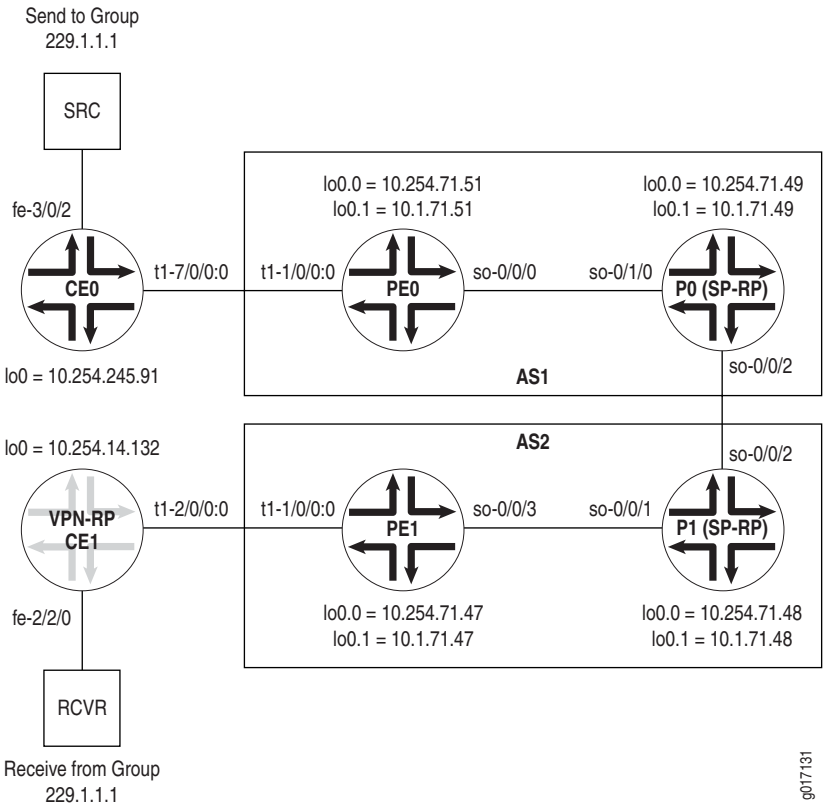
```
user@PE1> show multicast route extensive

Family: INET
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
239.1.1.1       10.254.71.46   /32 A   F  76    11014      0          360
    Upstream interface: so-0/1/0.0
    Session name: Administratively Scoped
    Forwarding rate: 1 kBps (10 pps)
239.1.1.1       10.254.71.51   /32 A   F  103   1          0          360
    Upstream interface: local
    Session name: Administratively Scoped
    Forwarding rate: 0 kBps (0 pps)

Family: INET6
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout

user@PE1> show multicast route extensive instance VPN-A

Family: INET
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
229.1.1.1       192.168.295.34 /32 A   F  99    10976      4          360
    Upstream interface: mt-1/1/0.49154
    Session name: Unknown
    Forwarding rate: 1 kBps (10 pps)

Family: INET6
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout

user@PE1> show multicast next-hops
Family: INET
ID      Refcount  KRefcount Downstream interface
75              2          1 so-0/1/0.0

99              2          1 t1-1/0/0:0.0

76              2          1 mt-1/1/0.49154

Family: INET6
```

Router CE1

```
user@CE1> show pim join
Instance: PIM.master Family: INET
Group: 229.1.1.1
    Source: 192.168.295.34
    Flags: dense
    Upstream interface: t1-7/0/0:0.0
Instance: PIM.master Family: INET6

user@CE1> show multicast route extensive

Family: INET
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout
229.1.1.1       192.168.295.34 /32 A   F  120   8010       0          360
    Upstream interface: t1-7/0/0:0.0
    Session name: Unknown
    Forwarding rate: 1 kBps (10 pps)

Family: INET6
Group           Source prefix     Act Pru NHid  Packets    IfMismatch Timeout

user@CE1> show multicast next-hops
Family: INET
ID      Refcount  KRefcount Downstream interface
120             2          1 fe-3/0/2.0
```

Example: IPv4 Multicast with Interprovider VPNs Configuration

Figure 72: IPv4 Multicast with Interprovider VPNs Topology Diagram



Interprovider VPNs are also mentioned in RFC 4364. An example is shown in Figure 72. The topology is slightly different; the main difference is the addition of MSDP between the two provider core transit (P) routers. In this limited topology, each P router is an SP-RP for the local autonomous system (AS), and Router CE1 is the VPN C-RP. VPN-A is the name of the routing instance on routers PE0 and PE1.

Router CE0

```
[edit]
protocols {
    pim {
        dense-groups {
            229.0.0.0/8;
        }
        rp {
            static {
                address 10.254.14.132;
            }
        }
        interface all {
            mode sparse-dense;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

Router PE0

```
[edit]
protocols {
    pim {
        rp {
            static {
                address 10.254.71.49;
            }
        }
        interface all {
            mode sparse;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

```
routing-instances {
    VPN-A {
        protocols {
            pim {
                dense-groups {
                    229.0.0.0/8;
                }
                vpn-group-address 239.1.1.1;
                rp {
                    static {
                        address 10.254.14.132;
                    }
                }
                interface t1-1/0/0:0.0 {
                    mode sparse-dense;
                    version 2;
                }
                interface lo0.1 {
                    mode sparse-dense;
                    version 2;
                }
            }
        }
    }
}
```

Router P0

```
[edit]
protocols {
    ...
    msdp {
        peer 10.254.71.48 {
            local-address 10.254.71.49;
        }
    }
    ...
    pim {
        rp {
            local {
                address 10.254.71.49;
            }
        }
        interface all {
            mode sparse;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

Router P1

```
[edit]
protocols {
    ...
    msdp {
        peer 10.254.71.49 {
            local-address 10.254.71.48;
        }
    }
    ...
    pim {
        rp {
            local {
                address 10.254.71.48;
            }
        }
        interface all {
            mode sparse;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

Router PE1

```
[edit]
protocols {
    pim {
        rp {
            static {
                address 10.254.71.48;
            }
        }
        interface all {
            mode sparse;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

```
routing-instances {
    VPN-A {
        protocols {
            pim {
                dense-groups {
                    229.0.0.0/8;
                }
                vpn-group-address 239.1.1.1;
                rp {
                    static {
                        address 10.254.14.132;
                    }
                }
                interface t1-1/0/0:0.0 {
                    mode sparse-dense;
                    version 2;
                }
                interface lo0.1 {
                    mode sparse-dense;
                    version 2;
                }
            }
        }
    }
}
```

Router CE1

```
[edit]
protocols {
    pim {
        dense-groups {
            229.0.0.0/8;
        }
        rp {
            local {
                address 10.254.14.132;
            }
        }
        interface all {
            mode sparse-dense;
            version 2;
        }
        interface fxp0.0 {
            disable;
        }
    }
}
```

Checking Your Work

The show commands used to verify proper functionality of multicast in an interprovider environment are the same ones used with the first Layer 3 VPN multicast example (see "Checking Your Work" on page 863).

The following output provides details for RP and the PIM join information:

Router CE0 Status

```
user@CE0> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.254.14.132
Learned via: static configuration
Time Active: 00:21:35
Holdtime: 0
Device Index: 119
Subunit: 32769
Interface: pe-6/0/0.32769
Group Ranges:
        224.0.0.0/4
Active groups using RP:

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout

Family: INET6

user@CE0> show pim join extensive
Instance: PIM.master Family: INET
Group: 229.1.1.1
    Source: 192.168.295.38
    Flags: dense
    Upstream interface: fe-3/0/2.0
    Downstream interfaces:
        t1-7/0/0:0.0

Instance: PIM.master Family: INET6
```

Router PE0 Status

```
user@PE0> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.254.71.49
Learned via: static configuration
Time Active: 00:22:07
Holdtime: 0
Device Index: 34
Subunit: 32769
Interface: pe-1/1/0.32769
Group Ranges:
        224.0.0.0/4
Active groups using RP:
        239.1.1.1

        total 1 groups active

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout
239.1.1.1       10.254.71.51    10.254.71.51    10.254.71.49    Suppress      20

Family: INET6

user@PE0> show pim rps extensive instance VPN-A
Instance: PIM.VPN-A

Family: INET
RP: 10.254.14.132
Learned via: static configuration
Time Active: 00:22:22
Holdtime: 0
Device Index: 34
Subunit: 32771
Interface: pe-1/1/0.32771
Group Ranges:
        224.0.0.0/4
Active groups using RP:

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout

Family: INET6
```

```
user@PE0> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.49
    Flags: sparse,rptree,wildcard
    Upstream interface: so-0/0/0.0
    Upstream State: Join to RP
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: SRW  Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.47
    Flags: sparse,spt-pending
    Upstream interface: so-0/0/0.0
    Upstream State: Join to Source
    Keepalive timeout: 198
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: S    Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse
    Upstream interface: local
    Upstream State: Local Source, Prune to RP
    Keepalive timeout: 198
    Downstream Neighbors:
        Interface: so-0/0/0.0
            192.168.296.42 State: Join   Flags: S    Timeout: 176

Instance: PIM.master Family: INET6

user@PE0> show pim join extensive instance VPN-A
Instance: PIM.VPN-A Family: INET
Group: 229.1.1.1
    Source: 192.168.295.38
    Flags: dense
    Upstream interface: t1-1/0/0:0.0
    Downstream interfaces:
        mt-1/1/0.32769

Instance: PIM.VPN-A Family: INET6
```

Router P0 Status

```
user@P0> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.254.71.49
Learned via: static configuration
Time Active: 00:30:43
Holdtime: 0
Device Index: 33
Subunit: 32768
Interface: pd-1/1/0.32768
Group Ranges:
        224.0.0.0/4
Active groups using RP:
        239.1.1.1

        total 1 groups active

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout
239.1.1.1       10.254.71.51    10.254.71.51    10.254.71.49    Receive

Family: INET6

user@P0> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.49
    Flags: sparse,rptree,wildcard
    Upstream interface: local
    Upstream State: Local RP
    Downstream Neighbors:
        Interface: so-0/1/0.0
            192.168.296.41 State: Join   Flags: SRW  Timeout: 184

Group: 239.1.1.1
    Source: 10.254.71.47
    Flags: sparse,spt-pending
    Upstream interface: so-0/0/2.0
    Upstream State: Local RP, Join to Source
    Keepalive timeout: 207
    Downstream Neighbors:
        Interface: so-0/1/0.0
            192.168.296.41 State: Join   Flags: S    Timeout: 184

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse,spt
    Upstream interface: so-0/1/0.0
    Upstream State: Local RP, Join to Source
    Keepalive timeout: 207
    Downstream Neighbors:
        Interface: so-0/0/2.0
            192.168.296.73 State: Join   Flags: S    Timeout: 186
        Interface: so-0/1/0.0             (pruned)
            192.168.296.41 State: Prune  Flags: SR   Timeout: 184

Instance: PIM.master Family: INET6
```

Router P1 Status

```
user@P1> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.254.71.48
Learned via: static configuration
Time Active: 06:26:56
Holdtime: 0
Device Index: 32
Subunit: 32768
Interface: pd-1/1/0.32768
Group Ranges:
        224.0.0.0/4
Active groups using RP:
        239.1.1.1

        total 1 groups active

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout
239.1.1.1       10.254.71.47    10.254.71.47    10.254.71.48    Receive        0

Family: INET6

user@P1> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.48
    Flags: sparse,rptree,wildcard
    Upstream interface: local
    Upstream State: Local RP
    Downstream Neighbors:
        Interface: so-0/0/1.0
            192.168.296.50 State: Join   Flags: SRW  Timeout: 174

Group: 239.1.1.1
    Source: 10.254.71.47
    Flags: sparse,spt
    Upstream interface: so-0/0/1.0
    Upstream State: Local RP, Join to Source
    Keepalive timeout: 196
    Downstream Neighbors:
        Interface: so-0/0/1.0             (pruned)
            192.168.296.50 State: Prune  Flags: SR   Timeout: 174
        Interface: so-0/0/2.0
            192.168.296.74 State: Join   Flags: S    Timeout: 178

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse,spt-pending
    Upstream interface: so-0/0/2.0
    Upstream State: Local RP, Join to Source
    Keepalive timeout: 196
    Downstream Neighbors:
        Interface: so-0/0/1.0
            192.168.296.50 State: Join   Flags: S    Timeout: 174

Instance: PIM.master Family: INET6
```

Router PE1 Status

```
user@PE1> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.254.71.48
Learned via: static configuration
Time Active: 00:25:13
Holdtime: 0
Device Index: 34
Subunit: 32770
Interface: pe-1/1/0.32770
Group Ranges:
        224.0.0.0/4
Active groups using RP:
        239.1.1.1

        total 1 groups active

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout
239.1.1.1       10.254.71.47    10.254.71.47    10.254.71.48    Suppress      42

Family: INET6

user@PE1> show pim rps extensive instance VPN-A
Instance: PIM.VPN-A

Family: INET
RP: 10.254.14.132
Learned via: static configuration
Time Active: 00:25:17
Holdtime: 0
Device Index: 34
Subunit: 32771
Interface: pe-1/1/0.32771
Group Ranges:
        224.0.0.0/4
Active groups using RP:

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout

Family: INET6
```

```
user@PE1> show pim join extensive
Instance: PIM.master Family: INET
Group: 239.1.1.1
    Source: *
    RP: 10.254.71.48
    Flags: sparse,rptree,wildcard
    Upstream interface: so-0/0/3.0
    Upstream State: Join to RP
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: SRW  Timeout: Infinity

Group: 239.1.1.1
    Source: 10.254.71.47
    Flags: sparse
    Upstream interface: local
    Upstream State: Local Source, Prune to RP
    Keepalive timeout: 173
    Downstream Neighbors:
        Interface: so-0/0/3.0
            192.168.296.49 State: Join   Flags: S    Timeout: 199

Group: 239.1.1.1
    Source: 10.254.71.51
    Flags: sparse,spt-pending
    Upstream interface: so-0/0/3.0
    Upstream State: Join to Source
    Keepalive timeout: 173
    Downstream Neighbors:
        Interface: mt-1/1/0.32769
            0.0.0.0 State: Join   Flags: S    Timeout: Infinity

Instance: PIM.master Family: INET6

user@PE1> show pim join extensive instance VPN-A
Instance: PIM.VPN-A Family: INET
Group: 229.1.1.1
    Source: 192.168.295.38
    Flags: dense
    Upstream interface: mt-1/1/0.32769
    Downstream interfaces:
        t1-1/0/0:0.0

Instance: PIM.VPN-A Family: INET6
```

Router CE1 Status

```
user@CE1> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.254.14.132
Learned via: static configuration
Time Active: 00:28:22
Holdtime: 0
Device Index: 69
Subunit: 32768
Interface: pd-3/1/0.32768
Group Ranges:
        224.0.0.0/4
Active groups using RP:

Register State for RP:

Group           Source          FirstHop        RP Address      State    Timeout

Family: INET6

user@CE1> show pim join extensive
Instance: PIM.master Family: INET
Group: 229.1.1.1
    Source: 192.168.295.38
    Flags: dense
    Upstream interface: t1-2/0/0:0.0
    Downstream interfaces:
        fe-2/2/0.0

Instance: PIM.master Family: INET6
```

For More Information

For additional information on multicast over Layer 3 VPNs, see the following resources:

- *JUNOS Multicast Protocols Configuration Guide*
- *JUNOS VPNs Configuration Guide*
- RFC 2547, *BGP/MPLS VPNs*
- RFC 3618, *Multicast Source Discovery Protocol (MSDP)*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- Internet draft draft-rosen-vpn-mcast-06.txt, *Multicast in MPLS/BGP VPNs* (expires April 2004)

Revision History

12 January 2007—Added support for MX960 Ethernet Services Routers. 8.2R1 Release. Fawn Damitio.

15 September 2006—Added RFC 4364, 8.1R1 Release. Richard Hendricks.

29 June 2006—8.0R1 Release. Richard Hendricks.

27 March 2006—7.6R1 Release. Richard Hendricks.

9 January 2006—7.5R1 Release. Richard Hendricks.

14 September 2005—7.4R1 Release. Richard Hendricks.

13 June 2005—7.3R1 Release. Richard Hendricks.

5 April 2005—Added support for MSDP in Layer 3 VPNs, 7.2R1 Release. Richard Hendricks.

2 February 2005—Added multicast distribution trees for data, 7.1R1 Release. Richard Hendricks.

6 October 2004—7.0R1 Release. Richard Hendricks.

6 July 2004—Added graceful restart information and mentioned that a PE router can now act as a VPN C-RP, 6.4R1 Release. Richard Hendricks.

5 April 2004—6.3R1 Release. Richard Hendricks.

22 December 2003—6.2R1 Release. Richard Hendricks.

22 September 2003—6.1R1 Release. Richard Hendricks.

30 June 2003—6.0R1 Release. Richard Hendricks.

2 April 2003—5.7R1 Release. Richard Hendricks.

27 December 2002—5.6R1 Release. Richard Hendricks.

30 September 2002—5.5R1 Release. Richard Hendricks.

27 August 2002—Reformatted the document in Feature Guide style. Richard Hendricks.

22 August 2002—Added PIM dense mode information. Bill Nowak.

8 February 2002—Initial 5.3 Quick Start Guide document. Bill Nowak.