Network Configuration Example

Configuring MBGP Multicast VPNs

Release
12.3

Published: 2012-11-14

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Configuring MBGP Multicast VPNs
Release 12.3

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Introduction

Multiprotocol BGP-based multicast VPNs (also referred to as next-generation Layer 3 VPN multicast) constitute the next evolution after dual multicast VPNs (draft-rosen) and provide a simpler solution for administrators who want to configure multicast over Layer 3 VPNs.

The main characteristics of multiprotocol BGP-based multicast VPNs are:

- They extend Layer 3 VPN service (RFC 2547) to support IP multicast for Layer 3 VPN service providers.
- They follow the same architecture as specified by RFC 2547 for unicast VPNs. Specifically, BGP is used as the control plane.
- They eliminate the requirement for the virtual router (VR) model, which is specified in Internet draft draft-rosen-vpn-mcast, *Multicast in MPLS/BGP VPNs*, for multicast VPNs.
- They rely on RFC-based unicast with extensions for intra-AS and inter-AS communication.

Related Documentation

- MBGP Multicast VPN Applications on page 1
- Example: Configuring MBGP Multicast VPNs on page 1

MBGP Multicast VPN Applications

There are several multicast applications driving the deployment of next-generation Layer 3 MVPNs. Some of the key emerging applications include the following:

- Layer 3 VPN multicast service offered by service providers to enterprise customers.
- Video transport applications for wholesale IPTV and multiple content providers attached to the same network.
- Distribution of media-rich financial services or enterprise multicast services.
- Multicast backhaul over a metro network.

Related Documentation

- Example: Configuring MBGP Multicast VPNs on page 1
- Introduction on page 1

Example: Configuring MBGP Multicast VPNs

This example provides a step-by-step procedure to configure multicast services across a multiprotocol BGP (MBGP) Layer 3 virtual private network.

- Requirements on page 2
- Overview and Topology on page 2
- Configuration on page 3

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.2 or later
- Five M Series, T Series, TX Series, or MX Series Juniper routers
- One host system capable of sending multicast traffic and supporting the Internet Group Management Protocol (IGMP)
- One host systems capable of receiving multicast traffic and supporting IGMP

Depending on the devices you are using, you might be required to configure static routes to:

- The multicast sender
- The Fast Ethernet interface to which the sender is connected on the multicast receiver
- The multicast receiver
- The Fast Ethernet interface to which the receiver is connected on the multicast sender

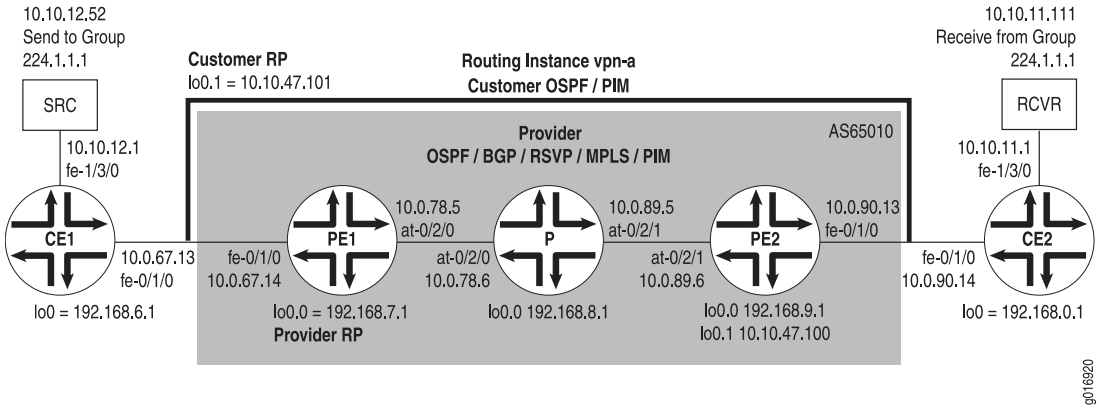
Overview and Topology

This example shows how to configure the following technologies:

- IPv4
- BGP
- OSPF
- RSVP
- MPLS
- PIM sparse mode
- Static RP

The topology of the network is shown in Figure 1 on page 3.

Figure 1: Multicast Over Layer 3 VPN Example Topology



Configuration

NOTE: In any configuration session, it is a good practice to periodically verify that the configuration can be committed using the commit check command.

In this example, the router being configured is identified using the following command prompts:

- **CE1** identifies the customer edge 1 (CE1) router
- **PE1** identifies the provider edge 1 (PE1) router
- **P** identifies the provider core (P) router
- **CE2** identifies the customer edge 2 (CE2) router
- **PE2** identifies the provider edge 2 (PE2) router

To configure MBGP multicast VPNs for the network shown in Figure 1 on page 3, perform the following steps:

Configuring Interfaces

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

1. On each router, configure an IP address on the loopback logical interface 0 (**lo0.0**).

   ```
   [edit interfaces]
   user@CE1# set lo0 unit 0 family inet address 192.168.6.1/32 primary

   user@PE1# set lo0 unit 0 family inet address 192.168.7.1/32 primary

   user@P# set lo0 unit 0 family inet address 192.168.8.1/32 primary

   user@PE2# set lo0 unit 0 family inet address 192.168.9.1/32 primary

   user@CE2# set lo0 unit 0 family inet address 192.168.0.1/32 primary
   ```

   Use the **show interfaces terse** command to verify that the IP address is correct on the loopback logical interface.

2. On the PE and CE routers, configure the IP address and protocol family on the Fast Ethernet interfaces. Specify the **inet** protocol family type.

   ```
   [edit interfaces]
   user@CE1# set fe-1/3/0 unit 0 family inet address 10.10.12.1/24
   user@CE1# set fe-0/1/0 unit 0 family inet address 10.0.67.13/30

   [edit interfaces]
   user@PE1# set fe-0/1/0 unit 0 family inet address 10.0.67.14/30

   [edit interfaces]
   user@PE2# set fe-0/1/0 unit 0 family inet address 10.0.90.13/30

   [edit interfaces]
   user@CE2# set fe-0/1/0 unit 0 family inet address 10.0.90.14/30
   user@CE2# set fe-1/3/0 unit 0 family inet address 10.10.11.1/24
   ```

   Use the **show interfaces terse** command to verify that the IP address is correct on the Fast Ethernet interfaces.

3. On the PE and P routers, configure the ATM interfaces' VPI and maximum virtual circuits. If the default PIC type is different on directly connected ATM interfaces, configure the PIC type to be the same. Configure the logical interface VCI, protocol family, local IP address, and destination IP address.

   ```
   [edit interfaces]
   user@PE1# set at-0/2/0 atm-options pic-type atm1
   user@PE1# set at-0/2/0 atm-options vpi 0 maximum-vcs 256
   user@PE1# set at-0/2/0 unit 0 vci 0.128
   user@PE1# set at-0/2/0 unit 0 family inet address 10.0.78.5/32 destination 10.0.78.6
   ```

```
[edit interfaces]
user@P# set at-0/2/0 atm-options pic-type atm1
user@P# set at-0/2/0 atm-options vpi 0 maximum-vcs 256
user@P# set at-0/2/0 unit 0 vci 0.128
user@P# set at-0/2/0 unit 0 family inet address 10.0.78.6/32 destination 10.0.78.5
user@P# set at-0/2/1 atm-options pic-type atm1
user@P# set at-0/2/1 atm-options vpi 0 maximum-vcs 256
user@P# set at-0/2/1 unit 0 vci 0.128
user@P# set at-0/2/1 unit 0 family inet address 10.0.89.5/32 destination 10.0.89.6
```

```
[edit interfaces]
user@PE2# set at-0/2/1 atm-options pic-type atm1
user@PE2# set at-0/2/1 atm-options vpi 0 maximum-vcs 256
user@PE2# set at-0/2/1 unit 0 vci 0.128
user@PE2# set at-0/2/1 unit 0 family inet address 10.0.89.6/32 destination 10.0.89.5
```

Use the **show configuration interfaces** command to verify that the ATM interfaces' VPI and maximum VCs are correct and that the logical interface VCI, protocol family, local IP address, and destination IP address are correct.

Configuring OSPF

Step-by-Step Procedure

1. On the P and PE routers, configure the provider instance of OSPF. Specify the **lo0.0** and ATM core-facing logical interfaces. The provider instance of OSPF on the PE router forms adjacencies with the OSPF neighbors on the other PE router and Router P.

```
user@PE1# set protocols ospf area 0.0.0.0 interface at-0/2/0.0
user@PE1# set protocols ospf area 0.0.0.0 interface lo0.0
```

```
user@P# set protocols ospf area 0.0.0.0 interface lo0.0
user@P# set protocols ospf area 0.0.0.0 interface all
user@P# set protocols ospf area 0.0.0.0 interface fxp0 disable
```

```
user@PE2# set protocols ospf area 0.0.0.0 interface lo0.0
user@PE2# set protocols ospf area 0.0.0.0 interface at-0/2/1.0
```

   Use the **show ospf interfaces** command to verify that the **lo0.0** and ATM core-facing logical interfaces are configured for OSPF.

2. On the CE routers, configure the customer instance of OSPF. Specify the loopback and Fast Ethernet logical interfaces. The customer instance of OSPF on the CE routers form adjacencies with the neighbors within the VPN routing instance of OSPF on the PE routers.

```
user@CE1# set protocols ospf area 0.0.0.0 interface fe-0/1/0.0
user@CE1# set protocols ospf area 0.0.0.0 interface fe-1/3/0.0
user@CE1# set protocols ospf area 0.0.0.0 interface lo0.0
```

```
user@CE2# set protocols ospf area 0.0.0.0 interface fe-0/1/0.0
user@CE2# set protocols ospf area 0.0.0.0 interface fe-1/3/0.0
user@CE2# set protocols ospf area 0.0.0.0 interface lo0.0
```

Use the **show ospf interfaces** command to verify that the correct loopback and Fast Ethernet logical interfaces have been added to the OSPF protocol.

3. On the P and PE routers, configure OSPF traffic engineering support for the provider instance of OSPF.

   The **shortcuts** statement enables the master instance of OSPF to use a label-switched path as the next hop.

   ```
   user@PE1# set protocols ospf traffic-engineering shortcuts

   user@P# set protocols ospf traffic-engineering shortcuts

   user@PE2# set protocols ospf traffic-engineering shortcuts
   ```

   Use the **show ospf overview** or **show configuration protocols ospf** command to verify that traffic engineering support is enabled.

Configuring BGP

Step-by-Step Procedure

1. On Router P, configure BGP for the VPN. The local address is the local **lo0.0** address. The neighbor addresses are the PE routers' **lo0.0** addresses.

   The **unicast** statement enables the router to use BGP to advertise network layer reachability information (NLRI). The **signaling** statement enables the router to use BGP as the signaling protocol for the VPN.

   ```
   user@P# set protocols bgp group group-mvpn type internal
   user@P# set protocols bgp group group-mvpn local-address 192.168.8.1
   user@P# set protocols bgp group group-mvpn family inet unicast
   user@P# set protocols bgp group group-mvpn family inet-mvpn signaling
   user@P# set protocols bgp group group-mvpn neighbor 192.168.9.1
   user@P# set protocols bgp group group-mvpn neighbor 192.168.7.1
   ```

   Use the **show configuration protocols bgp** command to verify that the router has been configured to use BGP to advertise NLRI.

2. On the PE and P routers, configure the BGP local autonomous system number.

   ```
   user@PE1# set routing-options autonomous-system 0.65010

   user@P# set routing-options autonomous-system 0.65010

   user@PE2# set routing-options autonomous-system 0.65010
   ```

   Use the **show configuration routing-options** command to verify that the BGP local autonomous system number is correct.

3. On the PE routers, configure BGP for the VPN. Configure the local address as the local **lo0.0** address. The neighbor addresses are the **lo0.0** addresses of Router P and the other PE router, PE2.

   ```
   user@PE1# set protocols bgp group group-mvpn type internal
   user@PE1# set protocols bgp group group-mvpn local-address 192.168.7.1
   user@PE1# set protocols bgp group group-mvpn family inet-vpn unicast
   user@PE1# set protocols bgp group group-mvpn family inet-mvpn signaling
   ```

```
user@PE1# set protocols bgp group group-mvpn neighbor 192.168.9.1
user@PE1# set protocols bgp group group-mvpn neighbor 192.168.8.1
```

```
user@PE2# set protocols bgp group group-mvpn type internal
user@PE2# set protocols bgp group group-mvpn local-address 192.168.9.1
user@PE2# set protocols bgp group group-mvpn family inet-vpn unicast
user@PE2# set protocols bgp group group-mvpn family inet-mvpn signaling
user@PE2# set protocols bgp group group-mvpn neighbor 192.168.7.1
user@PE2# set protocols bgp group group-mvpn neighbor 192.168.8.1
```

Use the **show bgp group** command to verify that the BGP configuration is correct.

4. On the PE routers, configure a policy to export the BGP routes into OSPF.

```
user@PE1# set policy-options policy-statement bgp-to-ospf from protocol bgp
user@PE1# set policy-options policy-statement bgp-to-ospf then accept
```

```
user@PE2# set policy-options policy-statement bgp-to-ospf from protocol bgp
user@PE2# set policy-options policy-statement bgp-to-ospf then accept
```

Use the **show policy bgp-to-ospf** command to verify that the policy is correct.

Configuring RSVP

Step-by-Step Procedure

1. On the PE routers, enable RSVP on the interfaces that participate in the LSP. Configure the Fast Ethernet and ATM logical interfaces.

```
user@PE1# set protocols rsvp interface fe-0/1/0.0
user@PE1# set protocols rsvp interface at-0/2/0.0
```

```
user@PE2# set protocols rsvp interface fe-0/1/0.0
user@PE2# set protocols rsvp interface at-0/2/1.0
```

2. On Router P, enable RSVP on the interfaces that participate in the LSP. Configure the ATM logical interfaces.

```
user@P# set protocols rsvp interface at-0/2/0.0
user@P# set protocols rsvp interface at-0/2/1.0
```

Use the **show configuration protocols rsvp** command to verify that the RSVP configuration is correct.

Configuring MPLS

Step-by-Step Procedure

1. On the PE routers, configure an MPLS LSP to the PE router that is the LSP egress point. Specify the IP address of the **lo0.0** interface on the router at the other end of the LSP. Configure MPLS on the ATM, Fast Ethernet, and **lo0.0** interfaces.

   To help identify each LSP when troubleshooting, configure a different LSP name on each PE router. In this example, we use the name **to-pe2** as the name for the LSP configured on PE1 and **to-pe1** as the name for the LSP configured on PE2.

```
user@PE1# set protocols mpls label-switched-path to-pe2 to 192.168.9.1
user@PE1# set protocols mpls interface fe-0/1/0.0
user@PE1# set protocols mpls interface at-0/2/0.0
user@PE1# set protocols mpls interface lo0.0
```

```
user@PE2# set protocols mpls label-switched-path to-pe1 to 192.168.7.1
user@PE2# set protocols mpls interface fe-0/1/0.0
user@PE2# set protocols mpls interface at-0/2/1.0
user@PE2# set protocols mpls interface lo0.0
```

Use the **show configuration protocols mpls** and **show route label-switched-path to-pe1** commands to verify that the MPLS and LSP configuration is correct.

After the configuration is committed, use the **show mpls lsp name to-pe1** and **show mpls lsp name to-pe2** commands to verify that the LSP is operational.

2. On Router P, enable MPLS. Specify the ATM interfaces connected to the PE routers.

```
user@P# set protocols mpls interface at-0/2/0.0
user@P# set protocols mpls interface at-0/2/1.0
```

Use the **show mpls interface** command to verify that MPLS is enabled on the ATM interfaces.

3. On the PE and P routers, configure the protocol family on the ATM interfaces associated with the LSP. Specify the **mpls** protocol family type.

```
user@PE1# set interfaces at-0/2/0 unit 0 family mpls

user@P# set interfaces at-0/2/0 unit 0 family mpls
user@P# set interfaces at-0/2/1 unit 0 family mpls

user@PE2# set interfaces at-0/2/1 unit 0 family mpls
```

Use the **show mpls interface** command to verify that the MPLS protocol family is enabled on the ATM interfaces associated with the LSP.

Configuring the VRF Routing Instance

Step-by-Step Procedure

1. On the PE routers, configure a routing instance for the VPN and specify the **vrf** instance type. Add the Fast Ethernet and **lo0.1** customer-facing interfaces. Configure the VPN instance of OSPF and include the BGP-to-OSPF export policy.

```
user@PE1# set routing-instances vpn-a instance-type vrf
user@PE1# set routing-instances vpn-a interface lo0.1
user@PE1# set routing-instances vpn-a interface fe-0/1/0.0
user@PE1# set routing-instances vpn-a protocols ospf export bgp-to-ospf
user@PE1# set routing-instances vpn-a protocols ospf area 0.0.0.0 interface all

user@PE2# set routing-instances vpn-a instance-type vrf
user@PE2# set routing-instances vpn-a interface lo0.1
user@PE2# set routing-instances vpn-a interface fe-0/1/0.0
user@PE2# set routing-instances vpn-a protocols ospf export bgp-to-ospf
user@PE2# set routing-instances vpn-a protocols ospf area 0.0.0.0 interface all
```

Use the **show configuration routing-instances vpn-a** command to verify that the routing instance configuration is correct.

2. On the PE routers, configure a route distinguisher for the routing instance. A route distinguisher allows the router to distinguish between two identical IP prefixes used

as VPN routes. Configure a different route distinguisher on each PE router. This example uses 65010:1 on PE1 and 65010:2 on PE2.

```
user@PE1# set routing-instances vpn-a route-distinguisher 65010:1

user@PE2# set routing-instances vpn-a route-distinguisher 65010:2
```

Use the **show configuration routing-instances vpn-a** command to verify that the route distinguisher is correct.

3. On the PE routers, configure default VRF import and export policies. Based on this configuration, BGP automatically generates local routes corresponding to the route target referenced in the VRF import policies. This example uses 2:1 as the route target.

NOTE: You must configure the same route target on each PE router for a given VPN routing instance.

```
user@PE1# set routing-instances vpn-a vrf-target target:2:1

user@PE2# set routing-instances vpn-a vrf-target target:2:1
```

Use the **show configuration routing-instances vpn-a** command to verify that the route target is correct.

4. On the PE routers, configure the VPN routing instance for multicast support.

```
user@PE1# set routing-instances vpn-a protocols mvpn

user@PE2# set routing-instances vpn-a protocols mvpn
```

Use the **show configuration routing-instance vpn-a** command to verify that the VPN routing instance has been configured for multicast support.

5. On the PE routers, configure an IP address on loopback logical interface 1 (**lo0.1**) used in the customer routing instance VPN.

```
user@PE1# set interfaces lo0 unit 1 family inet address 10.10.47.101/32

user@PE2# set interfaces lo0 unit 1 family inet address 10.10.47.100/32
```

Use the **show interfaces terse** command to verify that the IP address on the loopback interface is correct.

Configuring PIM

Step-by-Step Procedure

1. On the PE and P routers, enable the provider instance of PIM. Add the core-facing ATM interfaces. On the PE routers, also configure the **lo0.0** interface. Specify the mode as **sparse** and the version as **2**.

```
user@PE1# set protocols pim interface at-0/2/0.0 mode sparse
user@PE1# set protocols pim interface at-0/2/0.0 version 2
user@PE1# set protocols pim interface lo0.0 mode sparse
```

```
user@PE1# set protocols pim interface lo0.0 version 2

user@P# set protocols pim interface at-0/2/0.0 mode sparse
user@P# set protocols pim interface at-0/2/0.0 version 2
user@P# set protocols pim interface at-0/2/1.0 mode sparse
user@P# set protocols pim interface at-0/2/1.0 version 2

user@PE2# set protocols pim interface at-0/2/1.0 mode sparse
user@PE2# set protocols pim interface at-0/2/1.0 version 2
user@PE2# set protocols pim interface lo0.0 mode sparse
user@PE2# set protocols pim interface lo0.0 version 2
```

Use the **show pim interfaces** command to verify that PIM sparse-mode is enabled on the core-facing ATM interfaces.

2. On the PE routers, enable the VPN customer instance of PIM. Configure the **lo0.1** and the customer-facing Fast Ethernet interface. Specify the mode as **sparse** and the version as **2**.

```
user@PE1# set routing-instances vpn-a protocols pim interface lo0.1 mode sparse
user@PE1# set routing-instances vpn-a protocols pim interface lo0.1 version 2
user@PE1# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 mode
  sparse
user@PE1# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 version
  2

user@PE2# set routing-instances vpn-a protocols pim interface lo0.1 mode sparse
user@PE2# set routing-instances vpn-a protocols pim interface lo0.1 version 2
user@PE2# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 mode
  sparse
user@PE2# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 version
  2
```

Use the **show pim interfaces instance vpn-a** command to verify that PIM sparse-mode is enabled on the **lo0.1** interface and the customer-facing Fast Ethernet interface.

3. On the CE routers, enable the customer instance of PIM. In this example, we configure all interfaces. Specify the mode as **sparse** and the version as **2**.

```
user@CE1# set protocols pim interface all

user@CE2# set protocols pim interface all mode sparse
user@CE2# set protocols pim interface all version 2
```

Use the **show pim interfaces** command to verify that PIM sparse mode is enabled on all interfaces.

Configuring the Provider Tunnel

Step-by-Step Procedure

1. On Router PE1, configure the provider tunnel. Specify the multicast address to be used.

   The **provider-tunnel** statement instructs the router to send multicast traffic across a tunnel. The **pim-asm** statement instructs the router to accept the multicast stream from any source.

```
user@PE1# set routing-instances vpn-a provider-tunnel pim-asm group-address
  224.1.1.1
```

Use the **show configuration routing-instance vpn-a** command to verify that the multicast group address is correct on Router PE1.

2. On Router PE2, configure the provider tunnel. Specify the multicast address to be used.

```
user@PE2# set routing-instances vpn-a provider-tunnel pim-asm group-address
  224.1.1.1
```

Use the **show configuration routing-instance vpn-a** command to verify that the multicast group address is correct on Router PE2.

Configuring the Rendezvous Point

Step-by-Step Procedure

1. Configure Router PE1 to be the rendezvous point for the provider instance of PIM. Specify the **lo0.0** address of Router PE1.

```
user@PE1# set protocols pim rp local address 192.168.7.1
```

Use the **show pim rps** command to verify that to correct local IP address is configured for the provider instance RP.

2. Configure the static rendezvous point on Router P and the PE2 router for the provider instance of PIM. Specify the **lo0.0** address of Router PE1. Specify the version as **2**.

```
user@P# set protocols pim rp static address 192.168.7.1 version 2

user@PE2# set protocols pim rp static address 192.168.7.1 version 2
```

Use the **show pim rps** command to verify that the correct static IP address is configured for the provider instance RP.

3. Configure Router PE1 to be the rendezvous point for the customer instance of PIM. Specify the **lo0.1** address of Router PE1. Specify the multicast address to be used.

```
user@PE1# set routing-instances vpn-a protocols pim rp local address 10.10.47.101
user@PE1# set routing-instances vpn-a protocols pim rp local group-ranges
  224.1.1.1/32
```

Use the **show pim rps instance vpn-a** command to verify that the correct local IP address is configured for the customer instance RP.

4. On Router PE2, configure the static rendezvous point for the customer instance of PIM. Specify the **lo0.1** address of Router PE1.

```
user@PE2# set routing-instances vpn-a protocols pim rp static address 10.10.47.101
```

Use the **show pim rps instance vpn-a** command to verify that the correct static IP address is configured for the customer instance RP.

5. On the CE routers, configure the static rendezvous point for the customer instance of PIM. Specify the **lo0.1** address of Router PE1.

```
user@CE1# set protocols pim rp static address 10.10.47.101 version 2

user@CE2# set protocols pim rp static address 10.10.47.101 version 2
```

Use the **show pim rps** command to verify that the correct static IP address is configured for the customer instance RP.

6. Use the **commit check** command to verify that the configuration can be successfully committed. If the configuration passes the check, commit the configuration.
7. Start the multicast sender device connected to CE1.
8. Start the multicast receiver device connected to CE2.
9. Verify that the receiver is receiving the multicast stream.
10. Use **show** commands to verify the routing, VPN, and multicast operation.

The configuration and verification parts of this example have been completed. The following section is for your reference.

The relevant sample configuration for Router CE1 follows.

Router CE1

```
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.6.1/32 {
          primary;
        }
      }
    }
  }
  fe-0/1/0 {
    unit 0 {
      family inet {
        address 10.0.67.13/30;
      }
    }
  }
  fe-1/3/0 {
    unit 0 {
      family inet {
        address 10.10.12.1/24;
      }
    }
  }
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface fe-0/1/0.0;
      interface lo0.0;
      interface fe-1/3/0.0;
    }
  }
  pim {
    rp {
      static {
        address 10.10.47.101 {
          version 2;
```

```
            }
          }
        }
        interface all;
      }
    }
```

The relevant sample configuration for Router PE1 follows.

Router PE1

```
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.7.1/32 {
          primary;
        }
      }
    }
  }
  fe-0/1/0 {
    unit 0 {
      family inet {
        address 10.0.67.14/30;
      }
    }
  }
  at-0/2/0 {
    atm-options {
      pic-type atm1;
      vpi 0 {
        maximum-vcs 256;
      }
    }
    unit 0 {
      vci 0.128;
      family inet {
        address 10.0.78.5/32 {
          destination 10.0.78.6;
        }
      }
      family mpls;
    }
  }
  lo0 {
    unit 1 {
      family inet {
        address 10.10.47.101/32;
      }
    }
  }
}
routing-options {
  autonomous-system 0.65010;
}
protocols {
  rsvp {
```

```
        interface fe-0/1/0.0;
        interface at-0/2/0.0;
    }
    mpls {
        label-switched-path to-pe2 {
            to 192.168.9.1;
        }
        interface fe-0/1/0.0;
        interface at-0/2/0.0;
        interface lo0.0;
    }
    bgp {
        group group-mvpn {
            type internal;
            local-address 192.168.7.1;
            family inet-vpn {
                unicast;
            }
            family inet-mvpn {
                signaling;
            }
            neighbor 192.168.9.1;
            neighbor 192.168.8.1;
        }
    }
    ospf {
        traffic-engineering {
            shortcuts;
        }
        area 0.0.0.0 {
            interface at-0/2/0.0;
            interface lo0.0;
        }
    }
    pim {
        rp {
            local {
                address 192.168.7.1;
            }
        }
        interface at-0/2/0.0 {
            mode sparse;
            version 2;
        }
        interface lo0.0 {
            mode sparse;
            version 2;
        }
    }
}
policy-options {
    policy-statement bgp-to-ospf {
        from protocol bgp;
        then accept;
    }
}
```

```
routing-instances {
  vpn-a {
    instance-type vrf;
    interface lo0.1;
    interface fe-0/1/0.0;
    route-distinguisher 65010:1;
    provider-tunnel {
      pim-asm {
        group-address 224.1.1.1;
      }
    }
    vrf-target target:2:1;
    protocols {
      ospf {
        export bgp-to-ospf;
        area 0.0.0.0 {
          interface all;
        }
      }
      pim {
        rp {
          local {
            address 10.10.47.101;
            group-ranges {
              224.1.1.1/32;
            }
          }
        }
        interface lo0.1 {
          mode sparse;
          version 2;
        }
        interface fe-0/1/0.0 {
          mode sparse;
          version 2;
        }
      }
      mvpn;
    }
  }
}
```

The relevant sample configuration for Router P follows.

Router P

```
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.8.1/32 {
          primary;
        }
      }
    }
  }
  at-0/2/0 {
    atm-options {
```

```
        pic-type atm1;
        vpi 0 {
          maximum-vcs 256;
        }
      }
      unit 0 {
        vci 0.128;
        family inet {
          address 10.0.78.6/32 {
            destination 10.0.78.5;
          }
        }
        family mpls;
      }
    }
    at-0/2/1 {
      atm-options {
        pic-type atm1;
        vpi 0 {
          maximum-vcs 256;
        }
      }
      unit 0 {
        vci 0.128;
        family inet {
          address 10.0.89.5/32 {
            destination 10.0.89.6;
          }
        }
        family mpls;
      }
    }
}
routing-options {
  autonomous-system 0.65010;
}
protocols {
  rsvp {
    interface at-0/2/0.0;
    interface at-0/2/1.0;
  }
  mpls {
    interface at-0/2/0.0;
    interface at-0/2/1.0;
  }
  bgp {
    group group-mvpn {
      type internal;
      local-address 192.168.8.1;
      family inet {
        unicast;
      }
      family inet-mvpn {
        signaling;
      }
      neighbor 192.168.9.1;
```

```
        neighbor 192.168.7.1;
      }
    }
    ospf {
      traffic-engineering {
        shortcuts;
      }
      area 0.0.0.0 {
        interface lo0.0;
        interface all;
        interface fxp0.0 {
          disable;
        }
      }
    }
    pim {
      rp {
        static {
          address 192.168.7.1 {
            version 2;
          }
        }
      }
      interface at-0/2/0.0 {
        mode sparse;
        version 2;
      }
      interface at-0/2/1.0 {
        mode sparse;
        version 2;
      }
    }
  }
```

The relevant sample configuration for Router PE2 follows.

Router PE2

```
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.9.1/32 {
          primary;
        }
      }
    }
  }
  fe-0/1/0 {
    unit 0 {
      family inet {
        address 10.0.90.13/30;
      }
    }
  }
  at-0/2/1 {
    atm-options {
      pic-type atm1;
```

```
        vpi 0 {
          maximum-vcs 256;
        }
      }
      unit 0 {
        vci 0.128;
        family inet {
          address 10.0.89.6/32 {
            destination 10.0.89.5;
          }
        }
        family mpls;
      }
    }
    lo0 {
      unit 1 {
        family inet {
          address 10.10.47.100/32;
        }
      }
    }
}
routing-options {
    autonomous-system 0.65010;
}
protocols {
    rsvp {
      interface fe-0/1/0.0;
      interface at-0/2/1.0;
    }
    mpls {
      label-switched-path to-pe1 {
        to 192.168.7.1;
      }
      interface lo0.0;
      interface fe-0/1/0.0;
      interface at-0/2/1.0;
    }
    bgp {
      group group-mvpn {
        type internal;
        local-address 192.168.9.1;
        family inet-vpn {
          unicast;
        }
        family inet-mvpn {
          signaling;
        }
        neighbor 192.168.7.1;
        neighbor 192.168.8.1;
      }
    }
    ospf {
      traffic-engineering {
        shortcuts;
      }
```

```
        area 0.0.0.0 {
          interface lo0.0;
          interface at-0/2/1.0;
        }
      }
      pim {
        rp {
          static {
            address 192.168.7.1 {
              version 2;
            }
          }
        }
        interface lo0.0 {
          mode sparse;
          version 2;
        }
        interface at-0/2/1.0 {
          mode sparse;
          version 2;
        }
      }
    }
    policy-options {
      policy-statement bgp-to-ospf {
        from protocol bgp;
        then accept;
      }
    }
    routing-instances {
      vpn-a {
        instance-type vrf;
        interface fe-0/1/0.0;
        interface lo0.1;
        route-distinguisher 65010:2;
        provider-tunnel {
          pim-asm {
            group-address 224.1.1.1;
          }
        }
        vrf-target target:2:1;
        protocols {
          ospf {
            export bgp-to-ospf;
            area 0.0.0.0 {
              interface all;
            }
          }
          pim {
            rp {
              static {
                address 10.10.47.101;
              }
            }
            interface fe-0/1/0.0 {
              mode sparse;
```

```
            version 2;
          }
          interface lo0.1 {
            mode sparse;
            version 2;
          }
        }
        mvpn;
      }
    }
  }
```

The relevant sample configuration for Router CE2 follows.

Router CE2

```
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.0.1/32 {
          primary;
        }
      }
    }
  }
  fe-0/1/0 {
    unit 0 {
      family inet {
        address 10.0.90.14/30;
      }
    }
  }
  fe-1/3/0 {
    unit 0 {
      family inet {
        address 10.10.11.1/24;
      }
      family inet6 {
        address fe80::205:85ff:fe88:ccdb/64;
      }
    }
  }
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface fe-0/1/0.0;
      interface lo0.0;
      interface fe-1/3/0.0;
    }
  }
  pim {
    rp {
      static {
        address 10.10.47.101 {
          version 2;
        }
```

```
        }
      }
      interface all {
        mode sparse;
        version 2;
      }
    }
  }
}
```

Related Documentation

- Multicast over Layer 3 VPNs Overview
- Configuring BGP, MPLS, RSVP, and an IGP on the PE and Core Routers for Draft Rosen VPNs
- Configuring BGP, MPLS, RSVP, and an IGP on the PE and Core Routers for MBGP MVPNs
- Configuring Interfaces for Layer 3 VPNs
- Configuring Intra-AS Inclusive Point-to-Multipoint Traffic Engineering LSPs
- Configuring Intra-AS Selective Provider Tunnels
- Configuring MBGP MVPNs to Support IPv6 Multicast Traffic
- Configuring PIM and the VPN Group Address in a Routing Instance
- Configuring Provider Tunnels
- Configuring the Master PIM Instance on the PE Router for BGP-Based Multicast VPNs
- Configuring the Master PIM Instance on the PE Router in the Service Provider Network
- Creating a Routing Instance for a Multiprotocol BGP-Based Multicast VPN
- Configuring the Router's IPv4 Bootstrap Router Priority
- Creating a Unique Logical Loopback Interface for the Routing Instance for Draft Rosen VPNs
- Creating a Unique Logical Loopback Interface for the Routing Instance for MBGP MVPNs
- Dual PIM Draft-Rosen Multicast VPN Operation
- Enabling Multicast VPN in BGP
- MBGP Multicast VPN Extranets Configuration Guidelines
- Option: Configuring MSDP Within a Layer 3 VPN
- Option: Configuring Multicast Distribution Trees for Data
- Option: Configuring PIM Sparse Mode Graceful Restart for a Layer 3 VPN
- Option: Configuring Sender and Receiver Sites
- Option: Specifying Route Targets
- Understanding MBGP Multicast VPN Extranets
- Understanding Multiprotocol BGP-Based Multicast VPNs: Next-Generation

