Network Configuration Example

PIM Snooping for VPLS

Release
12.3

Published: 2012-11-27

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

Network Configuration Example PIM Snooping for VPLS
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 1
PIM Snooping for VPLS Use Cases 1
Understanding PIM Snooping for VPLS 1
Example: Configuring PIM Snooping for VPLS 2

Introduction

This document describes the advantages of and uses for PIM snooping. It also provides a step-by-step procedure for configuring and verifying PIM snooping for VPLS.

PIM Snooping for VPLS Use Cases

In a virtual private LAN service (VPLS), the provider edge (PE) devices provide a logical interconnect such that the customer edge (CE) devices belonging to a specific VPLS instance appear to be connected by a single LAN. Since a VPLS provides LAN emulation for layer 2 and layer 3 devices, the unicast and multicast traffic should use the same path for layer 2 protocols to work accurately. Hence, multicast traffic is treated like broadcast traffic and forwarded to all sites in the VPLS instance. This event of forwarding traffic out of every port other than the port it arrived on is called flooding and wastes network bandwidth in the VPLS.

Hence, in a VPLS, multicast traffic is replicated to non-member sites. This can be avoided by restricting traffic to only interested devices that are members of the specific multicast group. This process of directing traffic is called snooping, where a device snoops on Layer 3 multicast protocol packets to identify the devices that are going to receive the traffic.

Snooping depends on the type of multicast protocol used for multicasting traffic in the network. Internet Group Management Protocol (IGMP) snooping is used at Layer 2 when IGMP is configured as the multicast protocol. This document explains how Protocol Independent Multicast (PIM) snooping can be configured in a VPLS that uses PIM as the multicast protocol.

PIM shares many common characteristics with a routing protocol, such as neighbor discovery using hello messages, topology database using the multicast tree, and error detection and notification using the dead timer and designated router election. PIM does not exchange databases. It uses the unicast routing table to provide reverse path information for building multicast trees.

PIM snooping eliminates the service provider tasks of providing the multicast service (running PIM, managing group addresses and multicast tunnels) to customers, saves time, and reduces load on the network. PIM snooping thus optimizes the IP multicast bandwidth in the VPLS core and provides cost savings.

Related Documentation

- Understanding PIM Snooping for VPLS on page 1
- Example: Configuring PIM Snooping for VPLS on page 2

Understanding PIM Snooping for VPLS

There are two ways to direct PIM control packets:

- By the use of PIM snooping
- By the use of PIM proxying

PIM snooping configures a device to examine and operate only on PIM hello and join/prune packets. A PIM snooping device snoops PIM hello and join/prune packets on each interface to find interested multicast receivers and populates the multicast forwarding tree with this information. PIM snooping differs from PIM proxying in that both PIM hello and join/prune packets are transparently flooded in the VPLS as opposed to the flooding of only hello packets in the case of PIM proxying. PIM snooping is configured on PE routers connected through pseudowires. PIM snooping ensures that no new PIM packets are generated in the VPLS, with the exception of PIM messages sent through LDP on pseudowires.

A device that supports PIM snooping snoops hello packets received on attachment circuits. It does not introduce latency in the VPLS core when it forwards PIM join/prune packets.

To configure PIM snooping on a PE router, use the **pim-snooping** statement at the **[edit routing-instances *instance-name* protocols]** hierarchy level:

```
routing-instances {
  customer {
    instance-type vpls;
    ...
    protocols {
      pim-snooping{
        traceoptions {
          file pim.log size 10m;
          flag all;
          flag timer disable;
        }
      }
    }
  }
}
```

"Example: Configuring PIM Snooping for VPLS" on page 2 explains the PIM snooping method. The use of the PIM proxying method is not discussed here and is outside the scope of this document. For more information about PIM proxying, see PIM Snooping over VPLS.

Related Documentation

- PIM Snooping for VPLS Use Cases on page 1
- Example: Configuring PIM Snooping for VPLS on page 2

Example: Configuring PIM Snooping for VPLS

This example shows how to configure PIM snooping in a virtual private LAN service (VPLS) to restrict multicast traffic to interested devices.

- Requirements on page 3
- Overview on page 3
- Configuration on page 4
- Verification on page 10

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers (except MX80)
- Junos OS Release 12.3 or later

Overview

The following example shows how to configure PIM snooping to restrict multicast traffic to interested devices in a VPLS.

NOTE: This example demonstrates PIM snooping by the use of a PIM snooping device to restrict multicast traffic. The use of the PIM proxying method to achieve PIM snooping is out of the scope of this document and is yet to be implemented in Junos OS.

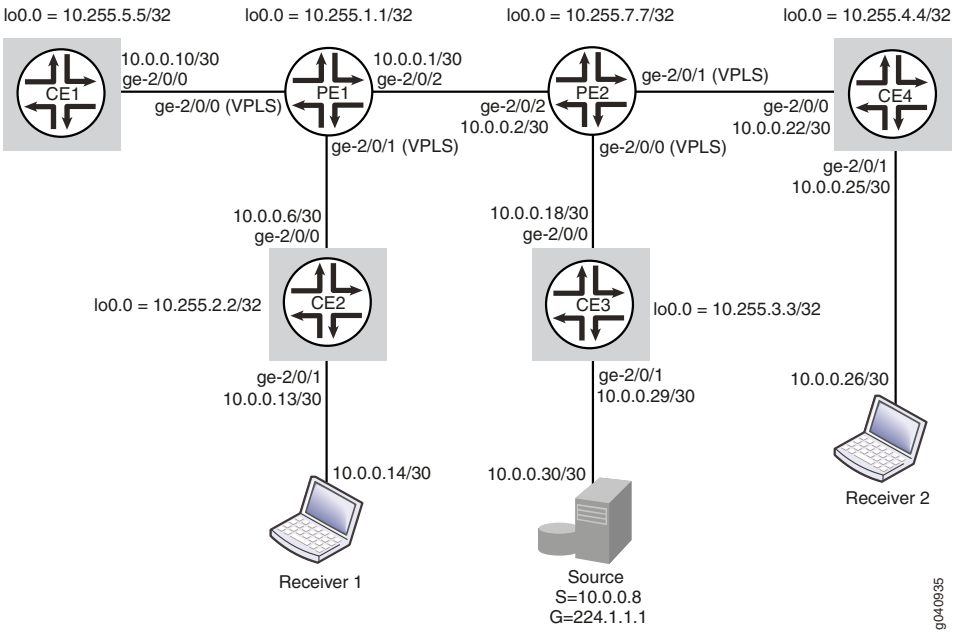
Topology

In this example, two PE routers are connected to each other through a pseudowire connection. Router PE1 is connected to Routers CE1 and CE2. A multicast receiver is attached to Router CE2. Router PE2 is connected to Routers CE3 and CE4. A multicast source is connected to Router CE3, and a second multicast receiver is attached to Router CE4.

PIM snooping is configured on Routers PE1 and PE2. Hence, data sent from the multicast source is received only by members of the multicast group.

Figure 1 on page 4 shows the topology used in this example.

Figure 1: PIM Snooping for VPLS



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Router PE1

```
set multicast-snooping-options traceoptions file snoop.log size 10m
set interfaces ge-2/0/0 encapsulation ethernet-vpls
set interfaces ge-2/0/0 unit 0 description toCE1
set interfaces ge-2/0/1 encapsulation ethernet-vpls
set interfaces ge-2/0/1 unit 0 description toCE2
set interfaces ge-2/0/2 unit 0 description toPE2
set interfaces ge-2/0/2 unit 0 family inet address 10.0.0.1/30
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.1.1/32
set routing-options router-id 10.255.1.1
set protocols mpls interface ge-2/0/1.0
set protocols bgp group toPE2 type internal
set protocols bgp group toPE2 local-address 10.255.1.1
set protocols bgp group toPE2 family l2vpn signaling
set protocols bgp group toPE2 neighbor 10.255.7.7
set protocols ospf area 0.0.0.0 interface ge-2/0/2.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface ge-2/0/2.0
set protocols ldp interface lo0.0
set routing-instances titanium instance-type vpls
set routing-instances titanium vlan-id none
set routing-instances titanium interface ge-2/0/0.0
set routing-instances titanium interface ge-2/0/1.0
set routing-instances titanium route-distinguisher 101:101
```

```
set routing-instances titanium vrf-target target:201:201
set routing-instances titanium protocols vpls vpls-id 15
set routing-instances titanium protocols vpls site pe1 site-identifier 1
set routing-instances titanium protocols pim-snooping
```

Router CE1

```
set interfaces ge-2/0/0 unit 0 description toPE1
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.10/30
set interfaces lo0 unit 0 family inet address 10.255.2.2./32
set routing-options router-id 10.255.2.2
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all
```

Router CE2

```
set interfaces ge-2/0/0 unit 0 description toPE1
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.6/30
set interfaces ge-2/0/1 unit 0 description toReceiver1
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.13/30
set interfaces lo0 unit 0 family inet address 10.255.2.2
set routing-options router-id 10.255.2.2
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all
```

Router PE2

```
set multicast-snooping-options traceoptions file snoop.log size 10m
set interfaces ge-2/0/0 encapsulation ethernet-vpls
set interfaces ge-2/0/0 unit 0 description toCE3
set interfaces ge-2/0/1 encapsulation ethernet-vpls
set interfaces ge-2/0/1 unit 0 description toCE4
set interfaces ge-2/0/2 unit 0 description toPE1
set interfaces ge-2/0/2 unit 0 family inet address 10.0.0.2/30
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.7.7/32
set routing-options router-id 10.255.7.7
set protocols mpls interface ge-2/0/2.0
set protocols bgp group toPE1 type internal
set protocols bgp group toPE1 local-address 10.255.7.7
set protocols bgp group toPE1 family l2vpn signaling
set protocols bgp group toPE1 neighbor 10.255.1.1
set protocols ospf area 0.0.0.0 interface ge-2/0/2.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ldp interface ge-2/0/2.0
set protocols ldp interface lo0.0
set routing-instances titanium instance-type vpls
set routing-instances titanium vlan-id none
set routing-instances titanium interface ge-2/0/0.0
set routing-instances titanium interface ge-2/0/1.0
set routing-instances titanium route-distinguisher 101:101
set routing-instances titanium vrf-target target:201:201
set routing-instances titanium protocols vpls vpls-id 15
set routing-instances titanium protocols vpls site pe2 site-identifier 2
set routing-instances titanium protocols pim-snooping
```

Router CE3 (RP)

```
set interfaces ge-2/0/0 unit 0 description toPE2
```

```
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.18/30
set interfaces ge-2/0/1 unit 0 description toSource
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.29/30
set interfaces lo0 unit 0 family inet address 10.255.3.3/32
set routing-options router-id 10.255.3.3
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp local address 10.255.3.3
set protocols pim interface all
```

Router CE4

```
set interfaces ge-2/0/0 unit 0 description toPE2
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.22/30
set interfaces ge-2/0/1 unit 0 description toReceiver2
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.25/30
set interfaces lo0 unit 0 family inet address 10.255.4.4/32
set routing-options router-id 10.255.4.4
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all
```

Configuring PIM Snooping for VPLS

Step-by-Step Procedure

The following example requires that you 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*.

NOTE: This section includes a step-by-step configuration procedure for one or more routers in the topology. For comprehensive configurations for all routers, see "CLI Quick Configuration" on page 4.

To configure PIM snooping for VPLS:

1. Configure the router interfaces forming the links between the routers.

   Router PE2

   ```
   [edit interfaces]
   user@PE2# set ge-2/0/0 encapsulation ethernet-vpls
   user@PE2# set ge-2/0/0 unit 0 description toCE3
   user@PE2# set ge-2/0/1 encapsulation ethernet-vpls
   user@PE2# set ge-2/0/1 unit 0 description toCE4
   user@PE2# set ge-2/0/2 unit 0 description toPE1
   user@PE2# set ge-2/0/2 unit 0 family mpls
   user@PE2# set ge-2/0/2 unit 0 family inet address 10.0.0.2/30
   user@PE2# set lo0 unit 0 family inet address 10.255.7.7/32
   ```

   NOTE: ge-2/0/0.0 and ge-2/0/1.0 are configured as VPLS interfaces and connect to Routers CE3 and CE4. See Configuring VPLS Encapsulation on CE-Facing Interfaces for more details.

Router CE3
[edit interfaces]
user@CE3# set ge-2/0/0 unit 0 description toPE2
user@CE3# set ge-2/0/0 unit 0 family inet address 10.0.0.18/30
user@CE3# set ge-2/0/1 unit 0 description toSource
user@CE3# set ge-2/0/1 unit 0 family inet address 10.0.0.29/30
user@CE3# set lo0 unit 0 family inet address 10.255.3.3/32

NOTE: The ge-2/0/1.0 interface on Router CE3 connects to the multicast source.

Router CE4
[edit interfaces]
user@CE4# set ge-2/0/0 unit 0 description toPE2
user@CE4# set ge-2/0/0 unit 0 family inet address 10.0.0.22/30
user@CE4# set ge-2/0/1 unit 0 description toReceiver2
user@CE4# set ge-2/0/1 unit 0 family inet address 10.0.0.25/30
user@CE4# set lo0 unit 0 family inet address 10.255.4.4/32

NOTE: The ge-2/0/1.0 interface on Router CE4 connects to a multicast receiver.

Similarly, configure Routers PE1, CE1, and CE2.

2. Configure the router IDs of all routers.

   Router PE2
   [edit routing-options]
   user@PE2# set router-id 10.255.7.7

   Similarly, configure other routers.

3. Configure an IGP on interfaces of all routers.

   Router PE2
   [edit protocols ospf area 0.0.0.0]
   user@PE2# set interface ge-2/0/2.0
   user@PE2# set interface lo0.0

   Similarly, configure other routers.

4. Configure the LDP, MPLS, and BGP protocols on the PE routers.

   Router PE2
   [edit protocols]
   user@PE2# set ldp interface lo0.0
   user@PE2# set mpls interface ge-2/0/2.0
   user@PE2# set bgp group toPE1 type internal
   user@PE2# set bgp group toPE1 local-address 10.255.7.7
   user@PE2# set bgp group toPE1 family l2vpn signaling
   user@PE2# set bgp group toPE1 neighbor 10.255.1.1
   user@PE2# set ldp interface ge-2/0/2.0

The BGP group is required for interfacing with the other PE router. Similarly, configure Router PE1.

5. Configure PIM on all CE routers.

   Ensure that Router CE3 is configured as the rendezvous point (RP) and that the RP address is configured on other CE routers.

   Router CE3
   [edit protocols pim]
   user@CE3# **set rp local address 10.255.3.3**
   user@CE3# **set interface all**

   Router CE4
   [edit protocols pim]
   user@CE4# **set rp static address 10.255.3.3**
   user@CE4# **set interface all**

   Similarly, configure Routers CE1 and CE2.

6. Configure multicast snooping options on the PE routers.

   Router PE2
   [edit multicast-snooping-options traceoptions]
   user@PE2# **set file snoop.log size 10m**

   Similarly, configure Router PE1.

7. Create a routing instance (**titanium**), and configure the VPLS on the PE routers.

   Router PE2
   [edit routing-instances titanium]
   user@PE2# **set instance-type vpls**
   user@PE2# **set vlan-id none**
   user@PE2# **set interface ge-2/0/0.0**
   user@PE2# **set interface ge-2/0/1.0**
   user@PE2# **set route-distinguisher 101:101**
   user@PE2# **set vrf-target target:201:201**
   user@PE2# **set protocols vpls vpls-id 15**
   user@PE2# **set protocols vpls site pe2 site-identifier 2**

   Similarly, configure Router PE1.

8. Configure PIM snooping on the PE routers.

   Router PE2
   [edit routing-instances titanium]
   user@PE2# **set protocols pim-snooping**

   Similarly, configure Router PE1.

From configuration mode, confirm your configuration by entering the **show interfaces**, **show routing-options**, **show protocols**, **show multicast-snooping-options**, and **show routing-instances** commands.

If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE2# show interfaces
```

```
ge-2/0/2 {
    unit 0 {
        description toPE1
        family inet {
            address 10.0.0.2/30;
        }
        family mpls;
    }
}
ge-2/0/0 {
    encapsulation ethernet-vpls;
    unit 0 {
         description toCE3;
           }
}
ge-2/0/1 {
    encapsulation ethernet-vpls;
    unit 0 {
         description toCE4;
           }
}
lo0 {
    unit 0 {
        family inet {
            address 10.255.7.7/32;
        }
    }
}

user@PE2# show routing-options
router-id 10.255.7.7;

user@PE2# show protocols
mpls {
    interface ge-2/0/2.0;
}
ospf {
    area 0.0.0.0 {
        interface ge-2/0/2.0;
        interface lo0.0;
    }
}
ldp {
    interface ge-2/0/2.0;
    interface lo0.0;
}
bgp {
    group toPE1 {
        type internal;
        local-address 10.255.7.7;
        family l2vpn {
            signaling;
        }
        neighbor 10.255.1.1;
    }

user@PE2# show multicast-snooping-options
traceoptions {
    file snoop.log size 10m;
}
```

```
user@PE2# show routing-instances
titanium {
    instance-type vpls;
    vlan-id none;
    interface ge-2/0/0.0;
    interface ge-2/0/1.0;
    route-distinguisher 101:101;
    vrf-target target:201:201;
    protocols {
        vpls {
            site pe2 {
                site-identifier 2;
            }
            vpls-id 15;
        }
        pim-snooping;
  }
}
```

Similarly, confirm the configuration on all other routers. If you are done configuring the routers, enter **commit** from configuration mode.

NOTE: Use the **show protocols** command on the CE routers to verify the configuration for the PIM RP .

Verification

Confirm that the configuration is working properly.

- Verifying PIM Snooping for VPLS on page 10

Verifying PIM Snooping for VPLS

Purpose Verify that PIM Snooping is operational in the network.

Action To verify that PIM snooping is working as desired, use the following commands:

- **show pim snooping interfaces**
- **show pim snooping neighbors detail**
- **show pim snooping statistics**
- **show pim snooping join**
- **show pim snooping join extensive**
- **show multicast snooping route extensive instance** *<instance-name>* **group** *<group-name>*

1. From operational mode on Router PE2, run the **show pim snooping interfaces** command.

```
user@PE2> show pim snooping interfaces
Instance: titanium

Learning-Domain: default

Name                 State IP NbrCnt
ge-2/0/0.0           Up    4       1
ge-2/0/1.0           Up    4       1

DR address: 10.0.0.22
DR flooding is ON
```

   The output verifies that PIM snooping is configured on the two interfaces connecting Router PE2 to Routers CE3 and CE4.

   Similarly, check the PIM snooping interfaces on Router PE1.

2. From operational mode on Router PE2, run the **show pim snooping neighbors detail** command.

```
user@PE2> show pim snooping neighbors detail
Instance: titanium
Learning-Domain: default

Interface: ge-2/0/0.0

    Address: 10.0.0.18
        Uptime: 00:17:06
        Hello Option Holdtime: 105 seconds 99 remaining
        Hello Option DR Priority: 1
        Hello Option Generation ID: 552495559
        Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
                                      Tracking is supported

Interface: ge-2/0/1.0

    Address: 10.0.0.22
        Uptime: 00:15:16
        Hello Option Holdtime: 105 seconds 103 remaining
        Hello Option DR Priority: 1
        Hello Option Generation ID: 1131703485
        Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
                                      Tracking is supported
```

   The output verifies that Router PE2 can detect the IP addresses of its PIM snooping neighbors (10.0.0.18 on CE3 and 10.0.0.22 on CE4).

   Similarly, check the PIM snooping neighbors on Router PE1.

3. From operational mode on Router PE2, run the **show pim snooping statistics** command.

```
user@PE2> show pim snooping statistics
Instance: titanium

Learning-Domain: default

Tx J/P messages                              0
```

```
RX J/P messages                              246
Rx J/P messages -- seen                        0
Rx J/P messages -- received                  246
Rx Hello messages                           1036
Rx Version Unknown                             0
Rx Neighbor Unknown                            0
Rx Upstream Neighbor Unknown                   0
Rx J/P Busy Drop                               0
Rx J/P Group Aggregate                         0
Rx Malformed Packet                            0

Rx No PIM Interface                            0
Rx Bad Length                                  0
Rx Unknown Hello Option                        0
Rx Unknown Packet Type                         0
Rx Bad TTL                                     0
Rx Bad Destination Address                     0
Rx Bad Checksum                                0
Rx Unknown Version                             0
```

The output shows the number of hello and join/prune messages received by Router PE2. This verifies that PIM sparse mode is operational in the network.

4. Send multicast traffic from the source terminal attached to Router CE3, for the multicast group 224.1.1.1.

5. From operational mode on Router PE2, run the **show pim snooping join**, **show pim snooping join extensive**, and **show multicast snooping route extensive instance *<instance-name>* group *<group-name>*** commands to verify PIM snooping.

```
user@PE2> show pim snooping join
Instance: titanium
Learning-Domain: default

Group: 224.1.1.1
    Source: *
    Flags: sparse,rptree,wildcard
    Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0

Group: 224.1.1.1
    Source: 10.0.0.30
    Flags: sparse
    Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
```

```
user@PE2> show pim snooping join extensive
Instance: titanium
Learning-Domain: default

Group: 224.1.1.1
    Source: *
    Flags: sparse,rptree,wildcard
    Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
        Downstream port: ge-2/0/1.0
            Downstream neighbors:
                10.0.0.22 State: Join Flags: SRW Timeout: 180

Group: 224.1.1.1
    Source: 10.0.0.30
    Flags: sparse
    Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
        Downstream port: ge-2/0/1.0
```



```
            Downstream neighbors:
                10.0.0.22 State: Join Flags: S Timeout: 180
```

The outputs show that multicast traffic sent for the group 224.1.1.1 is sent to Receiver 2 through Router CE4 and also display the upstream and downstream neighbor details.

```
user@PE2> show multicast snooping route extensive instance titanium group 224.1.1.1
Nexthop Bulking: OFF

             Family: INET

Group: 224.1.1.1/32
    Bridge-domain: titanium
    Mesh-group: __all_ces__
    Downstream interface list:
        ge-2/0/1.0 -(1072)
    Statistics: 0 kBps, 0 pps, 0 packets
    Next-hop ID: 1048577
    Route state: Active
    Forwarding state: Forwarding

Group: 224.1.1.1/32
    Source: 10.0.0.8
    Bridge-domain: titanium
    Mesh-group: __all_ces__
    Downstream interface list:
        ge-2/0/1.0 -(1072)
    Statistics: 0 kBps, 0 pps, 0 packets
    Next-hop ID: 1048577
    Route state: Active
    Forwarding state: Forwarding
```

Meaning PIM snooping is operational in the network.

Related Documentation

- PIM Snooping for VPLS Use Cases on page 1
- Understanding PIM Snooping for VPLS on page 1