

Chapter 15

Source-Specific Multicast

Source-specific multicast (SSM) is a service model that identifies session traffic by both source and group address. SSM implemented in the JUNOS software has the efficient explicit join procedures of Protocol Independent Multicast (PIM) sparse mode but eliminates the immediate shared tree and rendezvous point (RP) procedures using (*, G) pairs. The (*) is a wildcard referring to any source sending to group G, and “G” refers to the IP multicast group. SSM builds shortest-path trees (SPTs) directly represented by (S,G) pairs. The “S” refers to the source’s unicast IP address, and the “G” refers to the specific multicast group address. The SSM (S,G) pairs are called channels to differentiate them from any-source multicast (ASM) groups. Although ASM supports both one-to-many and many-to-many communications, ASM’s complexity is in its method of source discovery. For example, if you click on a link in a browser, the receiver is notified about the group information, but not the source information. With SSM, the client receives both source and group information.

SSM is ideal for one-to-many multicast services such as network entertainment channels. However, many-to-many multicast services might require ASM.

To deploy SSM successfully, you need an end-to-end multicast-enabled network and applications that use an Internet Group Management Protocol version 3 (IGMPv3) stack or configure SSM mapping from IGMPv1/IGMPv2 to IGMPv3. An IGMPv3 stack is the capability of a host operating system to use the IGMPv3 protocol. Most operating systems today use an IGMPv2 stack, but IGMPv3 is available for Windows XP, and upgrades are available on some UNIX operating systems.

SSM mapping allows operators to support an SSM network without requiring all hosts to support IGMPv3. This support exists in static (S,G) configurations, but SSM mapping also supports dynamic per-source group state information, which changes as hosts join and leave the group using IGMP.

For information about standards supported for source-specific multicast, see “IP Multicast Standards” on page 28.

This chapter discusses the following topics:

- Source-Specific Multicast Groups Overview on page 130
- Source-Specific Multicast Examples on page 132

Source-Specific Multicast Groups Overview

SSM is typically supported with a subset of IGMPv3 and PIM sparse mode known as PIM SSM. Using SSM, a client can receive multicast traffic directly from the source. PIM SSM uses the PIM sparse-mode functionality to create an SPT between the client and the source, but builds the SPT without the help of an RP.

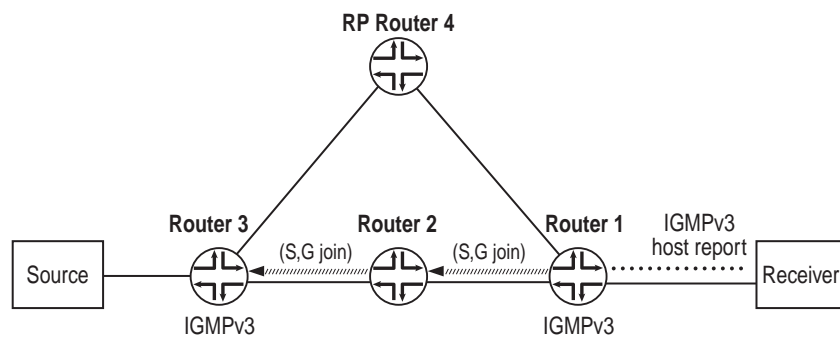
By default, the SSM group multicast address is limited to the IP address range 232.0.0.0 to 232.255.255.255. However, you can extend SSM operations into another Class D range by including the address statement at the [edit routing-options multicast ssm-groups] hierarchy level.

An SSM-configured network has distinct advantages over a traditionally configured PIM sparse-mode network. There is no need for shared trees or RP mapping (no RP is required), or for RP-to-RP source discovery through the Multicast Source Discovery Protocol (MSDP).

Deploying SSM is easy. You need only configure PIM sparse mode on all router interfaces and issue the necessary SSM commands, including specifying IGMPv3 on the receiver's LAN. If PIM sparse mode is not explicitly configured on both the source and group members interfaces, multicast packets are not forwarded. Source lists, supported in IGMPv3, are used in PIM SSM. Only sources that are specified send traffic to the SSM group.

In a PIM SSM-configured network, a host subscribes to an SSM channel (by means of IGMPv3), announcing a desire to join group G and source S (see Figure 10). The directly connected PIM sparse-mode router, the receiver's designated router (DR), sends an (S,G) join message to its reverse-path forwarding (RPF) neighbor for the source. Notice in Figure 10 that the RP is not contacted in this process by the receiver, as would be the case in normal PIM sparse-mode operations.

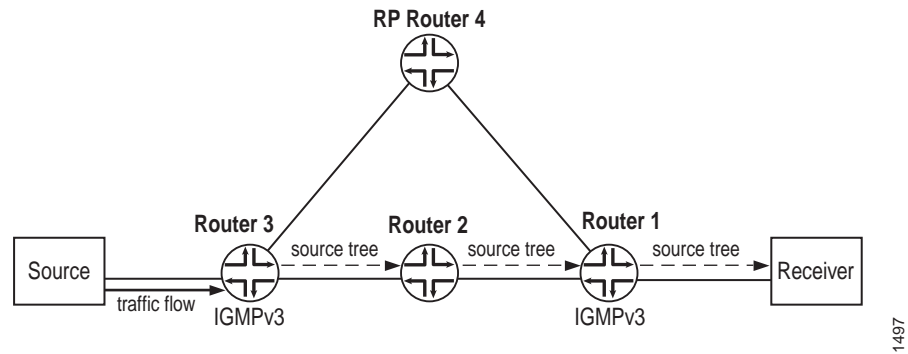
Figure 10: Receiver Announces Desire to Join Group G and Source S



1496

The (S,G) join message initiates the source tree, then builds it out hop by hop until it reaches the source. In Figure 11, the source tree is built across the network to Router 3, the last-hop router connected to the source.

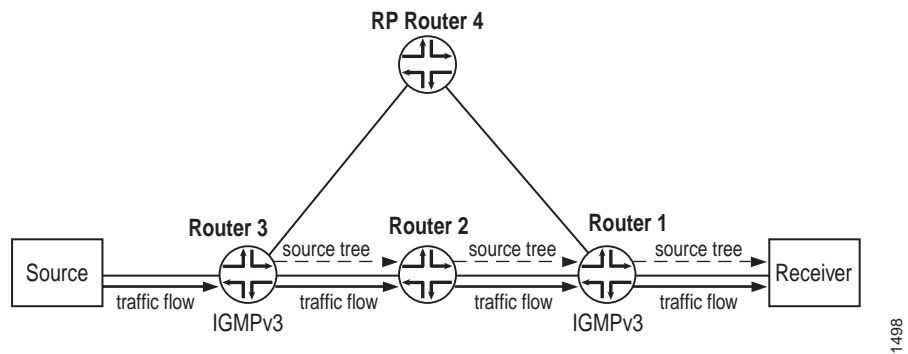
Figure 11: Router 3 (Last-Hop Router) Joins the Source Tree



1497

Using the source tree, multicast traffic is delivered to the subscribing host (see Figure 12).

Figure 12: The (S,G) State Is Built Between the Source and the Receiver



1498

To configure additional SSM groups, include the `ssm-groups` statement:

```
multicast {
  ssm-groups {
    address;
  }
}
```

For a list of the hierarchy levels at which you can configure this statement, see the statement summary section for this statement.

For an overview of logical routers and a detailed example of logical router configuration, see the logical routers chapter of the *JUNOS Feature Guide*.

Source-Specific Multicast Examples

This section discusses the following topics:

- Example: Configuring an SSM-Only Domain on page 132
- Example: Configuring PIM SSM on a Network on page 133
- Example: Configuring SSM Mapping on page 134

Example: Configuring an SSM-Only Domain

Deploying an SSM-only domain is much simpler than deploying an ASM domain; it only requires a few configuration steps. Enable PIM sparse mode on all interfaces by adding the `mode` statement at the `[edit protocols pim interface all]` hierarchy level. When configuring all interfaces, exclude the `fxp0.0` management interface by adding the `disable` statement for that interface. Then configure IGMPv3 on all host-facing interfaces by adding the `version` statement at the `[edit protocols igmp interface interface-name]` hierarchy level.

In the following example, the host-facing interface is `fe-0/1/2`:

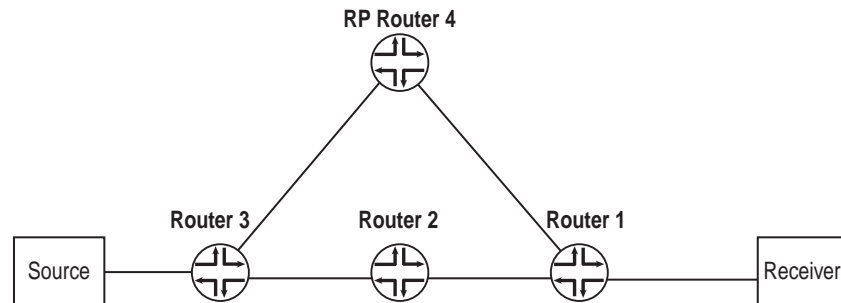
```
[edit]
protocols {
  pim {
    interface all {
      mode sparse;
      version 2;
    }
    interface fxp0.0 {
      disable;
    }
  }

  igmp {
    interface fe-0/1/2 {
      version 3;
    }
  }
}
```

Example: Configuring PIM SSM on a Network

The following example shows how PIM SSM is configured between a receiver and a source in the network illustrated in Figure 13.

Figure 13: Network on Which to Configure PIM SSM



1499

The configuration establishes IGMPv3 on all receiving host interfaces. You then can use the following `show` commands to verify the PIM SSM configuration:

- Issue the `show igmp interface` command to display IGMP interfaces, configurable parameters, and IGMP version.
- Issue the `show pim join extensive` command to display the PIM state.

This example discusses the following topics that provide information about configuring and verifying operation of PIM SSM:

- Enabling IGMPv3 on all Host-Facing Interfaces on page 133
- Displaying the IGMP State on page 134
- Displaying the PIM State on page 134

Enabling IGMPv3 on all Host-Facing Interfaces

To enable IGMPv3 on all host-facing interfaces, include the `version 3` statement under the `interface all` statement at the `[edit protocols igmp]` hierarchy level:

```

[edit protocols igmp]
interface all {
  version 3;
}
interface fxp0.0 {
  disable;
}

```



NOTE: When you configure IGMPv3 on a router, hosts on interfaces configured with IGMPv2 cannot join the source tree.

Displaying the IGMP State

To show IGMP information about the interfaces on Router 1, use the `show igmp interface` command:

```
user@router1> show igmp interface
Interface      State  Querier      Timeout Version Groups
fxp1.0         Up     0             0       3       0
fe-0/0/0.0     Up     198.58.3.245 213     3       0
fe-0/0/1.0     Up     198.58.3.241 220     3       0
fe-0/0/2.0     Up     198.58.3.237 218     3       0..
```

Configured Parameters:

```
IGMP Query Interval (1/10 secs): 1250
IGMP Query Response Interval (1/10 secs): 100
IGMP Last Member Query Interval (1/10 secs): 10
IGMP Robustness Count: 2
```

Derived Parameters:

```
IGMP Membership Timeout (1/10 secs): 2600
IGMP Other Querier Present Timeout (1/10 secs): 2550
```

Displaying the PIM State

To show the PIM state on Router 2 and Router 3 (the upstream routers), use the `show pim join extensive` command:

```
user@router2> show pim join extensive
232.1.1.1      10.4.1.2      sparse
  Upstream interface: fe-1/1/3.0
  Upstream State: Local Source
  Keepalive timeout: 209
  Downstream Neighbors:
    Interface: so-1/0/2.0
      10.10.71.1      State: Join  Flags: S  Timeout: 209
```

To show the PIM state on Router 1 (the router connected to the receiver), use the `show pim join extensive` command:

```
user@router1> show pim join extensive
232.1.1.1      10.4.1.2      sparse
  Upstream interface: so-1/0/2.0
  Upstream State: Join to Source
  Keepalive timeout: 209
  Downstream Neighbors:
    Interface: fe-0/2/3.0
      10.3.1.1      State: Join  Flags: S  Timeout: Infinity
```

Example: Configuring SSM Mapping

SSM mapping does not require all hosts to support IGMPv3. SSM mapping translates IGMPv1 or IGMPv2 membership reports to an IGMPv3 report. This allows hosts running IGMPv1/IGMPv2 to participate in SSM until the hosts transition to IGMPv3.

There are three steps to configuring SSM mapping. First, you create a policy to match the group addresses you want to translate to IGMPv3. Then you define the SSM map that associates the policy with the source addresses where these group addresses are found. SSM mapping applies to all group addresses that match the policy, not just those that conform to SSM addressing conventions (232/8 for IPv4, ff30::/32 through ff3F::/32 for IPv6). Finally, you apply the SSM map to one or more IGMP (for IPv4) or MLD (for IPv6) interfaces.

We recommend separate SSM maps for IPv4 and IPv6 if both address families require SSM support. If you apply an SSM map containing both IPv4 and IPv6 addresses to an interface in an IPv4 context (using IGMP), only the IPv4 addresses in the list are used. If there are no such addresses, no action is taken. Similarly, if you apply an SSM map containing both IPv4 and IPv6 addresses to an interface in an IPv6 context (using MLD), only the IPv6 addresses in the list are used. If there are no such addresses, no action is taken.

- Creating the SSM Policy on page 135
- Defining the SSM Map on page 136
- Applying SSM Mapping to Interfaces on page 136
- Displaying the SSM Maps on page 136

Creating the SSM Policy

This example creates an SSM policy called `ssm-policy-example`. The policy terms match the IPv4 SSM group address `232.1.1.1/32` and the IPv6 SSM group address `ff35::1/128`. All other addresses are rejected.

```
[edit policy-options]
policy-statement ssm-policy-example {
  term A {
    from {
      route-filter 232.1.1.1/32 exact;
    }
    then accept;
  }
  term B {
    from {
      route-filter ff35::1/128 exact;
    }
    then accept;
  }
  then reject;
}
```

The group addresses must match the configured policy for SSM mapping to occur.

Defining the SSM Map

This example defines two SSM maps, one called `ssm-map-ipv6-example` and one called `ssm-map-ipv4-example`, by applying the policy and configuring the source addresses as a multicast routing option.

```
[edit routing-options]
multicast {
  ssm-map ssm-map-ipv6-example {
    policy ssm-policy-example;
    source [ fec0::1 fec0::12 ];
  }
  ssm-map ssm-map-ipv4-example {
    policy ssm-policy-example;
    source [ 10.10.10.4 192.168.43.66 ];
  }
}
```

We recommend separate SSM maps for IPv4 and IPv6.

Applying SSM Mapping to Interfaces

You should apply SSM maps for IPv4 to IGMP interfaces and SSM maps for IPv6 to MLD interfaces.

```
[edit protocols]
igmp {
  interface fe-0/1/0.0 {
    ssm-map ssm-map-ipv4-example;
  }
}
mld {
  interface fe-0/1/1.0 {
    ssm-map ssm-map-ipv6-example;
  }
}
```

Displaying the SSM Maps

To show the SSM maps that are applied to an interface, use the `show igmp interface` or the `show mld interface` command:

```
user@router1> show igmp interface fe-0/1/0.0
Interface: fe-0/1/0.0
  Querier: 192.168.224.28
  State:          Up Timeout:    None Version:  2 Groups:  2
  SSM Map: ssm-map-ipv4-example

user@router1> show mld interface fe-0/1/1.0
Interface: fe-0/1/1.0
  Querier: fec0:0:0:1::12
  State:          Up Timeout:    None Version:  2 Groups:  2
  SSM Map: ssm-map-ipv6-example
```