Source Specific Multicast

Last Updated: January 29, 2013

- Finding Feature Information, page 1
- Information About Source Specific Multicast, page 1
- How to Configure Source Specific Multicast, page 4
- Configuration Examples for Source Specific Multicast, page 6
- Additional References, page 7
- Feature Information for Source Specific Multicast, page 8

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Source Specific Multicast

- SSM Components, page 1
- How SSM Differs from Internet Standard Multicast, page 2
- SSM Operations, page 2
- IGMPv3 Host Signaling, page 3
- Benefits of Source Specific Multicast, page 3

SSM Components

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569. The following two components together support the implementation of SSM:
• Protocol Independent Multicast source-specific mode (PIM-SSM)
• Internet Group Management Protocol Version 3 (IGMPv3)

Protocol Independent Multicast (PIM) SSM, or PIM-SSM, is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which is required for SSM. In order for SSM to run with IGMPv3, SSM must be supported in the device, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The standard IP multicast infrastructure in the Internet and many enterprise intranets is based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have proved to be reliable, extensive, and efficient. However, they are bound to the complexity and functionality limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic. With SSM, this information is provided by receivers through the source addresses relayed to the last-hop devices by IGMPv3. SSM is an incremental response to the issues associated with ISM and is intended to coexist in the network with the protocols developed for ISM. In general, SSM provides IP multicast service for applications that utilize SSM.

ISM service is described in RFC 1112. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the host group. Membership in a host group simply requires signaling the host group through IGMP Version 1, 2, or 3. In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the (S, G) channel. In both SSM and ISM, no signaling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signaling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMP Version 3.

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Internet Assigned Numbers Authority (IANA) has reserved the address range from 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. The software allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 through 239.255.255.255. When an SSM range is defined, an existing IP multicast receiver application will not receive any traffic when it tries to use addresses in the SSM range unless the application is modified to use explicit (S, G) channel subscription or is SSM-enabled through a URL Rendezvous Directory (URD).

SSM Operations

An established network in which IP multicast service is based on PIM-SM can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM. That is, SSM does not require an RP, so there is no need for an RP mechanism such as Auto-RP, MSDP, or bootstrap router (BSR).

If SSM is deployed in a network that is already configured for PIM-SM, then only the last-hop devices must be upgraded to a software image that supports SSM. Routers that are not directly connected to
receivers do not have to upgrade to a software image that supports SSM. In general, these non-last-hop
devices must only run PIM-SM in the SSM range. They may need additional access control configuration
to suppress MSDP signaling, registering, or PIM-SM shared-tree operations from occurring within the SSM
range.

The SSM mode of operation is enabled by configuring the SSM range using the `ip pim ssm` global
configuration command. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3
  INCLUDE mode membership reports.
- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-
  SM. In this mode, only PIM (S, G) Join and Prune messages are generated by the device. Incoming
  messages related to rendezvous point tree (RPT) operations are ignored or rejected, and incoming PIM
  register messages are immediately answered with Register-Stop messages. PIM-SSM is backward-
  compatible with PIM-SM unless a device is a last-hop device. Therefore, devices that are not last-hop
devices can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- For groups within the SSM range, no MSDP Source-Active (SA) messages within the SSM range will
  be accepted, generated, or forwarded.

**IGMPv3 Host Signaling**

IGMPv3 is the third version of the IETF standards track protocol in which hosts signal membership to last-
hop devices of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership that
allows filtering capabilities with respect to sources. A host can signal either that it wants to receive traffic
from all sources sending to a group except for some specific sources (a mode called EXCLUDE) or that it
wants to receive traffic only from some specific sources sending to the group (a mode called INCLUDE).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode reports are
accepted by the last-hop router. In SSM, only INCLUDE mode reports are accepted by the last-hop router.

**Benefits of Source Specific Multicast**

**IP Multicast Address Management Not Required**

In the ISM service, applications must acquire a unique IP multicast group address because traffic
distribution is based only on the IP multicast group address used. If two applications with different sources
and receivers use the same IP multicast group address, then receivers of both applications will receive
traffic from the senders of both applications. Even though the receivers, if programmed appropriately, can
filter out the unwanted traffic, this situation would cause generally unacceptable levels of unwanted traffic.

Allocating a unique IP multicast group address for an application is still a problem. Most short-lived
applications use mechanisms like Session Description Protocol (SDP) and Session Announcement Protocol
(SAP) to get a random address, a solution that does not work well with a rising number of applications in
the Internet. The best current solution for long-lived applications is described in RFC 2770, but this
solution suffers from the restriction that each autonomous system is limited to only 255 usable IP multicast
addresses.

In SSM, traffic from each source is forwarded between devices in the network independent of traffic from
other sources. Thus different sources can reuse multicast group addresses in the SSM range.

**Denial of Service Attacks from Unwanted Sources Inhibited**

In SSM, multicast traffic from each individual source will be transported across the network only if it was
requested (through IGMPv3, IGMP v3lite, or URD memberships) from a receiver. In contrast, ISM
forwards traffic from any active source sending to a multicast group to all receivers requesting that multicast group. In Internet broadcast applications, this ISM behavior is highly undesirable because it allows unwanted sources to easily disturb the actual Internet broadcast source by simply sending traffic to the same multicast group. This situation depletes bandwidth at the receiver side with unwanted traffic and thus disrupts the undisturbed reception of the Internet broadcast. In SSM, this type of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

Easy to Install and Manage

SSM is easy to install and provision in a network because it does not require the network to maintain which active sources are sending to multicast groups. This requirement exists in ISM (with IGMPv1, IGMPv2, or IGMPv3).

The current standard solutions for ISM service are PIM-SM and MSDP. Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or BSR) and MSDP is required only for the network to learn about active sources. This management is not necessary in SSM, which makes SSM easier than ISM to install and manage, and therefore easier than ISM to operationally scale in deployment. Another factor that contributes to the ease of installation of SSM is the fact that it can leverage preexisting PIM-SM networks and requires only the upgrade of last hop devices to support IGMPv3, IGMP v3lite, or URD.

Ideal for Internet Broadcast Applications

The three benefits previously described make SSM ideal for Internet broadcast-style applications for the following reasons:

- The ability to provide Internet broadcast services through SSM without the need for unique IP multicast addresses allows content providers to easily offer their service (IP multicast address allocation has been a serious problem for content providers in the past).
- The prevention against DoS attacks is an important factor for Internet broadcast services because, with their exposure to a large number of receivers, they are the most common targets for such attacks.
- The ease of installation and operation of SSM makes it ideal for network operators, especially in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains).

How to Configure Source Specific Multicast

- Configuring Source Specific Multicast, page 4

Configuring Source Specific Multicast

This section describes how to configure Source Specific Multicast (SSM).

If you want to use an access list to define the SSM range, configure the access list before you reference the access list in the `ip pim ssm` command.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip multicast-routing [distributed]`
4. `ip pim ssm {default | range access-list}`
5. `interface type number`
6. `ip pim sparse-mode`
7. Repeat Steps 1 through 6 on every interface that uses IP multicast.
8. `ip igmp version 3`
9. Repeat Step 8 on all host-facing interfaces.
10. `end`
11. `show ip igmp groups [group-name | group-address| interface-type interface-number] [detail]`
12. `show ip mroute`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>ip multicast-routing [distributed]</code></td>
<td>Enables IP multicast routing.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ip multicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `ip pim ssm {default</td>
<td>range access-list}`</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ip pim ssm default</td>
<td></td>
</tr>
</tbody>
</table>

*The distributed keyword enables Multicast Distributed Switching.*

*The default keyword defines the SSM range access list as 232/8.*

*The range keyword specifies the standard IP access list number or name that defines the SSM range.*
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>interface type number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config)# interface gigabitethernet 1/0/0</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>ip pim sparse-mode</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-if)# ip pim sparse-mode</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Repeat Steps 1 through 6 on every interface that uses IP multicast. -</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>ip igmp version 3</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-if)# ip igmp version 3</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Repeat Step 8 on all host-facing interfaces. -</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-if)# end</strong></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>**show ip igmp groups [group-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device# show ip igmp groups</strong></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>show ip mroute</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device# show ip mroute</strong></td>
</tr>
</tbody>
</table>

**Configuration Examples for Source Specific Multicast**
The following example shows how to configure a device (running IGMPv3) for SSM:

```plaintext
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
description backbone interface
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-mode
description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

**Additional References**

The following sections provide references related to customizing IGMP.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Commands List, All Releases</em></td>
</tr>
<tr>
<td>Cisco IOS IP SLAs commands</td>
<td><em>Cisco IOS IP Multicast Command Reference</em></td>
</tr>
<tr>
<td>Overview of the IP multicast technology area</td>
<td>“IP Multicast Technology Overview” module</td>
</tr>
<tr>
<td>Basic IP multicast concepts, configuration tasks, and examples</td>
<td>“Configuring Basic IP Multicast” or “Configuring IP Multicast in IPv6 Networks” module</td>
</tr>
</tbody>
</table>

**Standards and RFCs**

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1112</td>
<td><em>Host extensions for IP multicasting</em></td>
</tr>
<tr>
<td>RFC 2236</td>
<td><em>Internet Group Management Protocol, Version 2</em></td>
</tr>
<tr>
<td>RFC 3376</td>
<td><em>Internet Group Management Protocol, Version 3</em></td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by these features, and support for existing MIBs has not been modified by these features.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Release</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Source Specific Multicast (SSM)</td>
<td>12.3(4)T</td>
</tr>
<tr>
<td></td>
<td>12.2(25)S</td>
</tr>
<tr>
<td></td>
<td>12.0(28)S</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SXH</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
</tr>
<tr>
<td></td>
<td>15.0(1)S</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.1</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.1.0SG</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.5S</td>
</tr>
</tbody>
</table>

SSM with IGMPv3 Example

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012-2013 Cisco Systems, Inc. All rights reserved.