



# Source Specific Multicast (SSM) Mapping

The Source Specific Multicast (SSM) Mapping feature extends the Cisco IOS suite of SSM transition tools, which also includes URL Rendezvous Directory (URD) and Internet Group Management Protocol Version 3 Lite (IGMP v3lite). SSM mapping supports SSM transition in cases where neither URD nor IGMP v3lite is available, or when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. SSM mapping enables you to leverage SSM for video delivery to legacy set-top boxes (STBs) that do not support IGMPv3 or for applications that do not take advantage of the IGMPv3 host stack.

## History for the SSM Mapping Feature

### Feature History

Release	Modification
12.3(2)T	This feature was introduced.
12.2(18)S	This feature was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD3	This feature was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for SSM Mapping, page 2](#)
- [Restrictions for SSM Mapping, page 2](#)
- [Information About SSM Mapping, page 2](#)
- [How to Configure SSM Mapping, page 8](#)
- [Configuration Examples for SSM Mapping, page 15](#)



**Corporate Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2003, 2005–2006 Cisco Systems, Inc. All rights reserved.

- [Where to Go Next, page 19](#)
- [Additional References, page 19](#)
- [Command Reference, page 20](#)
- [Glossary, page 39](#)

## Prerequisites for SSM Mapping

- One option available for using SSM mapping is to install it together with a Domain Name System (DNS) server to simplify administration of the SSM Mapping feature in larger deployments.

Before you can configure and use SSM mapping with DNS lookups, you need to be able to add records to a running DNS server. If you do not already have a DNS server running, you need to install one. The Cisco IOS software does not provide for DNS server functionality.

You may want to use a product such as Cisco Network Registrar (CNR). See the following URL for more information about CNR:

<http://www.cisco.com/warp/public/cc/pd/nemnsw/nerr/index.shtml>

## Restrictions for SSM Mapping

- The SSM Mapping feature does not share the benefit of full SSM (unlike URD or IGMP v3lite). Because SSM mapping takes a group G join from a host and identifies this group with an application associated with one or more sources, it can only support one such application per group G. Nevertheless, full SSM applications may still share the same group also used in SSM mapping. That is, SSM mapping is compatible with simultaneous URD, IGMP v3lite or IGMPv3 membership reports.
- Enable IGMPv3 with care on the last hop router when you rely solely on SSM mapping as a transition solution for full SSM.

When both SSM mapping and IGMPv3 are enabled, the router will send out IGMPv3 membership query messages instead of IGMPv3 membership messages. If the receiver hosts that are to be supported with SSM mapping can only support IGMPv1 or IGMPv2, then enabling SSM mapping on an interface with IGMPv3 is fine. IGMPv3 membership query messages will be interpreted as IGMPv1 or IGMPv2 queries and the host will continue to report with IGMPv1 or IGMPv2 reports.

However, when both SSM mapping and IGMPv3 are enabled and the hosts already support IGMPv3 (but not SSM), then they will start to send IGMPv3 group reports. These IGMPv3 group reports are not supported with SSM mapping and the router will not correctly associate sources with these reports.

## Information About SSM Mapping

To configure the SSM Mapping feature, you should understand the following concepts:

- [SSM Components, page 3](#)
- [SSM Benefits, page 3](#)

- [SSM Transition Solutions, page 4](#)
- [SSM Mapping Overview, page 5](#)
- [SSM Mapping Benefits, page 7](#)

## SSM Components

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 Cisco IOS components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

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. IGMPv3 supports source filtering, which is required for SSM. For SSM to run with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself.

## SSM Benefits

### IP Multicast Address Management

In the Internet Standard Multicast (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, 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 problematic. 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 among routers in the network independently of traffic from other sources. Thus different sources can reuse multicast group addresses in the SSM range.

### Inhibition of Denial of Service Attacks

In SSM, multicast traffic from each individual source will be transported across the network only if it was requested (through IGMPv3 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 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.

### Installation and Management

SSM is easy to install and provision in a network because it does not require the network to maintain information about 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 Multicast Source Discovery Protocol (MSDP). Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or bootstrap router [BSR]) and MSDP is required only for the network to learn about active sources. This management is not necessary in SSM. SSM is therefore easier than ISM to install and manage and easier 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.

### Internet Broadcast Applications

The three benefits listed above 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 of 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).

## SSM Transition Solutions

The Cisco IOS suite of SSM transition solutions consists of the following transition solutions that enable the immediate development and deployment of SSM services, without the need to wait for the availability of full IGMPv3 support in host operating systems and SSM receiver applications:

- Internet Group Management Protocol Version 3 lite (IGMP v3lite)
- URL Rendezvous Directory (URD)
- SSM mapping

IGMP v3lite is a solution for application developers that allows immediate development of SSM receiver applications switching to IGMPv3 as soon as it becomes available.

For more information about IGMP v3lite, see the “IGMP v3lite Host Signalling” section in the “IP Multicast” part of the “Configuring Source Specific Multicast” chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt3/1cfssm.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfssm.htm)

URD is an SSM transition solution for content providers and content aggregators that allows them to deploy receiver applications that are not yet SSM enabled (through support for IGMPv3) by enabling the receiving applications to be started and controlled through a web browser.

For more information about URD, see the “URD Host Signalling” section in the “IP Multicast” part of the *Cisco IOS IP Configuration Guide*, Release 12.2 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt3/1cfssm.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfssm.htm)

SSM mapping supports SSM transition in cases where neither URD nor IGMP v3lite are available, or when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons.

## SSM Mapping Overview

SSM mapping supports SSM transition in cases where neither URD nor IGMP v3lite is available, or when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. Using SSM to deliver live streaming video to legacy STBs that do not support IGMPv3 is a typical application of SSM mapping.

Prior to the introduction of SSM mapping, the following conditions would have prevented SSM transition in the case of legacy STB deployments with STB receivers that only support IGMPv1 or IGMPv2:

- The operating system on the receivers do not support IGMPv3; thus, IGMPv3 cannot be used to support SSM.
- Moreover, the application running on the receivers cannot be upgraded to support SSM; thus, IGMPv3 lite cannot be used to support SSM transition.
- Furthermore, the application itself cannot be started through a web browser; thus, URD cannot be used to support SSM transition.

SSM mapping provides an SSM transition solution for hosts and applications that meet those conditions.

In a typical STB deployment, each TV channel uses one separate IP multicast group and has one active server host sending the TV channel. A single server may of course send multiple TV channels, but each to a different group. In this network environment, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group G, the report implicitly addresses the well-known TV server for the TV channel associated with the multicast group.

SSM mapping introduces a means for the last hop router to discover sources sending to groups. When SSM mapping is configured, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group G, the router translates this report into one or more (S, G) channel memberships for the well-known sources associated with this group.



### Note

As is the case for the other SSM transition solutions (URD and IGMP v3lite), SSM mapping only needs to be configured on the last hop router connected to receivers. No support is needed on any other routers in the network. SSM mapping, in addition, is fully compatible with IGMPv3, IGMP v3lite, and URD.

When the router receives an IGMPv1 or IGMPv2 membership report for a group G, the router uses SSM mapping to determine one or more source IP addresses for the group G. SSM mapping then translates the membership report as an IGMPv3 report INCLUDE (G, [S1, G], [S2, G]...[Sn, G] and continues as if it had received an IGMPv3 report. The router then sends out PIM joins toward (S1, G) to (Sn, G) and continues to be joined to these groups as long as it continues to receive the IGMPv1 or IGMPv2 membership reports and as long as the SSM mapping for the group remains the same. SSM mapping, thus, enables you to leverage SSM for video delivery to legacy STBs that do not support IGMPv3 or for applications that do not take advantage of the IGMPv3 host stack.

SSM mapping enables the last hop router to determine the source addresses either by a statically configured table on the router or by consulting a DNS server. When the statically configured table is changed, or when the DNS mapping changes, the router will leave the current sources associated with the joined groups.

## Static SSM Mapping

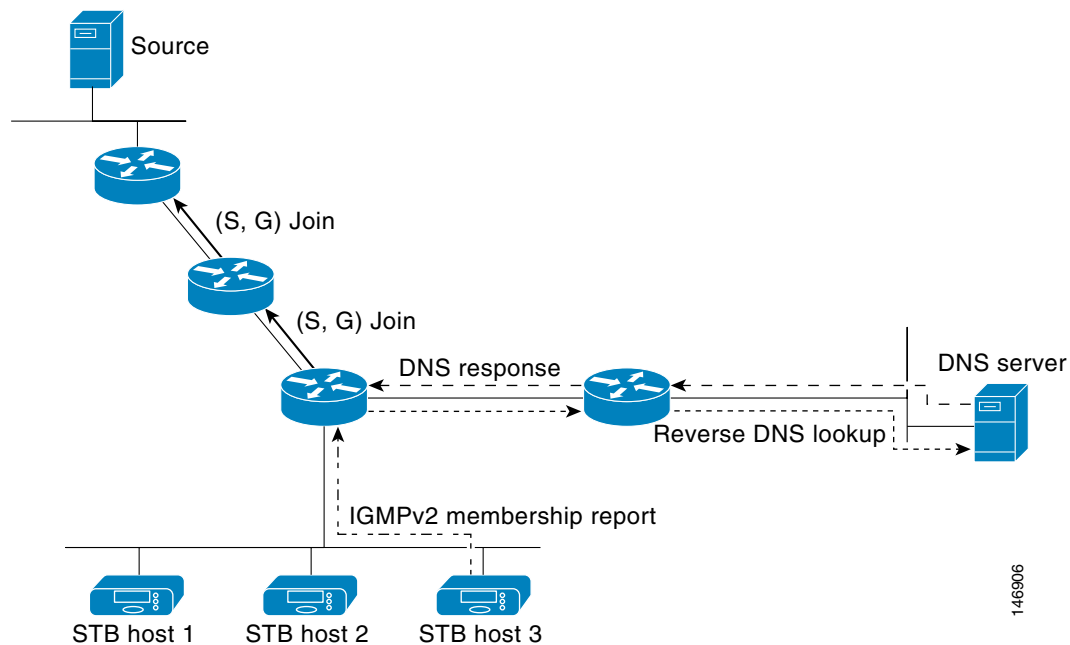
SSM static mapping enables you to configure the last hop router to use a static map to determine the sources sending to groups. Static SSM mapping requires that you configure access lists (ACLs) to define group ranges. The groups permitted by those ACLs then can be mapped to sources using the **ip igmp static ssm-map** command.

You can configure static SSM mapping in smaller networks when a DNS is not needed or to locally override DNS mappings that may be temporarily incorrect. When configured, static SSM mappings take precedence over DNS mappings.

## DNS-Based SSM Mapping

DNS-based SSM mapping enables you to configure the last hop router to perform a reverse DNS lookup to determine sources sending to groups (see [Figure 1](#)). When DNS-based SSM mapping is configured, the router constructs a domain name that includes the group address G and performs a reverse lookup into the DNS. The router looks up IP address resource records (IP A RRs) to be returned for this constructed domain name and uses the returned IP addresses as the source addresses associated with this group. SSM mapping supports up to 20 sources for each group. The router joins all sources configured for a group.

**Figure 1** DNS-Based SSM-Mapping



146906

The SSM mapping mechanism that enables the last hop router to join multiple sources for a group can be used to provide source redundancy for a TV broadcast. In this context, the redundancy is provided by the last hop router using SSM mapping to join two video sources simultaneously for the same TV channel. However, to prevent the last hop router from duplicating the video traffic, it is necessary that the video sources utilize a server-side switchover mechanism where one video source is active while the other backup video source is passive. The passive source waits until an active source failure is detected before sending the video traffic for the TV channel. The server-side switchover mechanism, thus, ensures that only one of the servers is actively sending the video traffic for the TV channel.

To look up one or more source addresses for a group G that includes G1, G2, G3, and G4, the following DNS resource records (RRs) must be configured on the DNS server:

```
G4.G3.G2.G1 [multicast-domain] [timeout] IN A source-address-1
                                     IN A source-address-2
                                     IN A source-address-n
```

The *multicast-domain* argument is a configurable DNS prefix. The default DNS prefix is in-addr.arpa. You should only use the default prefix when your installation is either separate from the internet or if the group names that you map are global scope group addresses (RFC 2770 type addresses that you configure for SSM) that you own.

The *timeout* argument configures the length of time for which the router performing SSM mapping will cache the DNS lookup. This argument is optional and defaults to the timeout of the zone in which this entry is configured. The timeout indicates how long the router will keep the current mapping before querying the DNS server for this group. The timeout is derived from the cache time of the DNS RR entry and can be configured for each group and source entry on the DNS server. You can configure this time for larger values if you want to minimize the number of DNS queries generated by the router. Configure this time for a low value if you want to be able to quickly update all routers with new source addresses.

**Note**

---

Refer to your DNS server documentation for more information about configuring DNS RRs.

---

To configure DNS-based SSM mapping in Cisco IOS software, you must configure a few global configuration commands but no per-channel specific configuration is needed. There is no change to the Cisco IOS configuration for SSM mapping if additional channels are added. When DNS-based SSM mapping is configured, the mappings are handled entirely by one or more DNS servers. All DNS techniques for configuration and redundancy management can be applied to the entries needed for DNS-based SSM mapping.

## SSM Mapping Benefits

- The SSM Mapping feature provides almost the same ease of network installation and management as a pure SSM solution based on IGMPv3. Some additional configuration is necessary to enable SSM mapping.
- The SSM benefit of inhibition of DoS attacks applies when SSM mapping is configured. When SSM mapping is configured the only segment of the network that may still be vulnerable to DoS attacks are receivers on the LAN connected to the last hop router. Since those receivers may still be using IGMPv1 and IGMPv2, they are vulnerable to attacks from unwanted sources on the same LAN. SSM mapping, however, does protect those receivers (and the network path leading towards them) from multicast traffic from unwanted sources anywhere else in the network.

- Address assignment within a network using SSM mapping needs to be coordinated, but it does not need assignment from outside authorities, even if the content from the network is to be transited into other networks.

## How to Configure SSM Mapping

This section contains the following tasks:

- [Configuring Static SSM Mapping, page 8](#) (required)
- [Configuring DNS-Based SSM Mapping, page 10](#) (required)
- [Configuring Static Traffic Forwarding with SSM Mapping, page 12](#) (optional)
- [Verifying SSM Mapping Configuration and Operation, page 13](#) (optional)

## Configuring Static SSM Mapping

Perform this task to configure the last hop router in an SSM deployment to use static SSM mapping to determine the IP addresses of sources sending to groups.

### Prerequisites

- Enable IP multicast routing, enable PIM sparse mode, and configure SSM before performing this task.

For more information, see the “Configuring Basic Multicast” chapter in the “Basic IP Multicast” part of the *IP Multicast Configuration Guide*, Release 12.4 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc\\_c/chap05/mcbbasic.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap05/mcbbasic.htm)

- Before you configure static SSM mapping, you must configure ACLs that define the group ranges to be mapped to source addresses.

For information about how to configure an ACL, see the “Configuring IP Access Lists” chapter in the “IP Access Lists” part of the *IP Application Services Configuration Guide*, Release 12.4 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiap\\_c/ch05/hipaclis.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiap_c/ch05/hipaclis.htm)

### Restrictions

- Enable IGMPv3 with care on the last hop router when you rely solely on SSM mapping as a transition solution for full SSM.

When both SSM mapping and IGMPv3 are enabled, the router will send out IGMPv3 membership query messages instead of IGMPv3 membership messages. If the receiver hosts that are to be supported with SSM mapping can only support IGMPv1 or IGMPv2, then enabling SSM mapping on an interface with IGMPv3 is fine. IGMPv3 reports will be interpreted as IGMPv1 or IGMPv2 queries and the host will continue to report with IGMPv1 or IGMPv2 reports.

However, when both SSM mapping and IGMPv3 are enabled, if the hosts already support IGMPv3 (but not SSM), then they will start to send IGMPv3 group reports. These IGMPv3 group reports are not supported with SSM mapping and the router will not correctly associate sources with these reports.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **no ip igmp ssm-map query dns**
5. **ip igmp ssm-map static** *access-list source-address*
6. Repeat Step 5 to configure additional static SSM mappings, if required.
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip igmp ssm-map enable</b>  <b>Example:</b> Router(config)# ip igmp ssm-map enable	Enables SSM mapping for groups in the configured SSM range. <b>Note</b> By default, this command enables DNS-based SSM mapping.
Step 4	<b>no ip igmp ssm-map query dns</b>  <b>Example:</b> Router(config)# no ip igmp ssm-map query dns	(Optional) Disables DNS-based SSM mapping. <b>Note</b> Disable DNS-based SSM mapping if you only want to rely on static SSM mapping. By default, the <b>ip igmp ssm-map</b> command enables DNS-based SSM mapping.

	Command or Action	Purpose
Step 5	<pre>ip igmp ssm-map static access-list source-address</pre> <p><b>Example:</b>  Router(config)# ip igmp ssm-map static 11 172.16.8.11</p>	<p>Configures static SSM mapping.</p> <ul style="list-style-type: none"> <li>The ACL supplied for the <i>access-list</i> argument defines the groups to be mapped to the source IP address entered for the <i>source-address</i> argument.</li> </ul> <p><b>Note</b> You can configure additional static SSM mappings. If additional SSM mappings are configured and the router receives an IGMPv1 or IGMPv2 membership report for a group in the SSM range, the Cisco IOS software determines the source addresses associated with the group by walking each configured <b>ip igmp ssm-map static</b> command. The Cisco IOS software associates up to 20 sources per group.</p>
Step 6	Repeat Step 5 to configure additional static SSM mappings, if required.	—
Step 7	<pre>end</pre> <p><b>Example:</b>  Router(config)# end</p>	Ends the current configuration session and returns to privileged EXEC mode.

## What to Do Next

Proceed to the “Configuring DNS-Based SSM Mapping” section on page 10 or to the “Verifying SSM Mapping Configuration and Operation” section on page 13.

## Configuring DNS-Based SSM Mapping

Perform this task to configure the last hop router to perform DNS lookups to learn the IP addresses of sources sending to a group.

### Prerequisites

- Enable IP multicast routing, enable PIM sparse mode, and configure SSM before performing this task.

For more information, see the “Configuring Basic Multicast” chapter in the “Basic IP Multicast” part of the *IP Multicast Configuration Guide*, Release 12.4 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc\\_c/chap05/mcbbasic.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/chap05/mcbbasic.htm)

- Before you can configure and use SSM mapping with DNS lookups, you need to be able to add records to a running DNS server. If you do not already have a DNS server running, you need to install one. The Cisco IOS software does not provide for DNS server functionality.

You may want to use a product such as Cisco Network Registrar (CNR). Refer to the following URL for more information about CNR:

<http://www.cisco.com/warp/public/cc/pd/nemnsw/nerr/index.shtml>

## Restrictions

- Enable IGMPv3 with care on the last hop router when you rely solely on SSM mapping as a transition solution for full SSM.

When both SSM mapping and IGMPv3 are enabled, the router will send out IGMPv3 membership query messages instead of IGMPv3 membership messages. If the receiver hosts that are to be supported with SSM mapping can only support IGMPv1 or IGMPv2, then enabling SSM mapping on an interface with IGMPv3 is fine. IGMPv3 reports will be interpreted as IGMP version 1 or IGMP version 2 queries and the host will continue to report with IGMPv1 or IGMPv2 reports.

However, when both SSM mapping and IGMPv3 are enabled, if the hosts already support IGMPv3 (but not SSM), then they will start to send IGMPv3 group reports. These IGMPv3 group reports are not supported with SSM mapping and the router will not correctly associate sources with these reports.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **ip igmp ssm-map query dns**
5. **ip domain multicast** *domain-prefix*
6. **ip name-server** *server-address1* [*server-address2*...*server-address6*]
7. Repeat Step 6 to configure additional DNS servers for redundancy, if required.

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip igmp ssm-map enable</b>  <b>Example:</b> Router(config)# ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
Step 4	<b>ip igmp ssm-map query dns</b>  <b>Example:</b> Router(config)# ip igmp ssm-map query dns	(Optional) Enables DNS-based SSM mapping. <ul style="list-style-type: none"><li>• By default, the <b>ip igmp ssm-map</b> command enables DNS-based SSM mapping. Only the <b>no</b> form of this command is saved to the running configuration.</li></ul> <b>Note</b> Use this command to reenables DNS-based SSM mapping if DNS-based SSM mapping is disabled.

	Command or Action	Purpose
Step 5	<pre>ip domain multicast domain-prefix</pre> <p><b>Example:</b> Router(config)# ip domain multicast ssm-map.cisco.com </p>	(Optional) Changes the domain prefix used by the Cisco IOS software for DNS-based SSM mapping. <ul style="list-style-type: none"> <li>By default, the Cisco IOS software uses the ip-addr.arpa domain prefix.</li> </ul>
Step 6	<pre>ip name-server server-address1 [server-address2...server-address6]</pre> <p><b>Example:</b> Router(config)# ip name-server 10.48.81.21 </p>	Specifies the address of one or more name servers to use for name and address resolution.
Step 7	Repeat Step 6 to configure additional DNS servers for redundancy, if required.	—

## What to Do Next

Proceed to the [“Configuring Static Traffic Forwarding with SSM Mapping”](#) section on page 12 or to the [“Verifying SSM Mapping Configuration and Operation”](#) section on page 13.

## Configuring Static Traffic Forwarding with SSM Mapping

Perform this task to configure static traffic forwarding with SSM mapping on the last hop router. Static traffic forwarding can be used in conjunction with SSM mapping to statically forward SSM traffic for certain groups. When static traffic forwarding with SSM mapping is configured, the last hop router uses DNS-based SSM mapping to determine the sources associated with a group. The resulting (S, G) channels are then statically forwarded.

## Prerequisites

This task does not include the steps for configuring DNS-based SSM mapping. See the [“Configuring DNS-Based SSM Mapping”](#) task for more information about configuring DNS-based SSM mapping.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp static-group** *group source ssm-map*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b> Router(config)# interface ethernet 1/0</p>	<p>Selects an interface on which to statically forward traffic for a multicast group using SSM mapping and enters interface configuration mode.</p> <p><b>Note</b> Static forwarding of traffic with SSM mapping works with either DNS-based SSM mapping or statically-configured SSM mapping.</p>
Step 4	<p><b>ip igmp static-group</b> <i>group-address</i> <b>source</b> <b>ssm-map</b></p> <p><b>Example:</b> Router(config-if)# ip igmp static-group 232.1.2.1 source ssm-map</p>	<p>Configures SSM mapping to be used to statically forward a (S, G) channel out of the interface.</p> <ul style="list-style-type: none"> <li>Use this command if you want to statically forward SSM traffic for certain groups, but you want to use DNS-based SSM mapping to determine the source addresses of the channels.</li> </ul>

## What to Do Next

Proceed to the [“Verifying SSM Mapping Configuration and Operation”](#) section on page 13.

## Verifying SSM Mapping Configuration and Operation

Perform this optional task to verify SSM mapping configuration and operation.

## SUMMARY STEPS

- enable**
- show ip igmp ssm-mapping**
- show ip igmp ssm-mapping** *group-address*
- show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]
- show host**
- debug ip igmp** *group-address*

## DETAILED STEPS

**Step 1 enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

**Step 2 show ip igmp ssm-mapping**

(Optional) Displays information about SSM mapping.

The following example shows how to display information about SSM mapping configuration. In this example, SSM static mapping and DNS-based SSM mapping are enabled.

```
Router# show ip igmp ssm-mapping

SSM Mapping   : Enabled
DNS Lookup    : Enabled
Mcast domain  : ssm-map.cisco.com
Name servers  : 10.0.0.3
               10.0.0.4
```

**Step 3 show ip igmp ssm-mapping group-address**

(Optional) Displays the sources that SSM mapping uses for a particular group.

The following example shows how to display information about the configured DNS-based SSM mapping. In this example, the router has used DNS-based mapping to map group 232.1.1.4 to sources 172.16.8.5 and 172.16.8.6. The timeout for this entry is 860000 milliseconds (860 seconds).

```
Router# show ip igmp ssm-mapping 232.1.1.4

Group address: 232.1.1.4
Database      : DNS
DNS name      : 4.1.1.232.ssm-map.cisco.com
Expire time   : 860000
Source list   : 172.16.8.5
               : 172.16.8.6
```

**Step 4 show ip igmp groups [group-name | group-address | interface-type interface-number] [detail]**

(Optional) Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

The following is sample output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword. In this example the “M” flag indicates that SSM mapping is configured.

```
Router# show ip igmp group 232.1.1.4 detail

Interface:      Ethernet2
Group:          232.1.1.4 SSM
Uptime:         00:03:20
Group mode:     INCLUDE
Last reporter:  0.0.0.0
CSR Grp Exp:   00:02:59
Group source list: (C - Cisco Src Report, U - URD, R - Remote,
                   S - Static, M - SSM Mapping)
Source Address  Uptime   v3 Exp  CSR Exp  Fwd  Flags
172.16.8.3     00:03:20 stopped 00:02:59 Yes  CM
172.16.8.4     00:03:20 stopped 00:02:59 Yes  CM
172.16.8.5     00:03:20 stopped 00:02:59 Yes  CM
172.16.8.6     00:03:20 stopped 00:02:59 Yes  CM
```

**Step 5 show host**

(Optional) Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

The following is sample output from the **show host** command. Use this command to display DNS entries as they are learned by the router.

```
Router# show host

Default domain is cisco.com
Name/address lookup uses domain service
Name servers are 10.48.81.21

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                Port    Flags    Age    Type    Address(es)
10.0.0.0.ssm-map.cisco.c  None  (temp, OK)  0      IP      172.16.8.5
                                     172.16.8.6
                                     172.16.8.3
                                     172.16.8.4
```

#### Step 6 **debug ip igmp group-address**

(Optional) Displays the IGMP packets received and sent and IGMP host-related events.

The following is sample output from the **debug ip igmp** command when SSM static mapping is enabled. The following output indicates that the router is converting an IGMPv2 join for group G into an IGMPv3 join:

```
IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using STATIC.
```

The following is sample output from the **debug ip igmp** command when DNS-based SSM mapping is enabled. The following output indicates that a DNS lookup has succeeded:

```
IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using DNS.
```

The following is sample output from the **debug ip igmp** command when DNS-based SSM mapping is enabled and a DNS lookup has failed:

```
IGMP(0): DNS source lookup failed for (*, 232.1.2.3), IGMPv2 report failed
```

## Configuration Examples for SSM Mapping

This section provides the following configuration examples:

- [SSM Mapping: Example, page 15](#)
- [DNS Server Configuration: Example, page 18](#)

### SSM Mapping: Example

The following configuration example shows a router configuration for SSM mapping. This example also displays a range of other IGMP and SSM configuration options to show compatibility between features. Do not use this configuration example as a model unless you understand all of the features used in the example.

**Note**

Address assignment in the global SSM range 232.0.0.0/8 should be random. If you copy parts or all of this sample configuration, make sure to select a random address range but not 232.1.1.x as shown in this example. Using a random address range minimizes the possibility of address collision and may prevent conflicts when other SSM content is imported while SSM mapping is used.

```

!
no ip domain lookup
ip domain multicast ssm.map.cisco.com
ip name-server 10.48.81.21
!
!
ip multicast-routing
ip igmp ssm-map enable
ip igmp ssm-map static 10 172.16.8.10
ip igmp ssm-map static 11 172.16.8.11
!
!
.
.
.
!
interface Ethernet0/0
  description Sample IGMP Interface Configuration for SSM-Mapping Example
  ip address 10.20.1.2 255.0.0.0
  ip pim sparse-mode
  ip igmp last-member-query-interval 100
  ip igmp static-group 232.1.2.1 source ssm-map
  ip igmp version 3
  ip igmp explicit-tracking
  ip igmp limit 2
  ip igmp v3lite
  ip urd
!
.
.
.
!
ip pim ssm default
!
access-list 10 permit 232.1.2.10
access-list 11 permit 232.1.2.0 0.0.0.255
!

```

[Table 1](#) describes the significant commands shown in the SSM mapping configuration example.

**Table 1** SSM Mapping Configuration Example Command Descriptions

Command	Description
<b>no ip domain lookup</b>	Disables IP DNS-based hostname-to-address translation. <b>Note</b> The <b>no ip domain-list</b> command is shown in the configuration only to demonstrate that disabling IP DNS-based hostname-to-address translation does not conflict with configuring SSM mapping. If this command is enabled, the Cisco IOS software will try to resolve unknown strings as hostnames.
<b>ip domain multicast ssm-map.cisco.com</b>	Specifies ssm-map.cisco.com as the domain prefix for SSM mapping.
<b>ip name-server 10.48.81.21</b>	Specifies 10.48.81.21 as the IP address of the DNS server to be used by SSM mapping and any other service in the Cisco IOS software that utilizes DNS.
<b>ip multicast-routing</b>	Enables IP multicast routing.
<b>ip igmp ssm-map enable</b>	Enables SSM mapping.
<b>ip igmp ssm-map static 10 172.16.8.10</b>	Configures the groups permitted by ACL 10 to use source address 172.16.8.10. <ul style="list-style-type: none"> <li>In this example, ACL 10 permits all groups in the 232.1.2.0/25 range except 232.1.2.10.</li> </ul>
<b>ip igmp ssm-map static 11 172.16.8.11</b>	Configures the groups permitted by ACL 11 to use source address 172.16.8.11. <ul style="list-style-type: none"> <li>In this example, ACL 11 permits group 232.1.2.10.</li> </ul>
<b>ip pim sparse-mode</b>	Enables PIM sparse mode.
<b>ip igmp last-member-query-interval 100</b>	Reduces the leave latency for IGMPv2 hosts. <b>Note</b> This command is not required for configuring SSM mapping; however, configuring this command can be beneficial for IGMPv2 hosts relying on SSM mapping.
<b>ip igmp static-group 232.1.2.1 source ssm-map</b>	Configures SSM mapping to be used to determine the sources associated with group 232.1.2.1. The resulting (S, G) channels are statically forwarded.
<b>ip igmp version 3</b>	Enables IGMPv3 on this interface. <b>Note</b> This command is shown in the configuration only to demonstrate that IGMPv3 can be configured simultaneously with SSM mapping; however, it is not required.
<b>ip igmp explicit-tracking</b>	Minimizes the leave latency for IGMPv3 host leaving a multicast channel. <b>Note</b> This command is not required for configuring SSM mapping.

Table 1 SSM Mapping Configuration Example Command Descriptions (continued)

Command	Description
<b>ip igmp limit 2</b>	Limits the number of IGMP states resulting from IGMP membership states on a per-interface basis. <b>Note</b> This command is not required for configuring SSM mapping.
<b>ip igmp v3lite</b>	Enables the acceptance and processing of IGMP v3lite membership reports on this interface. <b>Note</b> This command is shown in the configuration only to demonstrate that IGMP v3lite can be configured simultaneously with SSM mapping; however, it is not required.
<b>ip urd</b>	Enables interception of TCP packets sent to the reserved URD port 465 on an interface and processing of URD channel subscription reports. <b>Note</b> This command is shown in the configuration only to demonstrate that URD can be configured simultaneously with SSM mapping; however, it is not required.
<b>ip pim ssm default</b>	Configures SSM service. <ul style="list-style-type: none"> <li>The <b>default</b> keyword defines the SSM range access list as 232/8.</li> </ul>
<b>access-list 10 permit 232.1.2.10</b> <b>access-list 11 permit 232.1.2.0 0.0.0.255</b>	Configures the ACLs to be used for static SSM mapping. <b>Note</b> These are the ACLs that are referenced by the <b>ip igmp ssm-map static</b> commands in this configuration example.

## DNS Server Configuration: Example

To configure DNS-based SSM mapping, you need to create a DNS server zone or add records to an existing zone. If the routers that are using DNS-based SSM mapping are also using DNS for other purposes besides SSM mapping, you should use a normally-configured DNS server. If DNS-based SSM mapping is the only DNS implementation being used on the router, you can configure a fake DNS setup with an empty root zone, or a root zone that points back to itself.

The following example shows how to create a zone and import the zone data using Network Registrar:

```
nrcmd> zone 1.1.232.ssm-map.cisco.com. create primary file=named.ssm-map
100 Ok
nrcmd> dns reload
100 Ok
```

The following example shows how to import the zone files from a named.conf file for BIND 8:

```
nrcmd> ::import named.conf /etc/named.conf
nrcmd> dns reload
100 Ok:
```

**Note**

Network Registrar version 8.0 and later support import BIND 8 format definitions.

## Where to Go Next

If you want to configure additional IP multicast features, see the *Cisco IOS IP Multicast Configuration Guide*, Release 12.4.

If you want to configure Network Registrar as a DNS server, see the *Cisco CNS Network Registrar* documentation.

## Additional References

The following sections provide additional references related to the SSM Mapping feature.

## Related Documents

Related Topic	Document Title
SSM concepts and configuration	“ <a href="#">Configuring Basic IP Multicast</a> ” in the <i>Cisco IOS IP Multicast Configuration Guide</i> , Release 12.4
Cisco IOS IP multicast commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	<i>Cisco IOS IP Multicast Command Reference</i> , Release 12.4
IGMP v3lite and URD concepts and configuration	“ <a href="#">Configuring Source Specific Multicast</a> ” chapter in the “IP Multicast” part of the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2
Cisco Network Registrar documentation	<i>Cisco CNS Network Registrar</i>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS 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>

## RFCs

RFCs	Title
RFC 2365	<i>Administratively Scoped IP Multicast</i>
RFC 2770	<i>GLOP Addressing in 233/8</i>
RFC 3569	<i>An Overview of Source-Specific Multicast</i>

## Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This section documents modified commands only.

- [debug ip igmp](#)
- [ip domain multicast](#)
- [ip igmp ssm-map enable](#)
- [ip igmp ssm-map query dns](#)
- [ip igmp ssm-map static](#)
- [ip igmp static-group](#)
- [show ip igmp groups](#)
- [show ip igmp ssm-mapping](#)

# debug ip igmp

To display Internet Group Management Protocol (IGMP) packets received and sent, and IGMP-host related events, use the **debug ip igmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip igmp [vrf vrf-name] [group-address]
```

```
no debug ip igmp [vrf vrf-name] [group-address]
```

## Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>group-address</i>	(Optional) Address of a particular group about which to display IGMP information.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
10.2	This command was introduced.
12.1(3)T	Fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	Fields were added to the output of this command to support the SSM Mapping feature. The <i>group-address</i> attribute was added.
12.2(18)SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

## Usage Guidelines

This command helps discover whether the IGMP processes are functioning. In general, if IGMP is not working, the router process never discovers that another host is on the network that is configured to receive multicast packets. In dense mode, this situation will result in packets being delivered intermittently (a few every 3 minutes). In sparse mode, packets will never be delivered.

Use this command in conjunction with the **debug ip pim** and **debug ip mrouting** commands to observe additional multicast activity and to learn the status of the multicast routing process, or why packets are forwarded out of particular interfaces.

When SSM mapping is enabled, a debug message is displayed to indicate that the router is converting an IGMP version 2 report from the group (G) into an IGMP version 3 join. After SSM mapping has generated the appropriate IGMP version 3 report, any debug output that follows is seen as if the router had received the same IGMP version 3 report directly.

**Examples**

The following is sample output from the **debug ip igmp** command:

```
Router# debug ip igmp

IGMP: Received Host-Query from 172.16.37.33 (Ethernet1)
IGMP: Received Host-Report from 172.16.37.192 (Ethernet1) for 224.0.255.1
IGMP: Received Host-Report from 172.16.37.57 (Ethernet1) for 224.2.127.255
IGMP: Received Host-Report from 172.16.37.33 (Ethernet1) for 225.2.2.2
```

The messages displayed by the **debug ip igmp** command show query and report activity received from other routers and multicast group addresses.

The following is sample output from the **debug ip igmp** command when SSM is enabled. Because IGMP version 3 lite (IGMPv3lite) requires the host to send IGMP version 2 (IGMPv2) packets, IGMPv2 host reports also will be displayed in response to the router IGMPv2 queries. If SSM is disabled, the word “ignored” will be displayed in the **debug ip igmp** command output.

```
IGMP:Received v3-lite Report from 10.0.119.142 (Ethernet3/3), group count 1
IGMP:Received v3 Group Record from 10.0.119.142 (Ethernet3/3) for 232.10.10.10
IGMP:Update source 224.1.1.1
IGMP:Send v2 Query on Ethernet3/3 to 224.0.0.1
IGMP:Received v2 Report from 10.0.119.142 (Ethernet3/3) for 232.10.10.10
IGMP:Update source 224.1.1.1
```

The following is sample output from the **debug ip igmp** command when SSM static mapping is enabled. The following output indicates that the router is converting an IGMP version 2 join for group (G) into an IGMP version 3 join:

```
IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using STATIC.
```

The following is sample output from the **debug ip igmp** command when SSM DNS-based mapping is enabled. The following output indicates that a DNS lookup has succeeded:

```
IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using DNS.
```

The following is sample output from the **debug ip igmp** command when SSM DNS-based mapping is enabled and a DNS lookup has failed:

```
IGMP(0): DNS source lookup failed for (*, 232.1.2.3), IGMPv2 report failed
```

**Related Commands**

Command	Description
<b>debug ip mrm</b>	Displays MRM control packet activity.
<b>debug ip mrouting</b>	Displays changes to the mroute table.
<b>debug ip pim</b>	Displays PIM packets received and sent and PIM-related events.

# ip domain multicast

To change the domain prefix used by the Cisco IOS software for Domain Name Service (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip domain multicast** command in global configuration mode. To revert to the default domain prefix, use the **no** form of this command.

```
ip domain multicast [vrf vrf-name] domain-prefix
```

```
no domain multicast [vrf vrf-name] domain-prefix
```

## Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>domain-prefix</i>	Name of the domain prefix to be used for DNS-based SSM mapping. The default is in-addr.arpa.

## Defaults

*domain-prefix*: in-addr.arpa

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

## Usage Guidelines

Use this command to change the domain prefix used by Cisco IOS software when DNS-based SSM mapping is configured. When a router attempts DNS-based SSM mapping for an IP group address (G = G1.G2.G3.G4), the router queries the domain name server for IP address resource records ("IP A" RRs) for the domain G4.G3.G2.G1 *domain-prefix*.

Use the **vrf** *vrf-name* keyword and argument to enable SSM mapping for a particular VRF.

## Examples

The following example shows how to change the domain prefix used for DNS-based SSM mapping to ssm-map.cisco.com:

```
ip domain multicast ssm-map.cisco.com
```

The following example shows how to change the domain prefix used for DNS-based SSM mapping to ssm-map.cisco.com or a VRF named vrf1:

```
ip domain multicast vrf vrf1 ssm-map.cisco.com
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip igmp ssm-map enable</b>	Enables SSM mapping for groups in a configured SSM range.
<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.

# ip igmp ssm-map enable

To enable Source Specific Multicast (SSM) mapping for groups in a configured SSM range, use the **ip igmp ssm-map enable** command in global configuration mode. To disable SSM mapping, use the **no** form of this command.

**ip igmp [vrf *vrf-name*] ssm-map enable**

**no ip igmp [vrf *vrf-name*] ssm-map enable**

## Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<b><i>vrf-name</i></b>	(Optional) Name assigned to the VRF.

## Defaults

This command is disabled by default. If this command is enabled, Domain Name System (DNS)-based SSM mapping is the default.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

## Usage Guidelines

Use this command to enable SSM mapping for groups in the configured SSM range. SSM mapping is applied only to received Internet Group Management Protocol (IGMP) version 1 or IGMP version 2 membership reports.

SSM mapping is compatible with URL Rendezvous Directory (URD) and IGMPv3 lite. SSM mapping is needed only in the router connecting to the receivers. No support is needed in any other routers in the network. SSM mapping can be configured only globally and cannot be configured per interface.

Use the **vrf *vrf-name*** keyword and argument to enable SSM mapping for a particular VRF.

## Examples

The following example shows how to enable SSM mapping:

```
ip igmp ssm-map enable
```

The following example shows how to enable SSM mapping for the VRF named vrf1:

```
ip igmp vrf vrf1 ssm-map enable
```

■ ip igmp ssm-map enable

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip domain multicast</b>	Changes the domain prefix used by Cisco IOS software for DNS-based SSM mapping.
	<b>ip igmp ssm-map query dns</b>	Configures DNS-based SSM mapping.
	<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.
	<b>ip pim ssm</b>	Defines the SSM range of IP multicast addresses.

## ip igmp ssm-map query dns

To configure Domain Name System (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip igmp ssm-map query dns** command in global configuration mode. To disable DNS-based SSM mapping, use the **no** form of this command.

**ip igmp [vrf *vrf-name*] ssm-map query dns**

**no ip igmp [vrf *vrf-name*] ssm-map query dns**

### Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<b><i>vrf-name</i></b>	(Optional) Name assigned to the VRF.

### Defaults

This command is enabled by default when the **ip igmp ssm-map enable** command is enabled.

### Command Modes

Global configuration

### Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

### Usage Guidelines

Use this command to enable DNS-based SSM mapping. Disable DNS-based SSM mapping if you want to rely only on statically configured SSM mapping. By default, the router will use both DNS-based SSM mapping and statically configured SSM mapping. If DNS-based SSM mapping is not explicitly disabled, the router will first try to find any statically mapped sources for the group and, if it does not find any, will use DNS-based SSM mapping.

This command is enabled by default when the **ip igmp ssm-map enable** command is configured. Use the **no ip igmp ssm-map query dns** command to disable DNS-based SSM mapping. When DNS-based SSM mapping is disabled, SSM mapping is performed only on SSM sources mapped by the **ip igmp ssm-map static** command.

To configure DNS-based SSM mapping, the router needs to find at least one correctly configured DNS server. The router can discover the DNS server by configuring the **ip name-server** global configuration command or by being directly connected to the DNS server.



#### Note

It is recommended to always configure the IP addresses of the DNS servers with the **ip name-server** command to prevent the router from sending each DNS query broadcast to all connected interfaces.

Only the **no** form of this command is saved to the running configuration.

Use the **vrf** *vrf-name* keyword and argument to enable DNS-based SSM mapping for a particular VRF.

---

**Examples**

The following example shows how to configure DNS-based SSM mapping:

```
ip name-server 10.0.0.0
ip igmp ssm-map enable
ip igmp ssm-map query dns
```

The following example shows how to configure DNS-based SSM mapping for a VRF named vrf1:

```
ip name-server 10.0.0.0
ip igmp ssm-map enable
ip igmp vrf vrf1 ssm-map query dns
```

---

**Related Commands**

Command	Description
<b>ip domain multicast</b>	Changes the domain prefix used by Cisco IOS software for DNS-based SSM mapping.
<b>ip igmp ssm-map enable</b>	Enables SSM mapping for groups in a configured SSM range.
<b>ip igmp ssm-map static</b>	Enables static SSM mapping.
<b>ip igmp static-group</b>	Configures the router to be a statically connected member of the specified group on the interface.
<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.

# ip igmp ssm-map static

To enable static Source Specific Multicast (SSM) mappings, use the **ip igmp ssm-map static** command in global configuration mode. To disable a static SSM mapping, use the **no** form of this command.

```
ip igmp ssm-map [vrf vrf-name] static access-list source-address
```

```
no ip igmp ssm-map [vrf vrf-name] static access-list source-address
```

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies that the static SSM mapping be applied to the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
<i>access-list</i>	Access list (ACL) to apply to the static SSM mapping.
<i>source-address</i>	Source address to use for the groups defined in the ACL specified for the <i>access-list</i> argument.

## Command Modes

No static SSM mappings are configured.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

## Usage Guidelines

Use the **ip igmp ssm-map static** command to configure static SSM mappings. Before configuring static SSM mappings, you must first globally enable SSM mapping with the **ip igmp ssm-map enable** command. When static SSM mappings are configured and the router receives an Internet Group Management Protocol (IGMP) membership report for a group G in the configured SSM range, the router tries to determine the source address or addresses associated with the group G by walking the configured **ip igmp ssm-map static** commands. If the group G matches the ACL in a configured static SSM mapping, then the source address (specified for the *source-address* argument in the **ip igmp ssm-map static** command) associated with the SSM mapping is statically mapped to the group G. If multiple static SSM mappings are configured, and a group G is permitted by multiple ACLs, the source addresses associated with all matching ACLs in configured SSM mappings are used (that is, the group G is statically mapped to those sources). The maximum number of configured static SSM mappings for each group is 20.

When both static SSM mappings and Domain Name System (DNS) SSM mappings are configured, static SSM mappings take precedence over the DNS mappings. If a router receives an IGMP membership report for a group G that does not match any of ACLs configured in static SSM mappings, the router then will revert to querying the DNS for the address mapping.

Use the **vrf** *vrf-name* keyword and argument to configure SSM static mapping for a particular MVRF.

### Examples

The following example shows how to enable static SSM mapping. In this example, the router is configured to statically map groups that match ACL 11 to source address 172.16.8.11 and to statically map groups that match ACL 10 to source address 172.16.8.10.

```
ip igmp ssm-map enable
ip igmp ssm-map static 11 172.16.8.11
ip igmp ssm-map static 10 172.16.8.10
```

The following example shows how to enable static SSM mapping for an MVRF. In this example, the router is configured to statically maps groups within the MVRF named test that match ACL 12 to source address 172.16.8.12.

```
ip igmp ssm-map enable
ip igmp ssm-map vrf test static 12 172.16.8.12
```

### Related Commands

Command	Description
<b>ip igmp ssm-map enable</b>	Enables SSM mapping for groups in a configured SSM range.
<b>ip igmp ssm-map query dns</b>	Configures DNS-based SSM mapping.
<b>ip igmp static-group</b>	Configures the router to be a statically connected member of the specified group on the interface, or to statically forward for a multicast group onto the interface.
<b>ip pim ssm</b>	Defines the SSM range of IP multicast addresses.

## ip igmp static-group

To configure the router to be a statically connected member of the specified group on the interface, or to statically forward for a multicast group onto the interface, use the **ip igmp static-group** command in interface configuration mode. To remove the router as a member of the group, use the **no** form of this command.

```
ip igmp static-group [* | group-address [source { source-address | ssm-map }]]
```

```
no ip igmp static-group [* | group-address [source { source-address | ssm-map }]]
```

### Syntax Description

<b>*</b>	Places the interface into all newly created multicast route (mroute) entries.
<i>group-address</i>	IP multicast group address of a group to which the router belongs.
<b>source</b>	(Optional) Statically forwards a (S, G) channel out of the interface.
<i>source-address</i>	(Optional) IP address of a system where multicast data packets originate.
<b>ssm-map</b>	(Optional) Configures Source Specific Multicast (SSM) mapping to be used to determine the source associated with this group. The resulting (S, G) channels are statically forwarded.

### Defaults

A router is not a statically connected member of an IP multicast group.

### Command Modes

Interface configuration

### Command History

Release	Modification
11.2	This command was introduced.
12.3(2)T	The <b>ssm-map</b> keyword was added.
12.2(18)S	The <b>ssm-map</b> keyword was added.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

### Usage Guidelines

When you configure the **ip igmp static-group** command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface.

Configuring the **ip igmp static-group** command is unlike configuring the **ip igmp join-group** command, which allows the router to join the multicast group. This configuration of the **ip igmp static-group** command would cause the upstream routers to maintain the multicast routing table information for that group, which would ensure that all the paths to that multicast group are active.

If you configure the **ip igmp join-group** command for the same group address as the **ip igmp static-group** command, the **ip igmp join-group** command takes precedence, and the group behaves like a locally joined group.

The use of SSM mapping determines the source or sources associated with a specific source S and group G combination and puts the particular interface in the outgoing interface list (OIL) for that (S, G) entry. Traffic coming from source S destined toward group G will be forwarded out that interface regardless of a receiver joining the group on that interface.

---

**Examples**

The following example shows how to configure group address 239.100.100.101 on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.100.100.101
```

The following example shows how to configure group address 239.1.2.1 to use SSM mapping for statically forwarded groups on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.1.2.1 source ssm-map
```

---

**Related Commands**

Command	Description
<b>ip igmp join-group</b>	Causes the router to join a multicast group.
<b>ip igmp ssm-map enable</b>	Enables SSM mapping for groups in a configured SSM range.
<b>ip igmp ssm-map query dns</b>	Configures DNS-based SSM mapping.
<b>ip igmp ssm-map static</b>	Enables static SSM mapping.
<b>ip pim ssm</b>	Defines the SSM range of IP multicast addresses.

# show ip igmp groups

To display the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show ip igmp groups** command in user EXEC or privileged EXEC mode.

```
show ip igmp [vrf vrf-name] groups [group-name | group-address | interface-type
interface-number] [detail]
```

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance and indicates the name assigned to the VRF.
<i>group-name</i>	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table.
<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted-decimal notation.
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and Interface number.
<b>detail</b>	(Optional) Provides a detailed description of the sources known through IGMP Version 3 (IGMPv3), IGMPv3lite, or URL Rendezvous Directory (URD).

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	Fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.
12.1(5)T	The <b>detail</b> keyword was added.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	A field was added to the output of this command to support the SSM mapping feature.
12.2(18)S	A field was added to the output of this command to support the SSM mapping feature.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

## Usage Guidelines

If you omit all optional arguments and keywords, the **show ip igmp groups** command displays by group address, interface type, and interface number all directly connected multicast groups.

**Examples**

The following is sample output from the **show ip igmp groups** command:

```
Router# show ip igmp groups
```

```
IGMP Connected Group Membership
Group Address      Interface          Uptime           Expires          Last Reporter
239.255.255.254   Ethernet3/1       1w0d            00:02:19        172.21.200.159
224.0.1.40        Ethernet3/1       1w0d            00:02:15        172.21.200.1
224.0.1.40        Ethernet3/3       1w0d            never           172.16.214.251
224.0.1.1         Ethernet3/1       1w0d            00:02:11        172.21.200.11
224.9.9.2         Ethernet3/1       1w0d            00:02:10        172.21.200.155
232.1.1.1         Ethernet3/1       5d21h          stopped         172.21.200.206
```

The following is sample output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword:

```
Router# show ip igmp groups 192.168.1.1 detail
```

```
Interface:      Ethernet3/2
Group:          192.168.1.1
Uptime:        01:58:28
Group mode:    INCLUDE
Last reporter: 10.0.119.133
CSR Grp Exp:   00:02:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote
                   S- Static, M - SSM Mapping)
  Source Address  Uptime   v3 Exp   CSR Exp   Fwd  Flags
  172.16.214.1   01:58:28 stopped  00:02:31 Yes   C
```

[Table 2](#) describes the significant fields shown in the displays.

**Table 2** *show ip igmp groups Field Descriptions*

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	Time in weeks, days, hours, minutes, and seconds that this multicast group has been known.
Expires	Time in weeks, days, hours, minutes, and seconds until the entry expires. If an entry expires, then the entry (for a short period) shows “now” before it is removed.  “never” indicates that the entry will not time out, because a local receiver is on this router for this entry.  “stopped” indicates that timing out of this entry is not determined by this expire timer. If the router is in INCLUDE mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to EXCLUDE mode before it times out).
Last Reporter	Last host to report being a member of the multicast group. Both IGMP v3lite and URD require a v2-report.
Group mode:	Either INCLUDE or EXCLUDE. The group mode is based on the type of membership reports that are received on the interface for the group. In the output for the <b>show ip igmp groups detail</b> command, the EXCLUDE mode also shows the Expires: field for the group entry (not shown in the output).

**Table 2** *show ip igmp groups Field Descriptions (continued)*

Field	Description
CSR Grp Exp	Shown for multicast groups in the SSM range. It indicates the time (in hours, minutes, and seconds) since the last received group membership report was received. Cisco IOS software needs to use these reports for the operation of URD and IGMP v3lite, but they do not indicate group membership by themselves.
Group source list:	Details of which sources have been requested by the multicast group.
Source Address	IP address of the source.
Uptime	Time since the source state was created.
v3 Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP operations. “stopped” displays if no member uses IGMPv3 (but only IGMP v3lite or URD).
CSR Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP v3lite or URD reports. “stopped” displays if members use only IGMPv3.
Fwd	Status of whether the router is forwarding multicast traffic due to this entry.
Flags	Information about the entry. The Remote flag indicates that an IGMPv3 report has been received by this source. The C flag indicates that an IGMP v3lite or URD report was received by this source. The U flag indicates that a URD report was received for this source.

**Related Commands**

Command	Description
<b>ip igmp query-interval</b>	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.
<b>ip igmp ssm-map enable</b>	Enables SSM mapping for groups in a configured SSM range.
<b>show ip igmp ssm-mapping</b>	Displays information about SSM mapping or displays the sources that SSM mapping uses for a particular group.

# show ip igmp ssm-mapping

To display information about Source Specific Multicast (SSM) mapping or to display the sources that SSM mapping uses for a particular group, use the **show ip igmp ssm-mapping** command in user EXEC or privileged EXEC mode.

```
show ip igmp [vrf vrf-name] ssm-mapping [group-address]
```

## Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>group-address</i>	(Optional) Address of the group about which to display SSM mapping information.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

## Usage Guidelines

Use this command to display the sources that SSM mapping is using for a particular group, or would use for a group if SSM mapping were configured. If no SSM mapping is known for the specified group, and Domain Name System (DNS)-based SSM mapping is enabled, this command sends out a DNS query for the group. The DNS query initiates DNS-based SSM mapping for this group. If no SSM mapping group is specified by the *group-address* argument, this command displays the configured SSM mapping state.

Use the **vrf** *vrf-name* keyword and argument to displays SSM mapping information for a particular VRF.

## Examples

The following example shows how to display information about the configured SSM mapping state:

```
Router# show ip igmp ssm-mapping

SSM Mapping : Enabled
DNS Lookup  : Enabled
Mcast domain : ssm-map.cisco.com
Name servers : 10.0.0.0
              10.0.0.1
```

Table 3 describes the significant fields shown in the display.

**Table 3** *show ip igmp ssm-mapping Field Descriptions*

Field	Description
SSM Mapping : Enabled	The SSM Mapping feature is enabled.
DNS Lookup : Enabled	DNS-based SSM mapping is enabled.
Mcast domain : ssm-map.cisco.com	Multicast domain.
Name servers : 10.0.0.0 10.0.0.1	Addresses of the configured named servers.

The following example shows how to display information about the configured DNS-based SSM mapping:

```
Router# show ip igmp ssm-mapping 232.1.1.4

Group address: 232.1.1.4
Database      : DNS
DNS name     : 4.1.1.232.ssm-map.cisco.com
Expire time  : 860000
Source list  : 172.16.8.5
              :172.16.8.6
```

Table 4 describes the significant fields shown in the display.

**Table 4** *show ip igmp ssm-mapping Field Descriptions*

Field	Description
Group address: 232.1.1.4	The router has mapped group 232.1.1.4.
Database : DNS	Group mapping is performed via DNS.
DNS name : 4.1.1.232.ssm-map.cisco.com	Name of the DNS that performs group mapping.
Expire time : 860000	Cache time of the DNS registration record on the DNS server, in milliseconds.
Source list : 172.16.8.5 :172.16.8.6	The group address is mapped via DNS to these source addresses.

The following example shows how to display information about the configured static SSM mapping:

```
Router# show ip igmp ssm-mapping 232.1.1.4

Group address: 232.1.1.4
Database      : Static
Source list   : 172.16.8.5
              : 172.16.8.6
```

Table 5 describes the significant fields shown in the display.

**Table 5** *show ip igmp ssm-mapping Field Descriptions*

Field	Description
Group address: 232.1.1.4	The address of the group with SSM mapping to the router.
Database : Static	Static SSM mapping is configured.
Source list : 172.16.8.5 : 172.16.8.6	Source addresses configured for static SSM mapping.

The following is sample output from the **show ip igmp ssm-mapping** command when no SSM mappings can be found:

```
Router# show ip igmp ssm-mapping 232.1.1.4
```

```
Can't resolve %i to source-mapping
```

#### Related Commands

Command	Description
<b>ip igmp ssm-map enable</b>	Enables SSM mapping for groups in a configured SSM range.
<b>show ip igmp group</b>	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

# Glossary

**DNS**—Domain Name System. System used on the Internet for translating names of network nodes into addresses.

**IGMP**—Internet Group Management Protocol. Protocol used by IP hosts to report their multicast group memberships to an adjacent multicast router.

**IGMPv3**—IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. Version 3 of IGMP adds support for source filtering, that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.

**PIM**—Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: dense and sparse.

**SSM**—Source Specific Multicast. A datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the Cisco implementation of the IP Multicast Lite suite of solutions targeted for audio and video broadcast application environments

**URD**—URL Rendezvous Directory. Multicast solution that directly provides the network with information about the specific source of a content stream. It enables the network to quickly establish the most direct distribution path from the source to the receiver, thus substantially reducing the time and effort required in receiving the streaming media. URD allows an application to identify the source of the content stream through a web page link or web directly. When that information is sent back to the application it is then conveyed back to the network using URD.

**VRF**—A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)  
partnership relationship between Cisco and any other company. (0711R)

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

© 2003, 2005–2006 Cisco Systems, Inc. All rights reserved.

