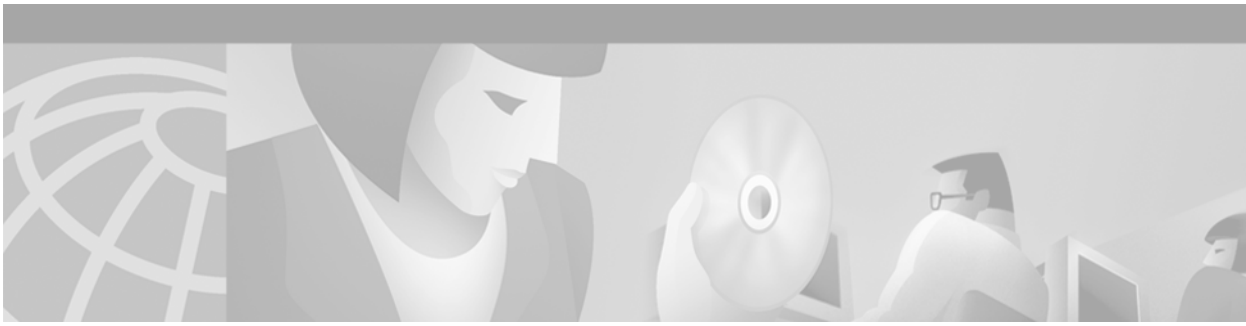

Source Specific Multicast with IGMPv3, IGMP v3lite, and URD

This feature module describes the Source Specific Multicast feature and includes the following sections:

Feature Overview

The Source Specific Multicast feature is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.

SSM Components Overview

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. This feature module discusses the following Cisco IOS components that support the implementation of SSM:

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

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

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. Version 3 of this protocol supports source filtering, which is required for SSM. To run SSM with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself. IGMP v3lite and URD are two Cisco-developed 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. 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. URD is a solution for content providers and content aggregators that enables them to deploy receiver applications that are not yet SSM enabled (through support for IGMPv3). IGMPv3, IGMP v3lite, and URD interoperate with each other, so that both IGMP v3lite and URD can easily be used as transitional solutions toward full IGMPv3 support in hosts.

How SSM Differs from Internet Standard Multicast

The current 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 proven 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 address(es) relayed to the last hop routers by IGMPv3, IGMP v3lite, or URD. 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 a more advantageous 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 to a host group simply requires signalling 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 signalling 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 signalling utilizes IGMP INCLUDE mode membership reports, which are supported only in Version 3 of IGMP.

SSM IP Address Range

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 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. Cisco IOS software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0

through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications will not receive any traffic when they try to use addresses in the SSM range (unless the application is modified to use explicit (S, G) channel subscription or is SSM enabled through 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 (for example, MSDP, Auto-RP, or bootstrap router [BSR]) if only SSM service is needed.

If SSM is deployed in a network already configured for PIM-SM (Cisco IOS Release 12.0 or later releases is recommended), then only the last hop routers must be upgraded to a Cisco IOS Release 12.0(15)S or later release image that supports SSM. Routers that are not directly connected to receivers can run Cisco IOS Release 12.0 or later releases. In general, these nonlast hop routers must only run PIM-SM in the SSM range, and may need additional access control configuration to suppress MSDP signalling, registering, or PIM-SM shared tree operations from occurring within the SSM range.

In Cisco IOS Release 12.0(15)S and later releases, the SSM mode of operation is enabled by configuring the SSM range through the **ip pim ssm** 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, IGMP v3lite, or URD (each of these methods must be configured on a per-interface basis). IGMP v3lite and URD (S, G) channel subscriptions are ignored for groups outside the SSM range.

  Both IGMP v3lite and URD are based on utilizing existing application IGMP group membership and extending it with their respective (S, G) channel subscription mechanism, which is ignored by Cisco IOS software outside the SSM range of addresses. Within the SSM range, IGMP Version 1 (IGMPv1) or Version 2 (IGMPv2) group membership reports or IGMPv3 EXCLUDE mode membership reports are acted upon only in conjunction with an (S, G) specific membership report from URD or IGMP v3lite.
- 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 router, and no (S, G) rendezvous point tree (RPT) or (*, G) RPT messages are generated. Incoming messages related to 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 router is a last hop router. Therefore, routers that are not last hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- No MSDP Source-Active (SA) messages within the SSM range will be accepted, generated, or forwarded.

IGMPv3 Host Signalling

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

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

IGMPv3 is described in more detail in the Cisco IOS Release 12.0(15)S *IGMP Version 3* feature module.

IGMP v3lite Host Signalling

IGMP v3lite is a Cisco-developed transitional solution for application developers to immediately start programming SSM applications. It allows you to write and run SSM applications on hosts that do not yet support IGMPv3 in their operating system kernel.

Applications must be compiled with the Host Side IGMP Library (HSIL) for IGMP v3lite. This software provides applications with a subset of the IGMPv3 applications programming interface (API) that is required to write SSM applications. HSIL was developed for Cisco by Talarian and is available from the following web page:

http://www.talarianmulticast.com/cgi-bin/igmpdownld

One part of the HSIL is a client library linked to the SSM application. It provides the SSM subset of the IGMPv3 API to the SSM application. If possible, the library checks whether the operating system kernel supports IGMPv3. If it does, then the API calls simply are passed through to the kernel. If the kernel does not support IGMPv3, then the library uses the IGMP v3lite mechanism.

When using the IGMP v3lite mechanism, the library tells the operating system kernel to join to the whole multicast group, because joining to the whole group is the only method for the application to receive traffic for that multicast group (if the operating system kernel only supports IGMPv1 or IGMPv2). In addition, the library signals the (S, G) channel subscriptions to an IGMP v3lite server process, which is also part of the HSIL. A server process is needed because multiple SSM applications may be on the same host. This server process will then send IGMP v3lite-specific (S, G) channel subscriptions to the last hop Cisco IOS router, which needs to be enabled for IGMP v3lite. This Cisco IOS router will then see both the IGMPv1 or IGMPv2 group membership report from the operating system kernel and the (S, G) channel subscription from the HSIL daemon. If the router sees both of these messages, it will interpret them as an SSM (S, G) channel subscription and join to the channel through PIM-SSM. We recommend referring to the documentation accompanying the HSIL software for further information on how to utilize IGMP v3lite with your application.

IGMP v3lite is supported by Cisco only through the API provided by the HSIL, not as a function of the router independent of the HSIL. By default, IGMP v3lite is disabled. When IGMP v3lite is configured through the **ip igmp v3lite** command on an interface, it will be active only for IP multicast addresses in the SSM range.

URD Host Signalling

URD is a Cisco-developed transitional solution that allows existing IP multicast receiver applications to be used with SSM without the need to modify the application and change or add any software on the receiver host running the application. URD is a content provider solution in which the receiver applications can be started or controlled through a web browser.

URD operates by passing a special URL from the web browser to the last hop router. This URL is called a URD intercept URL. A URD intercept URL is encoded with the (S, G) channel subscription and has a format that allows the last hop router to easily intercept it.

As soon as the last hop router intercepts both an (S, G) channel subscription encoded in a URD intercept URL and sees an IGMP group membership report for the same multicast group from the receiver application, the last hop router will use PIM-SSM to join toward the (S, G) channel as long as the application maintains the membership for the multicast group G. The URD intercept URL is thus only needed initially to provide the last hop router with the address of the source(s) to join to.

A URD intercept URL has the following syntax:

```
http://webserver:659/path?group=group&source=source1&...source=sourceN&
```

The *webserver* string is the name or IP address to which the URL is targeted. This target need not be the IP address of an existing web server, except for situations where the web server wants to recognize that the last hop router failed to support the URD mechanism. The number 659 indicates the URD port. Port 659 is reserved for Cisco by the IANA for the URD mechanism so that no other applications can use this port.

When the browser of a host encounters a URD intercept URL, it will try to open a TCP connection to the web server on port 659. If the last hop router is enabled for URD on the interface where the router receives the TCP packets from the host, it will intercept all packets for TCP connections destined to port 659 independent of the actual destination address of the TCP connection (independent of the address of the web server). Once intercepted, the last hop router will "speak" a very simple subset of HTTP on this TCP connection, emulating a web server. The only HTTP request that the last hop router will understand and reply to is the following GET request:

```
GET argument HTTP/1.0
argument = /path?group=group&source=source1&...source=sourceN&
```

When it receives a GET command, the router tries to parse the argument according to this syntax to derive one or more (S, G) channel memberships. The *path* string of the argument is anything up to, but not including, the first question mark, and is ignored. The *group* and *source1* through *sourceN* strings are the IP addresses or fully qualified domain names of the channels for which this argument is a subscription request. If the argument matches the syntax shown, the router interprets the argument to be subscriptions for the channels (*source1*, *group*) through (*sourceN*, *group*).

The router will accept the channel subscription(s) if the following conditions are met:

- The IP address of the multicast group is within the SSM range.
- The IP address of the host that originated the TCP connection is directly connected to the router.

If the channel subscription is accepted, the router will respond to the TCP connection with the following HTML page format:

```
HTTP/1.1 200 OK
Server:cisco IOS
Content-Type:text/html
<html>
<body>
Retrieved URL string successfully
</body>
</html>
```

If an error condition occurs, the <body> part of the returned HTML page will carry an appropriate error message. The HTML page is a by-product of the URD mechanism. This returned text may, depending on how the web pages carrying a URD intercept URL are designed, be displayed to the user or be sized so that the actual returned HTML page is invisible.

The primary effect of the URD mechanism is that the router will remember received channel subscriptions and will match them against IGMP group membership reports received by the host. The router will "remember" a URD (S, G) channel subscription for up to 3 minutes without a matching IGMP group membership report. As soon as the router sees that it has received both an IGMP group

membership report for a multicast group G and a URD (S, G) channel subscription for the same group G, it will join the (S, G) channel through PIM-SSM. The router will then continue to join to the (S, G) channel based only on the presence of a continuing IGMP membership from the host. Thus, one initial URD channel subscription is all that is needed to be added through a web page to enable SSM with URD.

If the last hop router from the receiver host is not enabled for URD, then it will not intercept the HTTP connection toward the web server on port 659. This situation will result in a TCP connection to port 659 on the web server. If no further provisions on the web server are taken, then the user may see a notice (for example, "Connection refused") in the area of the web page reserved for displaying the URD intercept URL (if the web page was designed to show this output). It is also possible to let the web server "listen" to requests on port 659 and install a Common Gateway Interface (CGI) script that would allow the web server to know if a channel subscription failed (for example, to subsequently return more complex error descriptions to the user).

Because the router returns a Content-Type of text and HTML, the best way to include the URD intercept URL into a web page is to use a frame. By defining the size of the frame, you can also hide the URD intercept URL on the displayed page.

By default, URD is disabled on all interfaces. When URD is configured through the **ip urd** command on an interface, it will be active only for IP multicast addresses in the SSM range.

Benefits

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 routers 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 to install and manage, and therefore 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 and requires only the upgrade of last hop routers 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 major 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).

Restrictions

Legacy Applications Within the SSM Range Restrictions

Existing applications in a network predating SSM will not work within the SSM range, unless they are modified to support (S, G) channel subscriptions or are enabled through URD. Therefore, enabling SSM in a network may cause problems for existing applications if they use addresses within the designated SSM range.

IGMP v3lite and URD Require a Cisco IOS Last Hop Router

SSM and IGMPv3 are solutions that are being standardized in the IETF. However, IGMP v3lite and URD are Cisco-developed solutions. For IGMP v3lite and URD to operate properly for a host, the last hop router toward that host must be a Cisco IOS router with IGMP v3lite or URD enabled.

Note This limitation does not apply to an application using the HSIL if the host has kernel support for IGMPv3, because then the HSIL will use the kernel IGMPv3 instead of IGMP v3lite.

Address Management Restrictions

Address management is still necessary to some degree when SSM is used with Layer 2 switching mechanisms. Cisco Group Management Protocol (CGMP), IGMP snooping, or Router-Port Group Management Protocol (RGMP) currently support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, then they will not benefit from these existing mechanisms. Instead, both

receivers will receive all (S, G) channel traffic (and filter out the unwanted traffic on input). Because of the ability of SSM to reuse the group addresses in the SSM range for many independent applications, this situation can lead to less than expected traffic filtering in a switched network. For this reason it is important to follow the recommendations set forth in the IETF drafts for SSM to use random IP addresses out of the SSM range for an application to minimize the chance for reuse of a single address within the SSM range between different applications. For example, an application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup will guarantee that multiple receivers to different channels within the same application service will never experience traffic aliasing in networks that include Layer 2 switches.

IGMP Snooping and CGMP Limitations

IGMPv3 uses new membership report messages that may not be recognized correctly by older IGMP Snooping switches, in which case hosts will not properly receive traffic. This situation is not an issue if URD or IGMP v3lite is used with hosts where the operating system is not upgraded for IGMPv3, because IGMP v3lite and URD rely only on IGMPv1 or IGMPv2 membership reports. For more information about switching issues related to IGMP (especially with CGMP), refer to the Cisco IOS Release 12.0(15)S *IGMP Version 3* feature module.

URD Intercept URL Limitations

A URD intercept URL string must be fewer than 256 bytes in length, starting from the */path* argument. In the HTTP/TCP connection, this string must also be contained within a single TCP/IP packet. For example, for a 256-byte string, a link maximum transmission unit (MTU) of 128 bytes between the host and intercepting router would cause incorrect operation of URD.

State Maintenance Limitations

In PIM-SSM, the last hop router will continue to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source will be maintained, even if the source is not sending traffic for longer periods of time (or even never).

This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S, G) state will be deleted and only reestablished after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

HSIL Limitations

As explained in the “IGMP v3lite Host Signalling” section, the HSIL tries to determine if the host operating system supports IGMPv3. This check is made so that a single application can be used both on hosts where the operating system has been upgraded to IGMPv3 and on hosts where the operating system only supports IGMPv1 or IGMPv2. Checking for the availability of IGMPv3 in the host operating system can only be made by the HSIL if IGMPv3 kernel support exists for at least one version of this operating system at the time when the HSIL was provided. If such an IGMPv3 kernel implementation has become available only recently, then users may need to also upgrade the HSIL on their hosts so that applications compiled with the HSIL will then dynamically bind to the newest version of the HSIL, which should support the check for IGMPv3 in the operating system kernel. Upgrading the HSIL can be done independently of upgrading the application itself.

Related Documents

- More information about IGMPv3 can be found in the *IGMP Version 3* feature module, Release 12.0(15)S.
- Updated information about SSM, IGMPv3 and other IP multicast related features and further references can be found at ftp://ftpeng.cisco.com/ipmulticast.html.
- A note from the IANA about the assignment of the 232/8 address space for SSM protocols and applications can be found at http://www.isi.edu/in-notes/iana/assignments/single-source-multicast.
- The features described in this feature module are based on the following IETF protocol specification drafts. These documents can be found at ftp://ftpeng.cisco.com/ipmulticast/drafts.
  - draft-holbrook-ssm-00.txt

    This draft describes the SSM model, its default usage with the 232/8 address range, and how IGMPv3 applies to SSM.
  - draft-bhaskar-pim-ss-00.txt

    This draft describes PIM-SSM mode as used with Cisco IOS SSM.
  - draft-ietf-idmr-igmp-v3-04.txt

    This draft describes IGMPv3 on which the host signalling of IGMP v3lite is based.
  - draft-ietf-idmr-msf-api-00.txt

    This draft describes the proposed API for IGMPv3 on hosts. A subset of this API is provided by the HSIL for implementation of IGMP v3lite.
  - draft-ietf-pim-v2-sm-01.txt

    This draft describes PIM-SM on which PIM-SSM mode is based.
  - draft-shepherd-ssm232-00.txt

    This draft describes the Best Current Practices (BCP) for using PIM-SM within the SSM range.

Supported Platforms

SSM with IGMPv3, IGMP v3lite, and URD is supported on all Cisco IOS Release 12.0(15)S platforms and later releases.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of MIBs supported by platform and Cisco IOS release and to download MIB modules, go to the Cisco web site on Cisco Connection Online (CCO) at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for SSM. Each task in the list is identified as either optional or required.

- Configuring SSM (Required)
- Verifying SSM (Optional)

Configuring SSM

	Command	Purpose
Step 1	`Router(config)# ip pim ssm [default | range access-list]`	Defines the SSM range of IP multicast addresses.
Step 2	`Router(config)# interface type number`	Selects an interface that is connected to hosts on which IGMPv3, IGMP v3lite, and URD can be enabled.
Step 3	`Router(config-if)# ip pim {sparse-mode | sparse-dense-mode}`	Enables PIM on an interface. You must use either sparse mode or sparse-dense mode.
Step 4	`Router(config-if)# ip igmp version 3`	Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2.
	or	or
	`Router(config-if)# ip igmp v3lite`	Enables the acceptance and processing of IGMP v3lite membership reports on an interface.
	or	or
	`Router(config-if)# ip urd`	Enables interception of TCP packets sent to the reserved URD port 659 on an interface and processing of URD channel subscription reports.

Verifying SSM

To verify configuration of multicast groups supporting SSM, use the following **show** commands:

- To display the (S, G) channel subscription through IGMPv3, IGMP v3lite, or URD, use the **show ip igmp groups detail** EXEC command.
- To verify whether a multicast group is supporting SSM service or whether a source-specific host report was received, use the **show ip mroute** EXEC command and examine the flags of the entries.

Configuration Examples

This section provides the following SSM configuration examples:

- SSM with IGMPv3 Example
- SSM with IGMP v3lite and URD Example
- SSM Filtering Example

SSM with IGMPv3 Example

The following example shows how to configure a router (running IGMPv3) for SSM:

```
ip multicast-routing
!
interface Ethernet3/1
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
 ip pim sparse-dense-mode
!
interface Ethernet3/2
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-dense-mode
 description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

SSM with IGMP v3lite and URD Example

The following example shows how to configure IGMP v3lite and URD on interfaces connected to hosts for SSM. Configuring IGMP v3lite and URD is not required or recommended on backbone interfaces.

```
interface ethernet 3/1
 ip address 172.21.200.203 255.255.255.0
 ip pim sparse-dense-mode
 description ethernet connected to hosts
!
interface ethernet 1
description ethernet connected to hosts
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-dense-mode
 ip urd
 ip igmp v3lite
```

SSM Filtering Example

The following example shows how to configure filtering on a legacy RP router running Cisco IOS releases earlier than Release 12.0(15)S for SSM routing. This filtering will suppress all unwanted PIM-SM and MSDP traffic in the SSM range. Without this filtering, SSM will still operate, but there may be additional RPT traffic if legacy first hop and last hop routers exist in the network.

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
```

```
ip pim accept-register list no-ssm-range

ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any

! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The "ip pim accept-register" command
! filters remote sources.
ip msdp redistribute list msdp-nono-list

! Filter received SA messages in SSM range. "Filtered on receipt" means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

Command Reference

This section documents the following new or modified commands. For other commands related to IGMPv3, refer to the Cisco IOS Release 12.0(15)S *IGMP Version 3* feature module. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **ip igmp v3lite**
- **ip pim ssm**
- **ip urd**
- **show ip igmp groups**
- **show ip mroute**

ip igmp v3lite

To enable acceptance and processing of Internet Group Management Protocol Version 3 lite (IGMP v3lite) membership reports on an interface, use the **ip igmp v3lite** interface configuration command. To disable IGMP v3lite, use the **no** form of this command.

ip igmp v3lite

no ip igmp v3lite

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.

Usage Guidelines

To use this command, you must define a Source Specific Multicast (SSM) range of IP addresses using the **ip pim ssm** global configuration command. When IGMP v3lite is enabled, it is supported in the SSM range of addresses only.

Examples

The following example shows how to configure IGMP v3lite on Ethernet interface 3/1:

```
Router(config)# interface ethernet 3/1
Router(config-if)# ip igmp v3lite
```

Related Commands

Command	Description
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** global configuration command. To disable the SSM range, use the **no** form of this command.

ip pim ssm {**default** | **range** *access-list*}

no ip pim ssm

Syntax Description

default	(Optional) Defines the SSM range access list to 232/8.
range *access-list*	(Optional) Standard IP access list defining the SSM range.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.

Usage Guidelines

When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.

Examples

The following example shows how to configure SSM service for the IP address range defined by access list 4:

```
Router(config)# access-list 4 permit 224.2.151.141
Router(config)# ip pim ssm range 4
```

Related Commands

Command	Description
ip igmp v3lite	Enables the acceptance and processing of IGMP v3lite membership reports on an interface.
ip urd	Enables interception of TCP packets sent to the reserved URD port 659 on an interface and processing of URD channel subscription reports.

ip urd

To enable interception of TCP packets sent to the reserved URL Rendezvous Directory (URD) port 659 on an interface and processing of URD channel subscription reports, use the **ip urd** command in interface configuration mode. To disable URD on an interface, use the **no** form of this command.

ip urd [**proxy**]

no ip urd [**proxy**]

Syntax Description

proxy	(Optional) Allows an interface to accept URL requests from any TCP connection sent to that interface. If the **proxy** keyword is not configured, the interface will accept URL requests from TCP connections only if the requests originated from directly connected hosts. The **proxy** option must be enabled on an interface if it is unnumbered or if it has downstream routers configured with Internet Group Managment Protocol (IGMP) proxy routing. To prevent users on the backbone from creating URD state on your router, do not enable the **proxy** option on a backbone interface of your router.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

To use this command, you must first define a Source Specific Multicast (SSM) range of IP addresses using the **ip pim ssm** global configuration command. When URD is enabled, it is supported in the SSM range of addresses only. We recommend that you not enable URD on backbone interfaces, but only on interfaces connecting to hosts.

URD functionality is available for multicast process switching, fast switching, and distributed fast-switching paths.

Examples

The following example shows how to configure URD on Ethernet interface 3/3:

```
interface ethernet 3/3
ip urd
```

Related Commands

Command	Description
ip pim ssm	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** EXEC command.

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

Syntax Description

group-name	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
type	(Optional) Interface type.
number	(Optional) Interface number.
detail	(Optional) Provides a detailed description of the sources known through IGMP Version 3 (IGMPv3), IGMP v3lite, or URL Rendezvous Directory (URD).

Command Modes

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 **detail** keyword was added.

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       171.69.214.251
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 232.1.1.1 detail

Interface:      Ethernet3/2
Group:          232.1.1.1
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)
  Source Address   Uptime    v3 Exp    CSR Exp   Fwd  Flags
  171.69.214.1     01:58:28  stopped   00:02:31  Yes  C
```

Table 1 describes the significant fields shown in the output.

Table 1 show ip igmp groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long in weeks, days, hours, minutes, and seconds this multicast group has been known.
Group mode:	Can be either INCLUDE or EXCLUDE. The Group mode is based on the type of membership report(s) received on the interface for the group. In the output for the **show ip igmp groups detail** command, the EXCLUDE mode also shows the "Expires:" field for the group entry (not shown in the output).
Expires	How long in hours, minutes, and seconds until the entry expires. If an entry expires, then it will (for a short period) show the word "now" before it is removed. The word "never" indicates that the entry will not time out, because a local receiver is on this router for this entry. The word "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 will time 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.
CSR Grp Exp	This field is 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:	Provides details of which sources have been requested by the multicast group.
Source Address	IP address of the source.
Uptime	Indicates the time since the source state was created.

Table 1 show ip igmp groups Field Descriptions (continued)

Field	Description
v3 Exp	Indicates the time in hours, minutes, and seconds until the membership for the source will time out according to IGMP operations. The word “stopped” is shown if no member uses IGMPv3 (but only IGMP v3lite or URD).
CSR Exp	Indicates the time in hours, minutes, and seconds until the membership for the source will time out according to IGMP v3lite or URD reports. The word “stopped” is shown if members use only IGMPv3.
Fwd	Indicates 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
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host-query messages.

show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** EXEC command.

show ip mroute [*group-name* | *group-address*] [*source*] [**summary**] [**count**] [**active** *kbps*]

Syntax Description

group-name | *group-address*	(Optional) IP address, name, or interface of the multicast group as defined in the Domain Name System (DNS) hosts table.
source	(Optional) IP address or name of a multicast source.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
active *kbps*	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at a rate of *kbps* or higher. The *kbps* argument defaults to 4 kbps.

Defaults

The **show ip mroute** command displays all groups and sources.

The **show ip mroute active** command displays all sources sending at a rate greater than or equal to 4 kbps.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	The U, s, and I flags for Source Specific Multicast (SSM) were introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP multicast routing table.

The Cisco IOS software populates the multicast routing table by creating (S, G) entries from (*, G) entries. The star refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Examples

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This command displays the contents of the IP multicast routing table for the multicast group named cbone-audio.

```
Router# show ip mroute cbone-audio

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 0.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 0.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(198.92.37.100/32, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 198.92.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(198.92.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

The following is sample output from the **show ip mroute** command that shows the virtual circuit descriptor (VCD) value, because an ATM interface with PIM multipoint signalling is enabled:

```
Router# show ip mroute 224.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:03:57/00:02:54, RP 130.4.101.1, flags: SJ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    ATM0/0, VCD 14, Forward/Sparse, 00:03:57/00:02:53
```

The following is sample output from the **show ip mroute** command with the **summary** keyword:

```
Router# show ip mroute summary

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.255.255.255), 2d16h/00:02:30, RP 171.69.10.13, flags: SJPC

(*, 224.2.127.253), 00:58:18/00:02:00, RP 171.69.10.13, flags: SJC

(*, 224.1.127.255), 00:58:21/00:02:03, RP 171.69.10.13, flags: SJC

(*, 224.2.127.254), 2d16h/00:00:00, RP 171.69.10.13, flags: SJCL
  (128.9.160.67/32, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
  (129.48.244.217/32, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
  (130.207.8.33/32, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
  (131.243.2.62/32, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
  (140.173.8.3/32, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
  (171.69.60.189/32, 224.2.127.254), 00:03:47/00:00:46, flags: CLJT
```

The following is sample output from the **show ip mroute** command with the **active** keyword:

```
Router# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 146.137.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

The following is sample output from the **show ip mroute** command with the **count** keyword:

```
Router# show ip mroute count

IP Multicast Statistics - Group count: 8, Average sources per group: 9.87
Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Group: 224.255.255.255, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.2.127.253, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.1.127.255, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.2.127.254, Source count: 9, Group pkt count: 14
  RP-tree: 0/0/0/0
  Source: 128.2.6.9/32, 2/0/796/0
  Source: 128.32.131.87/32, 1/0/616/0
  Source: 128.125.51.58/32, 1/0/412/0
  Source: 130.207.8.33/32, 1/0/936/0
  Source: 131.243.2.62/32, 1/0/750/0
```

```
  Source: 140.173.8.3/32, 1/0/660/0
  Source: 146.137.28.69/32, 1/0/584/0
  Source: 171.69.60.189/32, 4/0/447/0
  Source: 204.162.119.8/32, 2/0/834/0

Group: 224.0.1.40, Source count: 1, Group pkt count: 3606
  RP-tree: 0/0/0/0
  Source: 171.69.214.50/32, 3606/0/48/0, RPF Failed: 1203

Group: 224.2.201.241, Source count: 36, Group pkt count: 54152
  RP-tree: 7/0/108/0
  Source: 13.242.36.83/32, 99/0/123/0
  Source: 36.29.1.3/32, 71/0/110/0
  Source: 128.9.160.96/32, 505/1/106/0
  Source: 128.32.163.170/32, 661/1/88/0
  Source: 128.115.31.26/32, 192/0/118/0
  Source: 128.146.111.45/32, 500/0/87/0
  Source: 128.183.33.134/32, 248/0/119/0
  Source: 128.195.7.62/32, 527/0/118/0
  Source: 128.223.32.25/32, 554/0/105/0
  Source: 128.223.32.151/32, 551/1/125/0
  Source: 128.223.156.117/32, 535/1/114/0
  Source: 128.223.225.21/32, 582/0/114/0
  Source: 129.89.142.50/32, 78/0/127/0
  Source: 129.99.50.14/32, 526/0/118/0
  Source: 130.129.0.13/32, 522/0/95/0
  Source: 130.129.52.160/32, 40839/16/920/161
  Source: 130.129.52.161/32, 476/0/97/0
  Source: 130.221.224.10/32, 456/0/113/0
  Source: 132.146.32.108/32, 9/1/112/0
```

The following is sample output from the **show ip mroute** command for a router supporting SSM services:

```
Router# show ip mroute 232.6.6.6

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C -
Connected, L - Local, P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set, J -
Join SPT, M - MSDP created entry, X - Proxy Join Timer Running, A - Advertised via MSDP,
U - URD, I - Received Source Specific Host Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 232.6.6.6), 00:01:20/00:02:59, RP 0.0.0.0, flags:sSJP
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:Null

(2.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags:CTI
  Incoming interface:Ethernet3/3, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet3/1, Forward/Sparse-Dense, 00:00:36/00:02:35
```

Table 2 describes the significant fields shown in the output.

Table 2 show ip mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
B - Bidir Group	Indicates that a multicast group is operating in bidirectional mode.
s - SSM Group	Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
C - Connected	A member of the multicast group is present on the directly connected interface.
L - Local	The router itself is a member of the multicast group.
P - Pruned	Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source.
R - RP-bit set	Indicates that the (S, G) entry is pointing toward the RP. This is typically prune state along the shared tree for a particular source.
F - Register flag	Indicates that the software is registering for a multicast source.
T - SPT-bit set	Indicates that packets have been received on the shortest path source tree.

Table 2 show ip mroute Field Descriptions (continued)

Field	Description

J - Join SPT	For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J- Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree.
	
	For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J- Join SPT flag is set for (S, G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.
	
	Note The router measures the traffic rate on the shared tree and compares the measured rate to the SPT- Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J- Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.
	
	If the default SPT-Threshold value of 0 kbps is used for the group, the J- Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest-path tree when traffic from a new source is received.

M - MSDP created entry	Indicates that a (*, G) entry was learned through a Multicast Source Discovery Protocol (MSDP) peer. This flag is only applicable for a rendezvous point (RP) running MSDP.
X - Proxy Join Timer Running	Indicates that the proxy join timer is running. This flag is only set for (S, G) entries of an RP or “turnaround” router. A “turnaround” router is located at the intersection of a shared path (*, G) tree and the shortest path from the source to the RP.
A - Advertised via MSDP	Indicates that an (S, G) entry was advertised through an MSDP peer. This flag is only applicable for an RP running MSDP.
U - URD	Indicates that a URD channel subscription report was received for the (S, G) entry.
I - Received Source Specific Host Report	Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by IGMPv3, URD, or IGMP v3lite. This flag is only set on the designated router (DR).
Outgoing interface flags:	Provides information about the entry.
H - Hardware switched	Indicates that a Multicast Multilayer Switching (MMLS) forwarding path has been established for this entry.

Table 2 show ip mroute Field Descriptions (continued)

Field	Description
Timers: Uptime/Expires	Uptime indicates per interface how long in hours, minutes, and seconds the entry has been in the IP multicast routing table. Expires indicates per interface how long in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.
Interface state:	Indicates the state of the incoming or outgoing interface.
Interface	Indicates the type and number of the interface listed in the incoming or outgoing interface list.
Next-Hop or VCD	Next hop specifies the IP address of the downstream neighbor. VCD specifies the virtual circuit descriptor number. VCD0 means the group is using the static map virtual circuit.
State/Mode	State indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or Time To Live (TTL) threshold. Mode indicates whether the interface is operating in dense, sparse, or sparse-dense mode.
(*, 224.0.255.1) and (198.92.37.100/32, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S, G) or "S comma G" entries. (*, G) entries are used to build (S, G) entries.
RP	Address of the rendezvous point (RP) router. For routers and access servers operating in sparse mode, this address is always 0.0.0.0.
flags:	Information about the entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor or RPF nbr	IP address of the upstream router to the source. "Tunneling" indicates that this router is sending data to the RP encapsulated in Register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used.
Dvmrp or Mroute	Indicates if the RPF information is obtained from the Distance Vector Multicast Routing Protocol (DVMRP) routing table or the static mroutes configuration.
Outgoing interface list:	Interfaces through which packets will be forwarded. When the **ip pim nbma-mode** command is enabled on the interface, the IP address of the Protocol Independent Multicast (PIM) neighbor is also displayed.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip pim	Enables PIM on an interface.
ip pim ssm	Defines the SSM range of IP multicast addresses.

Debug Commands

This section documents the following new and modified **debug** commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **debug ip igmp**
- **debug ip urd**

debug ip igmp

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

debug ip igmp

no debug ip igmp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command History

Release	Modification
10.2	This command was introduced.
12.1(3)T	Additional fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.

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 what is happening to the multicast routing process, or why packets are forwarded out of particular interfaces.

Examples

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

```
Router# debug ip igmp

IGMP: Received Host-Query from 172.24.37.33 (Ethernet1)
IGMP: Received Host-Report from 172.24.37.192 (Ethernet1) for 224.0.255.1
IGMP: Received Host-Report from 172.24.37.57 (Ethernet1) for 224.2.127.255
IGMP: Received Host-Report from 172.24.37.33 (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 (IGMP v3lite) 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 1.1.1.1
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 1.1.1.1
```

Related Commands

Command	Description
debug ip mrm	Displays MRM control packet activity.
debug ip pim	Displays PIM packets received and sent, and PIM-related events.

debug ip urd

To display debug messages for URL Rendezvous Directory (URD) channel subscription report processing, use the **debug ip urd** EXEC command. To disable debugging of URD reports, use the **no** form of this command.

debug ip urd [*hostname* | *ip-address*]

no debug ip urd

Syntax Description

hostname	(Optional) Domain Name System (DNS) name.
ip-address	(Optional) IP address.

Defaults

If no host name or IP address is specified, all URD reports are debugged.

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.

Examples

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

```
Router# debug ip urd

13:36:25 pdt:URD:Data intercepted from 171.71.225.103
13:36:25 pdt:URD:Enqueued string:
'/cgi-bin/error.pl?group=232.16.16.16&port=32620&source=171.69.214.1&li'
13:36:25 pdt:URD:Matched token:group
13:36:25 pdt:URD:Parsed value:232.16.16.16
13:36:25 pdt:URD:Creating IGMP source state for group 232.16.16.16
```

Glossary

first hop router—A router that is directly connected to a host that is sending traffic (for example, a router on the same Ethernet as the host). To illustrate, if the host is sending multicast traffic to a group in PIM-SM, then one of the first hop routers (specifically, the one that is elected as designated router) must send PIM-SM register messages for this host toward the RP.

last hop router—A router that is directly connected to a host that is receiving traffic (for example, a router on the same Ethernet as the host). To illustrate, if the host wants to receive multicast traffic, then the last hop router must listen to the IGMP membership reports sent by the host.