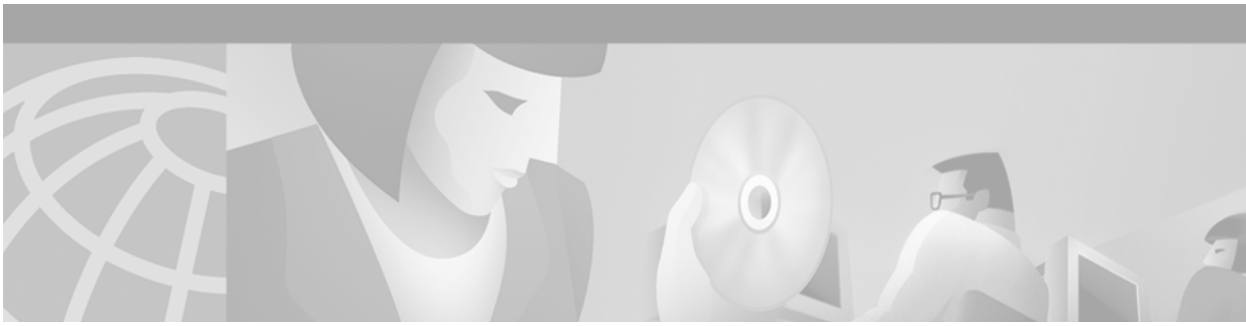

IGMP Version 3

This feature module describes the IGMP Version 3 feature and includes the following sections:

Feature Overview

Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast memberships to neighboring multicast routers.

This feature module introduces support for Version 3 of IGMP. In previous versions of Cisco IOS software only Version 1 and Version 2 were supported. IGMP Version 3 (IGMPv3) adds support for "source filtering," which enables a multicast receiver host to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. This membership information enables Cisco IOS software to forward traffic only from those sources from which receivers requested the traffic.

IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic. With IGMPv3, receivers signal membership to a multicast host group in the following two modes:

- INCLUDE mode—In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the INCLUDE list) from which it wants to receive traffic.
- EXCLUDE mode—In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the EXCLUDE list) from which it does not want to receive traffic. This indicates that the host wants to receive traffic only from other sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, like in the case of the Internet Standard Multicast (ISM) service model, a host expresses EXCLUDE mode membership with an empty EXCLUDE list.

IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in Source Specific Multicast (SSM). SSM was introduced in Cisco IOS Release 12.1(3)T, however SSM support for IGMPv3 was introduced in 12.1(5)T. For SSM to rely on IGMPv3, IGMPv3 must be available in last hop routers and host operating system network stacks, and be used by the applications running on those hosts.

In SSM deployment cases where IGMPv3 cannot be used because it is not supported by the receiver host or the receiver applications, there are two Cisco-developed transition solutions that enable the immediate deployment of SSM services: URL Rendezvous Directory (URD) and IGMP Version 3 lite (IGMP v3lite). Both of these features are documented in the Cisco IOS Release 12.0(15)S *Source Specific Multicast with IGMPv3, IGMP v3lite, and URD* feature module.

Benefits

- Enables new multicast services—SSM.
- Optimized bandwidth utilization—Receiver may request to receive traffic only from explicitly known sources.
- Improved security—No denial of service attacks from unknown sources.

Restrictions

Traffic Filtering with Multicast Groups That Are Not Configured in SSM Mode

In Cisco IOS Release 12.0(15)S, IGMPv3 membership reports are not utilized by Cisco IOS software to filter or restrict traffic for multicast groups that are not configured in SSM mode. Effectively, Cisco IOS software interprets all IGMPv3 membership reports for groups configured in dense, sparse, or bidirectional mode to be group membership reports and forwards traffic from all active sources onto the network.

Interoperability with IGMP Snooping

You must be careful when using IGMPv3 with switches that support and are enabled for IGMP snooping, because IGMPv3 messages are different from the messages used in IGMP Version 1 (IGMPv1) and Version 2 (IGMPv2). If a switch does not recognize IGMPv3 messages, then hosts will not correctly receive traffic if IGMPv3 is being used. In this case, either IGMP snooping may be disabled on the switch or the router may be configured for IGMPv2 on the interface (which would remove the ability to use SSM for host applications that cannot resort to URD or IGMP v3lite).

Interoperability with CGMP

Networks using Cisco Group Management Protocol (CGMP) will have better group leave behavior if they are configured with IGMPv2 than IGMPv3. If CGMP is used with IGMPv2 and the switch is enabled for the CGMP leave functionality, then traffic to a port joined to a multicast group will be removed from the port shortly after the last member on that port has dropped membership to that group. This fast-leave mechanism is part of IGMPv2 and is specifically supported by the CGMP fast-leave enabled switch.

With IGMPv3, there is currently no CGMP switch support of fast-leave. If IGMPv3 is used in a network, CGMP will continue to work, but CGMP fast-leave support is ineffective and the following conditions apply:

- Each time a host on a new port of the CGMP switch joins a multicast group, that port is added to the list of ports to which the traffic of this group is sent.
- If all hosts on a particular port leave the multicast group, but there are still hosts on other ports (in the same virtual LAN) joined to the group, then nothing happens. In other words, the port continues to receive traffic from that multicast group.
- Only when the last host in a virtual LAN (VLAN) has left the multicast group does forwarding of the traffic of this group into the VLAN revert to no ports on the switch forwarding.

This join behavior only applies to multicast groups that actually operate in IGMPv3 mode. If legacy hosts only supporting IGMPv2 are present in the network, then groups will revert to IGMPv2 and fast-leave will work for these groups.

If fast-leave is needed with CGMP-enabled switches, we recommend that you not enable IGMPv3 but configure IGMPv2 on that interface.

If IGMPv3 is needed to support SSM, then you have two configuration alternatives:

- Only configure the interface for IGMPv2 and use IGMP v3lite and URD.
- Enable IGMPv3 and accept the higher leave latencies through the CGMP switch.

Related Features and Technologies

The IGMP Version 3 feature is related to the existing Source Specific Multicast, URD, and IGMP v3lite features, which are documented in the Cisco IOS Release 12.0(15)S *Source Specific Multicast with IGMPv3, IGMP v3lite, and URD* feature module.

Related Documents

- *Source Specific Multicast with IGMPv3, IGMP v3lite, and URD* feature module, Release 12.0(15)S
- *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1
- *Cisco IOS IP and IP Routing Command Reference*, Release 12.1
- RFC 2236, *Internet Group Management Protocol, Version 2*
- draft-ietf-idmr-igmp-v3-04.txt. This Internet Engineering Task Force (IETF) protocol specification draft describes IGMPv3 and can be found at ftp://ftpeng.cisco.com/ipmulticast/drafts.

Supported Platforms

IGMPv3 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 the IGMP Version 3 feature. Each task in the list is identified as either optional or required:

- Configuring IGMPv3 (Required)
- Verifying IGMPv3 (Optional)

Configuring IGMPv3

You must configure IGMPv3 explicitly on a router. To configure IGMPv3 on a router, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface type number`	Selects an interface that is connected to hosts on which IGMPv3, IGMP v3lite, and URD can be enabled.
Step 2	`Router(config-if)# ip pim {sparse-mode | sparse-dense-mode}`	Enables Protocol Independent Multicast (PIM) on an interface. You must use either sparse mode or sparse-dense mode.
Step 3	`Router(config-if)# ip igmp version 3`	Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2.

Verifying IGMPv3

To verify that IGMPv3 is configured properly, use the following **show** commands:

- **show ip igmp groups**
- **show ip mroute**

The following sample output shows a router sending IGMPv3 queries and a host (172.21.200.41) responding with an INCLUDE report for (171.69.214.1, 232.1.1.1):

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.0.1.40       Ethernet3/2          4d22h     00:02:51  131.108.1.1
224.0.1.40       Ethernet3/1          6w3d      00:02:22  172.21.200.203
232.1.1.1        Ethernet3/1          4d21h     never     172.21.200.41

Router# show ip igmp groups 232.1.1.1 detail

Interface: Ethernet3/1
Group: 232.1.1.1
Uptime: 4d21h
Router mode: INCLUDE
Host mode: INCLUDE
Last reporter: 172.21.200.41
CSR Grp Exp: now
Group source list:(C - Cisco Src Report, U - URD, R - Remote)
  Source Address   Uptime    Expires   CSR Exp  Fwd  Flags
  171.69.214.1     4d21h     00:02:17  now       Yes  R 4
```

```
Router# show ip mroute 232.1.1.1

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

(*, 232.1.1.1), 4d21h/00:02:59, RP 0.0.0.0, flags:sSJP
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:Null

(171.69.214.1, 232.1.1.1), 4d21h/00:02:45, flags:CTI
  Incoming interface:Ethernet3/2, RPF nbr 131.108.1.1
  Outgoing interface list:
    Ethernet3/1, Forward/Sparse-Dense, 4d21h/00:02:45
```

Configuration Examples

The following configuration 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
 ip pim sparse-dense-mode
 ip igmp version 3
!
interface Ethernet3/2
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp version 3
!
ip pim ssm default
```

Command Reference

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

- **ip igmp version**
- **show ip igmp groups**

ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** interface configuration command. To restore the default value, use the **no** form of this command.

ip igmp version {**1** | **2** | **3**}

no ip igmp version

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.
3	IGMP Version 3.

Defaults

Version 2

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(5)T	The **3** keyword was added.

Usage Guidelines

All routers on a subnet must be configured for the same version of IGMP. A Cisco IOS Release 12.0 and later releases do not automatically detect Version 1 systems and switch to Version 1, as did prior releases of the Cisco IOS software. Hosts can have any IGMP version (1, 2, of 3) and the router will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2 or 3, such as the **ip igmp query-max-response-time** and **ip igmp query-timeout** commands.

Examples

The following example configures the router to use IGMP Version 3.

```
ip igmp version 3
```

Related Commands

Command	Description
ip igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp query-timeout	Configures the timeout time before the router takes over as the querier for the interface, after the previous querier has stopped querying.

Command	Description
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays multicast-related information about an interface.

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.