



IGMP State Limit

The IGMP State Limit feature provides protection against denial of service (DoS) attacks caused by Internet Group Management Protocol (IGMP) packets. The new command-line interface (CLI) introduced by this feature allows you to configure a limit on the number of IGMP states that results from IGMP, IGMP Version 3 lite (IGMP v3lite), and URL Rendezvous Directory (URD) membership reports on a per-interface or global basis. Membership reports in excess of the configured limits will not be entered in the IGMP cache, and traffic for those excess membership reports will not be forwarded.

Feature Specifications for the IGMP State Limit Feature

Feature History

Release	Modification
12.2(14)S	This feature was introduced.
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(14)S and 12.2(15)T, consult Cisco Feature Navigator.

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 IGMP State Limit, page 2](#)
- [Information About IGMP State Limit, page 2](#)
- [Information About IGMP State Limit, page 2](#)
- [How to Configure IGMP State Limit, page 3](#)
- [Configuration Examples for IGMP State Limit, page 7](#)
- [Where to Go Next, page 7](#)

- [Additional References, page 7](#)
- [Command Reference, page 9](#)
- [Glossary, page 17](#)

Prerequisites for IGMP State Limit

Before this feature can be enabled, multicast routing must be enabled on the router, Protocol Independent Multicast (PIM) must be enabled on the router's interfaces, and the router must be configured to be part of a multicast group.

Information About IGMP State Limit

To configure the IGMP State Limit feature, you need to understand the following concepts:

- [Benefits of IGMP State Limit, page 2](#)
- [Feature Design of IGMP State Limit, page 2](#)
- [IGMP State Limit and SSM, page 3](#)

Benefits of IGMP State Limit

The IGMP State Limit feature limits the vulnerability of a router to DoS attacks with IGMP packets. A high rate of IGMP messages sent to a router can pose a DoS attack scenario because the router processes IGMP, IGMP v3lite, and URD messages at the process level.

The IGMP State Limit feature enables you to limit the number of multicast streams sent to a router to a level that is sustainable by the router. You can limit the number of multicast streams per interface, per subinterface, or globally.

Feature Design of IGMP State Limit

The IGMP State Limit feature limits the number of IGMP states that can be joined to a router on a per-interface, per-subinterface, or global level. Use the **ip igmp limit** command to configure a limit on the number of IGMP states that can be joined to a router from IGMP, IGMP v3lite, and URD membership reports. Membership reports exceeding the configured limits are not entered into the IGMP cache and traffic for the excess membership reports is not forwarded.

Per-interface and global IGMP limits operate independently of each other. Both per-interface and global IGMP limits can be configured on the same router. A membership report that exceeds either the per-interface or the global state limit is ignored.

Use the **except** *access-list* keyword and attribute to exclude certain groups or channels from being counted against the IGMP limit so that they can be joined to an interface without counting against the interface limit.

IGMP State Limit and SSM

The IGMP State Limit feature is available with Source Specific Multicast (SSM).

When the IGMP State Limit feature is used with routers configured for SSM, counting rules apply to both the per-interface and global counting. These counters are kept separate and may be associated with different access control lists.

If the IGMP State Limit feature is configured without the *access-list* attribute of the **ip igmp limit** command, for either a system counter or an interface counter, the default access list is used to match all states.

An IGMP group state for (G) needs to be counted (either per interface or globally) if (0.0.0.0, G) is permitted by the default or configured by the *access-list* attribute. The IGMP group state for (G) is not counted if it is denied by the access list.

When the IGMP State Limit feature is configured, an IGMP state is accounted for only if it is associated with IGMP, IGMP v3lite, or URD. The IGMP State Limit feature does not enforce a limit on IGMP state messages created through explicit configuration in the router. Any state that is both requested by a host via IGMPv3Lite or URD, but that is also explicitly configured, is accounted.

An IGMP group state for (G) that is in INCLUDE mode is accounted for only if there is no source record associated with it and if (G) is permitted by the default or configured access control list.

How to Configure IGMP State Limit

This section contains the following procedures:

- [Configuring IGMP State Limit on an Interface, page 3](#)
- [Verifying IGMP State Limit, page 5](#)

Configuring IGMP State Limit on an Interface

Perform this task to configure IGMP state limiting to limit the number of IGMP membership reports sent to an interface or subinterface of a router to a level sustainable by the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp limit** *number* [**except** *access-list*]
5. Repeat Step 3 and Step 4.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface ethernet 0/1.1	Specifies an interface and places the router in interface configuration mode.
Step 4	ip igmp limit <i>number</i> [except <i>access-list</i>] Example: Router(config-if)# ip igmp limit 100	Limits the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership reports on the interface.
Step 5	Repeat Step 3 and Step 4.	(Optional) Configures IGMP state limiting on additional interfaces or subinterfaces.

What to Do Next

If you want to configure IGMP state limiting globally, proceed to the [“Configuring IGMP State Limit Globally”](#) section. Otherwise, proceed to the [“Verifying IGMP State Limit”](#) section.

Configuring IGMP State Limit Globally

Perform this task to configure IGMP state limiting to limit the number of IGMP membership reports sent to a router to a level sustainable by the router.

SUMMARY STEPS

- enable**
- configure terminal**
- ip igmp limit** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip igmp limit <i>number</i> Example: Router(config)# ip igmp limit 100	Limits the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership reports globally on the router.

What to Do Next

Proceed to the [“Verifying IGMP State Limit”](#) section.

Verifying IGMP State Limit

Perform this task to verify the configured global or per-interface IGMP state limits.

SUMMARY STEPS

1. **enable**
2. **show ip igmp interface**
3. **show ip igmp interface [*type number*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip igmp interface Example: Router# show ip igmp interface	Displays multicast-related information globally.
Step 3	show ip igmp interface [type number] Example: Router# show ip igmp interface ethernet 0	Displays multicast-related information on the specified interface.

Examples

This section provides an output example of the **show ip igmp interface** command, which displays the global configured and reached IGMP state limits:

```
Router# show ip igmp interface

Global IGMP state limit: 300 active out of 500 max
Ethernet0 is up, line protocol is up
Internet address is 192.168.37.6, subnet mask is 255.255.255.0
IGMP is enabled on interface
IGMP query interval is 60 seconds
Interface IGMP state limit: 1 active out of 1 max
Inbound IGMP access group is not set
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 192.168.37.33
No multicast groups joined
Ethernet1 is up, line protocol is up
Internet address is 192.168.36.129, subnet mask is 255.255.255.0
IGMP is enabled on interface
IGMP query interval is 60 seconds
Inbound IGMP access group is not set
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 192.168.36.131
Multicast groups joined: 225.2.2.2 226.2.2.2
Tunnel0 is up, line protocol is up
Internet address is 10.1.37.2, subnet mask is 255.255.0.0
IGMP is enabled on interface
IGMP query interval is 60 seconds
Inbound IGMP access group is not set
Multicast routing is enabled on interface
Multicast TTL threshold is 0
No multicast groups joined
```

Configuration Examples for IGMP State Limit

This section provides the following configuration examples:

- [Configuring IGMP State Limit on an Interface Example, page 7](#)
- [Configuring IGMP State Limit Globally Example, page 7](#)

Configuring IGMP State Limit on an Interface Example

The following example shows how to limit the number of IGMP membership reports on Ethernet interface 0:

```
interface ethernet 0
 ip igmp limit 100
```

The following example shows how to limit the number of IGMP membership reports on Ethernet interface 0. In this example, any IGMP membership reports from access list 0.0.0.1 do not count toward the configured state limit:

```
interface ethernet 0
 ip igmp limit 100 except 0.0.0.1
```

Configuring IGMP State Limit Globally Example

The following example shows how to limit the number of IGMP membership reports globally on a router. In this example, a global limit of 30 is configured and all IGMP states resulting from IGMP, IGMP v3lite, and URD membership reports are limited.

```
ip igmp limit 30
```

Where to Go Next

Cisco IOS software provides other features that can enhance the traffic control of IP multicast traffic, including Committed Access Rate (CAR), priority queueing, IP multicast rate limiting, IGMP access groups, and RP level access control. Refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2 and the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*, Release 12.2 for more information about these features.

Additional References

For additional information related to the IGMP State Limit feature, see the following sections:

- [Related Documents, page 8](#)
- [Standards, page 8](#)
- [MIBs, page 8](#)
- [RFCs, page 9](#)
- [Technical Assistance, page 9](#)

Related Documents

Related Topic	Document Title
Quality of service features, including CAR and priority queueing	<i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , Release 12.2
IP multicast commands	<i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i> , Release 12.2
IP multicast configuration information	<i>Cisco IOS IP Configuration Guide</i> , Release 12.2, Part 3, “IP Multicast”

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 existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature and support existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 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.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

- [ip igmp limit \(global\)](#)
- [ip igmp limit \(interface\)](#)

ip igmp limit (global)

To globally limit the number of Internet Group Management Protocol (IGMP) states resulting from IGMP, IGMP Version 3 lite (IGMP v3lite), and URL Rendezvous Directory (URD) membership states, use the **ip igmp limit** command in global configuration mode. To disable a configured IGMP state limit, use the **no** form of this command.

ip igmp limit *number*

no ip igmp limit *number*

Syntax Description	<i>number</i>	Maximum number of IGMP states allowed on a router. The valid range is from 1 to 64000.
---------------------------	---------------	--

Defaults	This command is not configured by default. There is no default number of IGMP limits configured. You must configure the number of maximum IGMP states allowed globally on a router when you configure this command.	
-----------------	---	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines	<p>Use this command to configure a limit on the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership reports on a global basis. Membership reports exceeding the configured limits are not entered in the IGMP cache and traffic for the excess membership reports is not forwarded.</p> <p>Use the ip igmp limit (interface) command to configure the per-interface IGMP state limit.</p> <p>Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.</p>
-------------------------	--

Examples	The following example shows how to limit the number of IGMP states on a router to 300:
-----------------	--

```
ip igmp limit 300
```

Related Commands	Command	Description
	ip igmp access-group	Controls the multicast groups that hosts on the subnet serviced by an interface can join.

Command	Description
ip igmp limit (interface)	Limits the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership states on a per-interface basis.
ip multicast rate-limit	Controls the rate a sender from the source list can send to a multicast group in the group list.

ip igmp limit (interface)

To limit the number of Internet Group Management Protocol (IGMP) states resulting from IGMP, IGMP Version 3 lite (IGMP v3lite), and URL Rendezvous Directory (URD) membership states on a per-interface basis, use the **ip igmp limit** command in interface configuration mode. To disable a configured IGMP state limit, use the **no** form of this command.

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit *number* [**except** *access-list*]

Syntax Description		
	<i>number</i>	Maximum number of IGMP states allowed on a router or interface. Range is from 1 to 64000.
	except	(Optional) Excludes an access list from the configured IGMP state limit.
	<i>access-list</i>	(Optional) Extended access list to exclude from the configured IGMP state limit.

Defaults This command is not configured by default. There is no default number of IGMP limits configured. You must configure the number of maximum IGMP states allowed per interface on a router when you configure this command.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines Use this command to configure a limit on the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership reports on a per-interface basis. Membership reports exceeding the configured limits are not entered in the IGMP cache and traffic for the excess membership reports is not forwarded.

Use the **ip igmp limit** (global) command to configure the global IGMP state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

If you do not configure the **except** *access-list* keyword and attribute, all IGMP states resulting from IGMP, IGMP v3lite, or URD are counted toward the configured cache limit on an interface. Use the **except** *access-list* keyword and attribute to exclude particular groups or channels from counting toward the IGMP cache limit. An IGMP membership report is counted against the per-interface limit if it is permitted by the extended access list specified by the **except** *access-list* keyword and attribute.

Examples

The following example shows how to limit the number of IGMP membership reports on Ethernet interface 0:

```
interface ethernet 0
 ip igmp limit 100
```

The following example shows how to limit the number of IGMP membership reports on Ethernet interface 0. In this example, any IGMP membership reports from access list 0.0.0.1 do not count toward the configured state limit:

```
interface ethernet 0
 ip igmp limit 100 except 0.0.0.1
```

Related Commands

Command	Description
ip igmp access-group	Controls the multicast groups that hosts on the subnet serviced by an interface can join.
ip igmp limit (global)	Globally limits the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership states.
ip multicast rate-limit	Controls the rate a sender from the source list can send to a multicast group in the group list.


```

Internet address is 192.168.36.129, subnet mask is 255.255.255.0
IGMP is enabled on interface
IGMP query interval is 60 seconds
Inbound IGMP access group is not set
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 192.168.36.131
Multicast groups joined: 225.2.2.2 226.2.2.2
Tunnel0 is up, line protocol is up
Internet address is 10.1.37.2, subnet mask is 255.255.0.0
IGMP is enabled on interface
IGMP query interval is 60 seconds
Inbound IGMP access group is not set
Multicast routing is enabled on interface
Multicast TTL threshold is 0
No multicast groups joined

```

Table 1 describes the significant fields shown in the display.

Table 1 *show ip igmp interface Field Descriptions*

Field	Description
Global IGMP state limit: 0 active out of 100 max	Global IGMP state limiting is configured to 100 with 0 current IGMP states.
Ethernet0 is up, line protocol is up	Interface type, number, and status.
Internet address is..., subnet mask is...	Internet address of the interface and subnet mask being applied to the interface, as specified with the ip address command.
IGMP is enabled on interface	Indicates whether IGMP has been enabled on the interface with the ip pim command.
Current IGMP host version is 2	Current IGMP version of the host.
Current IGMP router version is 2	Current IGMP version of the router.
IGMP query interval is 60 seconds	Interval, in seconds, at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages, as specified with the ip igmp query-interval command.
IGMP querier timeout is 120 seconds	Interval, in seconds, that the router waits after the previous querier has stopped querying and before it takes over as the querier.
IGMP max query response time is 10 seconds	The maximum response time, in seconds, advertised in IGMP queries.
Last member query count is 2	Number of responses received from the last IGMP query.
Last member query response interval is 1000 ms	Time interval, in milliseconds, of the response received after the last IGMP query.
Inbound IGMP access group is not set	Indicates whether an IGMP access group has been configured with the ip igmp access-group command.
IGMP activity:1 joins, 0 leaves	Number of IGMP joins and leaves.
Interface IGMP State Limit: 0 active out of 10 max	IGMP state limiting on this interface is configured to 10 with 0 current IGMP states.
Multicast routing is enabled on interface	Indicates whether multicast routing has been enabled on the interface with the ip pim command.

Table 1 *show ip igmp interface Field Descriptions (continued)*

Field	Description
Multicast TTL threshold is 0	Packet time-to-threshold, as specified with the ip multicast ttl-threshold command.
Multicast designated router (DR) is	IP address of the designated router for this LAN segment (subnet).
No multicast groups joined	Indicates whether this interface is a member of any multicast groups and, if so, lists the IP addresses of the groups.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip igmp limit (global)	Globally limits the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership states.
ip igmp limit (interface)	Limits the number of IGMP states resulting from IGMP, IGMP v3lite, and URD membership states on a per-interface basis.
ip igmp access-group	Controls the multicast groups that hosts on the subnet serviced by an interface can join.
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.
ip multicast ttl-threshold	Configures the TTL threshold of packets being forwarded out an interface.
ip pim	Enables PIM on an interface.

Glossary

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

IGMPv3—IGMP Version 3. Adds support in Cisco IOS software 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 sources this traffic is expected.

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

SSM—Source Specific Multicast. An extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined.

URD—URL Rendezvous Directory. 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).

**Note**

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