# C through ip igmp

# clear ip cgmp

To clear all group entries from the caches of Catalyst switches, use the **clear ip cgmp** command in privileged EXEC mode.

**clear ip cgmp** [*interface-type interface-number*]

## Syntax Description

| | |
|---|---|
| *interface-type interface-number* | (Optional) Interface type and number. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command sends a Cisco Group Management Protocol (CGMP) leave message with a group address of 0000.0000.0000 and a unicast address of 0000.0000.0000. This message instructs the switches to clear all group entries they have cached.

If an interface type and number are specified, the leave message is sent only on that interface. Otherwise, it is sent on all CGMP-enabled interfaces.

## Examples

The following example clears the CGMP cache:

```
Router# clear ip cgmp
```

## Related Commands

| Command | Description |
|---|---|
| **ip cgmp** | Enables CGMP on an interface of a router connected to a Catalyst 5000 switch. |

# clear ip msdp peer

To clear the TCP connection to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **clear ip msdp peer** command in privileged EXEC mode.

**clear ip msdp**[**vrf** *vrf-name*]**peer**{*peer-address*| *peer-name*}

## Syntax Description

| | |
|---|---|
| **vrf** | (Optional) Supports the multicast VPN routing and forwarding (VRF) instance. |
| *vrf-name* | (Optional) Name assigned to the VRF. |
| *peer-address* \| *peer-name* | IP address or name of the MSDP peer to which the TCP connection is cleared. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |
| 12.0(23)S | The **vrf** keyword and *vrf-name* argument were added. |
| 12.2(13)T | The **vrf** keyword and *vrf-name* argument were added. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command closes the TCP connection to the peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

## Examples

The following example shows how to clear the TCP connection to the MSDP peer at 10.3.32.154:

```
Router# clear ip msdp peer 10.3.32.154
```

## Related Commands

| Command | Description |
|---|---|
| **ip msdp peer** | Configures an MSDP peer. |

# clear ip msdp sa-cache

To clear Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache entries, use the **clear ip msdp sa-cache** command in privileged EXEC mode.

**clear ip msdp** [**vrf** *vrf-name*] **sa-cache** [*group-address*| *group-name*]

## Syntax Description

| | |
|---|---|
| **vrf** | (Optional) Supports the multicast VPN routing and forwarding (VRF) instance. |
| *vrf-name* | (Optional) Name assigned to the VRF. |
| *group-address* \| *group-name* | (Optional) Multicast group address or name for which SA entries are cleared from the SA cache. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |
| 12.0(23)S | The **vrf** keyword and *vrf-name* argument were added. |
| 12.2(13)T | The **vrf** keyword and *vrf-name* argument were added. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

In order to have any SA entries in the cache to clear, SA caching must have been enabled with the **ip msdp cache-sa-state** command.

If no multicast group is identified by group address or name, all SA cache entries are cleared.

## Examples

The following example shows how to clear the SA entries for the multicast group 10.3.50.152 from the cache:

```
Router# clear ip msdp sa-cache 10.3.50.152
```

## Related Commands

| Command | Description |
|---|---|
| **ip host** | Configures an MSDP peer. |
| **ip msdp cache-sa-state** | Enables the router to create SA state. |
| **show ip msdp sa-cache** | Displays (S, G) state learned from MSDP peers. |

# clear ip msdp statistics

To clear statistics counters for one or all of the Multicast Source Discovery Protocol (MSDP) peers without resetting the sessions, use the **clear ip msdp statistics** command in privileged EXEC mode.

**clear ip msdp**[**vrf** *vrf-name*]**statistics**{*peer-address*| *peer-name*}

## Syntax Description

| | |
|---|---|
| **vrf** | (Optional) Supports the multicast VPN routing and forwarding (VRF) instance. |
| *vrf-name* | (Optional) Name assigned to the VRF. |
| *peer-address* \| *peer-name* | (Optional) Address or name of the MSDP peers whose statistics counters, reset count, and input/output count are cleared. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |
| 12.0(23)S | The **vrf** keyword and *vrf-name* argument were added. |
| 12.2(13)T | The **vrf** keyword and *vrf-name* argument were added. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Examples

The following example shows how to clear the counters for the peer named peer1:

```
Router# clear ip msdp statistics peer1
```

## Related Commands

| Command | Description |
|---|---|
| **show ip msdp sa-cache** | Displays (S, G) state learned from MSDP peers. |

# ip cgmp

To enable Cisco Group Management Protocol (CGMP) on an interface of a router connected to a Cisco Catalyst switch, use the ip cgmp command in interface configuration mode. To disable CGMP routing, use the no form of this command.

**ip cgmp** [**proxy**| **router-only**]

**no ip cgmp**

## Syntax Description

| | |
|---|---|
| **proxy** | (Optional) Enables CGMP and the CGMP proxy function. |
| router-only | (Optional) Enables the router to send only CGMP self-join and CGMP self-leave messages. |

## Command Default

CGMP is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.2 | The **router-only** keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When enabled on an interface, this command triggers a CGMP join message. This command should be used only on 802 media (that is, Ethernet, FDDI, or Token Ring) or ATM. When a no **ip cgmp** command is issued, a triggered CGMP leave message is sent for the MAC address on the interface for group 0000.0000.0000 (all groups). CGMP can run on an interface only if Protocol Independent Multicast (PIM) is configured on the same interface.

A Cisco router will send CGMP join messages in response to receiving Internet Group Management Protocol (IGMP) reports from IGMP-capable members. Only the CGMP querier Cisco router sends these CGMP join messages on behalf of hosts.

The **ip cgmp router-only** command enables the routers in a VLAN to send only CGMP self-join and CGMP self-leave messages--no other types of CGMP messages will be sent. This feature allows other CGMP-capable routers to learn about multicast router ports. If the **ip cgmp router-only** command is not available on any of the external routers in the network, the **ip cgmp** command can be used instead. Issuing the **ip cgmp** command on a router enables that router to send CGMP self-join and CGMP self-leave messages as well as other types of CGMP messages.

When the **proxy** keyword is specified, the CGMP proxy function is also enabled. That is, any router that is not CGMP-capable will be advertised by the proxy router. The proxy router advertises the existence of other non-CGMP-capable routers by sending a CGMP join message with the MAC address of the non-CGMP-capable router and a group address of 0000.0000.0000.

Initially supported is Distance Vector Multicast Routing Protocol (DVMRP) proxying. If a DVMRP report is received from a router that is not a PIM router, a Cisco IGMP querier will advertise the MAC address of the DVMRP router in a CGMP join message with the group address 0000.0000.0000.

To perform CGMP proxy, a Cisco router must be the IGMP querier. If you configure the **ip cgmp proxy** command, you must manipulate the IP addresses so that a Cisco router will be the IGMP querier, which might be the highest or lowest IP address, depending on which version of IGMP is being run on the network. An IGMP Version 2 querier is selected based on the lowest IP addressed router on the interface. An IGMP Version 1 querier is selected based on the multicast routing protocol used on the interface.

When multiple Cisco routers are connected to a switched network and the **ip cgmp proxy** command is needed, we recommend that all routers be configured in the following manner:

- With the same CGMP option.
- To have precedence of becoming IGMP querier over non-Cisco routers.

## Examples

The following example enables CGMP:

```
ip cgmp
```

The following example enables CGMP and CGMP proxy:

```
ip cgmp proxy
```

# ip igmp access-group

To restrict hosts (receivers) on a subnet to joining only multicast groups that are permitted by a standard IP access list or to restrict hosts (receivers) on a subnet to membership to only the (S,G) channels that are permitted by an extended IP access list, use the **ip igmp access-group** command in interface configuration mode. To disable this control, use the **no** form of this command.

**ip igmp access-group** *access-list*

**no ip igmp access-group** *access-list*

## Syntax Description

| | |
|---|---|
| *access-list* | Access list number or name. |

## Command Default

Disabled (no access lists are configured for receiver access control).

## Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.3(7)T | Extended access list support was added. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |

## Usage Guidelines

Use the **ip igmp access-group** command to filter groups from Internet Group Management Protocol (IGMP) reports by use of a standard access list or to filter sources and groups from IGMPv3 reports by use of an extended access list. This command is used to restrict hosts on a subnet to joining only multicast groups that are permitted by a standard IP access list or to restrict hosts on a subnet to membership to only those (S, G) channels that are permitted by an extended IP access list.

IGMP Version 3 (IGMPv3) accommodates extended access lists, which allow you to leverage an important advantage of Source Specific Multicast (SSM) in IPv4, that of basing access on source IP address. Prior to

this feature, an IGMP access list accepted only a standard access list, allowing membership reports to be filtered based only on multicast group addresses.

IGMPv3 allows multicast receivers not only to join to groups, but to groups including or excluding sources. For appropriate access control, it is therefore necessary to allow filtering of IGMPv3 messages not only by group addresses reported, but by group and source addresses. IGMP extended access lists introduce this functionality. Using SSM with an IGMP extended access list allows you to permit or deny source S and group G (S, G) in IGMPv3 reports, thereby filtering SSM traffic based on source address, group address, or both.

**Source Addresses in IGMPv3 Reports for ASM Groups**

Additionally, IGMP extended access lists can be used to permit or filter traffic based on (0.0.0.0, G); that is, (*, G), in IGMP reports that are non-SSM, such as Any Source Multicast (ASM).

**Note** The permit and deny statements equivalent to (*, G) are **permit host 0.0.0.0 host** *group-address* and **deny host 0.0.0.0 host group** *group-address*, respectively.

Filtering applies to IGMPv3 reports for both ASM and SSM groups, but it is most important for SSM groups because multicast routing ignores source addresses in IGMPv3 reports for ASM groups. Source addresses in IGMPv3 membership reports for ASM groups are stored in the IGMP cache (as displayed with the **show ip igmp membership** command), but PIM-based IP multicast routing considers only the ASM groups reported. Therefore, adding filtering for source addresses for ASM groups impacts only the IGMP cache for ASM groups.

**How IGMP Checks an Extended Access List**

When an IGMP extended access list is referenced in the **ip igmp access-group** command on an interface, the (S, G) pairs in the permit and deny statements of the extended access list are matched against the (S, G) pair of the IGMP reports received on the interface. The first part of the extended access list clause controls the source, and the second part of the extended access list clause controls the multicast group.

Specifically, if an IGMP report with (S1, S2...Sn, G) is received, first the group (0, G) is checked against the access list statements. If the group is denied, the entire IGMP report is denied. If the group is permitted, each individual (S, G) pair is checked against the access list. Denied sources are taken out of the IGMP report, thereby denying any sources that match the access list from sending to the group.

**Note** The convention (0, G) means (*, G), which is a wildcard source with a multicast group number.

## Examples

The following example shows how to configure a standard access list to filter the groups that are available on an interface for receivers to join. In this example, Ethernet interface 1/3 is configured to restrict receivers from joining groups in the range 226.1.0.0 through 226.1.255.255. Receivers are permitted to join all other groups on Ethernet interface 1/3.

```
access-list 1 deny 226.1.0.0 0.0.255.255
access-list 1 permit any log
!
interface ethernet 1/3
 ip igmp access-group 1
```

**Note** Access lists are very flexible; there is a seemingly limitless combination of permit and deny statements one could use in an access list to filter multicast traffic. The examples in this section simply provide a few examples of how it can be done.

The following example shows how to deny all states for a group G. In this example, FastEthernet interface 0/0 is configured to filter all sources for SSM group 232.2.2.2 in IGMPv3 reports, which effectively denies this group.

```
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface FastEthernet0/0
 ip igmp access-group test1
!
```

The following example shows how to deny all states for a source S. In this example, Ethernet interface 1/1 is configured to filter all groups for source 10.2.1.32 in IGMPv3 reports, which effectively denies this source.

```
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface Ethernet1/1
 ip igmp access-group test2
```

The following example shows how to permit all states for a group G. In this example, Ethernet interface 1/1 is configured to accept all sources for SSM group 232.1.1.10 in IGMPv3 reports, which effectively accepts this group altogether.

```
ip access-list extended test3
 permit igmp any host 232.1.1.10
!
interface Ethernet1/1
 ip igmp access-group test3
```

The following example shows how to permit all states for a source S. In this example, Ethernet interface 1/2 is configured to accept all groups for source 10.6.23.32 in IGMPv3 reports, which effectively accepts this source altogether.

```
!
ip access-list extended test4
 permit igmp host 10.6.23.32 any
!
interface Ethernet1/2
 ip igmp access-group test4
!
```

The following example shows how to filter a particular source S for a group G. In this example, Ethernet interface 0/3 is configured to filter source 232.2.2.2 for SSM group 232.2.30.30 in IGMPv3 reports.

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface Ethernet0/3
 ip igmp access-group test5
```

# ip igmp helper-address

To cause the system to forward all Internet Group Management Protocol ( IGMP) host reports and leave messages received on the interface to the specified IP address, use the **ip igmp helper-address**command in interface configuration mode. To disable such forwarding, use the **no** form of this command.

**ip igmp helper-address** *ip-address*

**no ip igmp helper-address**

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address to which IGMP host reports and leave messages are forwarded . Specify the IP address of an interface on the central router. |

## Command Default

IGMP host reports and leave messages are not forwarded.

## Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 11.2 F | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |

## Usage Guidelines

This command and the **ip pim neighbor-filter** command together enable stub multicast routing. The IGMP host reports and leave messages are forwarded to the IP address specified. The reports are re-sent out the next hop interface toward the IP address, with the source address of that interface. This command enables a type of "dense-mode" join, allowing stub sites not participating in Protocol Independent Multicast (PIM) to indicate membership in IP multicast groups.

## Examples

The following example enables stub multicast routing on Router A, which has an outgoing interface with IP address 10.0.0.1. Router B is a central router with an incoming interface with address 10.0.0.2. Access list 1 filters PIM messages from the source (stub Router A).

## Examples

```
ip multicast-routing
 ip pim dense-mode
 ip igmp helper-address 10.0.0.2
```

## Examples

```
ip multicast-routing
 ip pim dense-mode : or ip pim sparse-mode
 ip pim neighbor-filter 1
access-list 1 deny 10.0.0.1
```

## Related Commands

| Command | Description |
|---|---|
| **ip pim neighbor-filter** | Prevents a router from participating in PIM (for example, to configure stub multicast routing). |

# ip igmp limit (global)

To configure a global limit on the number of multicast route (mroute) states created as a result of Internet Group Management Protocol (IGMP) membership reports (IGMP joins), use the **ip igmp limit** command in global configuration mode. To remove the limit imposed by the global IGMP state limiter, use the **no** form of this command.

**ip igmp limit** *number*

**no ip igmp limit** *number*

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of IGMP membership reports that can be cached. The range is from 1 to 64000. |

## Command Default

A global IGMP state limiter is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(14)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to configure a global limit on the number of mroute states created as a result of IGMP membership reports (IGMP joins). When configured globally, the limit is referred to as a global IGMP state limiter. Membership reports exceeding the configured limits are not entered into the IGMP cache. This command can be used to prevent DoS attacks.

**Note** IGMP state limiters impose limits on the number of mroute states resulting from IGMP, IGMP v3lite, and URL Rendezvous Directory (URD) membership reports on a global or per interface basis.

Use the **ip igmp limit** (interface)command to configure a per interface limit on the number mroute states created as a result of IGMP membership reports (IGMP joins).

**Note** When configuring IGMP state limiters, you can only configure one global limit on a router and one limit per interface.

The mechanics of IGMP state limiters are as follows:

- Each time a router receives an IGMP membership report for a particular group or channel, the Cisco IOS software checks to see if either the limit for the global IGMP state limiter or the limit for the per interface IGMP state limiter has been reached.
  - If only a global IGMP state limiter has been configured and the limit has not been reached, IGMP membership reports are honored. When the configured limit has been reached, subsequent IGMP membership reports are then ignored (dropped) and a warning message in one of the following formats is generated:

```
%IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on <interface
 type number> by host <ip address>
```

or

```
%IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address, group address)>
 on <interface type number> by host <ip address>
```

  - If only per interface IGMP state limiters are configured, then each limit is only counted against the interface on which it was configured.
  - If both a global IGMP state limiter and per interface IGMP state limiters are configured, the limits configured for the per interface IGMP state limiters are still enforced but are constrained by the global limit.

- If a per interface IGMP state limiter has been configured using the **ip igmp limit** (interface) command, the Cisco IOS software also checks to see if an access control list (ACL) is specified (with the optional **except** keyword and *access-list* argument) to prevent groups or channels from being counted against the interface limit.
  - If an ACL has been configured and the group or channel in the IGMP membership report matches, then the state for the IGMP membership is counted against the global limit and not the interface limit.
  - If no ACL has been configured, the per interface IGMP state limiter accounts for all IGMP membership reports that do not exceed the configured limit.

## Examples

The following example shows how to configure a global IGMP state limiter that limits the number of mroute states created as result of IGMP membership reports to 300:

```
ip igmp limit 300
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp limit (interface)** | Limits the number of mroute states created as a result of IGMP membership reports on a per interface basis. |

| Command | Description |
|---|---|
| **show ip igmp groups** | Displays information about the status and configuration of IGMP and multicast routing on interfaces. |

# ip igmp limit (interface)

To configure a per interface limit on the number of multicast route (mroute) states created as a result of Internet Group Management Protocol (IGMP) membership reports (IGMP joins), use the **ip igmp limit** command in interface configuration mode. To remove the limit imposed by a per interface IGMP state limiter, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of IGMP states allowed on a router or interface. The range is from 1 to 64000. |
| **except** *access-list* | (Optional) Prevent groups or channels from being counted against the interface limit. A standard or an extended access control list (ACL) can be specified for the *access-limit* argument.<br>• A standard ACL can be used to define the (*, G) state to be excluded from the limit on an interface.<br>• An extended ACLs can be used to define the (S, G) state to be excluded from the limit on an interface. An extended ACL also can be used to define the (*, G) state to be excluded from the limit on an interface, by specifying 0.0.0.0 for the source address and source wildcard--referred to as (0, G)--in the permit or deny statements that compose the extended access list. |

## Command Default

No per interface IGMP state limiters are configured.

## Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 12.2(14)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |

## Usage Guidelines

Use this command to configure per interface limits on the number mroute states created as a result of IGMP membership reports (IGMP joins). When configured on an interface, the limit is referred to as a *per interface IGMP state limiter* . Membership reports exceeding the configured limits for the interface are not entered into the IGMP cache. This command can be used to prevent DoS attacks or to provide a multicast Call Admission Control (CAC) mechanism in network environments where all the multicast flows roughly utilize the same amount of bandwidth.

**Note** IGMP state limiters impose limits on the number of mroute states resulting from IGMP, IGMP v3lite, and URD membership reports on a global or per interface basis.

For the required *number* argument, specify a limit on the number of IGMP membership reports that can be cached for the specified interface. The range is from 1 to 64000.

Use the optional except access-list keyword and argument to prevent groups or channels from being counted against the interface limit. A standard or an extended ACL can be specified.

- • A standard ACL can be used to define the (*, G) state to be excluded from the limit on an interface.
  - An extended ACLs can be used to define the (S, G) state to be excluded from the limit on an interface. An extended ACL also can be used to define the (*, G) state to be excluded from the limit on an interface, by specifying 0.0.0.0 for the source address and source wildcard--referred to as (0, G)--in the permit or deny statements that compose the extended access list.

Use the **ip igmp limit** (global)command to configure a global limit on the number of mroute states created as a result of IGMP membership reports (IGMP joins).

**Note** When configuring IGMP state limiters, you can only configure one global limit on a router and one limit per interface.

The mechanics of IGMP state limiters are as follows:

- Each time a router receives an IGMP membership report for a particular group or channel, the Cisco IOS software checks to see if either the limit for the global IGMP state limiter or the limit for the per interface IGMP state limiter has been reached.
  - If only a global IGMP state limiter has been configured and the limit has not been reached, IGMP membership reports are honored. When the configured limit has been reached, subsequent IGMP

membership reports are then ignored (dropped) and a warning message in one of the following formats is generated:

```
%IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on <interface
 type number> by host <ip address>
```

or

```
%IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address, group address)>
 on <interface type number> by host <ip address>
```

- • If only per interface IGMP state limiters are configured, then each limit is only counted against the interface on which it was configured.
  - If both a global IGMP state limiter and per interface IGMP state limiters are configured, the limits configured for the per interface IGMP state limiters are still enforced but are constrained by the global limit.
- If a per interface IGMP state limiter has been configured using the **ip igmp limit** (interface) command, the Cisco IOS software also checks to see if an ACL is specified (with the optional **except** keyword and *access-list* argument) to prevent groups or channels from being counted against the interface limit.
  - If an ACL has been configured and the group or channel in the IGMP membership report matches, then the state for the IGMP membership is counted against the global limit and not the interface limit.
  - If no ACL has been configured, the per interface IGMP state limiter accounts for all IGMP membership reports that do not exceed the configured limit.

## Examples

The following example shows how configure a per interface limiter that limits the number of mroute states created as result of IGMP membership reports on Gigabit Ethernet interface 0/1 to 100:

```
interface GigabitEthernet 0/1
 ip igmp limit 100
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp limit (global)** | Globally limits the number of IGMP states resulting from IGMP membership reports (IGMP joins). |
| **show ip igmp groups** | Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP. |
| **show ip igmp interface** | Displays information about the status and configuration of IGMP and multicast routing on interfaces. |

# ip igmp mroute-proxy

To enable Internet Group Management Protocol (IGMP) report forwarding of proxied (*, G) multicast static route (mroute) entries, use the **ip igmp mroute-proxy** command in interface configuration mode. To disable this service, use the **no** form of this command.

**ip igmp mroute-proxy** *interface-type interface-number*

**no ip igmp mroute-proxy** *interface-type interface-number*

## Syntax Description

| | |
|---|---|
| *interface-type interface-number* | Interface type and number. |

## Command Default

The command is disabled.

## Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |

## Usage Guidelines

When used with the **ip igmp proxy-service** interface command, this command enables forwarding of IGMP reports to a proxy service interface for all (*, G) forwarding entries for this interface in the multicast forwarding table.

## Examples

The following example shows how to configure the **ip igmp mroute-proxy** command on Ethernet interface 1 to request that IGMP reports be sent to loopback interface 0 for all groups in the mroute table that are forwarded to Ethernet interface 1. This example also shows how to configure the **ip igmp proxy-service** command on loopback interface 0 to enable the forwarding of IGMP reports out the interface for all groups on interfaces registered through the **ip igmp mroute-proxy** command.

```
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim dense-mode
```

```
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
interface ethernet 0
ip address 10.2.1.1 255.255.255.0
ip pim dense-mode
ip igmp unidirectional link
!
interface ethernet 1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp proxy-service** | Enables the mroute proxy service. |
| **ip igmp unidirectional-link** | Configures an interface to be unidirectional and enables it for IGMP UDLR. |

# ip igmp proxy-service

To enable the mroute proxy service, use the **ip igmp proxy-service** command in interface configuration mode. To disable forwarding, use the **no** form of this command.

**ip igmp proxy-service**

**no ip igmp proxy-service**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The command is disabled.

## Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |

## Usage Guidelines

Based on the Internet Group Management Protocol (IGMP) query interval, the router periodically checks the multicast static route (mroute) table for (*, G) forwarding entries that match interfaces configured with the **ip igmp mroute-proxy** command. Where there is a match, one IGMP report is created and received on this interface. The **ip igmp proxy-service**command is intended to be used with the **ip igmp helper-address (UDL)** command, in which case the IGMP report would be forwarded to an upstream router.

## Examples

The following example shows how to configure the **ip igmp mroute-proxy** command on Ethernet interface 1 to request that IGMP reports be sent to loopback interface 0 for all groups in the mroute table that are forwarded to Ethernet interface 1. This example also shows how to configure the **ip igmp proxy-service** command on loopback interface 0 to enable the forwarding of IGMP reports out the interface for all groups on interfaces registered through the **ip igmp mroute-proxy** command.

```
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim dense-mode
ip igmp helper-address udl ethernet 0
```

```
ip igmp proxy-service
!
interface ethernet 0
ip address 10.2.1.1 255.255.255.0
ip pim dense-mode
ip igmp unidirectional link
!
interface ethernet 1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp helper-address (UDL)** | Configures IGMP helpering as required for IGMP UDLR. |
| **ip igmp mroute-proxy** | Enables IGMP report forwarding of proxied (*, G) mroute entries. |
| **ip igmp unidirectional-link** | Configures an interface to be unidirectional and enables it for IGMP UDLR. |

# ip igmp snooping

To enable Internet Group Management Protocol (IGMP) snooping globally or on an interface, use the **ip igmp snooping** command in the global configuration mode, interface configuration, or bridge domain configuration mode. To disable IGMP snooping, use the **no** form of this command.

**ip igmp snooping**

**no ip igmp snooping**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IGMP snooping is enabled globally.

## Command Modes

Global configuration (config)

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

## Command History

| Release | Modification |
|---|---|
| 12.0(5.2)WC(1) | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(14)SX | Support for this command was implemented on the Supervisor Engine 720. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S. Support for this command was added to the bridge domain configuration mode. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all existing VLAN interfaces.

When IGMP snooping is globally disabled, IGMP snooping is disabled on all existing bridge domain interfaces. When IGMP snooping is globally enabled, IGMP snooping is enabled on all existing bridge domain interfaces unless IGMP snooping was also explicitly disabled on a specific bridge domain interface. When IGMP

snooping is disabled globally and on a specific bridge domain interface, globally enabling IGMP snooping will not enable snooping on the bridge domain interface; it must be explicitly re-enabled on the bridge domain interface.

Use the **show ip igmp snooping** privileged EXEC command to verify your IGMP settings.

The configuration is saved in NVRAM.

**For Cisco 7600 series routers:** Before you can enable IGMP snooping for Cisco 7600 series routers, you must configure the VLAN interface for multicast routing.

## Examples

The following examples show how to globally disable IGMP snooping and how to disable IGMP snooping on a specified bridge domain interface:

```
Router(config)# no ip igmp snooping
Router(config)# exit
Router# show running-config
.
.
.
no ip igmp snooping
Router(config)# bridge-domain1
Router(config-bdomain)# no ip igmp snooping
Router(config-bdomain)# end
Router# show running-config
.
.
.
bridge-domain 1
 no ip igmp snooping
!
!
```

The following example shows how to globally enable IGMP snooping after it was explicitly disabled:

```
Router(config)# ip igmp snooping
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping fast-leave** | Enables the IGMPv3-snooping fast-leave processing. |
| **ip igmp snooping vlan** | Enables IGMP snooping on a VLAN interface. |
| **ip igmp snooping vlan immediate-leave** | Enables IGMP Immediate-Leave processing. |
| **ip igmp snooping vlan mrouter** | Configures a Layer 2 port as a multicast router port. |
| **ip igmp snooping vlan static** | Configures a Layer 2 port as a member of a group. |
| **show ip igmp snooping** | Displays the IGMP snooping configuration. |

# ip igmp snooping last-member-query-interval

To configure the last member query interval for IGMP snooping, use the **ip igmp snooping last-member-query-interval** command in the interface configuration or bridge domain configuration mode. To return to the default settings, use the **no** form of this command.

**ip igmp snooping last-member-query-interval** *interval*

**no ip igmp snooping last-member-query-interval**

## Syntax Description

| | |
|---|---|
| *interval* | Length of time, in milliseconds, after which the group record is deleted if no reports are received. The default is 1000. See the "Usage Guidelines" section for more information.<br>For interfaces, the range is from 100 to 999, in multiples of 100. If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.<br>For bridge domain interfaces, the range is from 100 to 32767. |

## Command Default

The default interval is 1000 milliseconds (1 second).

## Command Modes

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | This command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was integrated into Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S. Support for this command was added to the bridge domain configuration mode. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-count** command to specify how often an IGMP query is sent in response to receiving an IGMP leave message.

The *interval* is the actual time that the Cisco 7600 series router waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no igmp snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of 1000. If you want this value, you must enter the **no ip igmp snooping last-member-query-interval** command to return to the default value (1000 milliseconds).

## Examples

This example shows how to configure the last-member-query-interval to 200 milliseconds:

```
Router(config-if)#
ip igmp snooping last-member-query-interval 200
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping fast-leave** | Enables the IGMP v3-snooping fast-leave processing. |
| **ip igmp snooping last-member-query-count** | Configures the interval for snooping queries sent. |
| **show ip igmp interface** | Displays the information about the IGMP-interface status and configuration. |

# ip igmp snooping report-suppression

To turn on IP IGMP snooping report suppression, use the **ip igmp snooping report-suppression** command in the global configuration, interface configuration, or bridge domain configuration mode. To turn off report suppression, use the **no** form of this command.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IGMP snooping report supression is disabled.

## Command Modes

Global configuration (config)

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S. Support for this command was added to the bridge domain configuration mode. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |

## Usage Guidelines

Use this command to enable report supression for all host reports responding to a general query or for all host reports on an interface or a bridge domain.

When you enable report suppression for all host reports responding to a general query, IP IGMP snooping forwards the first report only and suppresses the remaining reports to constrain IGMP traffic to the multicast router.

## Examples

This example shows how to enable IP IGMP snooping report suppression:

```
Router(config-if)# ip igmp snooping report-suppression
```

This example shows how to disable IP IGMP snooping report suppression:

```
Router(config-bdomain)# no ip igmp snooping report-suppression
```

# ip igmp snooping vlan

To enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN, use the **ip igmp snooping vlan**command in global configuration mode. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.

**ip igmp snooping vlan** *vlan-id*

**no ip igmp snooping vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN ID value. The range is from 1 to 1001. Do not enter leading zeroes. |

## Command Default

By default, IGMP snooping is enabled when each VLAN is created.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5.2)WC(1) | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |

## Usage Guidelines

This command automatically configures the VLAN if it is not already configured. The configuration is saved in NVRAM.

## Examples

The following example shows how to enable IGMP snooping on VLAN 2:

```
Router(config)# ip igmp snooping vlan 2
```

The following example shows how to disable IGMP snooping on VLAN 2:

```
Router(config)# no
 ip igmp snooping vlan 2
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping** | Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN. |
| **ip igmp snooping vlan immediate-leave** | Enables IGMP Immediate-Leave processing. |
| **ip igmp snooping vlan mrouter** | Configures a Layer 2 port as a multicast router port. |
| **ip igmp snooping vlan static** | Configures a Layer 2 port as a member of a group. |
| **show ip igmp snooping** | Displays the IGMP snooping configuration. |

# ip igmp snooping vlan immediate-leave

To enable Internet Group Management Protocol (IGMP) Immediate-Leave processing on a VLAN interface, use the **ip igmp snooping vlan immediate-leave**command in global configuration mode. To disable Immediate-Leave processing on the VLAN interface, use the **no** form of this command.

**ip igmp snooping vlan** *vlan-id* **immediate-leave**

**no ip igmp snooping vlan** *vlan-id* **immediate-leave**

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN ID value. The range is between 1 to 1001. Do not enter leading zeroes. |

## Command Default

By default, IGMP Immediate-Leave processing is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5.2)WC(1) | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |

## Usage Guidelines

Use Immediate-Leave processing only when there is only one IP multicast receiver present on every port in the VLAN. The Immediate-Leave configuration is saved in NVRAM.

Immediate-Leave processing is supported only with IGMP version 2 hosts.

## Examples

The following example shows how to enable IGMP Immediate-Leave processing on VLAN 1:

```
Router(config)# ip igmp snooping vlan 1 immediate-leave
```

The following example shows how to disable IGMP Immediate-Leave processing on VLAN 1:

```
Router(config)# no
 ip igmp snooping vlan 1 immediate-leave
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping** | Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN. |
| **ip igmp snooping vlan mrouter** | Configures a Layer 2 port as a multicast router port. |
| **ip igmp snooping vlan static** | Configures a Layer 2 port as a member of a group. |
| **show ip igmp snooping** | Displays the IGMP snooping configuration. |
| **show mac-address-table multicast** | Displays the Layer 2 multicast entries for a VLAN. |

# ip igmp snooping vlan mrouter

To add a multicast router port and to configure the multicast router learning method, use the **ip igmp snooping vlan mrouter**command in global configuration mode. To remove the configuration, use the **no** form of this command.

**ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id*| **learn pim-dvmrp**}

**no ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id*| **learn pim-dvmrp**}

## Syntax Description

| | |
|---|---|
| *vlan-id* | Specifies the VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes. |
| **interface** *interface-id* | Specifies the interface of the member port that is configured to a static router port. |
| **learn pim-dvmrp** | Specifies the multicast router snooping PIM-DVMRP packets multicast router learning method. |

## Command Default

The default learning method is **pim-dvmrp**.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5.2)WC(1) | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |

## Usage Guidelines

The configured learning method is saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

## Examples

The following example shows how to configure Fast Ethernet interface 0/6 as a multicast router port:

```
Router(config)# ip igmp snooping vlan 1 mrouter interface fastethernet0/6
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping** | Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN. |
| **ip igmp snooping vlan** | Enables IGMP snooping on the VLAN interface. |
| **ip igmp snooping vlan immediate-leave** | Configures IGMP Immediate-Leave processing. |
| **ip igmp snooping vlan static** | Configures a Layer 2 port as a member of a group. |
| **show ip igmp snooping mrouter** | Displays the statically and dynamically learned multicast router ports. |

# ip igmp snooping vlan static

To add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static**command in global configuration mode. To remove the configuration, use the **no** form of this command.

**ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id*

**no ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | Specifies the VLAN ID. The range is 1 to 1001. Do not enter leading zeroes. |
| *mac-address* | Specifies the static group MAC address. |
| **interface** *interface-id* | Specifies the interface configured to a static router port. |

## Command Default

No Layer 2 ports are configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5.2)WC(1) | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |

## Usage Guidelines

This command is used to statically configure the IP multicast group member ports.

The static ports and groups are saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

Use the **show mac-address-table multicast**privileged EXEC command to verify your Layer 2 multicast entries.

## Examples

The following example shows how to statically configure a host on an interface:

```
Router(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface fastethernet0/6
Configuring port FastEthernet 0/6 on group 0100.5e02.0203
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping** | Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN. |
| **ip igmp snooping vlan** | Enables IGMP snooping on the VLAN interface. |
| **ip igmp snooping vlan immediate-leave** | Configures IGMP Immediate-Leave processing. |
| **ip igmp snooping vlan mrouter** | Configures a Layer 2 port as a multicast router port. |
| **show mac-address-table multicast** | Displays the Layer 2 multicast entries for a VLAN. |

# ip igmp static-group

To configure static group membership entries on an interface, use the **ip igmp static-group** command in interface configuration mode. To delete static group membership entries, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| ***** | Places the interface into all created multicast route (mroute) entries. |
| *group-address* | IP multicast group address to configure as a static group member on the interface. |
| **source** | (Optional) Statically forwards a (S, G) channel out of the interface. |
| *source-address* | (Optional) IP address of a system where multicast data packets originate. |
| **ssm-map** | (Optional) Configures Source Specific Multicast (SSM) mapping to be used on the interface to determine the source associated with this group. The resulting (S, G) channels are statically forwarded. |
| **class-map** *class-map-name* | Attaches an Internet Group Management Protocol (IGMP) static group range class map to the interface. |

## Command Default

No static group membership entries are configured on interfaces.

## Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.3(2)T | This command was modified. The **ssm-map** keyword was added. |
| 12.2(18)S | This command was modified. The **ssm-map** keyword was added. |
| 12.2(18)SXD3 | This command was integrated into Cisco IOS Release 12.2(18)SXD3. |

| Release | Modification |
|---|---|
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(18)SXF5 | This command was modified. The **class-map** keyword and *class-map-name* argument were added. |
| 15.0(1)M | This command was modified. The **class-map** keyword and *class-map-name* argument were added. |
| 12.2(33)SRE | This command was modified. The **class-map** keyword and *class-map-name* argument were added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |
| 15.0(1)SY | This command was integrated into Cisco IOS Release 15.0(1)SY. |
| 15.1(1)SG | This command was integrated into Cisco IOS Release 15.1(1)SG. |
| Cisco IOS XE Release 3.3SG | This command was integrated into Cisco IOS XE Release 3.3SG. |

## Usage Guidelines

Use the **ip igmp static-group** command to configure static group membership entries on an interface. When you configure this command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface. Once configured, static group membership entries are added to the IGMP cache and mroute table.

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

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

Use the **ip igmp static-group** command with the **ssm-map** keyword to configure static traffic forwarding with SSM mapping on the last hop router. Static traffic forwarding can be used in conjunction with SSM mapping to statically forward SSM traffic for certain groups. When static traffic forwarding with SSM mapping is configured, the last hop router uses Domain Name System (DNS)-based SSM mapping to determine the sources associated with a group. The resulting (S, G) channels are then statically forwarded.

Use the **ip igmp static-group class-map** command with the **class-map** keyword and *class-map-name* argument to attach an IGMP static group class map to an interface. Once attached, all groups entries that are defined in the class map become static members on the interface and are added to the IGMP cache and to the mroute table.

**For Cisco IOS Release 15.1(1)T and later releases**

The MFIB maintains a (*, G/m) entry that handles dense mode packets. When the first dense mode packet arrives on a router, it matches this (*, G/m) entry. The packet is punted to the route processor only if at least

one of the following two conditions is met: The source of the packet is directly connected to this router or the interface on which the packet was received has at least one PIM neighbor. If neither of these conditions is met, the (*, G/m) entry in the MFIB drops the packet without punting it. If the interface of a last hop router does not have any PIM neighbors and does not have a receiver, configure the **ip igmp static-group** command with the ***** keyword before any receiver joins (before any (*, G) state is created on the router) to simulate the presence of a receiver for all multicast group addresses on the interface, causing the interface to be added to the olist of the mroute entry and preventing incoming last hop router traffic for a dense mode group on the interface from being dropped.

## Examples

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

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

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

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

The following example shows how to attach an IGMP static group range class map named static1 to GigabitEthernet interface 1/1:

```
interface GigabitEthernet1/1
 ip igmp static-group class-map static1
```

## Related Commands

| Command | Description |
|---|---|
| **class-map type multicast-flows** | Enters multicast-flows class-map configuration mode to create or modify IGMP static group class maps. |
| **ip igmp join-group** | Causes the router to join a multicast group. |
| **ip igmp ssm-map enable** | Enables SSM mapping for groups in a configured SSM range. |
| **ip igmp ssm-map query dns** | Configures DNS-based SSM mapping. |
| **ip igmp ssm-map static** | Enables static SSM mapping. |
| **ip pim ssm** | Defines the SSM range of IP multicast addresses. |

# ip igmp unidirectional-link

To configure an interface to be unidirectional and enable it for Internet Group Management Protocol (IGMP) unidirectional link routing (UDLR), use the **ip igmp unidirectional-link**command in interface configuration mode. To disable the unidirectional link (UDL), use the **no** form of this command.

**ip igmp unidirectional-link**

**no ip igmp unidirectional-link**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No UDLR occurs.

## Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |

## Usage Guidelines

One example of when you might configure this command is if you have traffic traveling via a satellite.

If you have a small number of receivers, another way to achieve UDLR is to configure a UDLR tunnel. See the descriptions of the **tunnel udlr receive-only** and **tunnel udlr send-only** commands.

## Examples

The following example configures an upstream router with UDLR on serial interface 0:

```
ip multicast-routing
!
! Unidirectional link
!
interface serial 0
 description Unidirectional to downlink-rtr
 ip address 10.0.0.1 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp unidirectional-link
 no keepalive
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp helper-address (UDL)** | Configures IGMP helpering as required for IGMP UDLR. |
| **ip igmp mroute-proxy** | Enables IGMP report forwarding of proxied (*, G) mroute entries. |
| **ip igmp proxy-service** | Enables the mroute proxy service. |
| **ip multicast default-rpf-distance** | Changes the distance given to the default RPF interface when configuring IGMP UDLR. |
| **show ip igmp udlr** | Displays UDLR information for directly connected multicast groups on interfaces that have a UDL helper address configured. |
| **tunnel udlr receive-only** | Configures a unidirectional, GRE tunnel to act as a back channel that can receive messages, when another interface is configured for UDLR to send messages. |
| **tunnel udlr send-only** | Configures a unidirectional, GRE tunnel to act as a back channel that can send messages, when another interface is configured for UDLR to receive messages. |

# ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version**command in interface configuration mode. 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. This is the default. |
| **3** | IGMP Version 3. |

## Command Default

Version 2

## Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.1(5)T | The **3**keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 3.2S | This Bandwidth-Based Call Admission Control for IP Multicast command was modified. Support was added for this command in virtual network interface configuration mode. |
| 15.0(1)SY | This command was integrated into Cisco IOS Release 15.0(1)SY. |
| 15.1(1)SG | This command was integrated into Cisco IOS Release 15.1(1)SG. |
| Cisco IOS XE Release 3.3SG | This command was integrated into Cisco IOS XE Release 3.3SG. |

## Usage Guidelines

All routers on the subnet must support the same version. The router does not automatically detect Version 1 routers and switch to Version 1 as did earlier releases of the Cisco IOS software. Hosts can have any IGMP version (1, 2, or 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. |
| **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. |