ip igmp access-group through ip igmp v3lite

- ip igmp access-group, page 3
- ip igmp explicit-tracking, page 6
- ip igmp helper-address, page 8
- ip igmp helper-address (UDL), page 10
- ip igmp immediate-leave, page 12
- ip igmp immediate-leave group-list, page 14
- ip igmp join-group, page 16
- ip igmp last-member-query-count, page 19
- ip igmp last-member-query-interval, page 21
- ip igmp limit (global), page 23
- ip igmp limit (interface), page 26
- ip igmp mroute-proxy, page 29
- ip igmp proxy-service, page 31
- ip igmp querier-timeout, page 33
- ip igmp query-interval, page 36
- ip igmp query-max-response-time, page 39
- ip igmp snooping, page 41
- ip igmp snooping check, page 43
- ip igmp snooping access-group, page 44
- ip igmp snooping explicit-tracking, page 46
- ip igmp snooping explicit-tracking limit, page 48
- ip igmp snooping fast-leave, page 50
- ip igmp snooping flooding, page 52
- ip igmp snooping immediate-leave, page 53

- ip igmp snooping l2-entry-limit, page 55
- ip igmp snooping last-member-query-count, page 56
- ip igmp snooping last-member-query-interval, page 58
- ip igmp snooping limit, page 60
- ip igmp snooping limit track, page 63
- ip igmp snooping minimum-version, page 65
- ip igmp snooping mrouter, page 67
- ip igmp snooping querier, page 69
- ip igmp snooping rate, page 71
- ip igmp snooping report-suppression, page 72
- ip igmp snooping robustness-variable, page 73
- ip igmp snooping source-only-learning age-timer, page 74
- ip igmp snooping ssm-safe-reporting, page 76
- ip igmp snooping static, page 77
- ip igmp snooping tcn flood, page 80
- ip igmp snooping tnc flood query count, page 81
- ip igmp snooping tcn query solicit, page 82
- ip igmp snooping vlan, page 83
- ip igmp snooping vlan immediate-leave, page 85
- ip igmp snooping vlan mrouter, page 87
- ip igmp snooping vlan static, page 89
- ip igmp ssm-map, page 91
- ip igmp ssm-map enable, page 93
- ip igmp ssm-map query dns, page 95
- ip igmp ssm-map static, page 97
- ip igmp static-group, page 99
- ip igmp tcn query, page 102
- ip igmp unidirectional-link, page 104
- ip igmp v3lite, page 106
- ip igmp version, page 107

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 explicit-tracking

To enable explicit tracking of hosts, groups, and channels for Internet Group Management Protocol Version 3 (IGMPv3), use the **ip igmp explicit-tracking** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ip igmp explicit-tracking

no ip igmp explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit tracking of hosts, groups and channels for IGMPv3 is disabled.

Command Modes

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

Command History

Release	Modification
12.0(19)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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

Use the **ip igmp explicit-tracking** command to enable a multicast router to explicitly track the membership of multicast hosts in a particular multiaccess network. This capability enables the router to track each individual host that is joined to a particular group or channel and to achieve minimal leave latencies when hosts leave a multicast group or channel.

Note Before configuring the **ip igmp explicit-tracking** command, IGMP must be enabled (IGMP is enabled by enabling PIM on an interface using the **ip pim** command). In addition, IGMPv3 should be configured on the interface. To configure IGMPv3, use the **ip igmp version 3** command in interface configuration mode.

Note When explicit tracking is enabled, the router uses more memory than if explicit tracking is disabled because the router must store the membership state of all hosts on the interface.

To monitor the IGMP membership of hosts, use the **show ip igmp membership** command.

Examples

The following example shows how to enable explicit tracking. The example shows a basic configuration for enabling IP multicast with SSM, IGMPv3, and explicit tracking.

```
ip multicast-routing
interface ethernet 0
 description access network to desktop systems
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-dense-mode
 ip mroute-cache
 ip igmp version 3
 ip igmp explicit-tracking
interface ethernet 1
 description backbone interface no connected hosts
 ip address 10.10.0.1 255.255.255.0
 ip pim sparse-dense-mode
 ip mroute-cache
ip pim ssm default
```

Related Commands

Command	Description
ip igmp version	Configures the version of IGMP that the router uses.
ip pim	Enables PIM on an interface.
show ip igmp membership	Displays the IGMP membership information for multicast groups and (S, G) channels.

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 helper-address (UDL)

To configure Internet Group Management Protocol (IGMP) helpering as required for IGMP unidirectional link routing (UDLR), use the **ip igmp helper-address**command in interface configuration mode. To disable such report forwarding, use the **no** form of this command.

ip igmp helper-address udl *interface-type interface-number*

no ip igmp helper-address

Syntax Description

udl *interface-type interface-number*	Specifies the interface type and number of a unidirectional interface.

Command Default

No forwarding occurs.

Command Modes

Interface configuration

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.

Usage Guidelines

This command is required on a downstream router on each interface connected to a potential multicast receiver. The command allows the downstream router to helper IGMP reports received from hosts to an upstream router connected to a unidirectional link (UDL) associated with the configured *interface-type* and *interface-number*arguments.

Examples

The following example configures a helper address on a downstream router:

```
ip multicast-routing
!
! Interface that receiver is attached to, configure for IGMP reports to be
! helpered for the unidirectional interface.
!
interface ethernet 0
 description Forward IGMP reports from this interface to UDL querier
 ip address 10.0.0.2 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp helper-address udl serial 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 immediate-leave

To minimize the leave latency of Internet Group Management Protocol (IGMP) memberships when IGMP Version 2 is used and only one receiver host is connected to each interface, use the **ip igmp immediate-leave**command in global or interface configuration mode. To disable this feature, use the **no** form of this command.

ip igmp immediate-leave group-list *access-list*

no ip igmp immediate-leave

Syntax Description

group-list *access-list*	Specifies a standard access list number or name that defines multicast groups in which the immediate leave feature is enabled.

Command Default

This command is disabled.

Command Modes

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

Command History

Release	Modification
12.1	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.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

You cannot configure this command in both interface and global configuration mode.

When this command is not configured, the router will send an IGMP group-specific query message upon receipt of an IGMP Version 2 (IGMPv2) group leave message. The router will stop forwarding traffic for that group only if no host replies to the query within the timeout period. The timeout period is determined by the **ip igmp last-member-query-interval** command and the IGMP robustness variable, which is defined by the IGMP specification. By default, the timeout period in Cisco IOS software is approximately 2.5 seconds.

If this command is configured, the router assumes that only one host has joined the group and stops forwarding the group's traffic immediately upon receipt of an IGMPv2 group leave message.

Global Configuration Mode

When this command is configured in global configuration mode, it applies to all IGMP-enabled interfaces. Any existing configuration of this command in interface configuration mode will be removed from the configuration. Also, any new configuration of this command in interface configuration mode will be ignored.

Interface Configuration Mode

When this command is configured in interface configuration mode, it applies to an individual interface. Configure this command on an interface if only one IGMP-enabled neighbor is connected to the interface. The neighbor can be either a host or switch running IGMP Snooping. When the **ip igmp immediate-leave** command is enabled on an interface, the router will not send IGMP group-specific host queries when an IGMP Version 2 leave group message is received from that interface. Instead, the router will immediately remove the interface from the IGMP cache for that group and send Protocol Independent Multicast (PIM) prune messages toward sources if this interface was the last one to join that group.

Examples

The following example shows how to enable the immediate leave feature on all interfaces for all multicast groups:

```
Router(config)# ip multicast-routing
Router(config)# ip igmp immediate-leave group-list all-groups
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.10.1 255.255.255.0
Router(config-if)# ip pim sparse-dense mode
Router(config-if)# exit
Router(config)# ip access-list standard all-groups
Router(config)# permit 224.0.0.0 15.255.255.255
```

The following example shows how to enable the immediate leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the tv-groups access list consists of groups that have only one host membership at a time per interface:

```
Router(config)# ip multicast-routing
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.10.1 255.255.255.0
Router(config-if)# ip pim sparse-dense-mode
Router(config-if)# ip igmp immediate-leave group-list tv-groups
Router(config-if)# exit
Router(config)# ip access-list standard tv-groups
Router(config)# permit 239.192.20.0 0.0.0.255
```

Related Commands

Command	Description
ip igmp last-member-query-interval	Configures the frequency at which the router sends IGMP group-specific host query messages.

ip igmp immediate-leave group-list

To enable the immediate processing of the IGMP leave-group messages, use the **ip igmp immediate-leave group-list**command in global or interface configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp immediate-leave group-list *acl*

no ip igmp immediate-leave group-list *acl*

Syntax Description

acl	Specifies the group ACL number; see the “Usage Guidelines” section for valid values.

Command Default

Disabled

Command Modes

Global or interface configuration

Command History

Release	Modification
12.2(14)SX	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.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you enter the **ip igmp immediate-leave group-list**command, you must enter this command in VLAN interface configuration mode only.

Valid values for the *acl* argument are as follows:

- Access-list number--1 to 99
- Expanded range access-list number--1300 to 1999
- Name of the standard IP access list

You can configure one or the other but not both configuration modes at the same time.

You can enter the *acl* to restrict the immediate-leave behavior to a simple access list for multicast groups. The IGMP leave-group messages for multicast groups that are not permitted by the *acl* has the standard inquiry mechanism/leave latency.

Examples

This example shows how to enable the immediate processing of the IGMP leave-group messages:

```
Router(config)# ip igmp immediate-leave group-list 3
```

ip igmp join-group

To configure an interface on the router to join the specified group or channel, use the **ip igmp join-group** command in interface configuration mode. To cancel membership in a multicast group, use the **no** form of this command.

ip igmp join-group *group-address* [**source** *source-address*]

no ip igmp join-group *group-address* [**source** *source-address*]

Syntax Description

group-address	Multicast group address.
source *source -address*	(Optional) Specifies a multicast source address. This keyword and argument pair can be used to enable the router to provide INCLUDE mode capability for the (S, G) channel specified for the *group-address*and *source-address* arguments.

Command Default

No multicast group memberships are predefined.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	This command was modified. The **source** keyword and *source-address* argument were 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.
12.2(33)SRE	This command was modified. The **source** keyword and *source-address* argument were added.
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.

Release	Modification
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **ip igmp join-group** command to configure an interface on the router to join the specified group or channel. With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching.

In support of the IGMPv3 Host Stack feature, the **source** keyword and *source-address* argument were added to the **ip igmp join-group** command to add INCLUDE mode capability to the IGMPv3 host stack for SSM groups.

The IGMPv3 Host Stack feature enables routers or switches to function as multicast network endpoints or hosts. The feature adds INCLUDE mode capability to the IGMPv3 host stack for SSM groups. Enabling the IGMPv3 host stack ensures that hosts on a LAN can leverage SSM by enabling the router or switch to initiate IGMPv3 joins, such as in environments where fast channel change is required in a SSM deployments.

Note Multiple **ip igmp join-group** command configurations with different source addresses for the same group are supported.

When the IGMPv3 Host Stack feature is configured, an IGMPv3 membership report is sent when one of the following events occurs:

- When the **ip igmp join-group** command is configured for a group and source and there is no existing state for this (S, G) channel, an IGMPv3 report of group record type ALLOW_NEW_SOURCES for the source specified is sent on that interface.
- When the **no** form of the **ip igmp join-group** command is configured for a group and source and there is state for this (S, G) channel, an IGMPv3 report of group record type BLOCK_OLD_SOURCES for the source specified is sent on that interface.
- When a query is received, an IGMPv3 report is sent as defined in RFC 3376.

Examples

The following example shows how to configure a router to forward multicast traffic in the absence of directly connected IGMP hosts using the **ip igmp join-group** command. With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching.

In following example, Fast Ethernet interface 0/0 on the router is configured to join the group 225.2.2.2.

```
interface FastEthernet0/0
 ip igmp join-group 225.2.2.2
```

The following example shows how to configure the interface (loopback 0) to join the PTP multicast group.

```
Device(config)# interface loopback 0
 Device(config-if)# ip igmp join-group 224.0.1.129
```

The following example shows how to add INCLUDE mode capability to the IGMPv3 host stack for SSM groups:

```
interface FastEthernet0/0
 ip igmp join-group 232.2.2.2 source 10.1.1.1
 ip igmp join-group 232.2.2.2 source 10.5.5.5
 ip igmp join-group 232.2.2.2 source 10.5.5.6
 ip igmp join-group 232.2.2.4 source 10.5.5.5
 ip igmp join-group 232.2.2.4 source 10.5.5.6
 ip igmp version 3
```

Related Commands

Command	Description
ip igmp static-group	Configures static group membership entries on an interface.

ip igmp last-member-query-count

To configure the number of times that the router sends Internet Group Management Protocol (IGMP) group-specific or group-source-specific (with IGMP version 3) query messages in response to receiving a group-specific or group-source-specific leave message, use the **ip igmp last-member-query-count** command in interface configuration mode. To set this interval to the default value, use the **no** form of this command.

ip igmp last-member-query-count *lmqc*

no ip igmp last-member-query-count *lmqc*

Syntax Description

lmqc	Last member query count. The number of times, from 1 through 7, that the router sends group- or group-source-specific queries upon receipt of a message indicating a leave.

Command Default

LMQC is 2

Command Modes

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

Command History

Release	Modification
12.1	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.
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 a router receives an IGMP version 2 (IGMPv2) or IGMP version 3 (IGMPv3) message indicating that a host wants to leave a group, source, or channel, it sends last-member-query-count group- or group-source-specific IGMP query messages at intervals of igmp-last-member-interval milliseconds. If no response is received after this period, the router stops forwarding for the group, source, or channel.

Caution Do not set the LMQC to 1, because in this situation the loss of a single packet--the query packet from the router to the host or the report packet from the host to the router--may result in traffic forwarding being stopped, even there is still a receiver. Traffic will continue to be forwarded after the next general query sent by the router, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to one last member query interval (LMQI) value when the router is processing more than one leave within a LMQI. In this case, the average leave latency is determined by the (LMQC + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 msec and a LMQC of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

If no response is received after this period, the router will stop forwarding traffic for that group, source, or channel only if no host replies to the query within the timeout period. The timeout period is determined by the **ip igmp last-member-query-interval** and the **ip igmp last-member-query-count** commands.

Examples

The following example changes the number of times that the router sends group-specific or group-source-specific query messages to 5:

```
interface tunnel 0
ip igmp last-member-query-count 5
```

Related Commands

Command	Description
ip igmp explicit-tracking	Enables explicit tracking of hosts, groups, and channels for IGMPv3.
ip igmp immediate-leave	Minimizes the leave latency of IGMP memberships when IGMPv2 is used and only one receiver host is connected to each interface.
ip igmp last-member-query- interval	Configures the interval at which the router sends IGMP group-specific or group-source-specific (with IGMPv3) query messages

ip igmp last-member-query-interval

To configure the interval at which the router sends Internet Group Management Protocol (IGMP) group-specific or group-source-specific (with IGMP Version 3) query messages, use the **ip igmp last-member-query-interval**command in interface configuration mode. To set this interval to the default value, use the **no** form of this command.

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

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

Syntax Description

interval	Interval, in milliseconds, at which IGMP group-specific host query messages are sent. The interval value is an integer from 100 to 25,500. The *interval* argument in 12.0 S, 12.1 E, 12.2, and 12.2 S releases is an integer from 100 through 65,535.

Command Default

interval : 1000 milliseconds (1 second)

Command Modes

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

Command History

Release	Modification
12.1	This command was introduced.
12.2(4)T	The highest *interval* integer value accepted was changed from 65,535 to 25,500.
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 a router receives an IGMP Version 2 (IGMPv2) or IGMP Version 3 (IGMPv3) message indicating that a host wants to leave a group, source, or channel, it sends last-member-query-count group, group-specific, or source-specific IGMP query messages at intervals set by the ip igmp last-member-query-interval command. If no response is received after this period, the router stops forwarding for the group, source, or channel.

The leave latency in Cisco IOS software may increase by up to one last member query interval (LMQI) value when the router is processing more than one leave within a LMQI. In this case, the average leave latency is determined by the (last member query count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 msec and a last member query count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

If no response is received after this period, the router will stop forwarding traffic for that group, source, or channel only if no host replies to the query within the timeout period. The timeout period is determined by the **ip igmp last-member-query-interval** and the **ip igmp last-member-query-count** commands.

Examples

The following example changes the IGMP group-specific host query message interval to 2000 milliseconds (2 seconds):

```
interface tunnel 0
 ip igmp last-member-query-interval 2000
```

Related Commands

Command	Description
ip igmp explicit-tracking	Enables explicit tracking of hosts, groups, and channels for IGMPv3.
ip igmp immediate-leave	Minimizes the leave latency of IGMP memberships when IGMPv2 is used and only one receiver host is connected to each interface.
ip igmp last-member-query-count	Configures the number of times that the router sends IGMP group-specific or group-source-specific (with IGMP version 3) query messages.

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. • 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.

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 querier-timeout

To configure the length of time before the router triggers Internet Group Management Protocol (IGMP) querier reelection for the interface, use the **ip igmp querier-timeout** command in the interface configuration or virtual network interface configuration mode. To restore the default value, use the **no** form of this command.

ip igmp querier-timeout *seconds*

no ip igmp querier-timeout

Syntax Description

seconds	Number of seconds that the router waits before the router triggers IGMP querier reelection for the interface. The range is from 60 to 300 seconds. The default is two times the IGMP query interval.

Command Default

The timeout period is two times the IGMP query interval.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

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.
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 querier-timeout** command to configure the period of time before the router triggers IGMP querier reelection for the interface. The IGMP querier timeout period applies to routers on the subnet that are not currently acting as the IGMP querier.

By default, a router on the subnet that is not currently acting as the querier waits twice the query interval specified by the **ip igmp query-interval** command, after which, if it has heard no queries, it triggers IGMP reelection. The router with the lowest IP address on the subnet is elected the IGMP querier.

In Cisco IOS XE 3.1S and earlier releases, the **ip igmp querier-timeout** command is not written to the configuration if the specified timeout value is equal to the default value of two times the query interval.

In Cisco IOS XE 3.2S and later releases, the **ip igmp querier-timeout** command is written to the configuration any time that the command is explicitly configured, regardless of the specified timeout value.

We recommend that you do not modify the IGMP query interval and IGMP querier timeout values. However, if you configure the appropriate commands to change the query interval and querier timeout default values, the following conditions apply:

- If you use the **ip igmp query-interval** command to configure the query interval, the timeout value is automatically adjusted to two times the query interval; the adjusted timeout value, however, is not reflected in the interface configuration.

  Note To confirm that the timeout value adjusted to two times the modified query interval, use the **show ip igmp interface** command to display the query interval and timeout values being used for the interface.

- Conversely, if you use the **ip igmp querier-timeout** command to configure the timeout value, the query interval does *not* automatically adjust to half of the modified timeout value, so it is possible to override the default timeout period of two times the query interval. If you must configure the timeout period, we recommend that you configure the timeout value in proportion to the query interval value.
- The query interval must be greater than the IGMP maximum query response time. Use the **ip igmp max-response-time** command to change the max-response-time value from the default (10 seconds) to a specified length of time, if required.

Examples

The following example shows how to configure the router to wait 240 seconds from the time it received the last query before it triggers the IGMP election process. In this example, the timeout period is manually modified in proportion to the IGMP query interval by using the **ip igmp querier-timeout** command.

```
interface GigabitEthernet1/1
 ip igmp query-interval 120
 ip igmp querier-timeout 240
```

The following example shows how to configure the router to wait 250 seconds from the time it received the last query until the time that the router triggers the IGMP election process. When the timeout value is explicitly configured, the query interval does not automatically adjust. Because the query interval was not explicitly configured to change the default value (60 seconds), the default timeout period of two times the query interval, or 120 seconds, is overridden by the specified value.

```
interface GigabitEthernet0/1
 ip igmp querier-timeout 250
```

Related Commands

Command	Description
ip igmp max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp query-interval	Configures the frequency at which the IGMP querier sends IGMP host-query messages from an interface.

Command	Description
show ip igmp interface	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp query-interval

Note We recommend that you do not change the default IGMP query interval.

To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the **ip igmp query-interval** command in interface configuration mode. To restore the default IGMP query interval, use the **no** form of this command.

ip igmp query-interval *seconds*

no ip igmp query-interval

Syntax Description

seconds	Frequency, in seconds, at which the router sends IGMP query messages from the interface. The range is from 1 to 18000. The default is 60.

Command Default

The IGMP query interval is 60 seconds.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.2	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

Use the **ip igmp query-interval** command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

Note We recommend that you use the default IGMP query interval and timeout period.

The Cisco IOS software uses a default IGMP query interval of 60 seconds, which is different from the RFC standard default of 125 seconds. Using a lower default IGMP query interval of 60 seconds allows routers to stop forwarding traffic faster when a member crashes without sending leaves (in IGMPv2 or IGMPv3 environment), or if using IGMPv1: 3 * 60 seconds versus 3 * 125 seconds.

If a lower version IGMP-enabled interface (that is, an interface running IGMPv1 or v2) receives a higher version IGMP query (IGMPv3) with a different query interval, the following events will occur:

- An error message in the following format will be displayed:

```
%IGMP-3-QUERY_INT_MISMATCH: Received a non-matching query interval <interval in seconds>,
from querier address <ip-address>
```

- If the query interval on the lower version IGMP-enabled interface has not been modified, the default query interval will appear under its respective interface configuration.
- If the query interval on the IGMP-enabled interface has been modified, the configured query interval will be updated to show the configured query interval under its respective interface configuration.

Note The **show ip igmp interface** command displays both the configured query interval and the received query interval in its output.

Be careful when increasing the query interval in an environment with IGMPv2 routers (the default) and Layer 2 (L2) snooping switches: An IGMPv2 snooping switch needs to know the query interval of the IGMP querier, because it is not signaled in IGMP messages (in IGMPv3 it is). The IGMP snooping switch will time out membership state based on what it thinks the query interval is. If the querier uses a query interval larger than what the IGMP snooping switch assumes, then this may lead to an unexpected timeout of multicast state on the IGMP snooping switch.

Note The default IGMP query interval on Cisco routers of 60 seconds is never an issue with Cisco IGMP snooping switches because they either assume a 60 second-interval or will try to determine the query interval by measuring the interval between IGMP general queries.

Be careful decreasing the query interval because it increases the processing load on the router (total number of IGMP reports received over a period of time)--especially on routers with a large number of interfaces and hosts connected to it (for example, a broadband aggregation router).

We recommend that you do not modify the IGMP query interval and IGMP querier timeout values. However, if you configure the appropriate commands to change the query interval and querier timeout default values, the following conditions apply:

- If you use the **ip igmp query-interval** command to configure the query interval, the timeout value is automatically adjusted to two times the query interval; the adjusted timeout value, however, is not reflected in the interface configuration.

Note To confirm that the timeout value adjusted to two times the modified query interval, use the **show ip igmp interface** command to display the query interval and timeout values being used for the interface.

- Conversely, if you use the **ip igmp querier-timeout** command to configure the timeout value, the query interval does *not* automatically adjust to half of the modified timeout value, so it is possible to override the default timeout period of two times the query interval. If you must configure the timeout period, we recommend that you configure the timeout value in proportion to the query interval value.
- The query interval must be greater than the IGMP maximum query response time. Use the **ip igmp max-response-time** command to change the max-response-time value from the default (10 seconds) to a specified length of time, if required.

Examples

The following example shows how to increase the frequency at which the IGMP querier sends IGMP host-query messages to 120 seconds. The IGMP timeout period will automatically adjust to two times the configured query interval (240 seconds, in this example).

```
interface tunnel 0
 ip igmp query-interval 120
```

Related Commands

Command	Description
ip igmp max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp querier-timeout	Configures the timeout period before the router triggers IGMP querier reelection for the interface.
show ip igmp interface	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **ip igmp query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. The default value is 10 seconds.

Command Default

seconds : 10 seconds

Command Modes

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

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.
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 is valid only when IGMP Version 2 is running.

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

Examples

The following example configures a maximum response time of 8 seconds:

```
ip igmp query-max-response-time 8
```

Related Commands

Command	Description
ip pim query-interval	Configures the frequency of PIM router query messages.
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

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 check

To enforce Internet Group Management Protocol (IGMP) snooping check and enable a device or interface to intercept packets, use the **ip igmp snooping check** command in the global configuration or bridge domain configuration mode. To return to the default, use the **no** form of the command.

ip igmp snooping check {**ttl**| **rtr-alert-option**}

no ip igmp snooping check {**ttl**| **rtr-alert-option**}

Syntax Description

ttl	Specifies the Time to Live (TTL) field for snooping check.
rtr-alert-option	Specifies the Router Alert (rtr-alert) option for snooping check.

Command Default

Snooping check is not enforced.

Command Modes

Global configuration (config)

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Enforcing IGMP snooping check enables a router or interface to intercept packets that are not directly addressed to the device or interface by using one of the following checking methods:

- TTL field: IGMP snooping checks the TTL field in the IGMP header and drops packets where TTL is not equal to 1.
- RTR-Alert option: IGMP snooping checks for the presence of the RTR-Alert option in the IP packet header of the IGMP message and drops packets that do not include this option.

To globally enforce snooping check, use this command in global configuration mode. To enforce snooping check on a specific bridge-domain interface, use this command in bridge domain configuration mode.

Examples

```
Router(config-bdomain)# ip igmp snooping check ttl
```

ip igmp snooping access-group

To configure an Internet Group Management Protocol (IGMP) group access group, use the **ip igmp snooping access-group** command in the interface configuration, bridge domain configuration, or Ethernet service configuration mode. To remove the IGMP group access group, use the **no** form of this command.

ip igmp snooping access-group {*acl-num*| *acl-name*} [**vlan** *vlan-id*]

no ip igmp snooping access-group {*acl-num*| *acl-name*} [**vlan** *vlan-id*]

Syntax Description

acl-num	Number of the Access Control List (ACL). Valid values are from 1 to 199.
acl-name	Name of the ACL.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN that packets arrive on if the switch port is a trunk port and applies the filter to that VLAN. This option is not valid in either the bridge domain configuration or Ethernet service configuration modes.

Command Default

No IGMP ACLS are created.

Command Modes

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

Ethernet service configuration (config-if-srv)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into the Cisco IOS XE Release 3.5S. Support for this command was added to the bridge domain configuration and Ethernet service configuration modes.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

IGMP filtering allows you to configure filters on a per-port basis or a per-Switched Virtual Interface (SVI) basis, or both, or on a per-bridge domain basis or per-Ethernet Flow Point (EFP) basis.

IGMP filtering is supported for IPv4 only.

You can list several groups or channels if you configure multiple access control entries in the access control list. Depending on the permit and deny statements in the ACL configuration, the corresponding group or channel is allowed or denied. The ACL you specify can be a simple or an extended ACL.

This command can be entered as follows:

- Per SVI as a default filter for all switch ports in access mode under that SVI and for all trunk ports that carry the corresponding VLAN for that VLAN only.
- Per switch port:
    - If the switch port is in access mode, this filter overrides any default SVI filter.
    - If the switch port is in trunk mode, this filter acts as a default for all VLANs on that trunk and overrides any default SVI filter.
- Per Layer 2-VLAN:
    - If the switch port is a trunk port, this filter applies only to IGMP packets arriving on the specified Layer 2 VLAN.
    - If the switch port is in trunk mode, this filter overrides any trunk default filter.
- Per-bridge domain for EVC-based IGMP snooping in Cisco IOS XE Release 3.5S and later releases.
- Per- EFP for EVC-based IGMP snooping in Cisco IOS XE Release 3.5S and later releases.

Examples

This example shows how to configure an IGMP group access group:

```
Router(config-if)# ip igmp snooping access-group 44
```

This example shows how to configure an IGMP group access group and apply the filter only to the IGMP packets arriving on the specified Layer 2 VLAN if the switch port is a trunk port:

```
Router(config-if)# no ip igmp snooping access-group 44 vlan 244
```

Related Commands

Command	Description
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
ip igmp snooping minimum-version	Filters on the IGMP protocol.
show ip igmp snooping filter	Displays the IGMP filtering rules.

ip igmp snooping explicit-tracking

To enable Internet Group Management Protocol (IGMP) snooping on an interface to build an explicit host-tracking database, use the **ip igmp snooping explicit-tracking** command in interface configuration or bridge domain configuration mode. To disable the explicit host tracking, use the **no** form of this command.

ip igmp snooping explicit-tracking

no ip igmp snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit tracking is enabled.

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(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 in the interface configuration mode to enable explicit tracking on a VLAN. Use this command in the bridge domain configuration mode to enable explicit tracking on a bridge domain interface.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

Explicit host tracking is supported only with IGMPv3 hosts.

IGMPv3 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN or a bridge domain interface, the IGMP snooping software processes the IGMPv3 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that is reported by the host.

- The list of sources for each group that is reported by the hosts.
- The router filter mode of each group.
- For each group, the list of hosts that request the source.

For Cisco 7600 series routers:

- This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.
- When you enable explicit host tracking and the Cisco 7600 series router is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Cisco 7600 series router forwards only the first report for a channel to the router and suppresses all other reports for the same channel.
- With IGMPv3 proxy reporting, the Cisco 7600 series router does proxy reporting for unsolicited reports and reports that are received in the general query interval.
- Proxy reporting is turned on by default. When you disable proxy reporting, the Cisco 7600 series router works in transparent mode, updates the IGMP snooping database as it receives reports, and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Examples

This example shows how to enable IGMPv3-explicit host tracking on an VLAN and on a bridge domain interface:

```
Router(config-if)# ip igmp snooping explicit-tracking
Router(config-if)# exit
Router(config)# bridge domain 100
Router(config-bdomain)#
ip igmp snooping explicit-tracking
```

This example shows how to disable IGMPv3-explicit host tracking on an interface:

```
Router(config-if)#
no ip igmp snooping explicit-tracking
```

Related Commands

Command	Description
ip igmp snooping limit track	Limits the size of the explicit-tracking database on a VLAN.
ip igmp snooping explicit-tracking limit	Configures an explicit-tracking database limit globally or on a bridge domain interface.
show ip igmp snooping explicit-tracking	Displays information about the explicit host-tracking status for IGMPv3 hosts.

ip igmp snooping explicit-tracking limit

To limit the number of reports in the Internet Group Management Protocol (IGMP) snooping explicit host-tracking database, use the **ip igmp snooping explicit-tracking limit** command in the global configuration or bridge domain configuration mode. To return to the default, use the **no** form of this command.

ip igmp snooping explicit-tracking limit *limit*

no ip igmp snooping explicit-tracking limit

Syntax Description

limit	Maximum number of reports in the database. The range is from 1 to 128000.

Command Default

No limit is configured.

Command Modes

Global configuration (config)

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command in global configuration mode to limit the number of reports in all explicit host-tracking databases for all interfaces on which explicit tracking is enabled for EVC-based IGMP snooping. Use this command in bridge domain configuration mode to limit the number of reports in an explicit host-tracking database for the bridge domain interface being configured.

When the explicit-tracking database exceeds the configured maximum number of reports, a syslog message is generated.

When you reduce the limit, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

The following example shows how to enable explicit tracking for EVC-based IGMP snooping and to limit the number of reports in the explicit-tracking database for the bridge domain interface being configured to 2000.

```
Router(config)# bridge domain 100
Router(config-bdomain)# ip igmp snooping explicit-tracking
Router(config-bdomain)# ip igmp snooping explicit-tracking limit 2000
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables IGMP snooping explicit tracking.

ip igmp snooping fast-leave

To enable the IGMPv3-snooping fast-leave processing, use the **ip igmp snooping fast-leave** command in interface configuration mode. To disable fast-leave processing, use the **no** form of this command.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are as follows:

- IGMP version 2--Disabled
- IGMP version 3--Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 720 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Enter this command in VLAN interface configuration mode only.

Note Fast-leave processing is enabled by default. To disable fast-leave processing, you must enter the **no ip igmp snooping fast-leave** command to disable fast-leave processing.

You should use the IGMPv3-snooping fast-leave processing when there is a single receiver for the MAC group for a specific VLAN.

Examples

This example shows how to enable IGMPv3-snooping fast-leave processing:

```
Router(config-if)#
ip igmp snooping fast-leave
```

This example shows how to disable IGMPv3-snooping fast-leave processing:

```
Router(config-if)#
no ip igmp snooping fast-leave
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping explicit-tracking	Enables explicit host tracking.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.
show mac-address-table	Displays the information about the MAC-address table.

ip igmp snooping flooding

To configure periodic flooding of multicast packets, use the **ip igmp snooping flooding** command in interface configuration mode. To disable periodic flooding, use the **no** form of this command.

ip igmp snooping flooding [**timer** *seconds*]

no ip igmp snooping flooding

Syntax Description

timer *seconds*	(Optional) Specifies the interval between flooding in a 24-hour period for source-only entries; valid values are from 0 to 86400 seconds.

Command Default

The defaults are as follows:

- Disabled.
- If enabled, *seconds* is **600** seconds (10 minutes).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is supported on source-only VLANs.

You can enter **0** seconds to disable flooding. If you enter a maximum of 86400 seconds, flooding would occur once every 24 hours.

Examples

This example shows how to specify the interval between flooding in a 24-hour period:

```
Router(config-if)#
ip igmp snooping flooding timer 300
```

ip igmp snooping immediate-leave

To enable the IGMP version 2 (v2) immediate-leave processing for IGMP snooping, use the **ip igmp snooping immediate-leave** command in bridge domain configuration mode. To disable IGMP v2 immediate-leave processing, use the **no** form of this command.

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

Syntax Description

This command has no arguments or keywords.

Command Default

IGMPv2 immediate-leave processing is disabled.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to enable IGMPv2 immediate-leave processing on the bridge-domain interface being configured.

Immediate-leave processing is supported only with IGMPv2 hosts.

IGMP snooping immediate-leave processing allows the bridge domain interface to remove a host from the forwarding-table entry without first sending group-specific queries. The host is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

Use immediate-leave processing only on bridge domains where only one host is connected to each interface. If immediate-leave is enabled in bridge domains where more than one host is connected to an interface, some hosts might be dropped inadvertently.

When both immediate-leave processing and the last-member-query-count are configured, immediate-leave processing takes precedence.

The immediate-leave configuration is saved in NVRAM.

Examples

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

Related Commands

Command	Description
ip igmp snooping last-member-query-count	Configures the interval for snooping queries sent when a last-member message is received.

ip igmp snooping l2-entry-limit

To configure the maximum number of Layer 2 entries that can be created by the Cisco 7600 series router, use the **ip igmp snooping l2-entry-limit** command in global configuration mode.

ip igmp snooping l2-entry-limit *max-entries*

Syntax Description

max-entries	Maximum number of Layer 2 entries that c an be created by the Cisco 7600 series router; valid values are from 1 to 100000.

Command Default

15488 Layer 2 entries

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to configure the maximum number of Layer 2 entries that can be created by the Cisco 7600 series router:

```
Router(config)#
ip igmp snooping l2-entry-limit 25000
```

Related Commands

Command	Description
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) nnooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration, interface configuration, or bridge domain configuration mode. To set this count to the default value, use the **no** form of this command.

ip igmp last-member-query-count *number*

no ip igmp last-member-query-count *number*

Syntax Description

number	The interval at which query messages are sent, in milliseconds. The range is from 1 to 7. The default is 2.

Command Default

A query is sent every 2 milliseconds.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Bridge domain (config-bdomain)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
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, IGMP queries are sent when the leave is seen until the last-member-query-interval timeout period expires. If no response to the last-member queries are received before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.

Caution Do not set the count to 1, because in this situation the loss of a single packet—the query packet from the router to the host or the report packet from the host to the router—may result in traffic forwarding being stopped, even if there is still a receiver. Traffic will continue to be forwarded after the next general query sent by the router, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to one last-member-query-interval (LMQI) value when the router is processing more than one leave within a LMQI. In this case, the average leave latency is determined by the (count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

Examples

```
Router(config)# interface tunnel 0
Router(config-if)#
 ip igmp last-member-query-count 5
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables explicit tracking of hosts, groups, and channels for IGMPv3.
ip igmp snooping immediate-leave	Enables IGMPv2 immediate-leave processing.
ip igmp snooping last-member-query- interval	Configures the length of time that IGMP snooping will wait for a report.

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. 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. 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 limit

To limit the number of Internet Group Management Protocol (IGMP) groups or channels allowed on an interface or an Ethernet Flow Point (EFP), use the **ip igmp snooping limit** command in the interface configuration, bridge domain configuration, or Ethernet service configuration mode. To return to the default, use the **no** form of this command.

ip igmp snooping limit *num* [**except** {*acl-num*| *acl-name*}] [**vlan** *vlan-id*]

no ip igmp snooping limit *num* [**except** {*acl-num*| *acl-name*}] [**vlan** *vlan-id*]

Syntax Description

num	Maximum number of groups or channels allowed on this interface. The range is from 1 to 64000.
except *acl-num*	(Optional) Specifies the access control list (ACL) group to exempt from the limit. The range is 100 to 199 for a standard ACL.
except *acl-name*	(Optional) Specifies the name of the access control list (ACL) to exempt from the limit.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN on which packets arrive if the switch port is a trunk port and applies the filter to that VLAN. This option is not valid in the bridge domain configuration mode or Ethernet service configuration mode.

Command Default

There is no limit for the number IGMP groups or channels that are allowed on an interface or EFP.

Command Modes

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

Ethernet service configuration (config-if-srv)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
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 and Ethernet service configuration modes.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Note If joins are received for (*,G1) and (S1,G1) on the same interface, these joins are counted as two separate joins. If the limit on an interface has been set to two, and the joins are received for (*,G1) and (S1,G1), all other joins (for groups/channels different from these two) are discarded.

IGMP filtering allows you to configure filters on a per-port basis, a per-Switched Virtual Interface (SVI) basis, or both for PM-based IGMP Snooping, or on a per-bridge domain or per-EFP basis for EVC-based IGMP Snooping.

IGMP filtering is supported for IPv4 only.

You can enter this command based on the following:

- Per-SVI basis.
- Per-Layer 2-switchport basis.
- Per-Layer 2-VLAN basis. The **vlan** keyword allows you to apply the filter only to the IGMP packets arriving on the specified Layer 2 VLAN if the switch port is a trunk port.
- Per-SVI basis as a default filter for all switch ports in access mode under that SVI and for all trunk ports that carry the corresponding VLAN for that VLAN only.
- Per-switch port basis as follows:
  - If the switch port is in access mode, this filter overrides any default SVI filter.
  - If the switch port is in trunk mode, this filter acts as a default for all VLANs on that trunk and overrides any default SVI filter.
- Per-Layer 2-VLAN basis. The filter applies only if the switch port is in trunk mode, and overrides any trunk default filter.
- Per-bridge domain basis for EVC-based IGMP Snooping in Cisco IOS XE Release 3.5S and later releases.
- Per-EFP basis for EVC-based IGMP Snooping in Cisco IOS XE Release 3.5S and later releases.

Examples

This example shows how to limit the number of IGMP groups or channels allowed on an interface:

```
Router(config-if)#
ip igmp snooping limit 4400
```

This example shows how to limit the number of IGMP groups or channels allowed on an interface except for a specific ACL:

```
Router(config-if)#
ip igmp snooping limit 1300 except test1
```

Related Commands

Command	Description
ip igmp snooping access-group	Configures an IGMP group access group.
ip igmp snooping minimum-version	Filters on the IGMP protocol.

Command	Description
show ip igmp snooping filter	Displays the IGMP filtering rules.

ip igmp snooping limit track

To limit the size of the explicit-tracking database, use the **ip igmp snooping limit track**command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping limit track *max-entries*

no ip igmp snooping limit track

Syntax Description

max-entries	Maximum number of entries in the explicit-tracking database; valid values are from 0 to 128000 entries.

Command Default

max-entries is **32000**

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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.

Usage Guidelines

Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* to **0**, explicit-tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries*, a syslog message is generated.

When you reduce the *max-entries*, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)#
 ip igmp snooping limit track 20000
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables explicit host tracking.

Command	Description
show ip igmp snooping explicit-tracking vlan	Displays information about the explicit host-tracking for IGMPv3 hosts.

ip igmp snooping minimum-version

To filter on the Internet Group Management Protocol (IGMP) protocol, use the **ip igmp snooping minimum-version** command in interface configuration or bridge domain configuration mode. To stop filtering on the IGMP protocol, use the **no** form of this command.

ip igmp snooping minimum-version {**2**| **3**}

no ip igmp snooping minimum-version {**2**| **3**}

Syntax Description

2	Filters out all IGMPv1 hosts.
3	Filters out all IGMPv1 and IGMPv2 hosts.

Command Default

IGMP is not filtered.

Command Modes

Interface configuration (config-if)

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
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.

Usage Guidelines

This command is allowed on a per-switched virtual interface (SVI) basis and a per-bridge domain interface basis.

Examples

This example shows how to filter all IGMPv1 hosts:

```
Router(config-if)# ip igmp snooping minimum-version 2
```

Related Commands

Command	Description
ip igmp snooping access-group	Configures an IGMP group access group.

Command	Description
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
show ip igmp snooping filter	Displays the IGMP filtering rules.

ip igmp snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ip igmp snooping mrouter** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

ip igmp snooping mrouter {**interface** *type number*| **port-channel** *number*| **learn** {**cgmp**| **pim-dvmrp**}}

no ip igmp snooping mrouter {**interface** *type number*| **port-channel** *number*| **learn** {**cgmp**| **pim-dvmrp**}}

Syntax Description

interface	Specifies the next-hop interface to the multicast router.
type	Interface type; possible valid values are **ethernet**, **fastethernet gigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
number	Module and port number; see the "Usage Guidelines" section for valid values.
port-channel *number*	Specifies the port-channel number; valid values are a maximum of 64 values ranging from 1 to 256.
learn	Specifies the learning method for the multicast router.
cgmp	Specifies the snooping Cisco Group Management Protocol (CGMP) packets for the multicast router.
pim-dvmrp	Specifies the snooping Protocol Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets for the multicast router.

Command Default

Specifies the snooping PIM-DVMRP packets for the multicast router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. The **learn cgmp** and **learn pim-dvmrp** options have been superseded. Multicast router ports will default to auto-learn through PIM or IGMP packets.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	This command was integrated into a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

The valid values for *interface* include the **ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Enter this command in VLAN interface configuration mode only.

The interface to the router must be in the VLAN where you are entering the command, the interface must be administratively up, and the line protocol must be up.

The *number* argument designates the module and port number. Valid values for *number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The CGMP learning method can decrease control traffic.

The learning method that you configure is saved in NVRAM.

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

Examples

The following example shows how to specify the next-hop interface to the multicast router:

```
Router(config-if)#
ip igmp snooping mrouter interface fastethernet 5/6
```

The following example shows how to specify the learning method for the multicast router:

```
Router(config-if)#
 ip igmp snooping mrouter learn cgmp
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping fast-leave	Enables the IGMPv3-snooping fast-leave processing.
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

ip igmp snooping querier

To enable multicast support within a subnet when no multicast routing protocol is configured in the VLAN or subnet, use the **ip igmp snooping querier** command in interface configuration mode. To disable multicast support within a subnet when no multicast routing protocol is configured, use the **no** form of this command.

ip igmp snooping querier

no ip igmp snooping querier

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Enter this command in VLAN interface configuration mode only.

You enable IGMP snooping on the Cisco 7600 series router, and disable PIM on the VLAN.

Configure the VLAN in global configuration mode.

Configure an IP address on the VLAN interface. When enabled, the IGMP-snooping querier uses the IP address as the query source address. If no IP address is configured on the VLAN interface, the IGMP-snooping querier does not start. The IGMP-snooping querier disables itself if you clear the IP address. When enabled, the IGMP-snooping querier restarts if you configure an IP address.

The IGMP-snooping querier supports IGMPv2.

When enabled, the IGMP-snooping querier does the following:

- Does not start if it detects IGMP traffic from a multicast router.
- Starts after 60 seconds when no IGMP traffic is detected from a multicast router.
- Disables itself if it detects IGMP traffic from a multicast router.

QoS does not support IGMP packets when IGMP snooping is enabled.

You can enable the IGMP-snooping querier on all the Cisco 7600 series routers in the VLAN. One Cisco 7600 series router is elected as the querier.

If multicast routers are not present on the VLAN or subnet, the Cisco 7600 series router becomes the IGMP querier for the VLAN when you enable the IGMP-snooping querier.

If you disable the IGMP-snooping querier, IGMP snooping functions only when you configure PIM in the subnet.

You can enter the **ip igmp snooping querier** command at any time, but the IGMP-snooping querier starts only when no other multicast routers are present in the VLAN or subnet.

You can use this command as an alternative to configuring PIM in a subnet; use this command when the multicast traffic does not need to be routed but you would like support for IGMP snooping on Layer 2 interfaces in your network.

Examples

This example shows how to enable the IGMP-snooping querier on the VLAN:

```
Router(config-if)#
 ip igmp snooping querier
```

Related Commands

Command	Description
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

ip igmp snooping rate

To set the rate limit for IGMP-snooping packets, use the **ip igmp snooping rate** command in global configuration mode. To disable the software rate limiting, use the **no** form of this command.

ip igmp snooping rate *pps*

no ip igmp snooping rate

Syntax Description

pps	Rate limit of incoming IGMP messages; valid values are from 100 to 6000 packets per second.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	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.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to enable software rate limiting:

```
Router(config)#
 ip igmp snooping rate 500
```

This example shows how to disable software rate limiting:

```
Router(config)#
 no ip igmp snooping rate
```

Related Commands

Command	Description
show ip igmp snooping rate-limit	Displays the information about the IGMP-snooping rate limit.

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 robustness-variable

To configure the robustness variable for Internet Group Management Protocol (IGMP) snooping, use the **ip igmp snooping robustness-variable** command in the global configuration or bridge domain configuration mode. To return to the default, use the **no** form of this command.

ip igmp snooping robustness-variable *variable*

no ip igmp snooping robustness-variable

Syntax Description

variable	Robustness variable number. The range is from 1 to 3. The default is 2.

Command Default

The default robustness variable value is 2.

Command Modes

Global configuration (config)

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

The robustness variable is the integer used by IGMP snooping during calcualtions for IGMP messages. The robustness variable provides fine tuning to allow for expected packet loss. The recommended value for the robustness variable is 2.

Use this command to change the value of the robustness variable for IGMP snooping from the default (2) to the specified value.

Examples

```
Router(config-bdomain)# ip igmp snooping access-group 3
Router(config-bdomain)#
```

ip igmp snooping source-only-learning age-timer

To flood multicast packets periodically to a Layer 2 segment that has only multicast sources and no receivers connected to it, use the **ip igmp snooping source-only-learning age-timer**command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping source-only-learning age-timer *seconds*

no ip igmp snooping source-only-learning age-timer

Syntax Description

seconds	Source-only entries age timer value in seconds; valid values are from 0 to 86400 seconds.

Command Default

seconds is **600** seconds (10 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE2	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.

Usage Guidelines

There are two source-only timers that run in an alternating fashion; the source_only_age_timer and the source_only_delete_timer. The value that you configure by entering the **ip igmp snooping source-only-learning age-timer** command sets the source_only_age_timer. The source_only_delete_timer has a fixed, nonconfigurable value of 5 minutes (300 seconds).

The expiration of one timer starts the other timer. At any time, only one timer is running.

Setting the age-timer to **0** stops the flooding in the source-only VLAN.

Note Setting the age-timer to a nonzero value causes flooding to occur every x (configured value) + 5 minutes (source_only_delete_timer) interval.

Examples

This example shows how to flood multicast packets periodically:

```
Router(config)#
 ip igmp snooping source-only-learning age-timer 300
```

This example shows how to return to the default settings:

```
Router(config)#
 no ip igmp snooping source-only-learning age-timer
```

ip igmp snooping ssm-safe-reporting

To enable SSM-safe reporting in the presence of a mix of IGMPv2 and IGMPv3 hosts, use the **ip igmp snooping ssm-safe-reporting** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping ssm-safe-reporting

no ip igmp snooping ssm-safe-reporting

Syntax Description

This command has no arguments or keywords.

Command Default

D isabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was deprecated.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

When you configure SSM-safe reporting, IGMPv3 becomes the group mode in the Cisco 7600 series router or the router even in the presence of IGMPv2 hosts.

A Layer-3 SVI must be configured for any Layer 2 VLAN that supports mixed-IGMPv3 receivers.

Within an SSM group, an IGMPv2 host does not receive the requested traffic until an IGMPv3 host that is connected to the same Cisco 7600 series router is receiving the same group traffic. When the last IGMPv3 host leaves the group, the IGMPv2 host stops receiving traffic for that group.

Examples

This example shows how to enable SSM-safe reporting:

```
Router(config-if)#
ip igmp snooping ssm-safe-reporting
```

ip igmp snooping static

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

ip igmp snooping static *ip-address* [**source** *source-address*] **interface** *port-type port-number member-number service-instance-id* [*port-type port-number member-number service-instance-id*]

no ip igmp snooping static *ip-address* [**source** *source-address*] **interface** *port-type port-number member-number service-instance-id* [*port-type port-number member-number service-instance-id*]

Syntax Description

ip-address	IP address of the IGMP snooping group.
source	(Optional) Specifies a source interface.
source-address	(Optional) The IP address of the interface out of which an (S, G) channel is to be forwarded.
interface	Specifies that one or more interfaces configured to a static router port are to be added to the group being configured.
port-type	Type of port on which the interface is configured. The following keywords are valid for the *port-type* argument: • **GigabitEthernet**: GigabitEthernet IEEE 802.3z. • **LongReach**: Ethernet Long-Reach interface. • **Port-channel**: Ethernet Channel of interfaces.

port-number	Port number on which the interface is configured. The *port-number* format varies depending on the network module or line card type and router chassis slot in which it is installed. Refer to the appropriate hardware manual for numbering information or press **Shift+?** for online help.
member-number	**Note** Configurable only when the **source** and *source-address* keyword and argument combination is used. (Optional) Required if you are adding more than a single host using this command. Order of membership for interfaces being added to the group. The range is from 1 to 8, to be entered in the order that the interface appears in the command string. Required only if you are adding more than a single host using this command.
service-instance-id	**Note** Configurable only when the **source** and *source-address* keyword and argument combination is used. Unique identifier of the service instance for an Ethernet Flow Point (EFP). Required if the **source** and *source-address keyword* and argument combination are configured. Value is a number from 1 to 100.

Command Default

No static group membership entries are configured.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

Hosts normally join multicast groups dynamically, but you can configure a host statically for a Layer 2 LAN port. Use this command is to configure a static connection to a multicast router.

You can configure up to eight individual ports at a time using this command. Multiple ports to be configured need only be separated by a space and must include a *member-number*.

The static ports and groups are saved in NVRAM.

The keywords for this command are not case sensitive. The keywords in online help contain uppercase letters to enhance readability only.

Configuring a service instance on a Layer 2 port creates a pseudoport or Ethernet Flow Point (EFP) on which you configure Ethernet Virtual Connection (EVC) features.

Examples

This example shows how to configure a host (192.0.2.1) statically for a bridge domain interface (44) on the Gigabit Ethernet port:

```
Router(config)# bridge domain 100
Router(config-bdomain) ip igmp snooping static 10.10.10.1 source 192.0.2.1 interface
gigbitethernet0/0/0 44
```

ip igmp snooping tcn flood

To enable flooding of multicast traffic during a spanning-tree Topology Change Notification (TCN) event for an Ethernet Flow Point (EFP) after TCN flooding is explicitly disabled on an EFP, use the **ip igmp snooping tcn flood** command in Ethernet service configuration mode. To disable TCN flooding on an EFP, use the **no** form of this command.

ip igmp snooping tcn flood

no ip igmp snooping tcn flood

Syntax Description

This command has no arguments or keywords.

Command Default

TCN flooding is enabled on EFPs.

Command Modes

Ethernet service configuration (config-if-srv)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to disable or enable TCN flooding on an EFP. TCN flooding is enabled on all EFPs by default.

The Spanning Tree Protocol (STP) operates on the virtual port level. When a virtual port receives a TCN event, all EFPs that operate under that virtual port are identified, along with the bridge domain to which the EFP belongs. Flooding is started to all EFPs on the bridge domain except the ones on which TCN flooding is explicitly disabled. This flooding can exceed the capacity of the virtual port and cause packet loss. Use the **no ip igmp snooping tcn flood** command to disable the flooding of multicast traffic on an EFP during a spanning-tree TCN event .

Examples

```
Router(config)# interface BDI100
Router(config-if)# service instance 333 ethernet
Router(config-if-srv)# no ip igmp snooping tcn flood
```

ip igmp snooping tnc flood query count

To configure the number of Internet Group Management Protocol (IGMP) queries IGMP snooping will receive before stopping the flooding of multicast traffic during a spanning-tree Topology Change Notification (TCN) event, use the **ip igmp snooping tcn flood query count** command in the global configuration mode. To return to the default, use the **no** form of this command.

ip igmp snooping tnc flood query count *count*

no ip igmp snooping tnc flood query count

Syntax Description

count	Number of queries after which the IGMP snooping will stop flooding. The range is from 1 to 10. The default is 2.

Command Default

The default number of queries is 2.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to change the value of query count from the default (2) to the specified number of queries, after which the flood mode for a TCN event is stopped .

Examples

```
Router(config)# ip igmp snooping tcn flood query count 5
Router(config)#
```

Related Commands

Command	Description
ip igmp snooping tcn flood	Toggles TCN flooding on an EFP.

ip igmp snooping tcn query solicit

To enable a multicast router to send IGMP queries during a spanning-tree Topology Change Notification (TCN) event even if the router is not the spanning-tree root, use the **ip igmp snooping tcn query solicit** command in global configuration mode. To disable TCN query solicit on an IP multicast router, use the **no** form of this command.

ip igmp snooping tcn query solicit

no ip igmp snooping tcn query solicit

Syntax Description

This command has no arguments or keywords.

Command Default

The IP multicast router will send a query solicitation during a TCN event only if it is the spanning-tree root.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

When a spanning-tree root router receives a topology change on an IGMP snooping-enabled interface, it issues a query solicitation that causes a Cisco IOS router to send one or more general queries.

Use this command to cause a multicast router to send a query solicitation whenever it notices a topology change, even if that router is not the spanning-tree root.

Examples

```
Router(config)# ip igmp snooping tcn query solicit
```

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 ssm-map

To enable and configure SSM mapping, use the **ip igmp ssm-map** command in global configuration mode. To disable SSM mapping, use the **no** form of this command.

ip igmp ssm-map {**enable**| **query dns**| **static** {*group-access-list*| *group-access-list-name*} *source-address*}

no ip igmp ssm-map {**enable**| **query dns**}

Syntax Description

enable	Enables SSM group to the source mapping.
query dns	Enables the DNS lookup.
static	Specifies an SSM static group to the source mapping.
group-access-list	Group access list to map to the source address.
group-access-list-name	Name of the group access list to map to the source address.
source-address	Source address.

Command Default

D isabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

By default, the locally configured static SSM mappings and the DNS server are queried. Local configured mappings have priority over dynamic mappings. If a DNS server is not available, you may want to disable DNS server lookups. To disable DNS lookups, use the **no ip igmp ssm-map query dns** command.

If a DNS server is not available, a locally configured static SSM mapping database is used to query. A database query uses the group address and receives the source list in return. As soon as the static SSM mappings are configured, the maps are used for the lookups. To build a static SSM mappings database, use the following commands:

ip igmp ssm-map static *acl-1 source-1-ip-address*

ip igmp ssm-map static *acl-2 source-2-ip-address*

The ACL specifies the group or groups that have to be mapped to the listed source. Because the content servers may send out more then one stream with the same source address, the access list is used to group the multicast destination addresses together. You can use wildcards if the addresses are contiguous.

If multiple sources have to be joined for a multicast group address, you must place the group in all ACLs that are associated with the source address. In the example above, if group G must join sources 1 and 2, the group address must be placed in both acl-1 and acl-2.

When you enable SSM mapping using the **ip igmp ssm-map enable** command, but the source mapping list is empty for the group, enter the **no ip igmp ssm-map query dns** command. The **ip igmp ssm-map enable**command is supported on statically configured SSM-mapped source entries only.

Examples

This example shows how to enable an SSM group to the source mapping:

```
Router(config)#
ip igmp ssm-map enable
```

This example shows how to enable DNS lookups:

```
Router(config)#
ip igmp ssm-map query dns
```

This example shows how to build a static SSM mapping database:

```
Router(config)#
ip igmp ssm-map static acl1 255.255.255.0
Router(config)#
ip igmp ssm-map static acl2 255.255.255.0
```

This example shows how to disable an SSM group to the source mapping:

```
Router(config)#
no ip igmp ssm-map enable
```

This example shows how to disable DNS lookups:

```
Router(config)#
no ip igmp ssm-map query dns
```

ip igmp ssm-map enable

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

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

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

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

Examples

The following example shows how to enable SSM mapping:

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

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

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

Related Commands

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

ip igmp ssm-map query dns

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

ip igmp ssm-map static

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

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

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

Syntax Description

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

Command Default

No static SSM mappings are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

Command	Description
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 static-group	Configures the router to be a statically connected member of the specified group on the interface, or to statically forward for a multicast group onto the interface.
ip pim ssm	Defines the SSM range of IP multicast addresses.

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 tcn query

To configure the number of IGMP topology change queries to be executed during a set interval time, use the **ip igmp tcn query**command. To disable IGMP topology change queries, use the **no** form of this command.

ip igmp tcn query {**count** *count*| **interval** *interval*}

no ip igmp tcn query {**count**| **interval**}

Syntax Description

count *count*	Specifies the number of queries needed to stop flooding multicast traffic after a TCN event; valid values are from 1 to 10.
interval *interval*	Specifies the time until the IGMP TCN querier expires; valid values are from 1 to 255 seconds.

Command Default

D isabled

Command Modes

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

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

The **ip igmp tcn query**command applies only to Layer 2 switch ports and EtherChannels; it does not apply to routed ports, VLAN interfaces, or Layer 3 channels.

Use **ip igmp tcn query count** command to control the time that multicast traffic is flooded after a TCN event. If you set the TCN flood query count to 1 by using the **ip igmp tcn query count** command, the flooding stops after receiving 1 general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Examples

This example shows how to set the number of queries to be executed:

```
Router(config)#
ip igmp tcn query count 5
Router(config)#
```

This example shows how to set the time until the query expires to 120 seconds:

```
Router(config)#
ip igmp tcn query interval 120
Router(config)#
```

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 v3lite

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

ip igmp v3lite

no ip igmp v3lite

Syntax Description

This command has no arguments or keywords.

Command Default

IGMPv3 lite membership reports are not accepted and processed.

Command Modes

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

Command History

Release	Modification
12.1(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

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

Examples

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

```
interface ethernet 3/1
ip igmp v3lite
```

Related Commands

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

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.