



Configuring IGMP Snooping

- [Prerequisites for IGMP Snooping, on page 1](#)
- [Restrictions for IGMP Snooping, on page 2](#)
- [Information about IGMP Snooping, on page 2](#)
- [How to Configure IGMP Snooping, on page 8](#)
- [Monitoring IGMP Snooping, on page 21](#)
- [Configuration Examples for IGMP Snooping, on page 23](#)
- [Feature History and Information for IGMP Snooping, on page 24](#)

Prerequisites for IGMP Snooping

Observe these guidelines when configuring the IGMP snooping querier:

- 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 there is no IP address configured on the VLAN interface, the IGMP snooping querier tries to use the configured global IP address for the IGMP querier. If there is no global IP address specified, the IGMP querier tries to use the VLAN switch virtual interface (SVI) IP address (if one exists). If there is no SVI IP address, the device uses the first available IP address configured on the device. The first IP address available appears in the output of the **show ip interface** privileged EXEC command. The IGMP snooping querier does not generate an IGMP general query if it cannot find an available IP address on the device.
- The IGMP snooping querier supports IGMP Versions 1 and 2.
- When administratively enabled, the IGMP snooping querier moves to the nonquerier state if it detects the presence of a multicast router in the network.
- When it is administratively enabled, the IGMP snooping querier moves to the operationally disabled state if IGMP snooping is disabled in the VLAN.
- Layer 3 multicast is not supported.
- MAC based snooping is supported in hardware.

Restrictions for IGMP Snooping

The following are the restrictions for IGMP snooping:

- IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2. IGMP version 2 is the default version for the device.

The actual leave latency in the network is usually the configured leave time. However, the leave time might vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.

- The IGMP throttling action restriction can be applied only to Layer 2 ports. You can use **ip igmp max-groups action replace** interface configuration command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups action {deny | replace}** command has no effect.

If you configure the throttling action and set the maximum group limitation after an interface has added multicast entries to the forwarding table, the forwarding-table entries are either aged out or removed, depending on the throttling action.

Information about IGMP Snooping

IGMP Snooping

Layer 2 devices can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN device to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the device receives an IGMP report from a host for a particular multicast group, the device adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

**Note**

For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The device creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The device supports IP multicast group-based bridging, instead of MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously

configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the device uses IP multicast groups, there are no address aliasing issues.

The IP multicast groups learned through IGMP snooping are dynamic. However, you can statically configure multicast groups by using the **ip igmp snooping vlan *vlan-id* static *ip_address* interface *interface-id*** global configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

You can configure an IGMP snooping querier to support IGMP snooping in subnets without multicast interfaces because the multicast traffic does not need to be routed.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

These sections describe IGMP snooping characteristics:

IGMP Versions

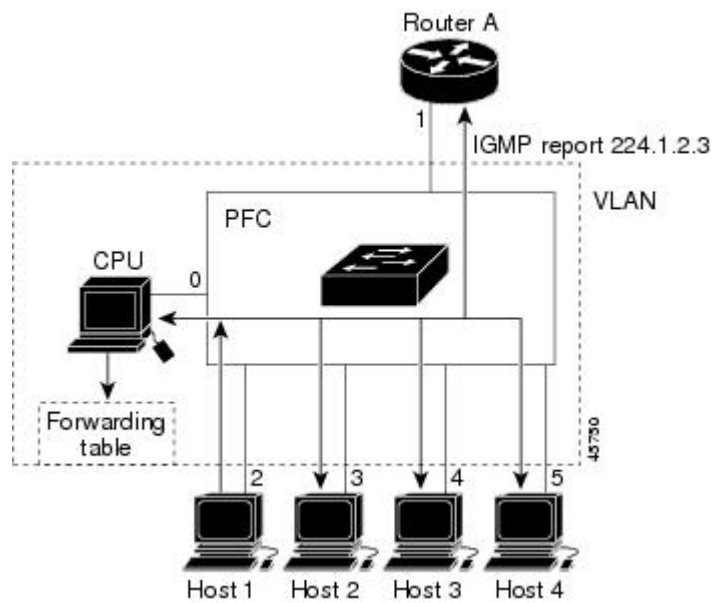
The device supports IGMP version 1, IGMP version 2, and IGMP version 3. These versions are interoperable on the device. For example, if IGMP snooping is enabled and the querier's version is IGMPv2, and the device receives an IGMPv3 report from a host, then the device can forward the IGMPv3 report to the multicast router.

An IGMPv3 device can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature.

Joining a Multicast Group

Figure 1: Initial IGMP Join Message

When a host connected to the device wants to join an IP multicast group and it is an IGMP version 2 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the device receives a general query from the router, it forwards the query to all ports in the VLAN. IGMP version 1 or version 2 hosts wanting to join the multicast group respond by sending a join message to the device. The device CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group.



Router A sends a general query to the device, which forwards the query to ports 2 through 5, all of which are members of the same VLAN. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group. The device CPU uses the information in the IGMP report to set up a forwarding-table entry that includes the port numbers connected to Host 1 and to the router.

Table 1: IGMP Snooping Forwarding Table

| Destination Address | Type of Packet | Ports |
|---------------------|----------------|-------|
| 224.1.2.3 | IGMP | 1, 2 |

The device hardware can distinguish IGMP information packets from other packets for the multicast group. The information in the table tells the switching engine to send frames addressed to the 224.1.2.3 multicast IP address that are not IGMP packets to the router and to the host that has joined the group.

Figure 2: Second Host Joining a Multicast Group

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group, the CPU receives that message and adds the port number of Host 4 to the forwarding table. Because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports on the device. Any known multicast traffic is forwarded to the group and not to the CPU.

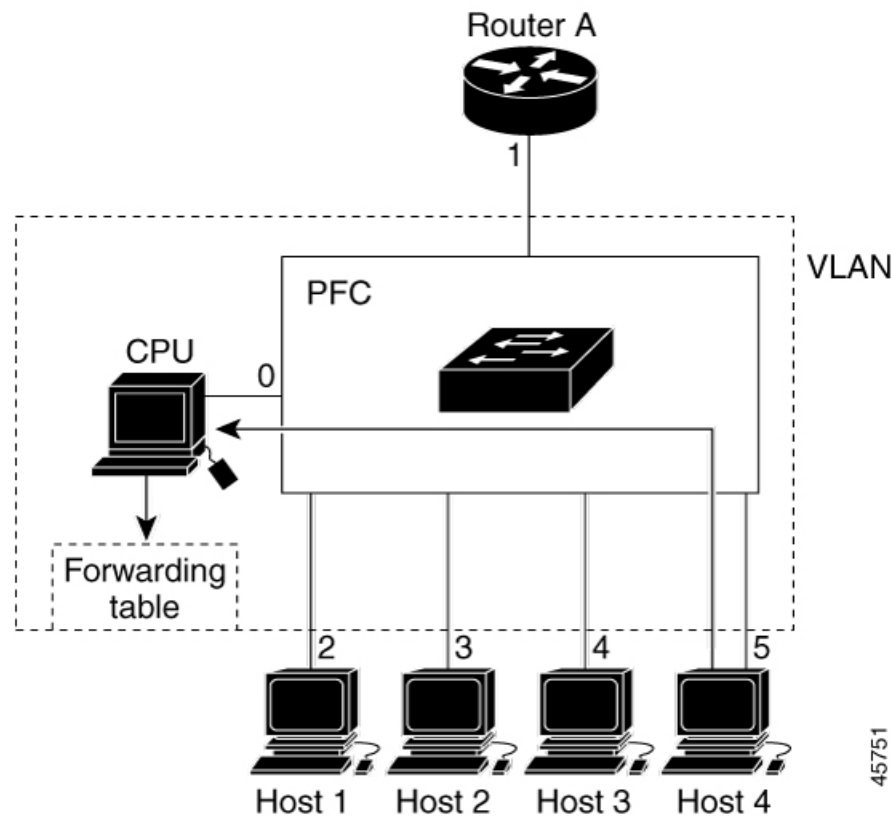


Table 2: Updated IGMP Snooping Forwarding Table

| Destination Address | Type of Packet | Ports |
|---------------------|----------------|---------|
| 224.1.2.3 | IGMP | 1, 2, 5 |

Leaving a Multicast Group

The router sends periodic multicast general queries, and the device forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wants to receive multicast traffic, the router continues forwarding the multicast traffic to the VLAN. The device forwards multicast group traffic only to those hosts listed in the forwarding table for that IP multicast group maintained by IGMP snooping.

When hosts want to leave a multicast group, they can silently leave, or they can send a leave message. When the device receives a leave message from a host, it sends a group-specific query to learn if any other devices connected to that interface are interested in traffic for the specific multicast group. The device then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

Immediate Leave

The device uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the device sending group-specific queries to the interface. The VLAN interface is

pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Immediate Leave is only supported on IGMP version 2 hosts. IGMP version 2 is the default version for the device.



Note You should use the Immediate Leave feature only on VLANs where a single host is connected to each port. If Immediate Leave is enabled on VLANs where more than one host is connected to a port, some hosts may be dropped inadvertently.

IGMP Configurable-Leave Timer

You can configure the time that the device waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be configured from 100 to 32767 milliseconds.

IGMP Report Suppression



Note IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The device uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the device sends the first IGMP report from all hosts for a group to all the multicast routers. The device does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the device forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers.

If the multicast router query also includes requests for IGMPv3 reports, the device forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression, all IGMP reports are forwarded to the multicast routers.

Default IGMP Snooping Configuration

This table displays the default IGMP snooping configuration for the device.

Table 3: Default IGMP Snooping Configuration

| Feature | Default Setting |
|-------------------------------|-------------------------------|
| IGMP snooping | Enabled globally and per VLAN |
| Multicast routers | None configured |
| IGMP snooping Immediate Leave | Disabled |

| Feature | Default Setting |
|------------------------------------|-----------------|
| Static groups | None configured |
| TCN ¹ flood query count | 2 |
| TCN query solicitation | Disabled |
| IGMP snooping querier | Disabled |
| IGMP report suppression | Enabled |

¹ (1) TCN = Topology Change Notification

IGMP Filtering and Throttling

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a switch port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a switch port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing. You can also set the maximum number of IGMP groups that a Layer 2 interface can join.

IGMP filtering controls only group-specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP or MVR is used to forward the multicast traffic.

IGMP filtering applies only to the dynamic learning of IP multicast group addresses, not static configuration.

With the IGMP throttling feature, you can set the maximum number of IGMP groups that a Layer 2 interface can join. If the maximum number of IGMP groups is set, the IGMP snooping forwarding table contains the maximum number of entries, and the interface receives an IGMP join report, you can configure an interface to drop the IGMP report or to replace the randomly selected multicast entry with the received IGMP report.



Note IGMPv3 join and leave messages are not supported on devices running IGMP filtering.

Default IGMP Filtering and Throttling Configuration

This table displays the default IGMP filtering and throttling configuration for the device.

Table 4: Default IGMP Filtering Configuration

| Feature | Default Setting |
|--------------|-----------------|
| IGMP filters | None applied. |

| Feature | Default Setting |
|------------------------------------|---|
| IGMP maximum number of IGMP groups | No maximum set. Note When the maximum number of groups is in the forwarding table, the default IGMP throttling action is to deny the IGMP report. |
| IGMP profiles | None defined. |
| IGMP profile action | Deny the range addresses. |

How to Configure IGMP Snooping

Enabling or Disabling IGMP Snooping on a Device

When IGMP snooping is globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. IGMP snooping is enabled on all VLANs by default, but can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the VLAN IGMP snooping. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable VLAN snooping.

Follow these steps to globally enable IGMP snooping on the device:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp snooping Example: Device(config)# ip igmp snooping | Globally enables IGMP snooping in all existing VLAN interfaces. Note To globally disable IGMP snooping on all VLAN interfaces, use the no ip igmp snooping global configuration command. |
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Enabling or Disabling IGMP Snooping on a VLAN Interface

Follow these steps to enable IGMP snooping on a VLAN interface:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp snooping vlan <i>vlan-id</i> Example: Device(config)# ip igmp snooping vlan 7 | Enables IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094. IGMP snooping must be globally enabled before you can enable VLAN snooping. Note To disable IGMP snooping on a VLAN interface, use the no ip igmp snooping vlan <i>vlan-id</i> global configuration command for the specified VLAN number. |
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 5 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring a Multicast Router Port

Perform these steps to add a multicast router port (enable a static connection to a multicast router) on the device.


Note

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

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> Example: Device(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet 1/0/1 | Specifies the multicast router VLAN ID and the interface to the multicast router. <ul style="list-style-type: none"> • The VLAN ID range is 1 to 1001 and 1006 to 4094. • The interface can be a physical interface or a port channel. The port-channel range is 1 to 128. Note To remove a multicast router port from the VLAN, use the no ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> global configuration command. |
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 5 | show ip igmp snooping mrouter [vlan <i>vlan-id</i>] Example: Device# show ip igmp snooping mrouter vlan 5 | Verifies that IGMP snooping is enabled on the VLAN interface. |
| Step 6 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring a Host Statically to Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Follow these steps to add a Layer 2 port as a member of a multicast group:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp snooping vlan <i>vlan-id</i> static <i>mac_address</i> interface <i>interface-id</i> Example: Device(config)# ip igmp snooping vlan 105 static 0100.5exx.xxxx interface gigabitethernet1/0/1 | Statically configures a Layer 2 port as a member of a multicast group: <ul style="list-style-type: none"> • <i>vlan-id</i> is the multicast group VLAN ID. The range is 1 to 1001 and 1006 to 4094. • <i>mac-address</i> is the group MAC address. • <i>interface-id</i> is the member port. It can be a physical interface or a port channel (1 to 6). <p>Note To remove the Layer 2 port from the multicast group, use the no ip igmp snooping vlan <i>vlan-id</i> static <i>mac-address</i> interface <i>interface-id</i> global configuration command.</p> |
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 5 | show ip igmp snooping groups Example: Device# show ip igmp snooping groups | Verifies the member port and the IP address. |
| Step 6 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Enabling IGMP Immediate Leave

When you enable IGMP Immediate Leave, the device immediately removes a port when it detects an IGMP Version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.



Note

Immediate Leave is supported only on IGMP Version 2 hosts. IGMP Version 2 is the default version for the device.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp snooping vlan <i>vlan-id</i> immediate-leave Example: Device(config)# ip igmp snooping vlan 21 immediate-leave | Enables IGMP Immediate Leave on the VLAN interface. Note To disable IGMP Immediate Leave on a VLAN, use the no ip igmp snooping vlan <i>vlan-id</i> immediate-leave global configuration command. |
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 5 | show ip igmp snooping vlan <i>vlan-id</i> Example: Device# show ip igmp snooping vlan 21 | Verifies that Immediate Leave is enabled on the VLAN interface. |

Configuring the IGMP Leave Timer

You can configure the leave time globally or on a per-VLAN basis. Follow these steps to enable the IGMP configurable-leave timer:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp snooping last-member-query-interval <i>time</i> Example: Device(config)# ip igmp snooping last-member-query-interval 1000 | Configures the IGMP leave timer globally. The range is 100 to 32767 milliseconds. The default leave time is 1000 milliseconds. Note To globally reset the IGMP leave timer to the default setting, use the no ip igmp snooping last-member-query-interval global configuration command. |
| Step 4 | ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval <i>time</i> Example: Device(config)# ip igmp snooping vlan 210 last-member-query-interval 1000 | (Optional) Configures the IGMP leave time on the VLAN interface. The range is 100 to 32767 milliseconds. Note Configuring the leave time on a VLAN overrides the globally configured timer. Note To remove the configured IGMP leave-time setting from the specified VLAN, use the no ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval global configuration command. |
| Step 5 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 6 | show ip igmp snooping Example: Device# show ip igmp snooping | (Optional) Displays the configured IGMP leave time. |
| Step 7 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring the IGMP Snooping Querier

Follow these steps to enable the IGMP snooping querier feature in a VLAN:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | ip igmp snooping querier Example: Device(config)# ip igmp snooping querier | Enables the IGMP snooping querier. |
| Step 3 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 4 | ip igmp snooping querier address <i>ip_address</i> Example: Device(config)# ip igmp snooping querier address 172.16.24.1 | (Optional) Specifies an IP address for the IGMP snooping querier. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier. Note The IGMP snooping querier does not generate an IGMP general query if it cannot find an IP address on the device. |
| Step 5 | ip igmp snooping querier query-interval <i>interval-count</i> Example: Device(config)# ip igmp snooping querier query-interval 30 | (Optional) Sets the interval between IGMP queries. The range is 1 to 18000 seconds. |
| Step 6 | ip igmp snooping querier tcn query [count <i>count</i> interval <i>interval</i>] Example: Device(config)# ip igmp snooping querier tcn query interval 20 | (Optional) Sets the time between Topology Change Notification (TCN) queries. The count range is 1 to 10. The interval range is 1 to 255 seconds. |
| Step 7 | ip igmp snooping querier timer expiry <i>timeout</i> Example: Device(config)# ip igmp snooping querier timer expiry 180 | (Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 8 | ip igmp snooping querier version <i>version</i> Example: Device(config)# ip igmp snooping querier version 2 | (Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2. |
| Step 9 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 10 | show ip igmp snooping vlan <i>vlan-id</i> Example: Device# show ip igmp snooping vlan 30 | (Optional) Verifies that the IGMP snooping querier is enabled on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| Step 11 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Disabling IGMP Report Suppression

Follow these steps to disable IGMP report suppression:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | no ip igmp snooping report-suppression Example: Device(config)# no ip igmp snooping report-suppression | Disables IGMP report suppression. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers. IGMP report suppression is enabled by default. When IGMP report suppression is enabled, the device forwards only one IGMP report per multicast router query. Note To re-enable IGMP report suppression, use the ip igmp snooping report-suppression global configuration command. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 5 | show ip igmp snooping Example: Device# show ip igmp snooping | Verifies that IGMP report suppression is disabled. |
| Step 6 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring IGMP Profiles

Follow these steps to create an IGMP profile:

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp profile <i>profile number</i> Example: Device(config)# ip igmp profile 3 | Assigns a number to the profile you are configuring, and enters IGMP profile configuration mode. The profile number range is 1 to 4294967295. When you are in IGMP profile configuration mode, you can create the profile by using these commands: <ul style="list-style-type: none">• deny—Specifies that matching addresses are denied; this is the default.• exit—Exits from igmp-profile configuration mode.• no—Negates a command or returns to its defaults. |

| | Command or Action | Purpose |
|---------------|---|--|
| | | <ul style="list-style-type: none"> • permit—Specifies that matching addresses are permitted. • range—Specifies a range of IP addresses for the profile. You can enter a single IP address or a range with a start and an end address. <p>The default is for the device to have no IGMP profiles configured.</p> <p>Note To delete a profile, use the no ip igmp profile <i>profile number</i> global configuration command.</p> |
| Step 4 | permit deny Example: Device(config-igmp-profile)# permit | (Optional) Sets the action to permit or deny access to the IP multicast address. If no action is configured, the default for the profile is to deny access. |
| Step 5 | range ip multicast address Example: Device(config-igmp-profile)# range 229.9.9.0 | <p>Enters the IP multicast address or range of IP multicast addresses to which access is being controlled. If entering a range, enter the low IP multicast address, a space, and the high IP multicast address.</p> <p>You can use the range command multiple times to enter multiple addresses or ranges of addresses.</p> <p>Note To delete an IP multicast address or range of IP multicast addresses, use the no range ip multicast address IGMP profile configuration command.</p> |
| Step 6 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 7 | show ip igmp profile <i>profile number</i> Example: Device# show ip igmp profile 3 | Verifies the profile configuration. |
| Step 8 | show running-config Example: Device# show running-config | Verifies your entries. |
| Step 9 | copy running-config startup-config Example: | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|--|---|---------|
| | Device# copy running-config startup-config | |

Applying IGMP Profiles

To control access as defined in an IGMP profile, you have to apply the profile to the appropriate interfaces. You can apply IGMP profiles only to Layer 2 access ports; you cannot apply IGMP profiles to routed ports or SVIs. You cannot apply profiles to ports that belong to an EtherChannel port group. You can apply a profile to multiple interfaces, but each interface can have only one profile applied to it.

Follow these steps to apply an IGMP profile to a switch port:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface interface-id Example: Device(config)# interface gigabitethernet 1/0/1 | Specifies the physical interface, and enters interface configuration mode. The interface must be a Layer 2 port that does not belong to an EtherChannel port group. |
| Step 4 | ip igmp filter profile number Example: Device(config-if)# ip igmp filter 321 | Applies the specified IGMP profile to the interface. The range is 1 to 4294967295. Note To remove a profile from an interface, use the no ip igmp filter profile number interface configuration command. |
| Step 5 | end Example: Device(config-if)# end | Returns to privileged EXEC mode. |
| Step 6 | show running-config Example: Device# show running-config | Verifies your entries. |
| Step 7 | copy running-config startup-config Example: | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|--|---|---------|
| | Device# <code>copy running-config startup-config</code> | |

Setting the Maximum Number of IGMP Groups

Follow these steps to set the maximum number of IGMP groups that a Layer 2 interface can join:

Before you begin

This restriction can be applied to Layer 2 ports only; you cannot set a maximum number of IGMP groups on routed ports or SVIs. You also can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> <code>enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# <code>configure terminal</code> | Enters global configuration mode. |
| Step 3 | interface interface-id Example: Device(config)# <code>interface gigabitethernet 1/0/2</code> | Specifies the interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or a EtherChannel interface. |
| Step 4 | ip igmp max-groups number Example: Device(config-if)# <code>ip igmp max-groups 20</code> | Sets the maximum number of IGMP groups that the interface can join. The range is 0 to 4294967294. The default is to have no maximum set. Note To remove the maximum group limitation and return to the default of no maximum, use the no ip igmp max-groups interface configuration command. |
| Step 5 | end Example: Device(config)# <code>end</code> | Returns to privileged EXEC mode. |
| Step 6 | show running-config interface interface-id Example: | Verifies your entries. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Device# <code>show running-config interface gigabitethernet1/0/1</code> | |
| Step 7 | copy running-config startup-config Example: Device# <code>copy running-config startup-config</code> | (Optional) Saves your entries in the configuration file. |

Configuring the IGMP Throttling Action

After you set the maximum number of IGMP groups that a Layer 2 interface can join, you can configure an interface to replace the existing group with the new group for which the IGMP report was received.

Follow these steps to configure the throttling action when the maximum number of entries is in the forwarding table:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> <code>enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# <code>configure terminal</code> | Enters global configuration mode. |
| Step 3 | interface interface-id Example: Device(config)# <code>interface gigabitethernet 1/0/1</code> | Specifies the physical interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or an EtherChannel interface. The interface cannot be a trunk port. |
| Step 4 | ip igmp max-groups action {deny replace} Example: Device(config-if)# <code>ip igmp max-groups action replace</code> | When an interface receives an IGMP report and the maximum number of entries is in the forwarding table, specifies the action that the interface takes: <ul style="list-style-type: none"> • deny—Drops the report. If you configure this throttling action, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out and the maximum number of entries is in the forwarding table, the device drops the next IGMP report received on the interface. |

| | Command or Action | Purpose |
|---------------|---|--|
| | | <ul style="list-style-type: none"> • replace—Replaces the existing group with the new group for which the IGMP report was received. If you configure this throttling action, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the device replaces a randomly selected entry with the received IGMP report. <p>To prevent the device from removing the forwarding-table entries, you can configure the IGMP throttling action before an interface adds entries to the forwarding table.</p> <p>Note To return to the default action of dropping the report, use the no ip igmp max-groups action interface configuration command.</p> |
| Step 5 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 6 | show running-config interface <i>interface-id</i> Example: Device(config)# show running-config interface gigabitethernet 1/0/1 | Verifies your entries. |
| Step 7 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Monitoring IGMP Snooping

Monitoring IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

Table 5: Commands for Displaying IGMP Snooping Information

| Command | Purpose |
|--|---|
| show ip igmp snooping [vlan <i>vlan-id</i> [detail]] | Displays the snooping configuration information for all VLANs on the device or for a specified VLAN. (Optional) Enter vlan <i>vlan-id</i> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| show ip igmp snooping groups [count vlan <i>vlan-id</i>] | Displays multicast table information for the device or about a specific parameter: <ul style="list-style-type: none"> • count—Displays the total number of entries for the specified command options instead of the actual entries. • vlan-id—The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| show ip igmp snooping mrouter [vlan <i>vlan-id</i>] | Displays information on dynamically learned and manually configured multicast router interfaces. Note When you enable IGMP snooping, the device automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces. (Optional) Enter the vlan <i>vlan-id</i> to display information for a particular VLAN. |
| show ip igmp snooping querier [vlan <i>vlan-id</i>] detail | Displays information about the IP address and receiving port of the most-recently received IGMP query message in the VLAN and the configuration and operational state of the IGMP snooping querier in the VLAN. |

Monitoring IGMP Filtering

You can display IGMP profile characteristics, and you can display the IGMP profile and maximum group configuration for all interfaces on the device or for a specified interface.

Table 6: Commands for Displaying IGMP Filtering

| Command | Purpose |
|---|---|
| show ip igmp profile [<i>profile number</i>] | Displays the specified IGMP profile or all the IGMP profiles defined on the device. |
| show running-config [interface <i>interface-id</i>] | Displays the configuration of the specified interface or the configuration of all interfaces on the device, including (if configured) the maximum number of IGMP groups to which an interface can belong and the IGMP profile applied to the interface. |

Configuration Examples for IGMP Snooping

Example: Enabling a Static Connection to a Multicast Router

This example shows how to enable a static connection to a multicast router:

```
Device# configure terminal
Device# ip igmp snooping vlan 200 interface gigabitethernet 1/0/2
Device# end
```

Example: Configuring a Host Statically to Join a Group

This example shows how to statically configure a host on a port:

```
Device# configure terminal
Device# ip igmp snooping vlan 105 static 0100.1212.0000 interface gigabitethernet 1/0/1
Device# end
```

Example: Enabling IGMP Immediate Leave

This example shows how to enable IGMP Immediate Leave on VLAN 130:

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 130 immediate-leave
Device(config)# end
```

Example: Setting the IGMP Snooping Querier Source Address

This example shows how to set the IGMP snooping querier source address to 10.0.0.64:

```
Device# configure terminal
Device(config)# ip igmp snooping querier 10.0.0.64
Device(config)# end
```

Example: Setting the IGMP Snooping Querier Maximum Response Time

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Device# configure terminal
Device(config)# ip igmp snooping querier query-interval 25
Device(config)# end
```

Example: Setting the IGMP Snooping Querier Timeout

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Device# configure terminal
Device(config)# ip igmp snooping querier timeout expiry 60
Device(config)# end
```

Example: Setting the IGMP Snooping Querier Feature

This example shows how to set the IGMP snooping querier feature to Version 2:

```
Device# configure terminal
Device(config)# no ip igmp snooping querier version 2
Device(config)# end
```

Example: Configuring IGMP Profiles

This example shows how to create IGMP profile 4 allowing access to the single IP multicast address and how to verify the configuration. If the action was to deny (the default), it would not appear in the **show ip igmp profile** output display.

```
Device(config)# ip igmp profile 4
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 229.9.9.0
Device(config-igmp-profile)# end
Device# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

Example: Applying IGMP Profile

This example shows how to apply IGMP profile 4 to a port:

```
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# ip igmp filter 4
Device(config-if)# end
```

Example: Setting the Maximum Number of IGMP Groups

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
Device(config-if)# end
```

Feature History and Information for IGMP Snooping

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS Release 15.2(7)E3k | This feature was introduced. |