



Configuring IGMP

- [Finding Feature Information, page 1](#)
- [Prerequisites for IGMP, page 1](#)
- [Restrictions for Configuring IGMP, page 2](#)
- [Information About IGMP, page 2](#)
- [How to Configure IGMP, page 8](#)
- [Monitoring IGMP, page 21](#)
- [Configuration Examples for IGMP, page 22](#)
- [Additional References, page 23](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IGMP

- Before performing the tasks in this module, you should be familiar with the concepts explained in the "IP Multicast Routing Technology Overview" module.
- The tasks in this module assume that IP multicast has been enabled and that the Protocol Independent Multicast (PIM) interfaces have been configured using the tasks described in the "Configuring Basic IP Multicast Routing" module.

Related Topics

[Configuring the Switch as a Member of a Group](#) , on page 8

[IGMP Join Process, on page 6](#)

[IGMP Leave Process, on page 7](#)

Restrictions for Configuring IGMP

The following are the restrictions for configuring IGMP:

- The switch supports IGMP Versions 1, 2, and 3.



Note For IGMP Version 3, only IGMP Version 3 BISS (Basic IGMPv3 Snooping Support) is supported.

- IGMP Version 3 uses new membership report messages that might not be correctly recognized by older IGMP snooping switches.
- IGMPv3 can operate with both ISM and SSM. In ISM, both exclude and include mode reports are applicable. In SSM, only include mode reports are accepted by the last-hop router. Exclude mode reports are ignored.

Related Topics

[IGMP Version 3, on page 3](#)

Information About IGMP

Role of the Internet Group Management Protocol

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Enabling PIM on an interface also enables IGMP. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

- A querier is a network device, such as a router, that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver, including routers, that sends report messages (in response to query messages) to inform the querier of a host membership. Hosts use IGMP messages to join and leave multicast groups.

Hosts identify group memberships by sending IGMP messages to their local multicast device. Under IGMP, devices listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP Multicast Addresses

IP multicast traffic uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

Multicast addresses in the range 224.0.0.0 to 224.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are transmitted using IP multicast group addresses as follows:

- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the device is querying.
- IGMP group membership reports are destined to the group IP address for which the device is reporting.
- IGMPv2 leave-group messages are destined to the address 224.0.0.2 (all devices on a subnet).
- IGMPv3 membership reports are destined to the address 224.0.0.22; all IGMPv3-capable multicast devices must listen to this address.

IGMP Versions

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

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

Related Topics

[Changing the IGMP Version, on page 12](#)

[Restrictions for IGMP Snooping](#)

IGMP Version 1

IGMP version 1 (IGMPv1) primarily uses a query-response model that enables the multicast router and multilayer switch to find which multicast groups are active (have one or more hosts interested in a multicast group) on the local subnet. IGMPv1 has other processes that enable a host to join and leave a multicast group. For more information, see RFC 1112.

IGMP Version 2

IGMPv2 extends IGMP functionality by providing such features as the IGMP leave process to reduce leave latency, group-specific queries, and an explicit maximum query response time. IGMPv2 also adds the capability for routers to elect the IGMP querier without depending on the multicast protocol to perform this task. For more information, see RFC 2236.

**Note**

IGMP version 2 is the default version for the switch.

IGMP Version 3

The switch supports IGMP version 3.

An IGMPv3 switch supports Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when your network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv2 or IGMPv1 hosts.

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

Related Topics

[Restrictions for Configuring IGMP, on page 2](#)

IGMPv3 Host Signalling

In IGMPv3, hosts signal membership to last hop routers of multicast groups. Hosts can signal group membership with filtering capabilities with respect to sources. A host can either signal that it wants to receive traffic from all sources sending to a group except for some specific sources (called exclude mode), or that it wants to receive traffic only from some specific sources sending to the group (called include mode).

IGMPv3 can operate with both Internet Standard Multicast (ISM) and Source Specific Multicast (SSM). In ISM, both exclude and include mode reports are applicable. In SSM, only include mode reports are accepted by the last-hop router. Exclude mode reports are ignored.

IGMP Versions Differences

There are three versions of IGMP, as defined by Request for Comments (RFC) documents of the Internet Engineering Task Force (IETF). IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group and IGMPv3 improves over IGMPv2 mainly by adding the ability to listen to multicast originating from a set of source IP addresses only.

Table 1: IGMP Versions

| IGMP Version | Description |
|--------------|--|
| IGMPv1 | Provides the basic query-response mechanism that allows the multicast device to determine which multicast groups are active and other processes that enable hosts to join and leave a multicast group. RFC 1112 defines the IGMPv1 host extensions for IP multicasting. |
| IGMPv2 | Extends IGMP, allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for devices to elect the IGMP querier without dependence on the multicast protocol to perform this task. RFC 2236 defines IGMPv2. |

**Note**

By default, enabling a PIM on an interface enables IGMPv2 on that device. IGMPv2 was designed to be as backward compatible with IGMPv1 as possible. To accomplish this backward compatibility, RFC 2236 defined special interoperability rules. If your network contains legacy IGMPv1 hosts, you should be familiar with these operability rules. For more information about IGMPv1 and IGMPv2 interoperability, see RFC 2236, Internet Group Management Protocol, Version 2 .

Devices That Run IGMPv1

IGMPv1 devices send IGMP queries to the “all-hosts” multicast address of 224.0.0.1 to solicit multicast groups with active multicast receivers. The multicast receivers also can send IGMP reports to the device to notify it that they are interested in receiving a particular multicast stream. Hosts can send the report asynchronously or in response to the IGMP queries sent by the device. If more than one multicast receiver exists for the same multicast group, only one of these hosts sends an IGMP report message; the other hosts suppress their report messages.

In IGMPv1, there is no election of an IGMP querier. If more than one device on the segment exists, all the devices send periodic IGMP queries. IGMPv1 has no special mechanism by which the hosts can leave the group. If the hosts are no longer interested in receiving multicast packets for a particular group, they simply do not reply to the IGMP query packets sent from the device. The device continues sending query packets. If the device does not hear a response in three IGMP queries, the group times out and the device stops sending multicast packets on the segment for the group. If the host later wants to receive multicast packets after the timeout period, the host simply sends a new IGMP join to the device, and the device begins to forward the multicast packet again.

If there are multiple devices on a LAN, a designated router (DR) must be elected to avoid duplicating multicast traffic for connected hosts. PIM devices follow an election process to select a DR. The PIM device with the highest IP address becomes the DR.

The DR is responsible for the following tasks:

- Sending PIM register and PIM Join and Prune messages toward the rendezvous point (RP) to inform it about host group membership.
- Sending IGMP host-query messages.
- Sending host-query messages by default every 60 seconds in order to keep the IGMP overhead on hosts and networks very low.

Devices That Run IGMPv2

IGMPv2 improves the query messaging capabilities of IGMPv1.

The query and membership report messages in IGMPv2 are identical to the IGMPv1 messages with two exceptions:

- IGMPv2 query messages are broken into two categories: general queries (identical to IGMPv1 queries) and group-specific queries.
- IGMPv1 membership reports and IGMPv2 membership reports have different IGMP type codes.

IGMPv2 also enhances IGMP by providing support for the following capabilities:

- Querier election process--Provides the capability for IGMPv2 devices to elect the IGMP querier without having to rely on the multicast routing protocol to perform the process.

- Maximum Response Time field--A new field in query messages permits the IGMP querier to specify the maximum query-response time. This field permits the tuning of the query-response process to control response burstiness and to fine-tune leave latencies.
- Group-Specific Query messages--Permits the IGMP querier to perform the query operation on a specific group instead of all groups.
- Leave-Group messages--Provides hosts with a method of notifying devices on the network that they wish to leave the group.

Unlike IGMPv1, in which the DR and the IGMP querier are typically the same device, in IGMPv2 the two functions are decoupled. The DR and the IGMP querier are selected based on different criteria and may be different devices on the same subnet. The DR is the device with the highest IP address on the subnet, whereas the IGMP querier is the device with the lowest IP address.

Query messages are used to elect the IGMP querier as follows:

- 1 When IGMPv2 devices start, they each multicast a general query message to the all-systems group address of 224.0.0.1 with their interface address in the source IP address field of the message.
- 2 When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. The device with the lowest IP address on the subnet is elected the IGMP querier.
- 3 All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down, and the election process is performed again to elect a new IGMP querier.

By default, the timer is two times the query interval.

IGMP Join and Leave Process

IGMP Join Process

When a host wants to join a multicast group, the host sends one or more unsolicited membership reports for the multicast group it wants to join. The IGMP join process is the same for IGMPv1 and IGMPv2 hosts.

In IGMPv3, the join process for hosts proceeds as follows:

- When a host wants to join a group, it sends an IGMPv3 membership report to 224.0.0.22 with an empty EXCLUDE list.
- When a host wants to join a specific channel, it sends an IGMPv3 membership report to 224.0.0.22 with the address of the specific source included in the INCLUDE list.
- When a host wants to join a group excluding particular sources, it sends an IGMPv3 membership report to 224.0.0.22 excluding those sources in the EXCLUDE list.



Note

If some IGMPv3 hosts on a LAN wish to exclude a source and others wish to include the source, then the device will send traffic for the source on the LAN (that is, inclusion trumps exclusion in this situation).

Related Topics

[Configuring the Switch as a Member of a Group](#) , on page 8

[Prerequisites for IGMP](#), on page 1

[Example: Configuring the Switch as a Member of a Multicast Group](#), on page 22

IGMP Leave Process

The method that hosts use to leave a group varies depending on the version of IGMP in operation.

IGMPv1 Leave Process

There is no leave-group message in IGMPv1 to notify the devices on the subnet that a host no longer wants to receive the multicast traffic from a specific group. The host simply stops processing traffic for the multicast group and ceases responding to IGMP queries with IGMP membership reports for the group. As a result, the only way IGMPv1 devices know that there are no longer any active receivers for a particular multicast group on a subnet is when the devices stop receiving membership reports. To facilitate this process, IGMPv1 devices associate a countdown timer with an IGMP group on a subnet. When a membership report is received for the group on the subnet, the timer is reset. For IGMPv1 devices, this timeout interval is typically three times the query interval (3 minutes). This timeout interval means that the device may continue to forward multicast traffic onto the subnet for up to 3 minutes after all hosts have left the multicast group.

IGMPv2 Leave Process

IGMPv2 incorporates a leave-group message that provides the means for a host to indicate that it wishes to stop receiving multicast traffic for a specific group. When an IGMPv2 host leaves a multicast group, if it was the last host to respond to a query with a membership report for that group, it sends a leave-group message to the all-devices multicast group (224.0.0.2).

IGMPv3 Leave Process

IGMPv3 enhances the leave process by introducing the capability for a host to stop receiving traffic from a particular group, source, or channel in IGMP by including or excluding sources, groups, or channels in IGMPv3 membership reports.

Related Topics

[Configuring the Switch as a Member of a Group](#) , on page 8

[Prerequisites for IGMP](#), on page 1

[Example: Configuring the Switch as a Member of a Multicast Group](#), on page 22

Default IGMP Configuration

This table displays the default IGMP configuration for the switch.

Table 2: Default IGMP Configuration

| Feature | Default Setting |
|--|-----------------------------------|
| Multilayer switch as a member of a multicast group | No group memberships are defined. |

| Feature | Default Setting |
|--|---|
| Access to multicast groups | All groups are allowed on an interface. |
| IGMP version | Version 2 on all interfaces. |
| IGMP host-query message interval | 60 seconds on all interfaces. |
| IGMP query timeout | 60 seconds on all interfaces. |
| IGMP maximum query response time | 10 seconds on all interfaces. |
| Multilayer switch as a statically connected member | Disabled. |

How to Configure IGMP

Configuring the Switch as a Member of a Group

You can configure the switch as a member of a multicast group and discover multicast reachability in a network. If all the multicast-capable routers and multilayer switches that you administer are members of a multicast group, pinging that group causes all of these devices to respond. The devices respond to ICMP echo-request packets addressed to a group of which they are members. Another example is the multicast trace-route tools provided in the software.



Caution

Performing this procedure might impact the CPU performance because the CPU will receive all data traffic for the group address.

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp join-group** *group-address*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Switch> enable</pre> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre> | Enters the global configuration mode. |
| Step 3 | <p>interface <i>interface-id</i></p> <p>Example:</p> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre> | <p>Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode.</p> <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> • A routed port—A physical port that has been configured as a Layer 3 port by entering the no switchport interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group. For a configuration example, see Example: Interface Configuration as a Routed Port. • An SVI—A VLAN interface created by using the interface vlan <i>vlan-id</i> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. For a configuration example, see Example: Interface Configuration as an SVI. <p>These interfaces must have IP addresses assigned to them.</p> |
| Step 4 | <p>ip igmp join-group <i>group-address</i></p> <p>Example:</p> <pre>Switch(config-if)# ip igmp join-group 225.2.2.2</pre> | <p>Configures the switch to join a multicast group.</p> <p>By default, no group memberships are defined.</p> <p>For <i>group-address</i>, specify the multicast IP address in dotted decimal notation.</p> <p>Note To cancel membership in a group, use the no ip igmp join-group <i>group-address</i> interface configuration command.</p> |
| Step 5 | <p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre> | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 6 | show ip igmp interface [<i>interface-id</i>] Example: Switch# show ip igmp interface | Verifies your entries. |
| Step 7 | copy running-config startup-config Example: Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Related Topics

[IGMP Join Process, on page 6](#)

[IGMP Leave Process, on page 7](#)

[Prerequisites for IGMP, on page 1](#)

[Example: Configuring the Switch as a Member of a Multicast Group, on page 22](#)

Controlling Access to IP Multicast Group

The switch sends IGMP host-query messages to find which multicast groups have members on attached local networks. The switch then forwards to these group members all packets addressed to the multicast group. You can place a filter on each interface to restrict the multicast groups that hosts on the subnet serviced by the interface can join.

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp access-group** *access-list-number*
5. **exit**
6. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
7. **end**
8. **show ip igmp interface** [*interface-id*]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Switch> enable</pre> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre> | Enters the global configuration mode. |
| Step 3 | <p>interface <i>interface-id</i></p> <p>Example:</p> <pre>Switch(config)# interface GigabitEthernet 1/0/12</pre> | Specifies the interface to be configured, and enters interface configuration mode. |
| Step 4 | <p>ip igmp access-group <i>access-list-number</i></p> <p>Example:</p> <pre>Switch(config-if)# ip igmp access-group 10</pre> | <p>Specifies the multicast groups that hosts on the subnet serviced by an interface can join.</p> <p>By default, all groups are allowed on an interface.</p> <p>For <i>access-list-number</i>, specify an IP standard access list number. The range is 1 to 199.</p> <p>Note To disable groups on an interface, use the no ip igmp access-group interface configuration command.</p> |
| Step 5 | <p>exit</p> <p>Example:</p> <pre>Switch(config-if)# exit</pre> | Returns to global configuration mode. |
| Step 6 | <p>access-list <i>access-list-number</i> {deny permit} <i>source</i> [<i>source-wildcard</i>]</p> <p>Example:</p> <pre>Switch(config)# access-list 10 permit</pre> | <p>Creates a standard access list.</p> <ul style="list-style-type: none"> For <i>access-list-number</i>, specify the access list created in Step 3. The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched. For <i>source</i>, specify the multicast group that hosts on the subnet can join. (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p> |

| | Command or Action | Purpose |
|---------------|---|----------------------------------|
| Step 7 | end Example: Switch(config-igmp-profile) # end | Returns to privileged EXEC mode. |
| Step 8 | show ip igmp interface [<i>interface-id</i>] Example: Switch# show ip igmp interface | Verifies your entries. |

Related Topics

[Example: Controlling Access to IP Multicast Groups, on page 22](#)

Changing the IGMP Version

By default, the switch uses IGMP Version 2, which provides features such as the IGMP query timeout and the maximum query response time.

All systems on the subnet must support the same version. The switch does not automatically detect Version 1 systems and switch to Version 1. You can mix Version 1 and Version 2 hosts on the subnet because Version 2 routers or switches always work correctly with IGMPv1 hosts.

Configure the switch for Version 1 if your hosts do not support Version 2.

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp version** {1 | 2 | 3 }
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Switch> enable</pre> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre> | Enters the global configuration mode. |
| Step 3 | <p>interface <i>interface-id</i></p> <p>Example:</p> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre> | Specifies the interface to be configured, and enters the interface configuration mode. |
| Step 4 | <p>ip igmp version {1 2 3 }</p> <p>Example:</p> <pre>Switch(config-if)# ip igmp version 2</pre> | <p>Specifies the IGMP version that the switch uses.</p> <p>Note If you change to Version 1, you cannot configure the ip igmp query-interval or the ip igmp query-max-response-time interface configuration commands.</p> <p>To return to the default setting, use the no ip igmp version interface configuration command.</p> |
| Step 5 | <p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 6 | <p>show ip igmp interface [<i>interface-id</i>]</p> <p>Example:</p> <pre>Switch# show ip igmp interface</pre> | Verifies your entries. |
| Step 7 | <p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Related Topics

[IGMP Versions, on page 3](#)

Modifying the IGMP Host-Query Message Interval

The switch periodically sends IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-hosts multicast group (224.0.0.1) with a time-to-live (TTL) of 1. The switch sends host-query messages to refresh its knowledge of memberships present on the network. If, after some number of queries, the software discovers that no local hosts are members of a multicast group, the software stops forwarding multicast packets to the local network from remote origins for that group and sends a prune message upstream toward the source.

The switch elects a PIM designated router (DR) for the LAN (subnet). The designated router is responsible for sending IGMP host-query messages to all hosts on the LAN. In sparse mode, the designated router also sends PIM register and PIM join messages toward the RP router. With IGMPv2, the DR is the router or multilayer switch with the highest IP address. With IGMPv1, the DR is elected according to the multicast routing protocol that runs on the LAN.

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **ip igmp query-interval *seconds***
5. **end**
6. **show ip igmp interface [*interface-id*]**
7. **copy running-config startup-config**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters the global configuration mode. |

| | Command or Action | Purpose |
|--------|--|---|
| Step 3 | <p>interface <i>interface-id</i></p> <p>Example:</p> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre> | <p>Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode.</p> <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> • A routed port—A physical port that has been configured as a Layer 3 port by entering the no switchport interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group. For a configuration example, see Example: Interface Configuration as a Routed Port. • An SVI—A VLAN interface created by using the interface vlan <i>vlan-id</i> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. For a configuration example, see Example: Interface Configuration as an SVI. <p>These interfaces must have IP addresses assigned to them.</p> |
| Step 4 | <p>ip igmp query-interval <i>seconds</i></p> <p>Example:</p> <pre>Switch(config-if)# ip igmp query-interval 75</pre> | <p>Configures the frequency at which the designated router sends IGMP host-query messages.</p> <p>By default, the designated router sends IGMP host-query messages every 60 seconds to keep the IGMP overhead very low on hosts and networks.</p> <p>The range is 1 to 65535.</p> <p>Note To return to the default setting, use the no ip igmp query-interval interface configuration command.</p> |
| Step 5 | <p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre> | <p>Returns to privileged EXEC mode.</p> |
| Step 6 | <p>show ip igmp interface [<i>interface-id</i>]</p> <p>Example:</p> <pre>Switch# show ip igmp interface</pre> | <p>Verifies your entries.</p> |
| Step 7 | <p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre> | <p>(Optional) Saves your entries in the configuration file.</p> |

Changing the IGMP Query Timeout for IGMPv2

If you are using IGMPv2, you can specify the period of time before the switch takes over as the querier for the interface. By default, the switch waits twice the query interval period controlled by the **ip igmp query-interval** interface configuration command. After that time, if the switch has received no queries, it becomes the querier.

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp querier-timeout** *seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters the global configuration mode. |
| Step 3 | interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet 1/0/1 | Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode. The specified interface must be one of the following: <ul style="list-style-type: none"> • A routed port—A physical port that has been configured as a Layer 3 port by entering the no switchport interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group. For a configuration example, see Example: Interface Configuration as a Routed Port. • An SVI—A VLAN interface created by using the interface vlan <i>vlan-id</i> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically |

| | Command or Action | Purpose |
|---------------|---|--|
| | | <p>connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. For a configuration example, see Example: Interface Configuration as an SVI.</p> <p>These interfaces must have IP addresses assigned to them.</p> |
| Step 4 | ip igmp querier-timeout <i>seconds</i> Example: <pre>Switch(config-if)# ip igmp querier-timeout 120</pre> | <p>Specifies the IGMP query timeout.</p> <p>The default is 60 seconds (twice the query interval). The range is 60 to 300.</p> <p>Note To return to the default setting, use the no ip igmp querier-timeout interface configuration command.</p> |
| Step 5 | end Example: <pre>Switch(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 6 | show ip igmp interface [<i>interface-id</i>] Example: <pre>Switch# show ip igmp interface</pre> | Verifies your entries. |
| Step 7 | copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Changing the Maximum Query Response Time for IGMPv2

If you are using IGMPv2, you can change the maximum query response time advertised in IGMP queries. The maximum query response time enables the switch to quickly detect that there are no more directly connected group members on a LAN. Decreasing the value enables the switch to prune groups faster.

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp query-max-response-time** *seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters the global configuration mode. |
| Step 3 | interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet 1/0/1 | <p>Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode.</p> <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> • A routed port—A physical port that has been configured as a Layer 3 port by entering the no switchport interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group. For a configuration example, see Example: Interface Configuration as a Routed Port. • An SVI—A VLAN interface created by using the interface vlan <i>vlan-id</i> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. For a configuration example, see Example: Interface Configuration as an SVI. <p>These interfaces must have IP addresses assigned to them.</p> |
| Step 4 | ip igmp query-max-response-time <i>seconds</i> | <p>Changes the maximum query response time advertised in IGMP queries. The default is 10 seconds. The range is 1 to 25.</p> |

| | Command or Action | Purpose |
|---------------|---|--|
| | Example: <pre>Switch(config-if)# ip igmp query-max-response-time 15</pre> | Note To return to the default setting, use the no ip igmp query-max-response-time interface configuration command. |
| Step 5 | end Example: <pre>Switch(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 6 | show ip igmp interface [<i>interface-id</i>] Example: <pre>Switch# show ip igmp interface</pre> | Verifies your entries. |
| Step 7 | copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Configuring the Switch as a Statically Connected Member

At various times, either there is not a group member on a network segment or a host that cannot report its group membership by using IGMP. However, you may want multicast traffic to be sent to that network segment. The following commands are used to pull multicast traffic down to a network segment:

- **ip igmp join-group**—The switch accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the switch from fast switching.
- **ip igmp static-group**—The switch does not accept the packets itself, but only forwards them. This method enables fast switching. The outgoing interface appears in the IGMP cache, but the switch itself is not a member, as evidenced by lack of an L (local) flag in the multicast route entry.

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp static-group** *group-address*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters the global configuration mode. |
| Step 3 | interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet 1/0/1 | <p>Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode.</p> <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> • A routed port—A physical port that has been configured as a Layer 3 port by entering the no switchport interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group. For a configuration example, see Example: Interface Configuration as a Routed Port. • An SVI—A VLAN interface created by using the interface vlan <i>vlan-id</i> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. For a configuration example, see Example: Interface Configuration as an SVI. <p>These interfaces must have IP addresses assigned to them.</p> |
| Step 4 | ip igmp static-group <i>group-address</i> | Configures the switch as a statically connected member of a group. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Example: <pre>Switch(config-if)# ip igmp static-group 239.100.100.101</pre> | By default, this feature is disabled. |
| Step 5 | end Example: <pre>Switch(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 6 | show ip igmp interface [<i>interface-id</i>] Example: <pre>Switch# show ip igmp interface gigabitethernet 1/0/1</pre> | Verifies your entries. |
| Step 7 | copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Monitoring IGMP

You can display specific statistics, such as the contents of IP routing tables, caches, and databases.



Note This release does not support per-route statistics.

You can display information to learn resource usage and solve network problems. You can also display information about node reachability and discover the routing path that packets of your device are taking through the network.

You can use any of the privileged EXEC commands in the following table to display various routing statistics.

Table 3: Commands for Displaying System and Network Statistics

| Command | Purpose |
|--|--|
| ping [<i>group-name</i> <i>group-address</i>] | Sends an ICMP Echo Request to a multicast group address. |

| Command | Purpose |
|---|---|
| <code>show ip igmp groups [type-number detail]</code> | Displays the multicast groups that are directly connected to the switch and that were learned through IGMP. |
| <code>show ip igmp interface [type number]</code> | Displays multicast-related information about an interface. |
| <code>show ip igmp profile [profile_number]</code> | Displays IGMP profile information. |
| <code>show ip igmp ssm-mapping [hostname/IP address]</code> | Displays IGMP SSM mapping information. |
| <code>show ip igmp static-group {class-map [interface [type]]}</code> | Displays static group information. |
| <code>show ip igmp vrf</code> | Displays the selected VPN routing/forwarding instance by name. |

Configuration Examples for IGMP

Example: Configuring the Switch as a Member of a Multicast Group

This example shows how to enable the switch to join multicast group 255.2.2.2:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
Switch(config-if)#
```

Related Topics

[Configuring the Switch as a Member of a Group](#), on page 8

[IGMP Join Process](#), on page 6

[IGMP Leave Process](#), on page 7

Example: Controlling Access to IP Multicast Groups

This example shows how to configure hosts attached to a port as able to join only group 255.2.2.2:

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp access-group 1
```

Related Topics

[Controlling Access to IP Multicast Group](#), on page 10

Additional References

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference, Cisco Release 15.2(2)E (Industrial Ethernet 3010 Switch)</i> |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Cisco IOS IP SLAs commands | Cisco IOS IP Multicast Command Reference |

Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

Standards and RFCs

| Standard/RFC | Title |
|--------------|--|
| RFC 1112 | Host Extensions for IP Multicasting |
| RFC 2236 | Internet Group Management Protocol, Version 2 |
| RFC 3376 | <i>Internet Group Management Protocol, Version 3</i> |

MIBs

| MIB | MIBs Link |
|--------------------------------------|--|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|--|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p>http://www.cisco.com/support</p> |