IGMP and IGMP Snooping

IP multicast is the transmission of data packets to multiple hosts through a common IP address. Networks use Internet Group Management Protocol (IGMP) to control the flow of layer 3 multicast traffic. Hosts request and maintain multicast group membership through IGMP messages. IGMP snooping is a layer 2 optimization for the layer 3 IGMP protocol that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets.

These sections describe the Arista IGMP and IGMP snooping implementation.

- Section 39.1: Introduction
- Section 39.2: IGMP Protocols
- Section 39.3: Configuring IGMP
- Section 39.4: Configuring IGMP Snooping
- Section 39.5: IGMP Host Proxy
- Section 39.6: IGMP and IGMP Snooping Commands

39.1 Introduction

39.1.1 Supported Features

For a list of the IGMP features that each Arista switch platform supports, referred to the supported features table here: https://www.arista.com/en/support/product-documentation/supported-features.
39.2 IGMP Protocols

39.2.1 IGMP

Networks use Internet Group Management Protocol (IGMP) to control the flow of layer 3 multicast traffic. Hosts request and maintain multicast group membership through IGMP messages. Multicast routers use IGMP to maintain a membership list of active multicast groups for each attached network.

- IGMP version 1 is defined in RFC 1112. Hosts can join multicast groups without a method to leave a group. Routers use a timeout-based process to determine when hosts lose interest in a group.
- IGMP version 2 is defined in RFC 2236. Version 2 adds leave messages that hosts use to terminate group membership.
- IGMP version 3 is defined in RFC 4604. Version 3 allows hosts to specify IP addresses within a group from where they receive traffic. Traffic from all other group addresses is blocked from the host.

With respect to each of its attached networks, a multicast router is either a querier or non-querier. Each physical network contains only one querier. A network with more than one multicast router designates the router with the lowest IP address as its querier.

Queriers solicit group membership information by periodically sending General Query messages. Queriers also receive unsolicited messages from hosts joining or leaving a multicast group. When a querier receives a message from a host, it updates its membership list for the group referenced in the message and the network where the message originated.

Queriers forward multicasts from remote sources only to networks as specified by its membership list. If a querier does not receive a report from a network host for a specific group, it removes the corresponding entry from the table and discontinues forwarding multicasts for that group on the network. Queriers also send group-specific queries after receiving a leave request from a host to determine if the network still contains active multicast group members. If it does not receive a membership report during the period defined by the last member query response interval, the querier removes the group-network entry from the membership list.

When a host receives a General Query, it responds with Membership Report messages for each of its multicast groups within the interval specified by the Max Response Time field in the query. IGMP suppresses multiple messages from different hosts on a network for the same group. Hosts send unsolicited Membership reports to join a multicast group and send leave messages to exit a group.

39.2.2 IGMP Snooping

IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients.

When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient’s port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient’s port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router’s port to the port list for all multicast groups.
**Snooping Querier**

Snooping requires an IGMP querier in the network to create multicast group tables. An IGMP snooping querier performs the multicast router (mrouter) role when the network does not have a router. When the snooping querier is enabled on a VLAN, the switch periodically broadcasts IGMP queries and listens for IGMP Reports that indicate host group memberships.

Networks that contain multiple snooping queriers elect one as the querier, based on IP address. When IGMP snooping querier is enabled on a VLAN, the switch performs as a querier only when it is elected or it is the only snooping querier on the network.

**L2 ReportFlooding**

L2 report flooding is an IGMP snooping feature that forwards membership report messages to specified ports. Relying on a single switch to maintain and send report messages can degrade performance. L2 report flooding addresses this by facilitating report message forwarding through any network port. This allows switches to bypass the querier when forwarding multicast traffic to its interested ports.

**IGMP Snooping Proxy**

IGMP snooping proxy is an enhancement over IGMP snooping. When snooping proxy is enabled, the switch starts sending proxy queries periodically to the downstream hosts and collects the IGMP reports and updates the local state. Later, when the switch receives an IGMP query from an upstream router, the switch immediately responds with a report based on its local state.

When IGMP snooping proxy is disabled, the IGMP queries in VLAN, and the reports from hosts are flooded. Enabling IGMP snooping proxy prevents a sudden burst in IGMP report traffic in response to every query. It also reduces the number of reports that the IGMP Querier needs to process in the VLAN. However, it introduces a latency in the propagation of the IGMP state through the VLAN.
39.3 Configuring IGMP

This section describes the following configuration tasks:

- Section 39.3.1: Enabling IGMP
- Section 39.3.2: Configuring IGMP Settings

39.3.1 Enabling IGMP

Enabling PIM also enables IGMP on that interface. When the switch fills the multicast routing table, it only adds interfaces when the interface receives join messages from downstream devices or when the interface is directly connected to a member of the IGMP group.

By default, PIM and IGMP are disabled on an interface. Use the `pim ipv4 sparse-mode` or `pim ipv4 bidirectional` command to enable PIM and IGMP on the configuration mode interface.

Example

- This command enables PIM and IGMP on VLAN interface 8.

  ```
  switch(config)#interface vlan 8
  switch(config-if-Vl8)#pim ipv4 sparse-mode
  switch(config-if-Vl8)#
  ```

In the unlikely event that the IGMP agent needs to run on an interface without PIM being enabled, use the `ip igmp` command.

Example

- This command enables IGMP on VLAN interface 8 without enabling PIM.

  ```
  switch(config)#interface vlan 8
  switch(config-if-Vl8)#ip igmp
  switch(config-if-Vl8)#
  ```

39.3.2 Configuring IGMP Settings

An interface that runs IGMP uses default protocol settings unless otherwise configured. The switch provides commands that alter startup query, last member query, and normal query settings.

IGMP Version

The switch supports IGMP versions 1 through 3. The `ip igmp version` command configures the IGMP version on the configuration mode interface. Version 3 is the default IGMP version.

Example

- This command configures IGMP version 3 on VLAN interface 4

  ```
  switch(config)#interface vlan 4
  switch(config-if-Vl4)#ip igmp version 3
  switch(config-if-Vl4)#
  ```

Startup Query

Membership queries are sent at an increased frequency immediately after an interface starts up to quickly establish the group state. Query count and query interval commands adjust the period between membership queries for a specified number of messages.

The `ip igmp startup-query-interval` command specifies the interval between membership queries that an interface sends immediately after it starts up. The `ip igmp startup-query-count` command specifies the number of queries that the switches sends from the interface at the startup interval rate.
Example

- These commands define a startup interval of 15 seconds for the first 10 membership queries sent from VLAN interface 12.
  
  ```
  switch(config)#interface vlan 12
  switch(config-if-Vl12)#ip igmp startup-query-interval 150
  switch(config-if-Vl12)#ip igmp startup-query-count 10
  switch(config-if-Vl12)#
  ```

Membership Queries

The router with the lowest IP address on a subnet sends membership queries as the IGMP querier. When a membership query is received from a source with a lower IP address, the router resets its query response timer. Upon timer expiry, the router begins sending membership queries. If the router subsequently receives a membership query originating from a lower IP address, it stops sending membership queries and resets the query response timer.

The `ip igmp query-interval` command configures the frequency at which the active interface, as an IGMP querier, sends membership query messages.

The `igmp query-max-response-time` command configures the time that a host has to respond to a membership query.

Example

- These commands define a membership query interval of 75 seconds and a query response timer reset value of 45 seconds for queries sent from VLAN interface 15.
  
  ```
  switch(config)#interface vlan 15
  switch(config-if-Vl15)#ip igmp query-interval 75
  switch(config-if-Vl15)#igmp query-max-response-time 450
  switch(config-if-Vl15)#
  ```

Last Member Query

When the querier receives an IGMP leave message, it verifies the group has no remaining hosts by sending a set of group-specific queries at a specified interval. If the querier does not receive a response to the queries, it removes the group state and discontinues multicast transmissions.

The `ip igmp last-member-query-count (LMQC)` command specifies the number of query messages the router sends in response to a group-specific or group-source-specific leave message.

The `ip igmp last-member-query-interval` command configures the transmission interval for sending group-specific or group-source-specific query messages to the active interface.

Example

- These commands program the switch to send 3 query messages, one every 25 seconds, when VLAN interface 15 receives an IGMP leave message.
  
  ```
  switch(config)#interface vlan 15
  switch(config-if-Vl15)#ip igmp last-member-query-interval 250
  switch(config-if-Vl15)#ip igmp last-member-query-count 3
  switch(config-if-Vl15)#
  ```

Static Groups

The `ip igmp static-group` command configure the configuration mode interface as a static member of the multicast group at the specified address. The router forwards multicast group packets through the interface without otherwise appearing or acting as a group member. No interface is a static member of a multicast group by default.
To become a static member of a multicast group, the switch must be the PIM designated router (DR) for the network. If it is not, you can use the `pim ipv4 dr-priority` command to make it the DR by configuring its PIM DR value to be the highest on the network.

**Example**

- These commands configure VLAN interface 15 as the PIM designated router, then configure it as a static member of the multicast group at address 231.1.1.15 for multicast data packets that originate at 10.1.1.1.

```plaintext
switch(config)#interface vlan 15
switch(config-if-Vl15)#pim ipv4 dr-priority 5000
switch(config-if-Vl15)#ip igmp static-group 231.1.1.45 10.1.1.1
switch(config-if-Vl15)#
```
39.4 Configuring IGMP Snooping

This section describes the following configuration tasks:

- Section 39.4.1: Enabling Snooping
- Section 39.4.2: Configuring Snooping Parameters
- Section 39.4.3: Snooping Querier
- Section 39.4.4: IGMP Snooping L2 Report Flooding
- Section 39.4.5: IGMP Snooping Filters
- Section 39.4.6: Configuring IGMP Snooping Proxy

39.4.1 Enabling Snooping

The switch provides two control settings for snooping IGMP packets:

- Global settings control the availability of IGMP snooping on the switch. Snooping is globally enabled by default.
- Per-VLAN settings control IGMP on individual VLANs. If snooping is enabled on the VLAN, it follows the global snooping state.

The `ip igmp snooping` command controls the global snooping setting. The `ip igmp snooping vlan` command configures snooping on individual VLANs.

Examples

- This command globally enables snooping on the switch.
  
  ```
  switch(config)#ip igmp snooping
  switch(config)#
  ```

- This command disables snooping on VLANs 2 through 4.
  
  ```
  switch(config)#no ip igmp snooping vlan 2-4
  switch(config)#
  ```

39.4.2 Configuring Snooping Parameters

Specifying a Static Multicast Router Connection

The `ip igmp snooping vlan multicast-router` command statically configures a port that connects to a multicast router to join all multicast groups. The port to the router must be in the specified VLAN range.

Snooping may not always be able to locate the IGMP querier. This command is for IGMP queriers that are known to connect through the network to a port on the switch.

Example

- This command configures the static connection to a multicast router through Ethernet port 3.
  
  ```
  switch(config)#ip igmp snooping vlan 2 mrouter interface ethernet 3
  switch(config)#
  ```

Adding a Port to a Multicast Group

The `ip igmp snooping vlan member` command adds an a port to a multicast group. The IP address must be an unreserved IPv4 multicast address. The interface to the port must be in the specified VLAN range.
Example

- This command configures the static connection to a multicast group at 237.2.1.4 through Ethernet port 3.

```
switch(config)#ip igmp snooping vlan 7 static 237.2.1.4 interface ethernet 3
switch(config)#
```

Robustness Variable

The robustness variable specifies the number of unacknowledged snooping queries that a switch sends before removing the recipient from the group list.

The `ip igmp snooping robustness-variable` command configures the robustness variable for all snooping packets sent from the switch. The default value is 2.

Example

- This command sets the robustness-variable value to 3.

```
switch(config)#ip igmp snooping robustness-variable 3
switch(config)#
```

Configuring Interface Startup Initial Query Times

The `ip igmp snooping interface-restart-query` command configures the interface startup initial query times in milliseconds. If nothing is configured, a default value of 2000 milliseconds is used. Issuing the command replaces any values already configured. Multiple values may be input in a single command; this makes the mechanism more resilient in the case of dropped packets.

Examples

- This command configures interfaces to send IGMP queries at 1000, 2000, and 4000 milliseconds (i.e., 1 second, 2 seconds, and 4 seconds) after an interface restart or spanning tree change.

```
switch(config)#ip igmp snooping interface-restart-query 1000 2000 4000
switch(config)#
```

Example

- This command configures interfaces to send a single IGMP query of 5000 milliseconds (5 seconds) after an interface restart or spanning tree change.

```
switch(config)#ip igmp snooping interface-restart-query 5000
switch(config)#
```

39.4.3 Snooping Querier

The IGMP snooping querier supports snooping by sending layer 2 membership queries to hosts attached to the switch. Note that if IGMP snooping is enabled, QoS will not apply to IGMP packets.

39.4.3.1 Enabling the Snooping Querier

Enabling the snooping querier on an interface requires the explicit configuration of a global querier address or a local querier address for the interface. See Section 39.4.3.2.

The switch provides two control settings for controlling the snooping querier:

- The global setting controls the querier on VLANs for which there is no snooping querier command.
- VLAN querier settings take precedence over the global querier setting.

The `ip igmp snooping querier` command controls the global querier setting. When enabled globally, the querier is controlled on individual VLANs through the `ip igmp snooping vlan querier` command.
The **ip igmp snooping vlan querier** command controls the querier for the specified VLANs. VLANs follow the global querier setting unless overridden by one of these commands:

- **ip igmp snooping vlan querier** enables the querier on specified VLANs.
- **no ip igmp snooping vlan querier** disables the querier on specified VLANs.

**Example**

- These commands globally enables the snooping querier on the switch, explicitly disables snooping on VLANs 1-4, and explicitly enables snooping on VLANs 5-8.

  ```plaintext
  switch(config)#ip igmp snooping querier
  switch(config)#no ip igmp snooping vlan 1-4 querier
  switch(config)#ip igmp snooping vlan 5-8 querier
  switch(config)#
  ```

- This command removes the querier setting for VLANs 3-6:

  ```plaintext
  switch(config)#default ip igmp snooping vlan 3-6 querier
  switch(config)#
  ```

**Globally Set the Snooping Querier Version**

The **ip igmp snooping querier version** command configures the IGMP snooping querier version. Version 2 is the default IGMP snooping version.

**Example**

- This command globally configures IGMP snooping querier version 2.

  ```plaintext
  switch(config)#ip igmp snooping querier version 2
  switch(config)#
  ```

The **ip igmp snooping vlan querier version** command configures IGMP globally on the VLAN. Version 2 is the default IGMP snooping version.

**Example**

- This command configures IGMP snooping vlan querier version VLAN 5.

  ```plaintext
  switch(config)#ip igmp snooping vlan 5 querier version 2
  switch(config)#
  ```

### 39.4.3.2 Configuring Snooping Querier Parameters

**Querier Address**

The switch provides two IP addresses for setting the querier source:

- The global address is used by VLANs for which there is no querier address command.
- VLAN querier address settings take precedence over the global querier address.

The snooping querier address specifies the source IP address for IGMP snooping query packets that the switch transmits. The source address is also used to elect a snooping querier when the subnet contains multiple snooping queriers.

The default global querier address is not defined. When the configuration includes a snooping querier, a querier address must be defined globally or for each interface that enables a querier.

The **ip igmp snooping querier address** command sets the global querier source IP address for the switch. VLANs use the global address unless overwritten with the **ip igmp snooping vlan querier address** command. The default global address is not defined.
The `ip igmp snooping vlan querier address` command sets the source IP address for query packets transmitted from the specified VLAN. This command overrides the `ip igmp snooping querier address` for the specified VLAN.

**Examples**

- This command sets the source IP address for query packets that the switch transmits to 10.1.1.41.
  
  ```
  switch(config)#ip igmp snooping querier address 10.1.1.41
  switch(config)#
  ```

- This command sets the source IP address for query packets that VLAN 2 transmits to 10.14.1.1.
  
  ```
  switch(config)#ip igmp snooping vlan 2 querier address 10.14.1.1
  switch(config)#
  ```

**Membership Query Interval**

The query interval is the period (seconds), between IGMP Membership Query message transmissions. The interval ranges from 5 to 3600 seconds.

The `ip igmp snooping querier query-interval` command specifies the global query interval for packets the switch sends as a snooper querier. The default global setting is 125 seconds.

The `ip igmp snooping vlan querier query-interval` command specifies the query interval for packets sent from the snooping querier to the specified VLAN, overriding the global setting. VLANs that do not specify a query interval use the global setting.

**Examples**

- This command sets a query interval of 150 seconds for queries transmitted from VLANs for which a query interval is not configured.
  
  ```
  switch(config)#ip igmp snooping querier query-interval 150
  switch(config)#
  ```

- This command sets the query interval of 240 seconds for queries transmitted from VLAN 2.
  
  ```
  switch(config)#ip igmp snooping vlan 2 querier query-interval 240
  switch(config)#
  ```

**Membership Query Response Interval**

The Max Response Time field, in Membership Query messages, specifies the longest time a host can wait before responding with a Membership Report message. In all other messages, the sender sets the field to zero and the receiver ignores it. The switch provides two values for setting this field:

- The global value is used by VLANs for which there is no Max Response Time command.
- VLAN values take precedence over the global value for the specified VLAN.

The `ip igmp snooping querier max-response-time` command specifies the global Max Response Time value used in snooping query packets transmitted from the switch. Values range from 1 to 25 seconds with a default of 10 seconds. VLANs use the global setting unless overwritten with the `ip igmp snooping vlan querier max-response-time` command.

The `ip igmp snooping vlan querier max-response-time` command configures the Max Response Time field contents for packets transmitted from the specified VLAN, overriding the global setting.
Examples

- This command sets the maximum response time of 15 seconds for queries transmitted from VLANs for which a maximum response time is not configured.
  
  switch(config)#ip igmp snooping querier max-response-time 15
  switch(config)#

- This command sets a maximum response time of 5 seconds for queries that VLAN 2 transmits.
  
  switch(config)#ip igmp snooping vlan 2 querier max-response-time 5
  switch(config)#

Last Member Query

When the querier receives an IGMP leave message, it verifies the group has no remaining hosts by sending a set of group-specific queries at a specified interval. If the querier does not receive a response to the queries, it removes the group state and discontinues multicast transmissions.

The switch provides two values for setting this field:

- The global value is used by VLANs for which there is no last-member-query-interval defined.
- VLAN values take precedence over the global value for the specified VLAN.

The `ip igmp snooping querier last-member-query-interval` command specifies the global last-member-query-interval used in snooping query packets transmitted from the switch. This value is used for VLANs that do not have a value specified. Values range from 1 to 25 seconds with a global default of one second.

The `ip igmp snooping vlan querier last-member-query-interval` command configures the last-member-query-interval field contents for packets transmitted from the specified VLAN, overriding the global setting.

Example

- This command sets the global snooping querier last-member-query-interval to five seconds and the VLAN 10 last-member-query-interval to 12 seconds.
  
  switch(config)#ip igmp snooping querier last-member-query-interval 5
  switch(config)#ip igmp snooping vlan 10 querier last-member-query-interval 12
  switch(config)#

Interface Restart Query Spoofing

When the port status (link status or spanning tree status) changes, an IGMP general query is spoofed based on the information of the last known IGMP querier. This facilitates faster network convergence time.

By default, interfaces wait 2000 milliseconds before sending the spoofed IGMP query. To configure the delay before the spoofed query is sent, use the `ip igmp snooping interface-restart-query` command. This setting is applied to all ports.

Example

- This command configures the switch to send general IGMP queries at 100 milliseconds, 200 milliseconds, and 300 milliseconds after interface restart or spanning tree status change.
  
  switch(config)# ip igmp snooping interface-restart-query 100 200 300
39.4.4 IGMP Snooping L2 Report Flooding

L2 report flooding is an IGMP snooping feature that forwards membership report messages to specified ports. Report flooding is disabled by default and must be enabled globally before it can be enabled on individual interfaces.

The list of ports that can forward membership report messages must be explicitly configured. Commands are available to define lists of ports that are valid for all VLANs and port lists that are valid for specified VLAN ranges. Ports can forward membership reports only if they are configured to handle VLAN traffic, regardless of any report flooding configuration settings.

Enabling L2 Report Flooding

These commands enable L2 report flooding:

- `ip igmp snooping report-flooding` enables report flooding globally.
- `ip igmp snooping vlan report-flooding` enables report flooding on a specified VLAN range.

Example

- These commands enable L2 report flooding globally, and on VLANs 201-205.

  ```
  switch(config)#ip igmp snooping report-flooding
  switch(config)#ip igmp snooping vlan 201-205 report-flooding
  switch(config)#
  ```

Configuring Forwarding Ports

These commands specify the ports that forward membership report messages:

- `ip igmp snooping report-flooding switch-port` configures ports globally.
- `ip igmp snooping vlan report-flooding switch-port` configures ports for a specified VLAN range.

Example

- These commands enable Ethernet ports 5-9 to forward reports on all VLANs and ports 12-15 on VLANs 201-205.

  ```
  switch(config)#ip igmp snooping report-flooding switch-port ethernet 5-9
  switch(config)#ip igmp snooping vlan 201-205 report-flooding switch-port ethernet 12-15
  switch(config)#
  ```

39.4.5 IGMP Snooping Filters

IGMP snooping filters assigns IGMP profiles only to Layer 2 interfaces, and for Layer 3 interfaces use multicast boundary filters to control the multicast groups that the interfaces can join. An IGMP profile specifies a filter type and a list of address ranges. The address ranges comprise the multicast groups covered by the profile. The filter type determines an interface’s accessibility to the multicast groups:

- Permit filters define the multicast groups the interface can join.
- Deny filters define the multicast groups the interface cannot join.

Profiles are created in IGMP-profile configuration mode, then applied to an interface in interface configuration mode.

The `ip igmp profile` command places the switch in IGMP profile configuration mode. The `permit / deny` and `range` commands specify the profile’s filter type and address range. A profile may contain multiple range statements to define a discontiguous address range.
Example

- These commands create an IGMP profile named list_1 by entering IGMP-profile configuration mode, configure the profile to permit multicast groups 231.22.24.0 through 231.22.24.127, and return the switch to global configuration mode.

```plaintext
switch(config)#ip igmp profile list_1
switch(config-igmp-profile-list_1)#permit
switch(config-igmp-profile-list_1)#range 231.22.24.0 231.22.24.127
switch(config-igmp-profile-list_1)#exit
switch(config)#
```

The `ip igmp snooping filter` command applies an IGMP profile to the configuration mode interface.

Example

- These commands apply the `list_1` snooping profile to Ethernet interface 7.

```plaintext
switch(config)#interface ethernet 7
switch(config-if-Et7)#ip igmp snooping filter list_1
switch(config-if-Et7)#
```

39.4.5.1 Verifying IGMP Snooping

Show commands are available to display various configurations and IGMP snooping status. IGMP snooping that are viewable include:

- `show ip igmp snooping`
- `show ip igmp snooping counters`
- `show igmp snooping querier`
- `show igmp snooping querier counters`
- `show igmp snooping querier membership`

**IGMP Snooping Status**

The `show ip igmp snooping` command displays the switch's IGMP snooping configuration.

Example

- This command displays the switch's IGMP snooping configuration.

```plaintext
switch>show ip igmp snooping
    Global IGMP Snooping configuration:
----------------------------------------
IGMP snooping                  : Enabled
Robustness variable            : 2                      

Vlan 1 :
--------
IGMP snooping                  : Enabled
Multicast router learning mode : pim-dvmrp

Vlan 20 :
--------
IGMP snooping                  : Enabled
Multicast router learning mode : pim-dvmrp

Vlan 2028 :

switch>
```
IGMP Snooping Counters

The `show ip igmp snooping counters` command displays the number of IGMP messages sent and received through each switch port. The display table sorts the messages by type.

**Example**

- This command displays the number of messages received on each port.

```
switch>show ip igmp snooping counters
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Queries</td>
<td>Reports</td>
</tr>
<tr>
<td>Cpu</td>
<td>15249</td>
<td>106599</td>
</tr>
<tr>
<td>Et1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et2</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Et3</td>
<td>0</td>
<td>10905</td>
</tr>
<tr>
<td>Et4</td>
<td>0</td>
<td>44475</td>
</tr>
<tr>
<td>Et5</td>
<td>0</td>
<td>355</td>
</tr>
<tr>
<td>Et6</td>
<td>0</td>
<td>475</td>
</tr>
<tr>
<td>Et7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et8</td>
<td>0</td>
<td>578</td>
</tr>
<tr>
<td>Et9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et10</td>
<td>0</td>
<td>12523</td>
</tr>
<tr>
<td>Et11</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et12</td>
<td>0</td>
<td>4509</td>
</tr>
<tr>
<td>Et13</td>
<td>0</td>
<td>392</td>
</tr>
<tr>
<td>Et14</td>
<td>0</td>
<td>88</td>
</tr>
<tr>
<td>Et15</td>
<td>0</td>
<td>16779</td>
</tr>
<tr>
<td>Et16</td>
<td>0</td>
<td>2484</td>
</tr>
<tr>
<td>Et17</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et18</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>Et19</td>
<td>0</td>
<td>4110</td>
</tr>
<tr>
<td>Et20</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et21</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et22</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et23</td>
<td>0</td>
<td>5439</td>
</tr>
<tr>
<td>Et24</td>
<td>0</td>
<td>2251</td>
</tr>
<tr>
<td>Po1</td>
<td>45360</td>
<td>540670</td>
</tr>
<tr>
<td>Po2</td>
<td>0</td>
<td>101399</td>
</tr>
<tr>
<td>Switch</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

IGMP Snooping Querier

The `show igmp snooping querier` command displays snooping querier configuration and status information. Command provides options to only include specific VLANs.

**Example**

- This command displays the querier IP address, version, and port servicing each VLAN.

```
switch>show igmp snooping querier
```

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>Version</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.17.0.37</td>
<td>v2</td>
<td>Po1</td>
</tr>
<tr>
<td>20</td>
<td>172.17.20.1</td>
<td>v2</td>
<td>Po1</td>
</tr>
<tr>
<td>26</td>
<td>172.17.26.1</td>
<td>v2</td>
<td>Cpu</td>
</tr>
<tr>
<td>2028</td>
<td>172.17.255.29</td>
<td>v2</td>
<td>Po1</td>
</tr>
</tbody>
</table>

switch>
Chapter 39: IGMP and IGMP Snooping

Configuring IGMP Snooping

**IGMP Snooping Querier Counters**

The `show igmp snooping querier counters` command displays the counters from the querier, as learned through Internet Group Management Protocol (IGMP).

**Example**

- This command displays the counters from the querier.

```
switch>show igmp snooping querier counters
------------------------------------------
Vlan: 1    IP Addr: 100.0.0.1       Op State: Querier     Version: v3
v1 General Queries Sent         :0
v1 Queries Received             :0
v1 Reports Received             :0
v2 General Queries Sent         :1
v2 Queries Received             :0
v2 Reports Received             :25
v2 Leaves Received              :0
v3 General Queries Sent         :655
v3 GSQ Queries Sent             :0
v3 GSSQ Queries Sent            :8
v3 Queries Received             :654
v3 Reports Received             :2385
Error Packets                   :0
Other Packets                   :0
```

**IGMP Snooping Querier Membership**

The `show igmp snooping querier membership` command displays the membership from the querier, as learned through Internet Group Management Protocol (IGMP).

**Example**

- This command displays the membership from the querier for VLAN 1.

```
switch>show igmp snooping querier membership
------------------------------------------
Vlan: 1    Elected: 100.0.0.1       QQI: 125  QRV: 2  QRI: 10  GMI: 260
Groups           Mode  Ver  Num of Sources
------------------------------------------
10.0.0.2        EX    v3   0     []
10.0.0.3        IN    v3   2     [ 3.3.3.3, 3.3.3.4 ]
10.0.0.4        EX    v3   0     []
10.0.0.13       EX    v3   0     []
10.0.0.22       EX    v3   0     []
10.0.0.1        IN    v3   3     [ 5.6.7.9, 5.6.7.8, ... ]
```

39.4.6 Configuring IGMP Snooping Proxy

Use the `ip igmp snooping proxy` command to enable IGMP snooping proxy globally. Enabling IGMP snooping proxy enables it for all VLANs where IGMP snooping is enabled. IGMP snooping proxy is globally disabled by default.

Use the `ip igmp snooping proxy` command to enable IGMP snooping proxy globally. Use the `no ip igmp snooping vlan` proxy command to disable IGMP snooping proxy on specified VLANs.
Examples

• This command globally enables IGMP snooping proxy on the switch.

  switch(config)#ip igmp snooping proxy
  switch(config)#

• This command disables IGMP snooping proxy on VLANs 2 through 4.

  switch(config)#no ip igmp snooping proxy vlan 2-4 proxy
  switch(config)#

39.4.6.1 Configuring Snooping Proxy Querier

To configure the IGMP snooping proxy querier use the existing **ip igmp snooping querier** commands. For more information on these commands, please refer to section 35.4.3 from the document.

Note

The proxy querier by default uses 0.0.0.0 IP address.

Example

In this example, IGMP snooping proxy is enabled using the **ip igmp snooping proxy** command and the snooping proxy is set to reports for all the VLANs except VLANs 100 through 110 using the **ip igmp snooping vlan** command. The proxy querier operates in version 3 and sends queries at a 15-second interval and hosts can take up to 5 seconds to respond.

  switch(config)#ip igmp snooping proxy
  switch(config)#no ip igmp snooping vlan 100-110 proxy
  switch(config)#ip igmp snooping querier query-interval 15
  switch(config)#ip igmp snooping querier max-response-time 5
  switch(config)#ip igmp snooping querier version 3
  switch(config)#ip igmp snooping querier
  switch(config)#
39.5 IGMP Host Proxy

Interfaces on the switch can be configured to serve as IGMP host proxies. An IGMP host proxy exchanges IGMP reports (joins/leaves) between networks whose connection does not support PIM along network boundaries.

39.5.1 IGMP Host Proxy Description

Figure 39-1 displays a typical IGMP host-proxy implementation. The customer network connects to the sender network through the edge switch’s Ethernet 1 interface, which is configured as an IGMP host proxy. PIM is enabled within the sender and customer networks but not on the connection between the networks.

The IGMP proxy agent sends unsolicited IGMP joins when a (S,G) or (*,G) entry arrives in the multicast routing table (mroute table). Subsequently, IGMP reports are sent when queries or group-specific queries arrive on the host proxy interface. When the customer network is void of active listeners, the connection eventually expires and the senders stop transmitting to the network.

IGMP host proxy requires the following:

- PIM multicast border router (MBR) must be enabled on the interface.
- IP IGMP and IP multicast must be enabled.
- The switch must be an RP or in each host’s RP path.
- Fast-drop entries are required when there are no interested listeners for the group.

IGMP host proxy is configurable to filter for specific multicast groups and sources.

39.5.2 IGMP Host Proxy Configuration

Enabling IGMP Host Proxy

Enable PIM MBR on the interface using the `pim ipv4 border-router` command. The IGMP host proxy service is then configured on the interface using the `ip igmp host-proxy` command. When the host proxy is configured, it sends reports for (S,G) entries in the multicast routing (mroute) table if these are the only routes there; if there are any (*,G) entries, it sends reports only for these. To send reports for a specific group even when there is no (*, G) entry in the mroute table for that group, include the group address in the `ip igmp host-proxy` command. Multiple `ip igmp host-proxy` statements are required to specify multiple groups. The interval between IGMP reports is configured by `ip igmp host-proxy report-interval`.

Figure 39-1: IP IGMP Host Proxy Implementation
Host Proxy IGMP Version and Source Filtering

IGMP host proxies can be configured with IGMP versions 1, 2, or 3, and use version 3 by default. When the host-proxy IGMP version is set to 3, the proxy can explicitly include or exclude source addresses. Otherwise, include/exclude configuration for source addresses is ignored. The IGMP version of unsolicited reports is specified with the `ip igmp host-proxy version` command. Reports that are triggered by IGMP queries, however, are sent in the same IGMP version as the received query. (An interface may also have a different IGMP version configured on it for other purposes using the `ip igmp version` command.)

Using ACLs

IGMP host proxy can also be enabled for the addresses defined by an ACL; if one or more groups are configured in addition to ACLs, the groups are processed first. Implicit deny in the ACL is ignored, but if the ACL includes an explicit deny rule, then the interface sends joins only to groups configured directly on the interface or included in a permit ACL. Deny rules take precedence over permit rules. If a group is configured with no filters and a host-proxy is configured with an ACL with rules having filters for the group, or configured with groups and source filters, then the filters are applied to the group.

Disabling Host Proxy or Removing an Individual Group or Source

The `no igmp host-proxy` command can be entered with group or source parameters to remove the specified group or source from the list. Entering the `no igmp host-proxy` command without specifying group or source disables the forwarding of all IGMP reports on the interface.

Examples

- These commands enable IGMP host proxy on Ethernet interface 17 for all multicast group addresses.
  ```
  switch(config)#interface ethernet 17
  switch(config-if-Et17)#pim ipv4 border-router
  switch(config-if-Et17)#ip igmp host-proxy
  switch(config-if-Et17)#
  ```

- These commands enable IGMP host proxy on Ethernet interface 18 for the multicast group at 231.10.10.1. The list of source addresses is not restricted.
  ```
  switch(config)#interface ethernet 18
  switch(config-if-Et18)#pim ipv4 border-router
  switch(config-if-Et18)#ip igmp host-proxy 231.10.10.1
  switch(config-if-Et18)#
  ```

- These commands enable IGMP host proxy on Ethernet interface 19 for the multicast group at 231.10.10.2. The list of source addresses only excludes 10.4.4.1 and 10.4.5.2.
  ```
  switch(config)#interface ethernet 19
  switch(config-if-Et19)#pim ipv4 border-router
  switch(config-if-Et19)#ip igmp host-proxy 231.10.10.2 exclude 10.4.4.1
  switch(config-if-Et19)#ip igmp host-proxy 231.10.10.2 exclude 10.4.5.2
  switch(config-if-Et19)#
  ```

- These commands enable IGMP host proxy on Ethernet interface 16 for the multicast group at 231.10.10.3. The list of source addresses for this group only includes 10.5.5.1 and 10.5.5.2
  ```
  switch(config)#interface ethernet 16
  switch(config-if-Et16)#pim ipv4 border-router
  switch(config-if-Et16)#ip igmp host-proxy 231.10.10.3 include 10.5.5.1
  switch(config-if-Et16)#ip igmp host-proxy 231.10.10.3 include 10.5.5.2
  switch(config-if-Et16)#
  ```
• These commands configure an IGMP host proxy interval of five seconds on port channel 100.
  switch(config)#interface port-channel 100
  switch(config-if-Po100)#ip igmp host-proxy report-interval 5
  switch(config-if-Po100)#

• These commands enable IGMP host proxy on Ethernet interface 17 for the group address(es)
  specified in ACL “acl1.”
  switch(config)#interface ethernet 17
  switch(config-if-Et17)#pim ipv4 border-router
  switch(config-if-Et17)#ip igmp host-proxy access-list acl1
  switch(config-if-Et17)#
39.6 IGMP and IGMP Snooping Commands

IGMP Configuration Commands (Interface Configuration Mode)

- `igmp query-max-response-time`
- `ip igmp last-member-query-count`
- `ip igmp last-member-query-interval`
- `ip igmp query-interval`
- `ip igmp router-alert`
- `ip igmp startup-query-count`
- `ip igmp startup-query-interval`
- `ip igmp static-group`
- `ip igmp static-group acl`
- `ip igmp static-group range`
- `ip igmp version`

IGMP Clear Commands

- `clear ip igmp group`
- `clear ip igmp statistics`

IGMP Display Commands

- `show ip igmp groups`
- `show ip igmp groups count`
- `show ip igmp interface`
- `show ip igmp static-groups`
- `show ip igmp static-groups acl`
- `show ip igmp static-groups group`
- `show ip igmp statistics`

IGMP Snooping Configuration Commands (Global Configuration Mode)

- `ip igmp`
- `ip igmp profile`
- `ip igmp snooping`
- `ip igmp snooping proxy`
- `ip igmp snooping querier`
- `ip igmp snooping querier address`
- `ip igmp snooping querier last-member-query-count`
- `ip igmp snooping querier last-member-query-interval`
- `ip igmp snooping querier max-response-time`
- `ip igmp snooping querier query-interval`
- `ip igmp snooping querier startup-query-count`
- `ip igmp snooping querier startup-query-interval`
- `ip igmp snooping querier version`
- `ip igmp snooping report-flooding`
- `ip igmp snooping report-flooding switch-port`
- `ip igmp snooping restart query-interval`
- `ip igmp snooping robustness-variable`
- `ip igmp snooping vlan`
- `ip igmp snooping vlan fast-leave`
- `ip igmp snooping vlan max-groups`
- `ip igmp snooping vlan member`
- `ip igmp snooping vlan multicast-router`
Chapter 39: IGMP and IGMP Snooping

IGMP and IGMP Snooping Commands

- ip igmp snooping vlan proxy
- ip igmp snooping vlan querier
- ip igmp snooping vlan querier address
- ip igmp snooping vlan querier last-member-query-count
- ip igmp snooping vlan querier last-member-query-interval
- ip igmp snooping vlan querier max-response-time
- ip igmp snooping vlan querier query-interval
- ip igmp snooping vlan querier startup-query-count
- ip igmp snooping vlan querier startup-query-interval
- ip igmp snooping vlan querier version
- ip igmp snooping vlan report-flooding
- ip igmp snooping vlan report-flooding switch-port

IGMP Configuration Commands (Interface Configuration Mode)

- ip igmp snooping filter

IGMP Snooping Clear Commands

- clear ip igmp snooping counters

IGMP Snooping Display Commands

- show igmp snooping querier
- show igmp snooping querier counters
- show igmp snooping querier membership
- show ip igmp profile
- show ip igmp snooping
- show ip igmp snooping counters
- show ip igmp snooping counters ethdev-pams
- show ip igmp snooping groups
- show ip igmp snooping groups count
- show ip igmp snooping mrouter
- show ip igmp snooping report-flooding

IGMP Profile Configuration Mode Commands

- permit / deny
- range

IGMP Host Proxy Commands

- ip igmp host-proxy
- ip igmp host-proxy report-interval
- ip igmp host-proxy version
- show ip igmp host-proxy config-sanity
- show ip igmp host-proxy interface
clear ip igmp group

The `clear ip igmp group` command deletes IGMP cache entries as follows:

- `clear ip igmp group` all entries from the IGMP cache.
- `clear ip igmp group gp_addr` all entries for a specified multicast group.
- `clear ip igmp group interface int_id` all entries that include a specified interface.
- `clear ip igmp group gp_addr interface int_id` all entries for a specified interface in a specified group.

Command Mode
Privileged EXEC

Command Syntax
`clear ip igmp group [gp_addr] [interface INT_ID]`

Parameters
- `gp_addr` multicast group IP address (dotted decimal notation).
- `INT_ID` interface name. Options include:
  - `ethernet e_num` Ethernet interface specified by `e_num`.
  - `loopback l_num` Loopback interface specified by `l_num`.
  - `management m_num` Management interface specified by `m_num`.
  - `port-channel p_num` Port-channel interface specified by `p_num`.
  - `vlan v_num` VLAN interface specified by `v_num`.
  - `vxlan vx_num` VXLAN interface specified by `vx_num`.

Examples
- This command deletes all IGMP cache entries for the multicast group 231.23.23.14.
  `switch#clear ip igmp group 231.23.23.14`
  `switch#`

- This command deletes IGMP cache entries for Ethernet interface 16 in multicast group 226.45.10.45.
  `switch#clear ip igmp group 226.45.10.45 interface ethernet 16`
  `switch#`
**clear ip igmp snooping counters**

The `clear ip igmp snooping counters` command resets the snooping message counters for the specified interface. The snooping counters for all interfaces are reset if the command does not include an interface name.

The `show ip igmp snooping counters` command displays the counter contents. See the `show ip igmp snooping counters` command description for a list of available snooping counters.

**Command Mode**

Privileged EXEC

**Command Syntax**

```
clear ip igmp snooping counters [INT_NAME]
```

**Parameters**

- `INT_NAME` interface name. Formats include:
  - `ethernet e_num` Ethernet interface specified by `e_num`.
  - `port-channel p_num` Port-channel interface specified by `p_num`.
  - `switch` virtual interface to an L2 querier.

**Example**

- This command clears the snooping counters for messages received on Ethernet interface 15.
  ```
  switch(config)#clear ip igmp snooping counters ethernet 15
  switch(config)#
  ```
clear ip igmp statistics

The `clear ip igmp statistics` command resets IGMP transmission statistic counters for the specified interface.

**Command Mode**

Privileged EXEC

**Command Syntax**

```
clear ip igmp statistics [INTF_ID]
```

**Parameters**

- `INTF_ID` interface name. Options include:
  - `<no parameter>` all interfaces.
  - `interface ethernet e_num` Ethernet interface specified by `e_num`.
  - `interface loopback l_num` Loopback interface specified by `l_num`.
  - `interface management m_num` Management interface specified by `m_num`.
  - `interface port-channel p_num` Port-channel interface specified by `p_num`.
  - `interface vlan v_num` VLAN interface specified by `v_num`.
  - `interface xlan vx_num` VXLAN interface specified by `vx_num`.

**Examples**

- This command resets IGMP transmission statistic counters on Ethernet 1 interface.
  ```
  switch#clear ip igmp statistics interface ethernet 1
  switch#
  ```
**igmp query-max-response-time**

The `igmp query-max-response-time` command configures the `query-max-response-time` variable for the configuration mode interface. This variable is used to set the Max Response Time field in outbound Membership Query messages. Max Response Time specifies the maximum period a recipient can wait before responding with a Membership Report.

The router with the lowest IP address on a subnet sends membership queries as the IGMP querier. When a membership query is received from a source with a lower IP address, the router resets its query response timer. Upon timer expiry, the router begins sending membership queries. If the router subsequently receives a membership query originating from a lower IP address, it stops sending membership queries and resets the query response timer.

The `no igmp query-max-response-time` and `default igmp query-max-response-time` commands restore the default query-max-response-time of 10 seconds for the configuration mode interface by removing the corresponding `igmp query max-response-time` command from `running-config`.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration
- Router-IGMP Configuration

**Command Syntax**
- Interface-Ethernet Configuration, Interface-Port-Channel Configuration, and Interface-VLAN Configuration modes
  - `igmp query-max-response-time period`
  - `no igmp query-max-response-time`
  - `default igmp query-max-response-time`

- Router-IGMP Configuration mode
  - `query-max-response-time period`
  - `no query-max-response-time`
  - `default query-max-response-time`

**Parameters**
- `period` maximum response time (deciseconds). Values range from 1 to 31744 (52 minutes, 54 seconds). Default is 100 (ten seconds).

**Example**
- This command configures the query-max-response-time of 18 seconds for VLAN interface 4.
  
  ```
  switch(config)#interface vlan 4
  switch(config-if-Vl4)# igmp query-max-response-time 180
  switch(config-if-Vl4)#
  ```
**ip igmp host-proxy**

The `ip igmp host-proxy` command enables the IGMP host proxy service on the configuration mode interface. The IGMP host proxy performs IGMP joins and leaves between networks that are directly connected by an exchange that does not support PIM on the network boundary.

**Note**

For an interface to serve as an IGMP host proxy, PIM MBR must also be enabled on that interface using the `pim ipv4 border-router` command.

The IGMP host proxy sends unsolicited IGMP join reports when an (S,G) or (*,G) entry arrives in the multicast routing (mroute) table. Reports are subsequently sent upon the arrival of queries on the interface. The interval between IGMP reports is configured through `ip igmp host-proxy report-interval`.

The `ip igmp host-proxy` command can also specify a group address; this ensures that reports are generated for the specified group even if there is no (*,G) entry in the mroute table for that group. Multiple `ip igmp host-proxy` statements are required to specify multiple groups.

When the host proxy IGMP version is set to 3 using the `ip igmp host-proxy version` command, the `ip igmp host-proxy` command can also include or exclude source addresses. These options are ignored when the interface runs host proxy IGMP version 1 or 2. Note that the IGMP version set using the `ip igmp version` command does not affect host proxy behavior.

An ACL can also be used in place of a group address by using the `access-list` option. If one or more groups are configured in addition to ACLs, the groups are processed first. Implicit deny in the ACL is ignored, but if the ACL includes an explicit deny rule, then the interface sends joins only to groups configured directly on the interface or included in a permit ACL. Deny rules take precedence over permit rules. If a group is configured with no filters and a host-proxy is configured with an ACL with rules having filters for the group, or configured with groups and source filters, then the filters are applied to the group.

The `no ip igmp host-proxy` and `default ip igmp host-proxy` commands remove the corresponding `ip igmp host-proxy` command from `running-config`. When these commands do not include a group address, all `ip igmp host-proxy` statements are deleted. When inclusion or exclusion parameters are not specified, all statements with the specified group address are deleted.

**Command Mode**

- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

```
ip igmp host-proxy [GROUP_ADDRESS [SOURCE_ADDRESS]] | [access-list acl]
no ip igmp host-proxy [GROUP_ADDRESS [SOURCE_ADDRESS]]
default ip igmp host-proxy [GROUP_ADDRESS [SOURCE_ADDRESS]]
```

**Parameters**

- **GROUP_ADDRESS** IPv4 address of group address for which host proxy sends reports.
- `<no parameter>` only groups for which there is a (*,G) entry in the mroute table.
- **ipv4_address** IP address of multicast group (dotted decimal notation). This ensures that reports are generated for this group even if it does not have a (*,G) entry in the mroute table.
- **SOURCE_ADDRESS** IPv4 address of a host that originates multicast data packets.
- `<no parameter>` Proxy sends report for all received or configured groups regardless of source address.
- **exclude ipv4_address** Proxy does not send reports for specified source address.
• **include ipv4_address**  Proxy always sends reports for specified source address.

Commands that list at least one parameter must specify a group address.
Parameters may be listed in any order.
When a command specifies include and exclude parameters, the exclude parameter is ignored.

• **access-list acl**  specifies an access control list (ACL); a join is sent for all groups and/or sources obtained by processing the rules from all configured ACLs.

• **version version**  specifies the IGMP version on IGMP host-proxy interface. The value ranges from 1 to 3. Default value is 3.

**Guidelines**

Multiple statements for a group address may be configured. The effect of entering a command depends on previously entered commands. The following describes command combination:

• **ip igmp host-proxy**: IGMP host proxy is enabled for all multicast groups and their source addresses. When enabled for all group addresses, the source address list cannot be restricted.

• **ip igmp host-proxy group_ipv4**: IGMP host proxy is enabled for a specified multicast group. The list of source addresses for this group is not restricted. Enabling host proxy for another group address requires another **ip igmp host-proxy** command.

• **ip igmp host-proxy group_ipv4 exclude source_ipv4**: IGMP host proxy is enabled for the specified multicast group. Sources for this group include all addresses not in an exclude statement. Multiple source addresses for the group are excluded by multiple statements.

• **ip igmp host-proxy group_ipv4 include source_ipv4**: IGMP host proxy is enabled for the specified group address for only the specified source address. Additional statements are required to include other source addresses for the group. The presence of one include parameter invalidates all exclude statements for the specified multicast group.

• **ip igmp host-proxy access-list acl**: IGMP host proxy is enabled for the addresses defined by the specified ACL. If one or more groups are configured in addition to ACLs, the groups are processed first. If the ACL has a “deny all” rule for a group, then this filter takes precedence over configurations with include/exclude keywords or permit/deny rules for that group. If a group is configured with no filters and a host-proxy is configured with an ACL with rules having filters for the group, or configured with groups and source filters, then the filters are applied to the group.

**Example**

• These commands enable IGMP host proxy on Ethernet interface 17 for all multicast group addresses.

  switch(config)#interface ethernet 17
  switch(config-if-Et17)#pim ipv4 border-router
  switch(config-if-Et17)#ip igmp host-proxy
  switch(config-if-Et17)#

• These commands enable IGMP host proxy on Ethernet interface 17 for the multicast group at 231.10.10.1. The list of source addresses is not restricted.

  switch(config)#interface ethernet 17
  switch(config-if-Et17)#pim ipv4 border-router
  switch(config-if-Et17)#ip igmp host-proxy 231.10.10.1
  switch(config-if-Et17)#
• These commands enable IGMP host proxy on Ethernet interface 17 for the multicast group at 231.10.10.2. The list of source addresses only excludes 10.4.4.1 and 10.4.5.2.

```bash
switch(config)#interface ethernet 17
switch(config-if-Et17)#pim ipv4 border-router
switch(config-if-Et17)#ip igmp host-proxy 231.10.10.2 exclude 10.4.4.1
switch(config-if-Et17)#ip igmp host-proxy 231.10.10.2 exclude 10.4.5.2
switch(config-if-Et17)#
```

• These commands enable IGMP host proxy on Ethernet interface 17 for the multicast group at 231.10.10.3. The list of source address for this group only includes 10.5.5.1 and 10.5.5.2

```bash
switch(config)#interface ethernet 17
switch(config-if-Et17)#pim ipv4 border-router
switch(config-if-Et17)#ip igmp host-proxy 231.10.10.3 include 10.5.5.1
switch(config-if-Et17)#ip igmp host-proxy 231.10.10.3 include 10.5.5.2
switch(config-if-Et17)#
```

• These commands enable IGMP host proxy on Ethernet interface 17 for the group address(es) specified in ACL "acl1"

```bash
switch(config)#interface ethernet 17
switch(config-if-Et17)#pim ipv4 border-router
switch(config-if-Et17)#ip igmp host-proxy access-list acl1
switch(config-if-Et17)#
```
The **ip igmp host-proxy report-interval** command configures the period between unsolicited join reports that the switch sends as an IGMP host proxy from the configuration mode interface to a sender network after a (S,G) or (*,G) entry arrives in the multicast route (mroute) table. When the interface receives a query in response, this interval is set to the **ip igmp last-member-query-interval**. This command also enables the host proxy on the configuration mode interface if it was not previously enabled.

The **no ip igmp host-proxy report-interval** and **default ip igmp host-proxy report-interval** commands reset the query interval to the default value of one second by removing the corresponding **ip igmp host-proxy report-interval** command from **running-config**. The **no ip igmp host-proxy** and **default ip igmp host-proxy** commands also remove the corresponding **report-interval** command.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

```
ip igmp host-proxy report-interval period
no ip igmp host-proxy report-interval
default ip igmp host-proxy report-interval
```

**Parameters**
- **period** transmission interval (seconds) between consecutive reports.
  
  Value range: 1 (one second) to 31744 (8 hours, 49 minutes, 4 seconds). Default is 1 (one second).

**Example**
- These commands configures a IGMP host proxy interval of five seconds on port channel 100.

```
switch(config)#interface port-channel 100
switch(config-if-Po100)#ip igmp host-proxy report-interval 5
switch(config-if-Po100)#
```
**ip igmp host-proxy version**

The **ip igmp host-proxy version** command configures the version number to be used in unsolicited reports when the interface is serving as an IGMP host proxy. To configure the IGMP version used by the interface for other purposes, use the **ip igmp version** command instead.

The **no ip igmp host-proxy version** and **default ip igmp host-proxy version** commands reset the version to the default value of 3.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**
```
ip igmp host-proxy version version_number
no ip igmp host-proxy version
default ip igmp host-proxy version
```

**Parameters**
- **version_number** values range from 1-3; default value is 3.

**Example**
- These commands configure the IGMP host proxy version on port channel interface 100 to 2.
  ```
  switch(config)#interface port-channel 100
  switch(config-if-Po100)#ip igmp host-proxy version 2
  switch(config-if-Po100)#
  ```
**ip igmp last-member-query-count**

The `ip igmp last-member-query-count` command specifies the number of query messages the switch sends in response to a group-specific or group-source-specific leave message.

After receiving a message from a host leaving a group, the switch sends query messages at intervals specified by `ip igmp last-member-query-interval`. If the switch does not receive a response to the queries after sending the number of messages specified by this parameter, it stops forwarding messages to the host.

Setting the last member query count (LMQC) to 1 causes the loss of a single packet to stop traffic forwarding. While the switch can start forwarding traffic again after receiving a response to the next general query, the host may not receive that query for a period defined by `ip igmp query-interval`.

The `no ip igmp last-member-query-count` and `default ip igmp last-member-query-count` commands reset the LMQC to the default value by removing the corresponding `ip igmp last-member-query-count` command from `running-config`.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

```
  ip igmp last-member-query-count number
  no ip igmp last-member-query-count
  default ip igmp last-member-query-count
```

**Parameters**
- `number` query message quantity. Values range from 0 to 3. Default is 2.

**Example**
- This command configures the last-member-query-count to 3 on VLAN interface 4.

```
  switch(config)#interface vlan 4
  switch(config-if-Vl4)#ip igmp last-member-query-count 3
  switch(config-if-Vl4)#
```
**ip igmp last-member-query-interval**

The `ip igmp last-member-query-interval` command configures the switch’s transmission interval for sending group-specific or group-source-specific query messages from the configuration mode interface.

When a switch receives a message from a host that is leaving a group it sends query messages at intervals set by this command. The `ip igmp startup-query-count` specifies the number of messages that are sent before the switch stops forwarding packets to the host.

If the switch does not receive a response after this period, it stops forwarding traffic to the host on behalf of the group, source, or channel.

The `no ip igmp last-member-query-interval` and `default ip igmp last-member-query-interval` commands reset the query interval to the default value of one second by removing the `ip igmp last-member-query-interval` command from `running-config`.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**
- `ip igmp last-member-query-interval period`
- `no ip igmp last-member-query-interval`
- `default ip igmp last-member-query-interval`

**Parameters**
- `period` transmission interval (decisseconds) between consecutive group-specific query messages.
  
  Value range: 10 (one second) to 317440 (8 hours, 49 minutes, 4 seconds). Default is 10 (one second).

**Example**
- This command configures the last member query interval of 6 seconds for VLAN interface 4.

```
switch(config)#interface vlan 4
switch(config-if-Vl4)#ip igmp last-member-query-interval 60
switch(config-if-Vl4)#
```
**ip igmp**

The `ip igmp` command enables IGMP on a routed interface or on SVI (VLAN interface) without enabling PIM.

The `no igmp` command removes the corresponding `ip igmp` command from *running-config*.

**Command Mode**

Interface Configuration

**Command Syntax**

- `ip igmp`
- `no ip igmp`

**Example**

- This command enables IGMP on Ethernet interface 5/2.

```
switch(config)#interface ethernet 5/2
switch(config-if-Et5/2)#ip igmp
switch(config-if-Et5/2)#
```
**ip igmp profile**

The `ip igmp profile` command places the switch in IGMP-profile configuration mode to configure an IGMP profile. IGMP profiles control the multicast groups that an interface can join.

Profiles consist of the filter type and an address range:

- Filter types specify accessibility to the listed address range:
  - Permit filters define the multicast groups the interface can join.
  - Deny filters define the multicast groups the interface cannot join.

Profiles are deny filters by default.

- Address ranges specify a list of addresses and ranges:
  - In permit filters, permitted groups are specified by the address range.
  - In deny filters, all groups are permitted except those specified by the address range.

Implementing IGMP filtering affects IGMP report forwarding as follows:

- IGMPv2: Report is forwarded to mrouter for permitted groups and dropped for disallowed groups.
- IGMPv3: There may be multiple group records in a report.
  - No groups are allowed: The report is dropped.
  - All groups are allowed: The report is forwarded to mrouter ports as normal.
  - Some groups are allowed: A revised report is forwarded to mrouter ports.

  The revised report includes records for the allowed group addresses with the same source MAC and IP addresses.

The `no ip igmp profile` and `default ip igmp profile` commands delete the specified IGMP profile from `running-config`.

IGMP-profile configuration mode is not a group change mode; `running-config` is changed immediately upon entering commands. Exiting IGMP-profile configuration mode does not affect the configuration. The `exit` command returns the switch to global configuration mode.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp profile  profile_name
no ip igmp profile  profile_name
default ip igmp profile  profile_name
```

**Parameters**

- `profile_name` name of the IGMP profile.

**Commands Available in igmp-profile Configuration Mode**

- `permit` / `deny`
- `range`

**Related Commands**

- `ip igmp snooping filter` applies an IGMP snooping filter to a configuration mode interface.
Example

- These commands enter IGMP-profile configuration mode and configure the profile as a permit list.

```
switch(config)#ip igmp profile list_1
switch(config-igmp-profile-list_1)#permit
switch(config-igmp-profile-list_1)#
```
ip igmp query-interval

The `ip igmp query-interval` command configures the frequency at which the configuration mode interface, as an IGMP querier, sends host-query messages.

An IGMP querier sends host-query messages to discover the multicast groups that have members on networks attached to the interface. The switch implements a default query interval of 125 seconds.

The `no ip igmp query-interval` and `default ip igmp query-interval` commands reset the IGMP query interval to the default value of 125 seconds by removing the `ip igmp query-interval` command from `running-config`.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**
```
  ip igmp query-interval  period
  no ip igmp query-interval
  default ip igmp query-interval
```

**Parameters**
- `period` interval (seconds) between IGMP query messages. Values range from 1 to 3175 (52 minutes, 55 seconds). Default is 125.

**Example**
- This command configures the query-interval of 2 minutes, 30 seconds for VLAN interface 4.
```
  switch(config)#interface vlan 4
  switch(config-if-Vl4)#ip igmp query-interval 150
  switch(config-if-Vl4)#
```
ip igmp router-alert

The **ip igmp router-alert** command configures the switch disposition of inbound IGMP packets to the configuration mode interface based on the presence of the router-alert option in the IP header. By default, the port accepts all IGMP packets that arrive on the local subnet and rejects all other packets that arrive without the router-alert option.

The command provides three IGMP packet disposition options:

- **mandatory**: packets are accepted only when router-alert is present.
- **optional**: packets are accepted regardless of router-alert presence.
- **optional connected**: packets are accepted from the same subnet; other packets require router-alert.

The **no ip igmp router-alert** and **default ip igmp router-alert** commands reset the default setting of **optional connected** on the configuration mode interface by removing the corresponding **ip igmp router-alert** command from **running-config**.

**Command Mode**

- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

- `ip igmp router-alert DISPOSITION`
- `no ip igmp router-alert`
- `default ip igmp router-alert`

**Parameters**

- **DISPOSITION**  
  IGMP packet disposition method. Options include:
  - **mandatory**  
    Rejects packets if router-alert is not present.
  - **optional**  
    Accepts packets regardless of router-alert presence.
  - **optional connected**  
    Accepts packets from same subnet. Other packets require router-alert.

**Example**

- This command configures the switch to accept IGMP packets on Ethernet interface 8 only if the IP header contains router alert.

  ```
  switch(config)#interface ethernet 8
  switch(config-if-Et8)#ip igmp router-alert mandatory
  switch(config-if-Et8)#
  ```
**ip igmp snooping**

The *ip igmp snooping* command enables snooping globally. By default, global snooping is enabled. When global snooping is enabled, *ip igmp snooping vlan* enables or disables snooping on individual VLANs. When global snooping is disabled, snooping cannot be enabled on individual VLANs.

QoS cannot be used for IGMP packets when IGMP snooping is enabled.

The *no ip igmp snooping* command disables global snooping. The *default ip igmp snooping* command restores the global snooping default setting of enabled by removing the *ip igmp snooping* command from *running-config*.

**Command Mode**
- Global Configuration

**Command Syntax**

- `ip igmp snooping`
- `no ip igmp snooping`
- `default ip igmp snooping`

**Example**

- This command globally enables snooping on the switch.

```plaintext
switch(config)#ip igmp snooping
switch(config)#
```
**ip igmp snooping proxy**

The **ip igmp snooping proxy** command enables snooping proxy globally. By default, IGMP snooping proxy is disabled globally.

When the snooping proxy is enabled globally, it enables IGMP snooping proxy on an individual VLANs and when the IGMP snooping proxy is globally disabled the snooping proxy is disabled on individual VLANs.

The **no and default** form of **ip igmp snooping proxy** command disables snooping proxy globally and on individual VLANs by removing the **ip igmp snooping proxy** command from **running-config**.

**Command Mode**
- Global Configuration

**Command Syntax**
- `ip igmp snooping proxy`
- `no ip igmp snooping proxy`
- `default ip igmp snooping proxy`

**Examples**
- This command globally enables snooping proxy on the switch.
  ```
  switch(config)#ip igmp snooping proxy
  switch(config)#
  ```
- This command explicitly disables IGMP snooping proxy on VLAN 20.
  ```
  switch(config)#no ip igmp snooping vlan 20 proxy
  switch(config)#
  ```
ip igmp snooping filter

The `ip igmp snooping filter` command applies the specified IGMP snooping profile to the configuration mode interface. An IGMP snooping profile specifies the multicast groups that an interface may join. Profiles consist of the filter type and an address range:

- **Filter type**: Specifies accessibility to the listed address range:
  - Permit filters define the multicast groups the interface can join.
  - Deny filters define the multicast groups the interface cannot join.
- **Address range**: Specifies a list of addresses and ranges.
  - In permit filters, the permitted groups are specified by the address range.
  - In deny filters, all groups are permitted except those specified by the address range.

An interface without a snooping profile assignment may join any multicast group.

Snooping profiles are configured in IGMP-profile configuration mode (`ip igmp profile`).

The `no ip igmp snooping filter` and `default ip igmp snooping filter` commands restore the default setting of allowing an interface to join any multicast group by deleting the corresponding `ip igmp snooping filter` command from `running-config`.

### Command Mode
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration

### Command Syntax
```bash
ip igmp snooping filter profile_name
no ip igmp snooping filter [profile_name]
default ip igmp snooping filter [profile_name]
```

### Parameters
- **profile_name** name of profile assigned to interface.

### Example
- This command applies the `list_1` snooping profile to Ethernet interface 7.
```
switch(config)#interface ethernet 7
switch(config-if-Et7)#ip igmp snooping filter list_1
switch(config-if-Et7)#
```
**ip igmp snooping interface-restart-query**

The `ip igmp snooping interface-restart-query` command configures the interface startup initial query time used for IGMP query spoofing. When an interface restarts or there is a change to the spanning tree, the interface will send general IGMP queries after this interval. The query is based on the information of the last known IGMP querier, and serves to facilitate faster network convergence times.

Multiple values can be configured with a single command; issuing the command again replaces any previously configured value(s).

The `no ip igmp snooping interface-restart-query` and `default ip igmp snooping interface-restart-query` commands restore the default setting of 2000 milliseconds by deleting the corresponding `ip igmp snooping interface-restart-query` command from `running-config`.

**Command Mode**
- General Configuration

**Command Syntax**

```
  ip igmp snooping interface-restart-query query_time  
  no ip igmp snooping interface-restart-query  
  default ip igmp snooping interface-restart-query
```

**Parameters**

- `query_time` interval (in milliseconds) after an interface restart or spanning tree change at which the interface will send general IGMP queries. Values range from 100 to 50000 milliseconds; default is 2000.

**Example**

- This command configures interfaces to send IGMP queries at 100, 200, and 300 milliseconds after an interface restart or spanning tree change.

  ```
  switch(config)#ip igmp snooping interface-restart-query 100 200 300
  switch(config)#
  ```
**ip igmp snooping querier**

The `ip igmp snooping querier` command enables the snooping querier globally, which controls the querier for VLANs that are not configured with a snooping querier command. The `ip igmp snooping vlan querier` command controls the querier on individual VLANs.

The IGMP snooping querier supports snooping by sending layer 2 membership queries to hosts attached to the switch. The snooping querier is functional on VLANs where hosts receive IP multicast traffic without access to a network IP multicast router. A snooping querier avoids flooding multicast packets in the VLAN by querying for hosts and routers.

The IGMP snooping querier is functional on VLANs that meet these criteria:

- Snooping is enabled.
- The corresponding SVI (VLAN interface) is active.
- The VLAN's querier IP address or the global querier IP address is configured.

The `no ip igmp snooping querier` and `default ip igmp snooping querier` commands disable the snooping querier globally by removing the `ip igmp snooping querier` statement from `running-config`. The snooping querier is globally disabled by default.

**Command Mode**

- Global Configuration

**Command Syntax**

- `ip igmp snooping querier`
- `no ip igmp snooping querier`
- `default ip igmp snooping querier`

**Guidelines**

- Enabling a querier after it was disabled is equivalent to establishing a new querier.
- Changing the querier's IP address is equivalent to establishing a new querier.

**Example**

- This command globally enables the snooping querier on the switch.

  ```
  switch(config)#ip igmp snooping querier
  switch(config)#
  ```
**ip igmp snooping querier address**

The `ip igmp snooping querier address` command sets the global querier source IP address, which specifies the source address for packets transmitted from VLANs for which a querier address (`ip igmp snooping vlan querier address`) is not configured. To use a snooping querier, an address must be explicitly configured globally or for the VLAN.

The switch does not define a default global querier address.

The `no ip igmp snooping querier address` and `default ip igmp snooping querier address` commands remove the global querier address command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

- `ip igmp snooping querier address ipv4_address`
- `no ip igmp snooping querier address`
- `default ip igmp snooping querier address`

**Parameters**

- `ipv4_address` source IPv4 address.

**Example**

- This command sets the source IP address to 10.1.1.41 for query packets transmitted from the switch.

  ```
  switch(config)#ip igmp snooping querier address 10.1.1.41
  switch(config)#
  ```
The `ip igmp snooping querier last-member-query-count` command configures the global IGMP snooping querier last member query count (LMQC) value. LMQC specifies the number of query messages the switch sends in response to group-specific or group-source-specific leave messages it receives from a host; the transmission frequency is specified by IGMP snooping querier last member query interval. The switch stops forwarding messages to the host if it does not receive a response to these query messages.

Setting LMQC to 1 causes the loss of one packet to stop traffic forwarding. While the switch can start forwarding traffic again after receiving a response to the next general query, the host may not receive that query for a period defined by `ip igmp snooping querier query-interval`.

VLANs use the global value when they are not assigned a value (`ip igmp snooping vlan querier last-member-query-count`). VLAN commands take precedence over the global value. The default global value is specified by the robustness variable (`ip igmp snooping robustness-variable`).

The `no igmp snooping querier last-member-query-count` and `default igmp snooping querier last-member-query-count` commands reset the LMQC to the default value by removing the corresponding `ip igmp snooping querier last-member-query-count` command from running-config.

**Command Mode**
Global Configuration

**Command Syntax**

```
ip igmp snooping querier last-member-query-count number
no ip igmp snooping querier last-member-query-count
default ip igmp snooping querier last-member-query-count
```

**Parameters**

- `number` query message quantity. Value ranges from 1 to 3. Default is set by robustness-variable.

**Example**

- This command configures the global last-member-query-count to 3.

  ```
  switch(config)#ip igmp snooping querier last-member-query-count 3
  switch(config)#show igmp snooping querier status
  Global IGMP Querier status
  -------------------------------------------------------
  admin state : Disabled
  source IP address : 0.0.0.0
  query-interval (sec) : 125.0
  max-response-time (sec) : 10.0
  querier timeout (sec) : 255.0
  last-member-query-interval (sec) : 1.0
  last-member-query-count : 3
  startup-query-interval (sec) : 31.25 (query-interval/4)
  startup-query-count : 2 (robustness)
  VLAN Admin IP Query Response Querier Operational Ver
  State Interval Time Timeout State
  -----------------------------------------------------------------------
  1 Disabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v2
  100 Disabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v2
  101 Disabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v2
  switch(config)#
  ```
ip igmp snooping querier last-member-query-interval

The \texttt{ip igmp snooping querier last-member-query-interval} command sets the global IGMP snooping last member query interval. The default interval is one second.

A multicast host sends an IGMP leave report when it leaves a group. To determine if the host was the last group member, the leave message recipient sends an IGMP query. The last-member-query-interval determines when the group record is deleted if no subsequent reports are received.

VLANs not assigned a \textit{last member query interval} value (\texttt{ip igmp snooping vlan querier last-member-query-interval}) use the global value. VLAN commands take precedence over the global value.

The \texttt{no ip igmp snooping querier last-member-query-interval} and \texttt{default ip igmp snooping querier last-member-query-interval} commands reset the \textit{last-member-query-interval} value the default interval of one second by removing the \texttt{ip igmp snooping querier last-member-query-interval} statement from \textit{running-config}.

\textbf{Command Mode}

Global Configuration

\textbf{Command Syntax}

\begin{verbatim}
ip igmp snooping querier last-member-query-interval period
no ip igmp snooping querier last-member-query-interval
default ip igmp snooping querier last-member-query-interval
\end{verbatim}

\textbf{Parameters}

\begin{itemize}
  \item \textit{period} \hspace{1cm} last member query interval (seconds). Value ranges from 1 to 25. Default is one second.
\end{itemize}

\textbf{Related Commands}

\begin{itemize}
  \item \texttt{ip igmp snooping vlan querier last-member-query-interval} assign a last member query interval value to the specified VLANs.
\end{itemize}

\textbf{Example}

\begin{itemize}
  \item This command sets the IGMP snooping querier last-member-query-interval to five seconds.
\end{itemize}

\begin{verbatim}
switch(config)#ip igmp snooping querier last-member-query-interval 5
switch(config)#
\end{verbatim}
The `ip igmp snooping querier max-response-time` command specifies the global `max-response-time` value. The switch uses `max-response-time` to set the Max Response Time field in outbound Membership Query messages. Max Response Time specifies the maximum period a recipient can wait before responding with a Membership Report.

VLANs not assigned a `max-response-time` value (ip igmp snooping vlan querier max-response-time) use the global value. VLAN commands take precedence over the global value.

Values range from 1 to 25 seconds. The default global value is 10 seconds.

The `no ip igmp snooping querier max-response-time` and `default ip igmp snooping querier max-response-time` commands restore the global `max-response-time` default value by removing the `ip igmp snooping querier max-response-time` statement from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
  ip igmp snooping querier max-response-time resp_sec
  no ip igmp snooping querier max-response-time
  default ip igmp snooping querier max-response-time
```

**Parameters**

- `resp_sec max-response-time` value (seconds). Values range from 1 to 25. Default (global) is 10.

**Example**

- This command sets the global max-response-time to 15 seconds.

  switch(config)#ip igmp snooping querier max-response-time 15
  switch(config)#
**ip igmp snooping querier query-interval**

The `ip igmp snooping querier query-interval` command sets the global query interval. This command also sets the query-interval of IGMP Snooping when using IGMP version 2. Values range from 5 to 3600 seconds. The default global value is 125 seconds. The query interval is the period between IGMP Membership Query messages sent from the querier. The global value specifies the query interval for VLANs with no query-interval command.

VLANs not assigned a `query interval` value (`ip igmp snooping vlan querier query-interval`) use the global value. VLAN commands take precedence over the global value.

The `no ip igmp snooping querier query-interval` and `default ip igmp snooping querier query-interval` commands reset the global query-interval value to 125 seconds by removing the `ip igmp snooping querier query-interval` statement from `running-config`.

**Command Mode**
- Global Configuration

**Command Syntax**

```plaintext
ip igmp snooping querier query-interval query_sec
no ip igmp snooping querier query-interval
default ip igmp snooping querier query-interval
```

**Parameters**
- `query_sec` query interval (seconds). Values range from 5 to 3600. Default (global) is 125.

**Example**
- This command sets the global query interval to 150 seconds.

```
switch(config)#ip igmp snooping querier query-interval 150
switch(config)#
```
**ip igmp snooping querier startup-query-count**

The `ip igmp snooping querier startup-query-count` command configures the global `startup query count` value. The `startup query count` specifies the number of query messages that the querier sends on a VLAN during the `startup query interval` (`ip igmp snooping querier startup-query-interval`).

When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The `startup-query-interval` and `startup-query-count` parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.

VLANs use the global `startup query count` value when they are not assigned a value (`ip igmp snooping vlan querier startup-query-count`). VLAN commands take precedence over the global value. The default global value is specified by the robustness variable (`ip igmp snooping robustness-variable`).

The `no ip igmp snooping querier startup-query-count` and `default ip igmp snooping querier startup-query-count` commands restore the default `startup-query-count` value by removing the corresponding `ip igmp snooping querier startup-query-count` command from `running-config`.

**Command Mode**
Global Configuration

**Command Syntax**
```
ip igmp snooping querier startup-query-count number
no ip igmp snooping querier startup-query-count
default ip igmp snooping querier startup-query-count
```

**Parameters**
- `number`: global startup query count. Value ranges from 1 to 3.

**Example**
- These commands configure the global startup query count value of 2, then displays the status of the snooping querier.

```
switch(config)#ip igmp snooping querier startup-query-count 2
switch(config)#show igmp snooping querier status

Global IGMP Querier status
-------------------------------------------------------
admin state                      : Disabled
source IP address                : 0.0.0.0
query-interval (sec)             : 125.0
max-response-time (sec)          : 10.0
querier timeout (sec)            : 255.0
last-member-query-interval (sec) : 1.0
last-member-query-count          : 2 (robustness)
startup-query-interval (sec)     : 31.25 (query-interval/4)
startup-query-count              : 2

Vlan Admin    IP              Query    Response Querier Operational Ver
State                    Interval Time     Timeout State
-----------------------------------------------------------------------
1   Disabled 0.0.0.0         125.0    10.0     255.0   Non-Querier v2
100 Disabled 0.0.0.0         125.0    10.0     255.0   Non-Querier v2
101 Disabled 0.0.0.0         125.0    10.0     255.0   Non-Querier v2
```

switch(config)#
ip igmp snooping querier startup-query-interval

The `ip igmp snooping querier startup-query-interval` command configures the global startup query interval value. The `startup query interval` specifies the period between query messages that the querier sends upon startup.

When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The `startup-query-interval` and `startup-query-count` parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.

VLANs use the global `startup query interval` value when they are not assigned a value (ip igmp snooping vlan querier startup-query-interval). VLAN commands take precedence over the global value. The default global value equals the query interval divided by four. (ip igmp snooping querier query-interval).

The `no ip igmp snooping querier startup-query-interval` and `default ip igmp snooping querier startup-query-interval` commands restore the default method of specifying the startup query interval by removing the corresponding `ip igmp snooping querier startup-query-interval` command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

- `ip igmp snooping querier startup-query-interval period`
- `no ip igmp snooping querier startup-query-interval`
- `default ip igmp snooping querier startup-query-interval`

**Parameters**

- `period` startup query interval (seconds). Value ranges from 1 to 3600 (1 hour).

**Example**

- This command configures the startup query count of one minute for VLAN interface 4.

  switch(config)#ip igmp snooping querier startup-query-interval 40
  switch(config)#show igmp snooping querier status

<table>
<thead>
<tr>
<th>admin state</th>
<th>Query Interval (sec)</th>
<th>Response Time (sec)</th>
<th>Querier Timeout (sec)</th>
<th>Operational Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>125.0</td>
<td>10.0</td>
<td>255.0</td>
<td>Non-Querier v3</td>
</tr>
<tr>
<td>Enabled</td>
<td>125.0</td>
<td>10.0</td>
<td>255.0</td>
<td>Non-Querier v3</td>
</tr>
<tr>
<td>Enabled</td>
<td>125.0</td>
<td>10.0</td>
<td>255.0</td>
<td>Non-Querier v3</td>
</tr>
</tbody>
</table>

switch(config)#
**ip igmp snooping querier version**

The `ip igmp snooping querier version` command configures the Internet Group Management Protocol (IGMP) snooping querier version on the configuration mode interfaces. Version 3 is the default IGMP version.

IGMP is enabled by the `pim ipv4 sparse-mode` or `pim ipv4 bidirectional` command. The `ig igmp snooping querier version` command does not affect the IGMP enabled status.

The `no ip igmp snooping querier version` and `default ip igmp snooping querier version` commands restore the configuration mode to IGMP version 3 by removing the `ip igmp snooping querier version` statement from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping querier version version_number
no ip igmp snooping querier version
default ip igmp snooping querier version
```

**Parameters**

- `version_number` IGMP version number. Value ranges from 1 to 3. Default value is 3.

**Example**

- This command configures IGMP snooping querier version 2.
  ```
  switch(config)#ip igmp snooping querier version 2
  switch(config)#
  ```

- This command restores the IGMP snooping querier to version 3.
  ```
  switch(config)# no ip igmp snooping querier version
  switch(config)#
  ```
ip igmp snooping report-flooding

The `ip igmp snooping report-flooding` command globally enables L2 report flooding on the switch. When report flooding is globally enabled, the `ip igmp snooping vlan report-flooding` configures a VLAN range to forward membership report messages to specified ports. When report flooding is not globally enabled, L2 report flooding cannot be enabled on individual VLANs.

L2 report flooding is an IGMP snooping feature that forwards membership report messages to specified ports. Relying on a single switch to maintain and send report messages can result in performance issues. L2 report flooding addresses this by facilitating report message transmissions through any network port. This allows switches to bypass the querier when forwarding multicast traffic to its interested ports.

The `no ip igmp snooping report-flooding` and `default ip igmp snooping report-flooding` commands disable global L2 report flooding by removing `ip igmp report flooding` from `running-config`. L2 report flooding is disabled by default.

**Command Mode**
- Global Configuration

**Command Syntax**
- `ip igmp snooping report-flooding`
- `no ip igmp snooping report-flooding`
- `default ip igmp snooping report-flooding`

**Related Commands**
- `ip igmp snooping vlan report-flooding` enables L2 report flooding on a specified VLAN range.

**Example**
- This command globally enables the snooping L2 report-flooding.

  ```
  switch(config)#ip igmp snooping report-flooding
  switch(config)#
  ```
ip igmp snooping report-flooding switch-port

The `ip igmp snooping report-flooding switch-port` command specifies Ethernet ports or port channels that can forward IGMP membership report messages for all VLANs where L2 report flooding is enabled. Ports that are connected to multicast routers or queriers continue to forward traffic as previously specified and are not affected by L2 report flooding commands.

L2 report flooding is an IGMP snooping feature that forwards membership report messages to specified ports. The `ip igmp snooping vlan report-flooding switch-port` command configures a list of forwarding ports for a specified VLAN range.

The `no ip igmp snooping report-flooding switch-port` and `default ip igmp snooping report-flooding switch-port` commands remove the specified ports from the global report flooding port list by deleting the corresponding `ip igmp snooping report-flooding switch-port` command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

ip igmp snooping report-flooding switch-port INTERFACE
no ip igmp snooping report-flooding switch-port INTERFACE
default ip igmp snooping report-flooding switch-port INTERFACE

**Parameters**

- **INTERFACE**  Membership report message forwarding is enabled on these ports:
  - `ethernet e_range` where `e_range` is the number, range, or list of ethernet ports
  - `port-channel p_range` where `p_range` is the number, range, or list of channel ports

**Related Commands**

- `ip igmp snooping report-flooding` globally enables L2 report flooding.
- `ip igmp snooping vlan report-flooding switch-port` specifies a port list for a VLAN range.

**Example**

- This command configures Ethernet ports 7-9 for report message forwarding for any VLAN where L2 report flooding is enabled.

```bash
switch(config)#ip igmp snooping report-flooding switch-port ethernet 7-9
switch(config)#
```
ip igmp snooping restart query-interval

The `ip igmp snooping restart query-interval` command sets the query interval for all VLANs during an IGMP snooping restart. By default, the query interval during an IGMP snooping restart is a VLAN’s configured query interval divided by five. This accelerates the transmission of robustness queries to establish the IGMP snooping state more quickly. However, some large scale configurations may not be able to process all of the queries at this query interval rate. The restart query interval, when configured, is valid for all VLANs.

The `no ip igmp snooping restart query-interval` and `default ip igmp snooping restart query-interval` commands removes the global restart query interval by deleting the `ip igmp snooping restart query-interval` statement from `running-config`.

Command Mode
Global Configuration

Command Syntax

```
ip igmp snooping restart query-interval query_sec
no ip igmp snooping restart query-interval
default ip igmp snooping restart query-interval
```

Parameters
- `query_sec` query interval (seconds). Values range from 2 to 400. Default (global) is 125.

Example
- This command sets the global query interval to 35 seconds.

```
switch(config)#ip igmp snooping restart query-interval 35
switch(config)#
```
ip igmp snooping robustness-variable

The `ip igmp snooping robustness-variable` command configures the robustness variable for snooping packets sent from any VLAN. Values range from 1 to 3 with a default of 2.

The robustness variable specifies the number of unacknowledged snooping queries that a switch sends before removing the recipient from the group list.

The `no ip igmp snooping robustness-variable` and `default ip igmp snooping robustness-variable` commands reset the robustness variable to 2 by removing the `ip igmp snooping robustness-variable` command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping robustness-variable robust_value
no ip igmp snooping robustness-variable
default ip igmp snooping robustness-variable
```

**Parameters**

- `robust_value`  robustness variable. Values range from 1 to 3. Default is 2.

**Example**

- This command sets the robustness-variable value to 3.

```
switch(config)#ip igmp snooping robustness-variable 3
switch(config)#
```
ip igmp snooping vlan

The `ip igmp snooping vlan` command enables snooping on the specified VLANs if snooping is globally enabled. IGMP snooping is globally enabled by default. The `ip igmp snooping` command enables snooping globally.

Note that if IGMP snooping is enabled, QoS will not apply to IGMP packets.

The `no ip igmp snooping vlan` command disables snooping on the specified VLANs.

The `default ip igmp snooping vlan` command returns the snooping setting for the specified VLANs to enabled by removing the corresponding `ip igmp snooping vlan` command from `running-config`.

**Command Mode**
Global Configuration

**Command Syntax**

- `ip igmp snooping vlan v_range`
- `no ip igmp snooping vlan v_range`
- `default ip igmp snooping vlan v_range`

**Parameters**
- `v_range` VLANs upon which snooping is enabled. Formats include a number, a number range, or a comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.

**Example**
- This command disables snooping on VLANs 2 through 4.
  ```
  switch(config)#no ip igmp snooping vlan 2-4
  switch(config)#
  ```
ip igmp snooping vlan fast-leave

The `ip igmp snooping vlan fast-leave` command enables fast-leave processing on specified VLANs. When fast-leave processing is enabled, the removal of a VLAN interface's multicast group entry from the IGMP table is not preceded by an IGMP group-specific query to the interface. The switch removes an interface from the forwarding table when it detects an IGMP leave message on the interface. IGMP fast-leave processing is enabled on all VLANs by default.

The `no ip igmp snooping vlan fast-leave` command disables fast-leave processing on the specified VLANs. The `default ip igmp snooping vlan fast-leave` command restores fast-leave processing on the specified VLANs by removing the corresponding `no ip igmp snooping vlan fast-leave` statement from `running-config`.

**Command Mode**
Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range fast-leave
no ip igmp snooping vlan v_range fast-leave
default ip igmp snooping vlan v_range fast-leave
```

**Parameters**
- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.

**Example**
- This command enables IGMP fast-leave processing on VLAN 10.

```
switch(config)#ip igmp snooping vlan 10 fast-leave
switch(config)#
```
**ip igmp snooping vlan max-groups**

The `ip igmp snooping vlan max-groups` command configures the quantity of multicast groups that the specified VLAN’s forwarding table can contain. After the limit is reached, attempts to join new groups are ignored. There is no default limit.

The `no ip igmp snooping vlan max-groups` and `default ip igmp snooping vlan max-groups` removes the maximum group limit by deleting the `ip igmp snooping vlan max-groups` statement from `running-config`.

**Command Mode**
- Global Configuration

**Command Syntax**
- `ip igmp snooping vlan v_range max-groups quantity`
- `no ip igmp snooping vlan v_range max-groups`
- `default ip igmp snooping vlan v_range max-groups`

**Parameters**
- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- `quantity` maximum number of groups that can access the VLAN. Value ranges from 0 to 65534.

**Examples**
- This command limits the number of multicast groups that hosts on VLAN 6 can simultaneously access to 25.
  
  `switch(config)#ip igmp snooping vlan 6 max-groups 25`
  
  `switch(config)#`

- This command allows each VLAN between 8 and 15 to receive multicast packets from 30 groups.
  
  `switch(config)#ip igmp snooping vlan 8-15 max-groups 30`
  
  `switch(config)#`

- This command removes the maximum group restriction from all VLAN interfaces between 1 and 50.
  
  `switch(config)#no ip igmp snooping vlan 1-50 max-groups`
  
  `switch(config)#`
ip igmp snooping vlan member

The `ip igmp snooping vlan member` command adds ports as static members to a multicast group. The ports must be in the specified VLAN range.

The `no ip igmp snooping vlan member` and `default ip igmp snooping vlan member` commands remove the specified ports from the multicast group by deleting the corresponding `ip igmp snooping member` statements from `running-config`.

Command Mode
Global Configuration

Command Syntax

```
ip igmp snooping vlan v_num member ipv4_addr interface STATIC_INT
no ip igmp snooping vlan v_num member ipv4_addr interface STATIC_INT
default ip igmp snooping vlan v_num member ipv4_addr interface STATIC_INT
```

Parameters

- `v_num` VLAN number. Value ranges from 1 to 4094.
- `ipv4_addr` multicast group IPv4 address.
- `STATIC_INT` interface the command configures as the static group member. Options include:
  - `ethernet e_range`, where `e_range` is the number, range, or list of Ethernet ports
  - `port-channel p_range`, where `p_range` is the number, range, or list of channel ports

Example

- This command configures the static connection to a multicast group at 237.2.1.4 through Ethernet port 3.

```
switch(config)#ip igmp snooping vlan 7 member 237.2.1.4 interface ethernet 3
```

```
**ip igmp snooping vlan multicast-router**

The **ip igmp snooping vlan multicast-router** command adds a multicast router as a static port to the specified VLANs. The router port must be in the specified VLAN range.

Snooping may not always be able to locate the IGMP querier. This command should specify IGMP queries that are known to connect to the network through a port on the switch.

The **no ip igmp snooping vlan multicast-router** and **default ip igmp snooping vlan multicast-router** commands remove the specified static port configuration by deleting the corresponding **ip igmp snooping vlan multicast-router** command from **running-config**.

**Command Mode**
- Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range multicast-router interface STATIC_INT
no ip igmp snooping vlan v_range multicast-router interface STATIC_INT
default ip igmp snooping vlan v_range multicast-router interface STATIC_INT
```

**Parameters**

- **v_range**  VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- **STATIC_INT**  interface the command configures as a static port. Selection options include:
  - **ethernet e_range**  where **e_range** is the number, range, or list of ethernet ports
  - **port-channel p_range**  where **p_range** is the number, range, or list of channel ports

The **STATIC_INT** interface must route traffic through a VLAN specified within **v_range**.

**Example**

- This command configures the static connection to a multicast router through Ethernet port 3.

```
switch(config)#ip igmp snooping vlan 2 multicast-router interface ethernet 3
switch(config)#
```
The **ip igmp snooping vlan proxy** command enables snooping proxy on individual VLAN, and to enable or disable IGMP snooping vlan proxy globally, use **ip igmp snooping proxy** command.

**Note**
The **ip igmp snooping proxy** command enables snooping proxy on all VLANs only where IGMP snooping is enabled.

The **no and default** form of **ip igmp snooping vlan proxy** command disables snooping proxy globally and on individual VLANs by removing the **ip igmp snooping vlan proxy** command from **running-config**.

**Command Mode**
Global Configuration

**Command Syntax**
```
ip igmp snooping vlan [ID | range] proxy
no ip igmp snooping vlan [ID | range] proxy
default ip igmp snooping vlan [ID | range] proxy
```

**Parameters**
- **v_range** specifies the range of VLAN IDs. Numbers range from 1 to 4094.
- **v_ID** specifies a individual VLAN ID. Numbers range from 1 to 4094.

**Examples**
- This command globally enables IGMP snooping proxy on the switch and on all VLANs where IGMP snooping is enabled.
  ```
  switch(config)#ip igmp snooping proxy
  switch(config)#
  ```
- This command enables IGMP snooping proxy on VLAN 20.
  ```
  switch(config)#ip igmp snooping vlan 20 proxy
  switch(config)#
  ```
- This command disables IGMP snooping proxy on VLAN 20.
  ```
  switch(config)#no ip igmp snooping vlan 20 proxy
  switch(config)#
  ```
ip igmp snooping vlan querier

The `ip igmp snooping vlan querier` command controls the querier for the specified VLANs. VLANs follow the global querier setting unless overridden by one of these commands:

- `ip igmp snooping vlan querier` enables the querier on specified VLANs.
- `no ip igmp snooping vlan querier` disables the querier on specified VLANs.

VLAN querier commands take precedence over the global querier setting. The `ip igmp snooping querier` controls the querier for VLANs with no snooping querier command.

The IGMP snooping querier supports snooping by sending layer 2 membership queries to hosts attached to the switch. The snooping querier is functional on VLANs where hosts receive IP multicast traffic without access to a network IP multicast router. A snooping querier avoids flooding multicast packets in the VLAN by querying for hosts and routers.

The IGMP snooping querier is functional on VLANs that meet these criteria:

- Snooping is enabled.
- The corresponding SVI (VLAN interface) is active.
- The VLAN's querier IP address or the global querier IP address is configured.

The `default ip igmp snooping vlan querier` command restores the usage of the global setting for the specified VLAN by removing the corresponding `ip igmp snooping vlan querier` or `no ip igmp snooping vlan querier` command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range querier
no ip igmp snooping vlan v_range querier
default ip igmp snooping vlan v_range querier
```

**Parameters**

- `v_range` VLAN IDs. Formats include a number, a number range, or a comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.

**Examples**

- These commands globally enable the snooping querier on the switch, explicitly disable snooping on VLANs 1-3, and explicitly enable snooping on VLANs 4-6.

```
switch(config)#ip igmp snooping querier
switch(config)#no ip igmp snooping vlan 1-3 querier
switch(config)#ip igmp snooping vlan 4-6 querier
```

After running these commands, the running-config file contains these lines, which indicate that the snooping querier is enabled on VLANs 4-6.

```
switch(config)#show running-config
<-------OUTPUT OMITTED FROM EXAMPLE-------->
no ip igmp snooping vlan 1 querier
no ip igmp snooping vlan 2 querier
no ip igmp snooping vlan 3 querier
ip igmp snooping vlan 4 querier
ip igmp snooping vlan 5 querier
ip igmp snooping vlan 6 querier
ip igmp snooping querier
<-------OUTPUT OMITTED FROM EXAMPLE-------->
```
- This command removes the querier setting for VLANs 2-5:
  
  ```
  switch(config)#default ip igmp snooping vlan 2-5 querier
  ```

  When executed after the previous commands, the snooping querier is disabled explicitly on VLANs 1-2, enabled implicitly on VLANs 3-6, and enabled explicitly on VLANs 7-8, as shown by `running-config`:

  ```
  no ip igmp snooping vlan 1 querier
  ip igmp snooping vlan 6 querier
  ip igmp snooping querier
  ```

- This command sets the global snooping querier to disabled by removing the global querier setting from `running-config`:

  ```
  switch(config)#no ip igmp snooping querier
  ```

  When executed after the previous commands, the snooping querier is disabled explicitly on VLANs 1-2, disabled implicitly on VLANs 3-6 and enabled explicitly on VLANs 7-8, as shown by `running-config`:

  ```
  no ip igmp snooping vlan 1 querier
  ip igmp snooping vlan 6 querier
  ```
Chapter 39: IGMP and IGMP Snooping

**ip igmp snooping vlan querier address**

The `ip igmp snooping vlan querier address` command sets the source address for query packets sent from specified VLANs. VLANs not assigned an address use the global address (`ip igmp snooping querier address`). VLAN querier address commands take precedence over the global address.

To use a snooping querier, an address must be explicitly configured globally or for the querier's VLAN.

The `no ip igmp vlan snooping querier address` and `default ip igmp snooping vlan querier address` commands reset the specified VLAN to use the global address by removing the corresponding `ip igmp snooping vlan querier address` command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range querier address ipv4_address
no ip igmp snooping vlan v_range querier address
default ip igmp snooping vlan v_range querier address
```

**Parameters**

- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- `ipv4_address` source IPv4 address.

**Example**

- This command sets the source IPv4 address of 10.14.1.1 for query packets transmitted from VLAN 2.

  ```
  switch(config)#ip igmp snooping vlan 2 querier address 10.14.1.1
  switch(config)#
  ```
The `ip igmp snooping vlan querier last-member-query-count` command specifies an *IGMP snooping querier last member query count* (LMQC) value for the specified VLANs. LMQC specifies the number of query messages the switch sends in response to group-specific or group-source-specific leave messages it receives from a host; the transmission frequency is specified by *IGMP snooping querier last member query interval*. The switch stops forwarding messages to the host if it does not receive a response to these query messages.

VLANs not assigned an LMQC value use the global value (`ip igmp snooping querier last-member-query-count`). VLAN commands take precedence over the global command.

Setting the last member query count (LMQC) to 1 causes the loss of a single packet to stop traffic forwarding. While the switch can start forwarding traffic again after receiving a response to the next general query, the host may not receive that query for a period defined by `ip igmp snooping querier query-interval`.

The `no igmp snooping vlan querier last-member-query-count` and `default igmp snooping vlan querier last-member-query-count` commands reset the specified VLAN to use the global LMQC by removing the corresponding `ip igmp snooping vlan querier last-member-query-count` command from *running-config*.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range querier last-member-query-count number
no ip igmp snooping vlan v_range querier last-member-query-count
default ip igmp snooping vlan v_range querier last-member-query-count
```

**Parameters**

- **v_range** VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- **number** query message quantity. Value ranges from 1 to 3.

**Example**

```
This command configures the last-member-query-count to 1 on VLAN interface 3.

switch(config)#ip igmp snooping vlan 3 querier last-member-query-count 1
switch(config)#
```
ip igmp snooping vlan querier last-member-query-interval

The `ip igmp snooping vlan querier last-member-query-interval` command configures the last-member-query-interval for packets sent from the specified VLANs. VLANs not assigned a value use the global setting (`ip igmp snooping querier last-member-query-interval`). VLAN commands take precedence over the global value. The global default is one second.

A multicast host sends an IGMP leave report when it leaves a group. To determine if the host was the last group member, the leave message recipient sends an IGMP query. The last-member-query-interval determines when the group record is deleted if no subsequent reports are received.

The `no ip igmp snooping vlan querier last-member-query-interval` and `default ip igmp snooping vlan querier last-member-query-interval` commands reset the specified VLAN to use the global last-member-query-interval by removing the corresponding `ip igmp snooping vlan querier last-member-query-interval` command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
    ip igmp snooping vlan  v_range  querier last-member-query-interval  period
    no ip igmp snooping vlan  v_range  querier last-member-query-interval
    default ip igmp snooping vlan  v_range  querier last-member-query-interval
```

**Parameters**

- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- `period` last member query interval (seconds). Value ranges from 1 to 25.

**Example**

- This command sets the last-member-query-interval for VLAN 10 to 12 seconds.

  ```
  switch(config)#ip igmp snooping vlan 10 querier last-member-query-interval 12
  switch(config)#
  ```
ip igmp snooping vlan querier max-response-time

The `ip igmp snooping vlan querier max-response-time` command configures `max-response-time` for packets sent from the specified VLANs. VLANs not assigned a value use the global setting (`ip igmp snooping querier max-response-time`). VLAN commands take precedence over the global value. The global default is 10 seconds.

Switches use `max-response-time` to set the Max Response Time field in outbound Membership Query messages. Max Response Time specifies the maximum period a recipient can wait before responding with a Membership Report.

The `no ip igmp snooping vlan querier max-response-time` and `default ip igmp snooping vlan querier max-response-time` commands reset the specified VLAN to use the global `max-response-time` by removing the corresponding `ip igmp snooping vlan querier max-response-time` command from `running-config`.

Command Mode
Global Configuration

Command Syntax
```
ip igmp snooping vlan v_range querier max-response-time resp_sec
no ip igmp snooping vlan v_range querier max-response-time
default ip igmp snooping vlan v_range querier max-response-time
```

Parameters
- `v_range` VLAN ID. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- `resp_sec` `max-response-time` value (seconds). Values range from 1 to 25.

Example
- This command sets the max-response-time for VLAN 2 to 5 seconds.

```
switch(config)#ip igmp snooping vlan 2 querier max-response-time 5
switch(config)#
```
**ip igmp snooping vlan querier query-interval**

The `ip igmp snooping vlan querier query-interval` command sets the query interval for the specified VLAN. VLANs not assigned a value use the global value (`ip igmp snooping querier query-interval`). VLAN commands have precedence over the global value. The query interval is the period between IGMP Membership Query messages sent from the querier.

The `no ip igmp snooping vlan querier query-interval` and `default ip igmp snooping vlan querier query-interval` commands reset the specified VLAN to use the global value by removing the corresponding `ip igmp snooping vlan querier query-interval` command from *running-config*.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range querier query-interval query_sec
no ip igmp snooping vlan v_range querier query-interval
default ip igmp snooping vlan v_range querier query-interval
```

**Parameters**

- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- `query_sec` query interval (seconds). Values range from 5 to 3600. Default (global) is 125.

**Example**

- This command sets the query interval for VLAN 10 to 240 seconds.
  
  ```
  switch(config)#ip igmp snooping vlan 10 querier query-interval 240
  switch(config)#
  ```
**ip igmp snooping vlan querier startup-query-count**

The `ip igmp snooping vlan querier startup-query-count` command specifies the startup query count value for the specified VLANs. The `startup query count` specifies the number of query messages that the querier sends on a VLAN during the `startup query interval` (ip igmp snooping vlan querier startup-query-interval).

When an interface starts running IGMP, it can establish the group state more quickly by sending query messages at a higher frequency. The `startup-query-interval` and `startup-query-count` parameters define the startup period and the query message transmission frequency during that period.

VLANs not assigned a `startup query count` value use the global value (ip igmp snooping querier startup-query-count). VLAN commands take precedence over the global command.

The no `ip igmp snooping vlan querier startup-query-count` and default `ip igmp snooping vlan querier startup-query-count` commands restore the default condition of using the global `startup query count` value by removing the corresponding `ip igmp snooping vlan querier startup-query-count` command from running-config.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range querier startup-query-count number
no ip igmp snooping vlan v_range querier startup-query-count
default ip igmp snooping vlan v_range querier startup-query-count
```

**Parameters**

- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- `number` startup query count. Value ranges from 1 to 3.

**Example**

- This command configures the startup query count of 3 for VLAN 100.
  ```
  switch(config)#ip igmp snooping vlan 100 querier startup-query-count 3
  switch(config)#
  ```
The `ip igmp snooping vlan querier startup-query-interval` command specifies the `startup query interval` value for the specified VLANs. The `startup query interval` specifies the period between query messages that the querier sends upon startup.

When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The `startup-query-interval` and `startup-query-count` parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.

VLANs not assigned a `startup query interval` value use the global value (`ip igmp snooping querier startup-query-count`). VLAN commands take precedence over the global command.

The `no ip igmp snooping vlan querier startup-query-interval` and `default ip igmp snooping vlan querier startup-query-interval` commands restore the default condition of using the global `startup query interval` value by removing the corresponding `ip igmp snooping vlan querier startup-query-interval` command from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range querier startup-query-interval period
no ip igmp snooping vlan v_range querier startup-query-interval
default ip igmp snooping vlan v_range querier startup-query-interval
```

**Parameters**

- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- `period` startup query interval (seconds). Value ranges from 1 to 3600 (1 hour). Default is 31.

**Example**

- This command configures the startup query count of one minute for VLAN interface 100.
  
  ```
  switch(config)#ip igmp snooping vlan 100 querier startup-query-interval 60
  switch(config)#
  ```
ip igmp snooping vlan querier version

The ip igmp snooping vlan querier version command configures the Internet Group Management Protocol (IGMP) snooping querier function on the VLAN. Version 3 is the default IGMP snooping version.

IGMP is enabled by the pim ipv4 sparse-mode or pim ipv4 bidirectional command. The ip igmp snooping vlan querier version command does not affect the IGMP enabled status.

The no ip igmp snooping vlan querier version and default ip igmp snooping vlan querier version commands restore the configuration mode interface to IGMP snooping VLAN querier version 3 by removing the ip igmp snooping vlan querier version statement from running-config.

Command Mode
Global Configuration

Command Syntax

ip igmp snooping vlan v_range querier version version_number
no ip igmp snooping vlan v_range querier version
default ip igmp snooping vlan v_range querier version

Parameters
• v_range VLAN ID. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
• version_number IGMP version number. Value ranges from 1 to 3. Default value is 3.

Example
• The example sets the querier version to 2 on vlan 5.
  switch(config)#ip igmp snooping vlan 5 querier version 2
  switch(config)#
• This command restores IGMP snooping querier version 3 to VLAN 5.
  switch(config)# no ip igmp snooping vlan 5 querier version
  switch(config)#
Chapter 39: IGMP and IGMP Snooping

**ip igmp snooping vlan report-flooding**

The `ip igmp snooping vlan report-flooding` command enables L2 report flooding on the specified VLANs if report flooding is globally enabled. When L2 report flooding is not globally enabled, this command has no effect. The `ip igmp snooping report-flooding` command globally enables L2 report flooding.

L2 report flooding is an IGMP snooping feature that forwards membership report messages to specified ports. Relying on a single switch to maintain and send report messages can degrade performance. L2 report flooding addresses this by facilitating report message forwarding through any network port. This allows switches to bypass the querier when forwarding multicast traffic to its interested ports.

Two commands specify the ports that forward reports:

- `ip igmp snooping vlan report-flooding switch-port` for a VLAN range.
- `ip igmp snooping report-flooding switch-port` for all VLANs where report flooding is enabled.

The `no ip igmp snooping vlan report-flooding` and `default ip igmp snooping vlan report-flooding` commands disable L2 report flooding for the specified VLAN by removing the corresponding `ip igmp snooping vlan report-flooding` statement from `running-config`.

**Command Mode**

Global Configuration

**Command Syntax**

```
ip igmp snooping vlan v_range report-flooding
no ip igmp snooping vlan v_range report-flooding
default ip igmp snooping vlan v_range report-flooding
```

**Parameters**

- `v_range` VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.

**Related Commands**

- `ip igmp snooping report-flooding` globally enables L2 report flooding.

**Example**

- These commands enable L2 report flooding globally and on VLANs 201 through 205.

```
switch(config)#ip igmp snooping report-flooding
switch(config)#ip igmp snooping vlan 201-205 report-flooding
switch(config)#
```
The **ip igmp snooping vlan report-flooding switch-port** command configures Ethernet ports or port channels to forward IGMP membership report messages for a specified VLAN range where L2 report flooding is enabled. Ports that are connected to multicast routers or queriers continue to forward traffic as previously specified and are not affected by L2 report flooding commands.

L2 report flooding is an IGMP snooping feature that forwards membership report messages to specified ports. The **no ip igmp snooping vlan report-flooding switch-port** command removes the listed ports from the specified report flooding port list by deleting the corresponding **ip igmp snooping vlan report-flooding switch-port** statements from **running-config**.

### Command Mode

Global Configuration

### Command Syntax

```
ip igmp snooping vlan v_range report-flooding switch-port INTERFACE
no ip igmp snooping vlan v_range report-flooding switch-port INTERFACE
default ip igmp snooping vlan v_range report-flooding switch-port INTERFACE
```

### Parameters

- **v_range** VLAN IDs. Formats include a number, number range, or comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
- **INTERFACE** Membership report message forwarding is enabled on these ports:
  - **ethernet e_range** where **e_range** is the number, range, or list of ethernet ports
  - **port-channel p_range** where **p_range** is the number, range, or list of channel ports

### Related Commands

- **ip igmp snooping report-flooding** globally enables L2 report flooding.
- **ip igmp snooping vlan report-flooding switch-port** specifies a port list for a VLAN range.
- **ip igmp snooping report-flooding switch-port** specifies a port list for all VLANs.

### Example

- These commands globally enable L2 report flooding, enable flooding on VLANs 201 through 205, and specify Ethernet ports 8-10 as the report flooding port list for VLANS 201-205.

```
switch(config)#ip igmp snooping report-flooding
switch(config)#ip igmp snooping vlan 201-205 report-flooding
switch(config)#ip igmp snooping vlan 201-205 report-flooding switch-port ethernet 8-10
switch(config)#
```
**ip igmp startup-query-count**

The `ip igmp startup-query-count` command specifies the number of query messages that an interface sends during the startup interval defined by `ip igmp startup-query-interval`.

When an interface starts running IGMP, it can establish the group state more quickly by sending query messages at a higher frequency. The `startup-query-interval` and `startup-query-count` parameters define the startup period and the query message transmission frequency during that period.

The `no ip igmp startup-query-count` and `default ip igmp startup-query-count` commands restore the default `startup-query-count` value of 2 for the configuration mode interface by removing the corresponding `ip igmp startup-query-count` command from `running-config`.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

```
ip igmp startup-query-count number
no ip igmp startup-query-count
default ip igmp startup-query-count
```

**Parameters**
- `number` quantity of queries. Values range from 1 to 65535. Default is 2.

**Example**
- This command configures the startup query count of 10 for VLAN interface 4.
  ```
  switch(config)#interface vlan 4
  switch(config-if-Vl4)#ip igmp startup-query-count 10
  switch(config-if-Vl4)#
  ```
ip igmp startup-query-interval

The `ip igmp startup-query-interval` command specifies the configuration mode interface’s IGMP startup period, during which query messages are sent at an accelerated rate.

When an interface starts running IGMP, it can establish the group state quicker by sending query messages at a higher frequency. The `startup-query-interval` and `startup-query-count` parameters define the startup period and the query message transmission frequency during that period.

The `no ip igmp startup-query-interval` and `default ip igmp startup-query-interval` commands restore the configuration mode interface’s default IGMP `startup-query-interval` of 31 seconds by removing the corresponding `ip igmp startup-query-interval` command from `running-config`.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**
```
ip igmp startup-query-interval period
no ip igmp startup-query-interval
default ip igmp startup-query-interval
```

**Parameters**
- `period` startup query interval, in deciseconds. Value ranges from 10 (one second) to 317440 (8 hours, 49 minutes, 4 seconds). Default is 31 seconds.

**Example**
- This command configures the startup query count of one minute for VLAN interface 4.
```
switch(config)#interface vlan 4
switch(config-if-Vl4)#ip igmp startup-query-interval 600
switch(config-if-Vl4)#
```
The `ip igmp static-group` command configures the configuration mode interface as a static member of a specified multicast group. This allows the router to forward multicast group packets through the interface without otherwise appearing or acting as a group member. By default, static group memberships are not configured on any interfaces.

If the command includes a source address, only multicast group messages received from the specified host address are fast-switched. Otherwise, all multicast messages of the specified group are fast-switched.

**Note**

To become a static member of a multicast group, the switch must be the PIM designated router (DR) for the network. If it is not, you can use the `pim ipv4 dr-priority` command to make it the DR by configuring its PIM DR value to be the highest on the network.

The `no ip igmp static-group` and `default ip igmp static-group` commands remove the configuration mode interface's group membership by removing the corresponding `ip igmp static-group` command from `running-config`.

**Command Mode**

- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

```
ip igmp static-group  group_address  [SOURCE_ADDRESS]
no ip igmp static-group  group_address  [SOURCE_ADDRESS]
default ip igmp static-group  group_address  [SOURCE_ADDRESS]
```

**Parameters**

- **group_address** IPv4 address of multicast group for which the interface fast-switches packets.
- **SOURCE_ADDRESS** IP address of host that originates multicast data packets.
  - <no parameter> all multicast messages of the specified group are fast-switched.
  - `ipv4_address` source IP address (dotted decimal notation).

**Related Commands**

- `ip igmp static-group acl` configures the configuration mode interface as a static member of the multicast groups specified by an IP access control list (ACL).
- `ip igmp static-group range` configures the configuration mode interface as a static member of multicast groups specified by an address range.

One `ip igmp static-group range` command is equivalent to multiple `ip igmp static-group` commands.

**Example**

These commands configure VLAN interface 15 as the PIM designated router, then configure it as a static member of the multicast group at address 231.1.1.15 for multicast data packets that originate at 10.1.1.1.

```
switch(config)#interface vlan 15
switch(config-if-Vl15)#pim ipv4 dr-priority 5000
switch(config-if-Vl15)#ip igmp static-group 231.1.1.45 10.1.1.1
switch(config-if-Vl15)#
```
ip igmp static-group acl

The **ip igmp static-group acl** command configures the configuration mode interface as a static member of the multicast groups specified by an IP access control list (ACL). This command is a variant of the **ip igmp static-group** command that uses ACL rules to specify a set of source-multicast group address pairs instead of specifying a single pair. Multiple static-group ACLs can be assigned to an interface. Static groups can be assigned manually and through ACLs simultaneously.

Access control lists that this command references must contain rules of the following format.

- **permit <protocol><source><destination>,** where
  - **<protocol>** has no effect on the static group.
  - **<source>** address of host originating multicast data packets. Must be a host address.
  - **<destination>** multicast group IP address or subnet. Must be a valid multicast address.

An ACL can contain multiple rules. An ACL can be applied to an interface only when all of its rules comply to the specified restrictions. The **show ip igmp static-groups acl** displays the source-multicast group pairs that the specified list configures and lists issues with illegal rules.

The **no ip igmp static-group acl** and **default ip igmp static-group acl** commands remove the specified static group ACL command from **running-config**.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

- `ip igmp static-group acl list_name`
- `no ip igmp static-group acl list_name`
- `default ip igmp static-group acl list_name`

**Parameters**

- **list_name** ACL that specifies multicast group addresses for which interface fast-switches packets.

**Example**

- This command configures VLAN interface 4 as a static member of the multicast group specified by the ACL named **LIST_1**.

  ```
  switch(config)#interface vlan 4
  switch(config-if-Vl4)#ip igmp static-group acl LIST_1
  switch(config-if-Vl4)#
  ```
Chapter 39: IGMP and IGMP Snooping

**ip igmp static-group range**

The **ip igmp static-group range** command configures the configuration mode interface as a static member of multicast groups specified by an address range. This allows the router to forward multicast group packets through the interface without otherwise appearing or acting as a group member. By default, no static group memberships are configured on interfaces.

This command is a variant of the **ip igmp static-group** command that allows the assignment of a subnet range of source addresses or a subnet range of multicast groups. A single **ip igmp static-group range** command is the equivalent of multiple **ip igmp static-group** commands, each of which can only assign a single multigroup-source pair to an interface. Running-config converts the range command to the equivalent list of **ip igmp static-group** commands.

If the command includes a source address range, only multicast group messages received from the range are fast-switched. Otherwise, all multicast messages of the specified group are fast-switched.

The **no ip igmp static-group range** and **default ip igmp static-group range** commands remove the specified range of static group statements from **running-config**. The **no ip igmp static-group** and **default ip igmp static-group** commands can remove an individual static-group command that was initially added to **running-config** by an **ip igmp static-group range** command.

**Command Mode**

- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

```
ip igmp static-group range GROUP_ADDR [SOURCE_ADDR]
no ip igmp static-group range GROUP_ADDR [SOURCE_ADDR]
default ip igmp static-group range GROUP_ADDR [SOURCE_ADDR]
```

**Parameters**

- **GROUP_ADDR** address of multicast group for which the interface fast-switches packets.
- **gp_ipv4_addr** multicast group IPv4 address.
- **gp_ipv4_subnet** IPv4 subnet address of multicast groups (CIDR or address-mask).
- **SOURCE_ADDR** IP address of a host range that originates multicast data packets.
- `<no parameter>` all multicast messages of the specified range are fast-switched.
- **source sr_ipv4_address** source IPv4 address (dotted decimal notation).
- **source sr_ipv4_subnet** IPv4 subnet address of source hosts (CIDR or address-mask).

**Warning**

A command cannot specify a subnet address for both multicast group and source.

**Examples**

- This command configures VLAN interface 4 as a static member of the multicast group range 241.1.4.1/24 for data packets that originate at 10.1.1.1.

```bash
switch(config)#interface vlan 4
switch(config-if-Vl4)#ip igmp static-group range 239.1.4.1/24 source 10.1.1.1
switch(config-if-Vl4)#
```
This command attempts to configure VLAN interface 4 as a static member of the multicast group range 241.1.4.1/24 for data packets that originate at the 10.1.1.1/29 subnet. Because the range and source cannot both be subnets, this command generates an error message.

```
switch(config-if-Vl4)# ip igmp static-group range 239.1.1.1/29 source 16.1.1.1/29
% Error: cannot specify source range with group range
switch(config-if-Vl4)#
```
**ip igmp version**

The *ip igmp version* command configures the Internet Group Management Protocol (IGMP) version on the configuration mode interface. Version 3 is the default IGMP version.

IGMP is enabled by the `pim ipv4 sparse-mode` or `pim ipv4 bidirectional` command. The `ig igmp version` command does not affect the IGMP enabled status.

The *no ip igmp version* and *default ip igmp version* commands restore the configuration mode interface to IGMP version 3 by removing the *ip igmp version* statement from *running-config*.

**Command Mode**
- Interface-Ethernet Configuration
- Interface-Port-Channel Configuration
- Interface-VLAN Configuration

**Command Syntax**

```
ip igmp version version_number
no ip igmp version
default ip igmp version
```

**Parameters**

- *version_number* IGMP version number. Value ranges from 1 to 3.

**Example**

- This command configures IGMP version 3 on VLAN interface 4.

  ```
  switch(config)#interface vlan 4
  switch(config-if-Vl4)#ip igmp version 3
  switch(config-if-Vl4)#
  ```
permit / deny

The **permit** command configures the configuration mode IGMP profile as a permit list. Applying a permit list to an interface restricts that interface from joining any multicast group not included in the list.

IGMP profiles are deny lists by default. When applied to an interface, a deny list allows the interface to join any multicast group that is not included in the list.

The **deny** command restores the IGMP list to its default type by removing the corresponding **permit** statement from **running-config**.

The **range** command adds and removes address ranges from the configuration mode profile.

**Command Mode**

IGMP-profile Configuration

**Command Syntax**

```plaintext
permit
deny
```

**Related Commands**

- **ip igmp profile** places the switch in IGMP-profile configuration mode.

**Example**

- These commands enter IGMP profile configuration mode and configure the profile as a permit list.

```plaintext
switch(config)#ip igmp profile list_1
switch(config-igmp-profile-list_1)#permit
switch(config-igmp-profile-list_1)#
```
range

The range command specifies an address range for the configuration mode IGMP profile. A permit range specifies the groups that an interface is permitted to join. A deny range specifies the groups that an interface is not permitted to join. The permit / deny command specifies the range type.

A profile may contain multiple range statements to define a discontiguous address range.

The no range and default range commands remove the specified address range from a previous specified list.

**Command Mode**
IGMP-profile Configuration

**Command Syntax**

```
range init_address [UPPER_RANGE]
no range init_address [UPPER_RANGE]
default range init_address [UPPER_RANGE]
```

**Parameters**

- **init_address** IP address of lower boundary of the address range (dotted decimal notation).
- **UPPER_RANGE** sets the upper boundary of the address range. Options include
  - <no parameter> upper boundary is equal to lower boundary: range consists of one address.
  - **range_address** IP address of upper boundary.

All addresses must be multicast addresses (10.0.0.0 to 239.255.255.255).

**Related Commands**

- ip igmp profile places the switch in IGMP-profile configuration mode.

**Example**

- These commands enter IGMP profile configuration mode, configure the profile as a permit list, and define the permit address list of 232.1.1.0 to 232.1.1.255 and 233.1.1.10.

```bash
switch(config)#ip igmp profile list_1
switch(config-igmp-profile-list_1)#permit
switch(config-igmp-profile-list_1)#232.1.1.0 232.1.1.255
switch(config-igmp-profile-list_1)#233.1.1.10
switch(config-igmp-profile-list_1)#ip igmp profile
```
show igmp snooping querier

The `show igmp snooping querier` command displays snooping querier configuration and status information. Command provides options to only include specific VLANs.

**Command Mode**

EXEC

**Command Syntax**

```
show igmp snooping querier [STATUS][VLAN_ID][DATA]
```

**Parameters**

- **STATUS** specifies the type of information displayed. Options include:
  - `<no parameter>` querier IP address, port, and IGMP version.
  - `status` querier configuration parameters.
- **VLAN_ID** specifies VLANs for which command displays information. Options include:
  - `<no parameter>` all VLANs.
  - `vlan v_num` specified VLAN.
- **DATA** specifies the type of information displayed. Options include:
  - `<no parameter>` displays VLAN number and port-list for each group.
  - `detail` displays port-specific data for each group; includes transmission times and expiration.

**Example**

- This command displays the querier IP address, version, and port servicing each VLAN.

  ```
  switch>show igmp snooping querier
  Vlan IP Address Version Port
  ---------------------------
  1  172.17.0.37    v2   Po1
  20 172.17.20.1    v2   Po1
  26 172.17.26.1    v2   Cpu
  2028 172.17.255.29    v2   Po1
  switch>
  ```

- This command displays the querier configuration parameters for each VLAN.

  ```
  switch>show igmp snooping querier status
  Global IGMP Querier status
  ------------------------------------
  admin state : Enabled
  source IP address : 0.0.0.0
  query-interval (sec) : 125.0
  max-response-time (sec) : 10.0
  querier timeout (sec) : 130.0
  ------------------------------------
  Vlan Admin IP Query Response Querier Operational
  State Interval Time Timeout State
  ----------------- --------------- ---- ---- ------------
  1    Enabled 0.0.0.0 125.0 10.0 130.0 Non-Querier
  4    Enabled 0.0.0.0 125.0 10.0 130.0 Non-Querier
  20   Enabled 0.0.0.0 125.0 10.0 130.0 Non-Querier
  22   Enabled 0.0.0.0 125.0 10.0 130.0 Non-Querier
  28   Enabled 0.0.0.0 125.0 10.0 130.0 Non-Querier
  ```
show igmp snooping querier counters

The show igmp snooping querier counters command displays the counters from the querier, as learned through Internet Group Management Protocol (IGMP).

Command Mode

EXEC

Command Syntax

show igmp snooping querier counters [VLAN_ID]

Parameters

- VLAN_ID specifies VLANs for which command displays information. Options include:
  - <no parameter> displays information for all VLANs.
  - vlan v_num displays information for specified VLAN.

Example

- This command displays the counters from the querier.

```
switch>show igmp snooping querier counters
-----------------------------------------------------------------------
Vlan: 1    IP Addr: 100.0.0.1       Op State: Querier     Version:  v3
v1 General Queries Sent         :0
v1 Queries Received             :0
v1 Reports Received             :0
v2 General Queries Sent         :1
v2 Queries Received             :0
v2 Reports Received             :25
v2 Leaves Received              :0
v3 General Queries Sent         :655
v3 GSQ Queries Sent             :0
v3 GSSQ Queries Sent            :8
v3 Queries Received             :654
v3 Reports Received             :2385
Error Packets                   :0
Other Packets                   :0
switch>
```
**show igmp snooping querier membership**

The `show igmp snooping querier membership` command displays the membership from the querier, as learned through Internet Group Management Protocol (IGMP).

**Command Mode**

**EXEC**

**Command Syntax**

```
show igmp snooping querier membership [VLAN_ID [GROUP_LIST]]
```

**Parameters**

- `VLAN_ID` specifies VLANs for which command displays information. Options include:
  - `<no parameter>` displays information for all VLANs.
  - `vlan v_num` displays information for specified VLAN.

- `GROUP_LIST` list of groups for which the command displays information. Options include:
  - `<no parameter>` all multicast groups within specified VLAN.
  - `group ipv4_addr` single multicast group address (dotted decimal notation).

**Example**

- This command displays the membership from the querier for VLAN 1.

```
switch>show igmp snooping querier membership
-------------------------------------------------------------------------
Vlan: 1    Elected: 10.0.0.1       QQI: 125  QRV: 2  QRI: 10  GMI: 260
Groups           Mode  Ver  Num of Sources
-------------------------------------------------------------------------
10.0.0.2        EX    v3   0 []
10.0.0.3        IN    v3   2 [ 3.3.3.3, 3.3.3.4 ]
10.0.0.4        EX    v3   0 []
10.0.0.13       EX    v3   0 []
10.0.0.22       EX    v3   0 []
10.0.0.1        IN    v3   3 [ 5.6.7.9, 5.6.7.8, ... ]
switch>
```
**show ip igmp groups**

The `show ip igmp groups` command displays multicast groups that have receivers directly connected to the switch, as learned through Internet Group Management Protocol (IGMP).

- `show ip igmp groups` all multicast groups.
- `show ip igmp groups group_addr` listed multicast group.
- `show ip igmp groups interface int_name` all multicast groups on specified interfaces.
- `show ip igmp groups group_addr interface int_name` listed multicast group on specified interface.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp groups GROUP_LIST [DATA]
```

**Parameters**

- `GROUP_LIST` list of groups for which the command displays information. Options include:
  - `<no parameter>` all multicast groups.
  - `group_addr` single multicast group address (dotted decimal notation).
  - `interface ethernet e_num` all multicast groups on specified Ethernet interface.
  - `interface loopback l_num` all multicast groups on specified Loopback interface.
  - `interface management m_num` all multicast groups on specified Management interface.
  - `interface port-channel p_num` all multicast groups on specified Port-Channel Interface.
  - `interface vlan v_num` all multicast groups on specified VLAN interface.
  - `interface vxlan vx_num` all multicast groups on specified VXLAN interface.
- `DATA` specifies the type of information displayed. Options include:
  - `<no parameter>` provides uptime, expiration, and address of reporter.
  - `detail` also include group mode and group source list.

**Example**

- This command displays multicast groups with receivers directly connected to the switch.

```
switch> show ip igmp groups
NOTE: static-group information not shown below. Use the 'show ip igmp static-groups' command.

IGMP Connected GroupMembership
Group Address    Interface    Uptime    Expires    Last Reporter
10.12.1.1        Vlan162      11d01h    00:02:57    172.17.2.110
10.12.1.2        Vlan162      11d01h    00:02:57    172.17.2.110
10.12.1.3        Vlan162      11d01h    00:02:57    172.17.2.110
10.12.1.4        Vlan162      11d01h    00:02:57    172.17.2.110
10.12.1.5        Vlan162      11d01h    00:02:57    172.17.2.110
switch>
```
show ip igmp groups count

The `show ip igmp groups count` command displays the number of multicast groups that are joined across the specified interfaces.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp groups [GROUP_LIST] count
```

**Parameters**

- `INTERF` Specifies the interface for which the command displays information. Options include:
  - `<no parameter>` all IGMP interfaces.
  - `interface ethernet e_num` Ethernet interface.
  - `interface loopback l_num` Loopback interface.
  - `interface management m_num` Management interface.
  - `interface port-channel p_num` Port-Channel Interface.
  - `interface vlan v_num` VLAN interface.
  - `interface vxlan vx_num` VXLAN interface.

**Example**

- This command displays the number of multicast groups joined across all interfaces.
  
  ```
  switch>show ip igmp groups count
  Number of total groups joined across all IGMP interfaces: 5
  switch>
  ```

- This command displays the number of multicast groups joined on Ethernet 3/4 interface.
  
  ```
  switch>show ip igmp groups interface ethernet 3/4 count
  Number of groups joined on Ethernet3/4: 2
  switch>
  ```
show ip igmp host-proxy config-sanity

The **show ip igmp host-proxy config-sanity** command displays diagnostic information about an IGMP host proxy configuration.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp host-proxy config-sanity
```

**Example**

- This command displays IGMP host proxy configuration diagnostic information.

```
switch>show ip igmp host-proxy config-sanity
Below are hints of potential IGMP Host-Proxy misconfigurations
IGMP host-proxy configured on interface Test3:
    Access-lists having "deny ip any any" rule:
        acl1
        acl2
    Groups with overlapping permit and deny configurations:
        192.168.1.1/32
        192.168.2.2/32
        192.168.4.4/32
    Groups with source filters configured with IGMP Host-Proxy set to version 2:
        192.168.2.2/32
        192.168.3.0/24
        192.168.3.3/32
        192.168.8.8/32
switch>
```
show ip igmp host-proxy interface

The `show ip igmp host-proxy interface` command displays per-interface IGMP host-proxy configuration information, including the IGMP groups joined on the interface. Command filters allow the list to display only data for a specified interface and to include packet counter statistics in the display.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp host-proxy interface [interface] [detail]
```

**Parameters**

- `interface` optional parameter to limit the display to a single interface. Omitting the parameter displays host-proxy configuration information for all interfaces on which IGMP host-proxy is configured. Options include:
  - `ethernet e_num` Ethernet interface specified by `e_num`.
  - `port-channel p_num` port-channel Interface specified by `p_num`.
  - `vlan v_num` VLAN interface specified by `v_num`.
- `detail` use this optional keyword to include packet counter statistics in the display.

**Examples**

- This command displays host-proxy information for all switch interfaces on which IGMP host-proxy is configured.

```
switch>show ip igmp host-proxy interface
IGMP host-proxy configured on: Test2
IGMP host-proxy version: 3
Unsolicited-report interval: 1.0
Device name: Test2
Interface     Group Address     IncludeSrc        ExcludeSrc
Test2        172.16.89.0
Test2        172.16.0.0        20.0.0.0
Test2        172.16.0.0        10.0.0.0
Test2        192.168.110.0                       20.0.0.0
```
This command displays host-proxy information for all switch interfaces on which IGMP host-proxy is configured, plus host-proxy statistics.

switch>show ip igmp host-proxy interface detail
IGMP host-proxy configured on: Test2
IGMP host-proxy version: 3
Unsolicited-report interval: 1.0
Device name: Test2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group Address</th>
<th>IncludeSrc</th>
<th>ExcludeSrc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test2</td>
<td>172.16.89.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test2</td>
<td>172.16.0.0</td>
<td>20.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Test2</td>
<td>172.16.0.0</td>
<td>10.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Test2</td>
<td>192.168.110.0</td>
<td></td>
<td>20.0.0.0</td>
</tr>
</tbody>
</table>

IGMP host-proxy statistics:

IGMP v1 Queries received: 0
IGMP v2 General-Queries received: 0
IGMP v2 Group-Queries received: 0
IGMP v3 General-Queries received: 0
IGMP v3 Group-Queries received: 0
IGMP v3 Group-Source Queries received: 0
IGMP v1 Reports sent: 0
IGMP v2 Reports sent: 0
IGMP v3 Reports sent: 1
**show ip igmp interface**

The `show ip igmp interface` command displays multicast information about the specified interface.

**Command Mode**

EXEC

**Command Syntax**

`show ip igmp interface [INT_NAME]`

**Parameters**

- `INT_NAME` Interface type and number. Values include
  - `<no parameter>` Displays information for all interfaces.
  - `ethernet e_num` Ethernet interface specified by `e_num`.
  - `loopback l_num` Loopback interface specified by `l_num`.
  - `management m_num` Management interface specified by `m_num`.
  - `port-channel p_num` Port-Channel Interface specified by `p_num`.
  - `vlan v_num` VLAN interface specified by `v_num`.
  - `vxlan vx_num` VXLAN interface specified by `vx_num`.

**Example**

- This command displays multicast related information about VLAN 26.

  ```
  switch>show ip igmp interface vlan 26
  Vlan26 is up
  Interface address: 172.17.26.1/23
  IGMP on this interface: enabled
  Multicast routing on this interface: enabled
  Multicast TTL threshold: 1
  Current IGMP router version: 2
  IGMP query interval: 125 seconds
  IGMP max query response time: 100 deciseconds
  Last member query response interval: 10 deciseconds
  Last member query response count: 2
  IGMP querier: 172.17.26.1
  Robustness: 2
  Require router alert: enabled
  Startup query interval: 312 deciseconds
  Startup query count: 2
  General query timer expiry: 00:00:22
  Multicast groups joined: 239.255.255.250
  ```

  switch>
**show ip igmp profile**

The `show ip igmp profile` command displays the contents of the specified IGMP profile. IGMP snooping filters use an IGMP profile to control the multicast groups that an interface can join.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp profile [PROFILES]
```

**Parameters**

- **PROFILES**  IGMP profiles for which command displays contents. Options include:
  - `<no parameter>`  displays all IGMP profiles.
  - `profile_name`  displays specified profile.

**Example**

- This command displays the IGMP profiles configured on the switch.

```
switch>show ip igmp profile
IGMP Profile list_1
  permit
      range 229.1.24.0 229.1.25.255
IGMP Profile list_2
  deny
      range 234.1.1.0 234.1.255.255
switch>
```
**show ip igmp snooping**

The `show ip igmp snooping` command displays the switch’s IGMP snooping configuration.

**Command Mode**

EXEC

**Command Syntax**

`show ip igmp snooping [VLAN_ID]`

**Parameters**

- `VLAN_ID` specifies VLANs for which command displays information. Options include:
  - `<no parameter>` displays information for all VLANs.
  - `vlan v_num` displays information for specified VLAN.

**Example**

- This command displays the switch’s IGMP snooping configuration.

```plaintext
switch>show ip igmp snooping
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                  : Enabled
Robustness variable            : 2

Vlan 1 :
-------
IGMP snooping                  : Enabled
Multicast router learning mode : pim-dvmrp

Vlan 20 :
-------
IGMP snooping                  : Enabled
Multicast router learning mode : pim-dvmrp

Vlan 26 :
-------
IGMP snooping                  : Enabled
Multicast router learning mode : pim-dvmrp

Vlan 2028 :
---------
IGMP snooping                  : Enabled
Multicast router learning mode : pim-dvmrp

switch>
```
**show ip igmp snooping counters**

The *show ip igmp snooping counters* command displays the number of IGMP messages sent and received through each switch port. The display table sorts the messages by type.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp snooping counters [DATA_TYPE][DATA_LEVEL]
```

**Parameters**

- **DATA_TYPE** Information displayed by the command. Options include:
  - `<no parameter>` displays transmission counters.
  - `errors` displays error counters.
- **DATA_LEVEL** specifies the type of information displayed. Options include:
  - `<no parameter>` number of packets on physical ports.
  - `detail` number of packets on physical ports.

**Example**

This command displays the number of messages received on each port.

```
switch>show ip igmp snooping counters
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Input</th>
<th>Queries</th>
<th>Reports</th>
<th>Leaves</th>
<th>Others</th>
<th>Errors</th>
<th>Output</th>
<th>Queries</th>
<th>Reports</th>
<th>Leaves</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cpu</td>
<td></td>
<td>15249</td>
<td>106599</td>
<td>4</td>
<td>269502</td>
<td>0</td>
<td>30242</td>
<td>102812</td>
<td>972</td>
<td>3625</td>
<td></td>
</tr>
<tr>
<td>Et1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et2</td>
<td>6</td>
<td>1</td>
<td>26</td>
<td>0</td>
<td>5415</td>
<td>0</td>
<td>0</td>
<td>731</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et3</td>
<td>0</td>
<td>10905</td>
<td>222</td>
<td>1037</td>
<td>0</td>
<td>15246</td>
<td>0</td>
<td>0</td>
<td>1448</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et4</td>
<td>4475</td>
<td>21</td>
<td>288</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2199</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et5</td>
<td>0</td>
<td>355</td>
<td>0</td>
<td>39</td>
<td>0</td>
<td>15211</td>
<td>0</td>
<td>0</td>
<td>2446</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et6</td>
<td>475</td>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2487</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et7</td>
<td>0</td>
<td>0</td>
<td>151</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2336</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et8</td>
<td>0</td>
<td>578</td>
<td>6</td>
<td>75</td>
<td>0</td>
<td>2859</td>
<td>0</td>
<td>0</td>
<td>931</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et9</td>
<td>0</td>
<td>0</td>
<td>27</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2460</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et10</td>
<td>0</td>
<td>12523</td>
<td>345</td>
<td>54</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2433</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et12</td>
<td>0</td>
<td>4509</td>
<td>41</td>
<td>22</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2465</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et13</td>
<td>0</td>
<td>392</td>
<td>29</td>
<td>119</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2368</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et14</td>
<td>0</td>
<td>88</td>
<td>3</td>
<td>6</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2481</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et15</td>
<td>0</td>
<td>16779</td>
<td>556</td>
<td>72</td>
<td>0</td>
<td>15117</td>
<td>0</td>
<td>0</td>
<td>66</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et16</td>
<td>0</td>
<td>2484</td>
<td>13</td>
<td>66</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2421</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et18</td>
<td>0</td>
<td>20</td>
<td>6</td>
<td>160</td>
<td>0</td>
<td>3688</td>
<td>0</td>
<td>0</td>
<td>803</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et19</td>
<td>0</td>
<td>4110</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2487</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et22</td>
<td>0</td>
<td>0</td>
<td>52</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2435</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et23</td>
<td>0</td>
<td>5439</td>
<td>181</td>
<td>138</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2349</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et24</td>
<td>0</td>
<td>2251</td>
<td>21</td>
<td>4</td>
<td>0</td>
<td>15247</td>
<td>0</td>
<td>0</td>
<td>2483</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1</td>
<td>45360</td>
<td>540670</td>
<td>8853</td>
<td>464900</td>
<td>0</td>
<td>15249</td>
<td>224751</td>
<td>618</td>
<td>2576</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po2</td>
<td>0</td>
<td>101399</td>
<td>58</td>
<td>17</td>
<td>0</td>
<td>15120</td>
<td>0</td>
<td>0</td>
<td>1121</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Switch</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**show ip igmp snooping counters ethdev-pams**

The `show ip igmp snooping counters` command displays the number of dropped IGMP packets messages sent and received through each switch port at the kernel level. The display table sorts the messages by type.

**Command Mode**

**EXEC**

**Command Syntax**

```
show ip igmp snooping counters ethdev-pams
```

**Example**

- This command displays the number of messages dropped at the kernel level.

```
switch> show ip igmp snooping counters ethdev-pams

<table>
<thead>
<tr>
<th>IntfName</th>
<th>rxErrors</th>
<th>txErrors</th>
<th>txDrops</th>
</tr>
</thead>
<tbody>
<tr>
<td>et9</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et18</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mlag9</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mlag8</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et17</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>po1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>po2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et15</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et6</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mlag10</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et16</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mlag7</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et11</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mlag5</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mlag4</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>cpu</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et13</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

switch>
show ip igmp snooping groups

The `show ip igmp snooping groups` command displays IGMP snooping statistics. Available information includes the physical ports that send and receive information, the time when multicast data was originally and most recently heard on the ports, and the version number of the IGMP messages. Command provides options that restrict the output to specific VLANs, ports, and groups.

Command Mode
EXEC

Command Syntax
```
show ip igmp snooping groups proxy [VLAN_ID] [PORT_INT] [GROUPS] [DATA]
```

Parameters
- **VLAN_ID** specifies VLAN for which command displays information. Options include:
  - `<no parameter>` displays information for all VLANs.
  - `vlan v_num` displays information for VLAN `v_num` (1 to 4094).
- **PORT_INT** specifies physical ports for which command displays information. Options include:
  - `<no parameter>` displays information for all physical ports.
  - `interface ethernet e_range`, where `e_range` is the number, range, or list of Ethernet ports.
  - `interface port-channel p_range`, where `p_range` is the number, range, or list of channel ports.
- **GROUPS** specifies the multicast groups. Options include:
  - `<no parameter>` all multicast groups on all specified ports.
  - `mgroup_address` multicast group specified by IPv4 address (dotted decimal notation).
  - `dynamic` multicast groups learned through IGMP.
  - `user` multicast groups manually added.
- **DATA** specifies the type of information displayed. Options include:
  - `<no parameter>` VLAN number and port-list for each group.
  - `detail` port-specific information for each group, including transmission times and expiration.
  - `proxy` displays IGMP snooping proxy information.

Examples
- This command displays the port lists for all multicast groups.
```
switch>show ip igmp snooping groups
Vlan  Group            Type     Version             Port-List
-------------------------------------------------------------------------------
                        -        -                   Po1, Po2
1     239.255.255.250  -        -                   Cpu, Et3, Et4, Et10, Et23, Et27
26    239.255.255.250  -        -                   Po1, Po2
```

switch>
• This command displays detailed port information of all multicast groups.

```
switch>show ip igmp snooping groups detail
Vlan  Group           IP              First     Last    Expire    Ver Filter Port Mode
Heard     Heard                 Mode
-------------------------------------------------------------------------------
- 1    239.255.255.250 172.17.3.73     2536:15   0:47    3:33      v2  0      Po2
1 239.255.255.250 172.17.0.37     31532:48  0:18    1:27     -   -      Po1
26 239.255.255.250 172.17.26.189   5:07      0:52    3:28      v2  0      Et3
26 239.255.255.250 172.17.26.182   17:34     3:02    1:18      v2  0      Et3
26 239.255.255.250 172.17.26.245   1046:47   0:57    3:23      v2  0      Et4
26 239.255.255.250 172.17.26.184   27:41     0:53    3:27      v2  0      Et10
26 239.255.255.250 172.17.26.161   9:16      0:56    3:24      v2  0      Et23
26 239.255.255.250 172.17.26.62    90:24     0:50    3:30      v2  0      Et27
26 239.255.255.250 172.17.26.1     31532:53  0:04    1:41     -   -      Cpu
switch>
```

• This command displays the port lists for all dynamic multicast groups.

```
switch>show ip igmp snooping groups dynamic
Vlan  Group            Type     Version             Port-List
-------------------------------------------------------------------------------
- 1    239.255.255.250  -        -                   Po1, Po2
26    239.255.255.250  -        -                   Cpu, Et3, Et4, Et10, Et23, Et27, Et34
switch>
```

• This command displays the detailed port information for all dynamic multicast groups.

```
switch>show ip igmp snooping groups dynamic detail
Vlan  Group           IP              First     Last    Expire    Ver Filter Port Mode
Heard     Heard                 Mode
-------------------------------------------------------------------------------
- 1    239.255.255.250 172.17.3.73     2539:16   1:37    2:43      v2  0      Po2
1 239.255.255.250 172.17.0.37     31535:49  0:19    1:26     -   -      Po1
26 239.255.255.250 172.17.26.189   8:08      3:53    0:27      v2  0      Et3
26 239.255.255.250 172.17.26.182   20:35     1:49    2:31      v2  0      Et3
26 239.255.255.250 172.17.26.245   1049:48   1:46    2:34      v2  0      Et4
26 239.255.255.250 172.17.26.184   30:42     1:44    2:36      v2  0      Et10
26 239.255.255.250 172.17.26.161   12:17     3:57    0:23      v2  0      Et23
26 239.255.255.250 172.17.26.143   1:53      1:53    2:27      v2  0      Et23
26 239.255.255.250 172.17.26.62    93:25     1:48    2:32      v2  0      Et27
26 239.255.255.250 172.17.26.1     31535:53  0:05    1:40     -   -      Cpu
switch>
```

• This command displays the port lists for all static (user configured) multicast groups.

```
switch>show ip igmp snooping groups user
Vlan  Group            Type     Version             Port-List
-------------------------------------------------------------------------------
- 1    239.255.255.250  -        -                   Po1, Po2
26    239.255.255.250  -        -                   Cpu, Et3, Et4, Et10, Et23, Et27, Et34
switch>
```
• This command displays detailed port information for all user configured (static) multicast groups.

```
switch>show ip igmp snooping groups user detail
Vlan Group       IP              First     Last    Expire    Ver Filter Port
Heard          Heard
-------------------------------------------------------------------
-  1    239.255.255.250 172.17.3.73     2539:50   0:06    4:14      v2  0      Po2
1    239.255.255.250 172.17.0.37     31536:23  0:23    1:22      -   -      Po1
26   239.255.255.250 172.17.26.182   21:09     0:21    3:59      v2  0      Et3
26   239.255.255.250 172.17.26.245   1050:22   0:17    4:03      v2  0      Et4
26   239.255.255.250 172.17.26.161   12:51     0:17    4:03      v2  0      Et23
26   239.255.255.250 172.17.26.143   2:27      2:27    1:53      v2  0      Et10
26   239.255.255.250 172.17.26.184   31:16     0:17    4:03      v2  0      Et23
26   239.255.255.250 172.17.26.164   93:59     0:22    3:58      v2  0      Et27
26   239.255.255.250 172.17.26.1     31536:27  0:09    1:36      -   -      Cpu
```

• This command displays detailed port information for multicast group 239.255.255.253 on VLAN 10.

```
switch>show ip igmp snooping groups vlan 10 239.255.255.253 detail
Vlan Group       IP              First     Last    Expire    Ver Filter Port
Heard          Heard
-------------------------------------------------------------------
-  10  239.255.255.253 10.255.255.246  7177:16   0:08    2:07      v2  0      Po7
10  239.255.255.253 10.255.255.247  7177:20   0:03    2:12      v2  0      Po7
10  239.255.255.253 10.255.255.248  7177:16   0:06    2:09      v2  0      Po7
10  239.255.255.253 10.255.255.254  7177:56   0:07    1:38      -   -      Cpu
```

• This command displays the groups that is present in IGMP report when a query is received on any of the ports listed under port-list.

```
switch>show ip igmp snooping groups proxy
Vlan  Group  Type  Port-List
----------------------------------
10    225.0.0.1  Proxy  Cpu, Et4, Et6
10    225.2.2.2  Proxy  Cpu, Et3, Et4
10    225.3.3.3  Proxy  Cpu, Et3, Et4, Et6
```

• This command displays all the information that is present in the IGMP report if a general IGMP query was received on Ethernet4.

```
switch>show ip igmp snooping groups proxy interface Ethernet4 detail
Vlan  Interface  Group  Source/Filter Mode
------------------------------------------
10    Ethernet4  225.0.0.1  Include
       150.227.112.250
       150.227.112.250
10    Ethernet4  225.2.2.2  Exclude
10    Ethernet4  225.3.3.3  Exclude
       150.227.112.250
```
show ip igmp snooping groups count

The `show ip igmp snooping groups count` command displays the number of multicast groups on the switch. Command provides options to only include specific VLANs and ports.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp snooping groups [VLAN_ID][PORT_INT] count [DATA]
```

**Parameters**

- **VLAN_ID** specifies VLAN for which command displays information. Options include:
  - `<no parameter>` all VLANs.
  - `vlan v_num` specified VLAN.
- **PORT_INT** specifies physical ports for which command displays information. Options include:
  - `<no parameter>` all physical ports.
  - `interface ethernet e_range` specified Ethernet ports.
  - `interface port-channel p_range` specified port channels.

Valid `e_range` and `p_range` formats include number, number range, or comma-delimited list of numbers and ranges.

- **DATA** specifies the type of information displayed. Options include:
  - `<no parameter>` number of multicast group on specified VLAN and ports.
  - `detail` number of multicast group on specified VLAN and ports.

**Example**

- This command displays the number of multicast groups on the switch.

  ```
  switch> show ip igmp snooping groups count
  Total number of multicast groups: 2
  switch>
  ```
show ip igmp snooping mrouter

The `show ip igmp snooping mrouter` command displays the status of dynamic and static multicast router ports. Command provides options to include only specific VLANs.

**Command Mode**
EXEC

**Command Syntax**
```
show ip igmp snooping mrouter [VLAN_ID] [DATA]
```

**Parameters**
- `VLAN_ID` specifies VLAN for which command displays information. Options include:
  - `<no parameter>` all VLANs.
  - `vlan v_num` specified VLAN.
- `DATA` specifies the type of information displayed. Options include:
  - `<no parameter>` displays VLAN number and port-list for each group.
  - `detail` displays port-specific data for each group; includes transmission times and expiration.

**Examples**
- This command displays port information of each multicast router on all VLANs.
  ```
  switch>show ip igmp snooping mrouter
  Vlan   Interface-ports
  -----------------------------------------------------------------------------
  1      Po1(dynamic)
  20     Po1(dynamic)
  26     Cpu(dynamic)
  2028   Cpu(dynamic), Pol(dynamic)
  switch>
  ```
- This command displays multicast router information for each port.
  ```
  switch>show ip igmp snooping mrouter detail
  Vlan   Intf   Address          FirstHeard LastHeard  Expires  Type
  -----------------------------------------------------------------------------
  1      Po1   172.17.0.37      31549:12  0:12     1:33   pim
  20     Po1   172.17.20.1      7066:51   0:19     1:26   pim
  26     Cpu   172.17.26.1      31549:16  0:28     1:17   pim
  2028   Po1   172.17.255.29    31549:10  0:18     1:27   pim
  2028   Cpu   172.17.255.30    31549:14  0:28     1:17   pim
  switch>
  ```
show ip igmp snooping report-flooding

The `show ip igmp snooping report-flooding` command displays IGMP snooping L2 report flooding configuration and status information. Command provides options to only include specific VLANs.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp snooping report-flooding [VLAN_ID][DATA]
```

**Parameters**

- **VLAN_ID** specifies VLANs for which command displays information. Options include:
  - <no parameter> all VLANs.
  - `vlan v_num` specified VLAN.
- **DATA** specifies the type of information displayed. Options include:
  - <no parameter> displays VLAN number and port-list for each group.
  - `detail` displays port-specific data for each group; includes transmission times and expiration.
show ip igmp static-groups

The show ip igmp static-groups command displays information about all configured IGMP multicast static groups. IGMP multicast static groups are assigned with the ip igmp static-group command.

Command Mode
EXEC

Command Syntax
show ip igmp static-groups [INFO_LEVEL] [interface INT_NAME]

Parameters
- **INFO_LEVEL** specifies the type of information displayed. Options include
  - <no parameter> VLAN number and port-list for each group.
  - detail port-specific information for each group, including transmission times and expiration.
- **INT_NAME** Interface type and number. Values include
  - <no parameter> static groups on all interfaces.
  - ethernet e_num Ethernet interface specified by e_num.
  - loopback l_num Loopback interface specified by l_num.
  - management m_num Management interface specified by m_num.
  - port-channel p_num Port-Channel Interface specified by p_num.
  - vlan v_num VLAN interface specified by v_num.
  - vxlan vx_num VXLAN interface specified by vx_num.

Related Commands
- show ip igmp static-groups acl
- show ip igmp static-groups group

Examples
- This command displays information about all multicast static groups.
  switch>show ip igmp static-groups
  Interface Vlan281:
  Manually configured groups:
  Interface Port-Channel999:
  Manually configured groups:
  switch>
- This command displays information about the multicast static groups on VLAN interface 21.
  switch>show ip igmp static-groups interface vlan 21
  Interface Vlan281:
  Manually configured groups:
  switch>
show ip igmp static-groups acl

The **show ip igmp static-groups acl** command displays information about the IGMP multicast static groups that are configured by the specified access control list (ACL). The command also displays problems with an ACL that prevent its assignment to an interface.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp static-groups acl
```

**Example**

The following `show ip igmp static-group acl` command example references these ACLs:

```
ip access-list 1
  10 permit igmp host 10.1.1.1 10.1.1.0/29
  20 permit igmp host 10.1.1.2 10.1.1.0/29
!
ip access-list 2
  10 permit igmp 10.1.1.0/29 host 10.1.1.1
!
ip access-list 3
  10 deny igmp host 10.1.1.1 255.1.1.0/29
!
ip access-list 4
  10 permit igmp host 10.1.1.1 10.1.1.0/29
  20 permit igmp 10.1.1.0/29 host 10.1.1.1
```

- This command displays static group configuration data about the various ACLs.

```
switch>show ip igmp static-group acl 1
acl 1
  ( 10.1.1.1, 10.1.1.0/29 )
  ( 10.1.1.2, 10.1.1.0/29 )
Interfaces using this ACL for static groups:
  Ethernet12
switch>show ip igmp static-group acl 2
acl 2
  Seq no 30: source address must be a single host or *, not a range
Interfaces using this ACL for static groups:
  Ethernet8
switch>show ip igmp static-group acl 3
acl 3
  Seq no 10: action must be 'permit'
Interfaces using this ACL for static groups:
  none
switch>show ip igmp static-group acl 4
acl 4
  Seq no 10: action must be 'permit'
Interfaces using this ACL for static groups:
  none
switch>show ip igmp static-group acl 5
acl 5
  ( 10.1.1.1, 10.1.1.0/29 )
  Seq no 20: source address must be a single host or *, not a range
Interfaces using this ACL for static groups:
  none
switch>
```
show ip igmp static-groups group

The `show ip igmp static-groups group` command displays information about all specified IGMP multicast static groups. IGMP multicast static groups are assigned with the `ip igmp static-group` command.

**Command Mode**

EXEC

**Command Syntax**

```
show ip igmp static-groups group [GROUP_LIST]
```

**Parameters**

- **GROUP LIST**  Groups for which command displays information
  - `<no parameter>`  all multicast groups.
  - `group_address`  single multicast group address (dotted decimal notation).

**Related Commands**

- `show ip igmp static-groups`
show ip igmp statistics

The `show ip igmp statistics` command displays IGMP transmission statistics for the specified interface.

**Command Mode**

EXEC

**Command Syntax**

```plaintext
show ip igmp statistics [INTERFACE_ID]
```

**Parameters**

- `INTERFACE_ID` Specifies interface for which command returns data. Options include:
  - `<no parameter>` all interfaces.
  - `interface ethernet e_num` Ethernet interface specified by `e_num`.
  - `interface loopback l_num` Loopback interface specified by `l_num`.
  - `interface management m_num` Management interface specified by `m_num`.
  - `interface port-channel p_num` Port-Channel Interface specified by `p_num`.
  - `interface vlan v_num` VLAN interface specified by `v_num`.
  - `interface vxlan vx_num` VXLAN interface specified by `vx_num`.

**Example**

- This command displays IGMP transmission statistics for ethernet 1 interface.

```
switch>show ip igmp statistics interface ethernet 1
IGMP counters for Ethernet1:
  V1 queries sent: 0
  V2 queries sent: 0
  V3 queries sent: 3
  Total general queries sent: 3
  V3 group specific queries sent: 0
  V3 group-source specific queries sent: 0
  V1 queries received: 0
  V2 queries received: 0
  V3 queries received: 0
  V1 reports received: 0
  V2 reports received: 0
  V3 reports received: 14
  V2 leaves received: 0
  Error Packets received: 0
  Other Packets received: 0
switch>
```