7
IGMP Snooping for IPv4 Multicast Traffic

Note

- For complete syntax and usage information for the commands used in this chapter, see these publications:

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.4SY supports only Ethernet interfaces. Cisco IOS Release 15.4SY does not support any WAN features or commands.
- To constrain IPv6 Multicast traffic, see Chapter 14, "IPv6 MLD Snooping."

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

Prerequisites for IGMP Snooping

None.

Restrictions for IGMP Snooping

General IGMP Snooping Restrictions

- Multicast packets are not bridged in a VLAN to local receivers that send IGMP joins when PIM snooping is enabled in the VLAN and IGMP snooping is disabled in the VLAN. (CSCta03980)
- For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.
- IGMP snooping supports private VLANs. Private VLANs do not impose any restrictions on IGMP snooping.
- IGMP snooping constrains traffic in MAC multicast groups 0100.5e00.0001 to 0100.5eff.ffff.
- IGMP snooping does not constrain Layer 2 multicasts generated by routing protocols.

IGMP Snooping Querier Restrictions

- The IGMP snooping querier does not support querier elections. Enable the IGMP snooping querier on only one switch in the VLAN. (CSCsk48795)
- Configure the VLAN in global configuration mode (see Chapter 26, "Virtual Local Area Networks (VLANs)").
- Configure an IP address on the VLAN interface (see Chapter 35, "Layer 3 Interfaces"). When enabled, the IGMP snooping querier uses the IP address as the query source address.
- If there is no IP address configured on the VLAN interface, the IGMP snooping querier does not start. The IGMP snooping querier disables itself if the IP address is cleared. When enabled, the IGMP snooping querier restarts if you configure an IP address.
- The IGMP snooping querier sends IGMPv3 querier messages. Although the IGMP version of the querier messages is not configurable, the querier is compatible with IGMPv2 hosts.
- When enabled, the IGMP snooping querier starts after 60 seconds with no IGMP traffic detected from a multicast router. If IGMP traffic from a multicast router, or from another IGMP snooping querier in the VLAN, is detected after the IGMP snooping querier has started, the querier will disable itself.
- QoS does not support IGMP packets when IGMP snooping is enabled.
- With Release 15.1(1)SY1 and later releases, IGMP snooping and PIM snooping constrain VPLS multicast traffic.

Information About IGMP Snooping

IGMP Snooping Overview

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. You can configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

Some applications use a single unicast cluster IP address and multicast cluster MAC address. Multicast traffic addressed to a unicast cluster IP address is forwarded to the last-hop router that is configured with the shared multicast MAC address. To support cluster-addressed multicast traffic, assign a static multicast MAC address for the destination IP address of the end host or cluster.

You can configure the IGMP snooping lookup method for each VLAN. Layer 3 IGMP snooping lookup uses destination IP addresses in the Layer 2 multicast table (this is the default). Layer 2 IGMP snooping lookup uses destination MAC addresses in the Layer 2 multicast table.

Note Changing the lookup mode is disruptive. Multicast forwarding is not optimal until all multicast entries are programmed with the new lookup mode. Also, if 32 IP addresses are mapped to a single MAC address, forwarding on the device might be suboptimal.

IGMP, which runs at Layer 3 on a multicast router, generates Layer 3 IGMP queries in subnets where the multicast traffic needs to be routed.

You can configure the IGMP snooping querier on the switch to support IGMP snooping in subnets that do not have any multicast router interfaces. For more information about the IGMP snooping querier, see the "Enabling the IGMP Snooping Querier" section on page 7-9.

IGMP (on a multicast router) or, locally, the IGMP snooping querier, sends out periodic general IGMP queries that the switch forwards through all ports in the VLAN and to which hosts respond. IGMP snooping monitors the Layer 3 IGMP traffic.

Note If a multicast group has only sources and no receivers in a VLAN, IGMP snooping constrains the multicast traffic to only the multicast router ports.

Joining a Multicast Group

Hosts join multicast groups either by sending an unsolicited IGMP join message or by sending an IGMP join message in response to a general query from a multicast router (the switch forwards general queries from multicast routers to all ports in a VLAN).

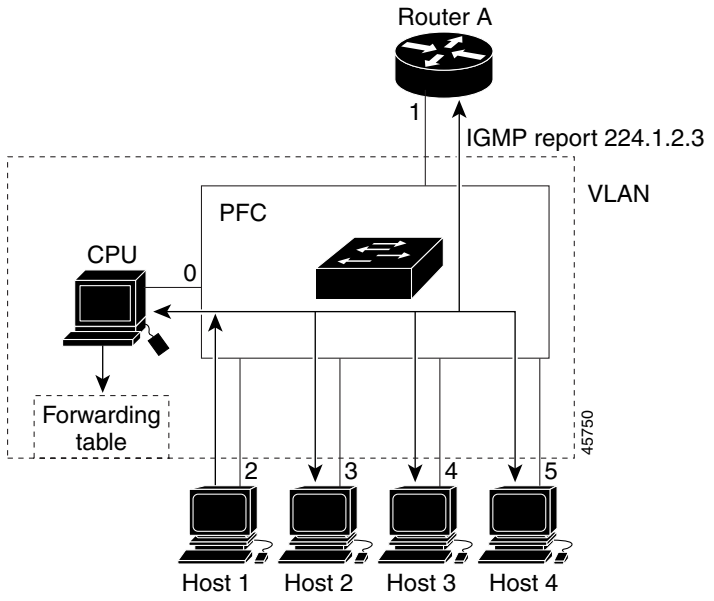
In response to an IGMP join request, the switch creates an entry in its Layer 2 forwarding table for the VLAN on which the join request was received. When other hosts that are interested in this multicast traffic send IGMP join requests, the switch adds them to the existing Layer 2 forwarding table entry. The switch creates only one entry per VLAN in the Layer 2 forwarding table for each multicast group for which it receives an IGMP join request.

IGMP snooping suppresses all but one of the host join messages per multicast group and forwards this one join message to the multicast router.

The switch forwards multicast traffic for the multicast group specified in the join message to the interfaces where join messages were received (see Figure 7-1).

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups using the **mac address-table static** command. When you specify group membership for a multicast group address statically, the static setting supersedes any IGMP snooping learning. Multicast group membership lists can consist of both static and IGMP snooping-learned settings.

Figure 7-1 Initial IGMP Join Message



Multicast router A sends a general query to the switch, which forwards the query to ports 2 through 5 (all members of the same VLAN). Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group with the equivalent MAC destination address of 0x0100.5E01.0203. When the CPU receives the IGMP report multicast by Host 1, the CPU uses the information in the IGMP report to set up a forwarding-table entry, that includes the port numbers of Host 1, the multicast router, and the switch internal CPU.

CPU installs snooping forwarding entry based on lookup type, either IP or MAC (by default, it is IP-based). Using IP-based forwarding can avoid group address aliasing problem and optimize per group or per group and source forwarding.

If IP-based is configured, IGMP snooping forwarding table has the following entry. The switch engine matches on the destination IP address of multicast data packets. If they are 224.1.2.3, send them to the host that has joined the group and multicast routers.

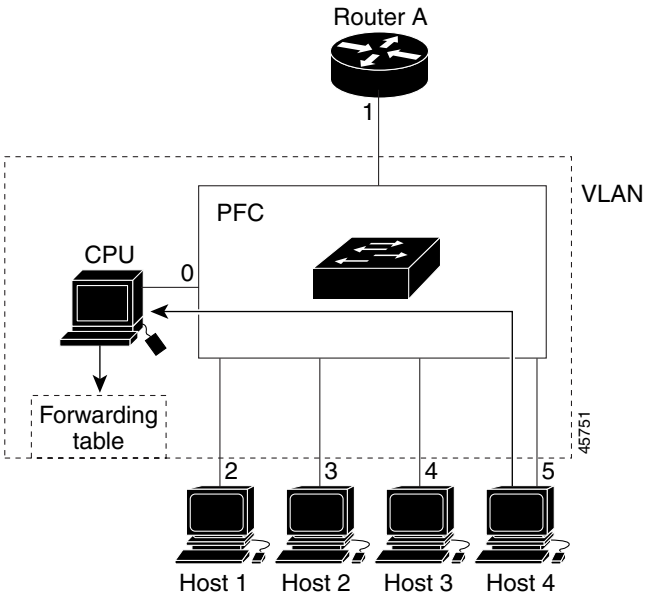
```
vlan        mac/ip address                        LTL         ports
+----+----------------------------------------+------+----------------------
200        ( *,224.1.2.3)                       0x924    Router, Gi3/11
```

If MAC-based is configured, the entry is as follows. In this case, the switch engine matches on the destination MAC address of the packets. The packets with 0100.5e01.0203 are sent to the host that has joined the group and multicast routers.

```
vlan        mac/ip address                        LTL         ports
+----+----------------------------------------+------+----------------------
200        0100.5e01.0203                        0x92C    Router, Gi3/11
```

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group (Figure 7-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table. Because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports. Any known multicast traffic is forwarded to the group and not to the CPU.

Figure 7-2 Second Host Joining a Multicast Group




```
vlan        mac/ip address                       LTL       ports
+----+-----------------------------------------+------+----------------------
200         ( *,224.1.2.3)                        0x924    Router, Gi3/11, Gi1/10
```

Leaving a Multicast Group

Normal Leave Processing

Interested hosts must continue to respond to the periodic general IGMP queries. As long as at least one host in the VLAN responds to the periodic general IGMP queries, the multicast router continues forwarding the multicast traffic to the VLAN. When hosts want to leave a multicast group, they can either ignore the periodic general IGMP queries (called a “silent leave”), or they can send a group-specific IGMPv2 leave message.

When IGMP snooping receives a group-specific IGMPv2 leave message from a host, it sends out a MAC-based general query to determine if any other devices connected to that interface are interested in traffic for the specific multicast group. If IGMP snooping does not receive an IGMP Join message in response to the general query, it assumes that no other devices connected to the interface are interested in receiving traffic for this multicast group, and it removes the interface from its Layer 2 forwarding table entry for that multicast group. If the leave message was from the only remaining interface with hosts interested in the group and IGMP snooping does not receive an IGMP Join in response to the general

query, it removes the group entry and relays the IGMP leave to the multicast router. If the multicast router receives no reports from a VLAN, the multicast router removes the group for the VLAN from its IGMP cache.

The interval for which the switch waits before updating the table entry is called the "last member query interval." To configure the interval, enter the **ip igmp snooping last-member-query-interval** *interval* command.

Immediate-Leave Processing

IGMP snooping immediate-leave processing allows IGMP snooping to remove a Layer 2 LAN interface from the forwarding-table entry without first sending out IGMP group-specific queries to the interface. Upon receiving a group-specific IGMPv2 leave message, IGMP snooping immediately removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Immediate-leave processing improves bandwidth management for all hosts on a switched network.

Note Use immediate-leave processing only on VLANs where only one host is connected to each Layer 2 LAN port. If immediate-leave is enabled in VLANs where more than one host is connected to a Layer 2 LAN port, some hosts might be dropped inadvertently. Immediate-leave processing is supported only with IGMP version 2 and 3 hosts.

Information about the IGMP Snooping Querier

Use the IGMP snooping querier to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed.

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. If the IP-multicast traffic in a VLAN only needs to be Layer 2 switched, an IP-multicast router is not required, but without an IP-multicast router on the VLAN, you must configure another switch as the IGMP querier so that it can send queries.

When enabled, the IGMP snooping querier sends out periodic IGMPv3 queries that trigger IGMP report messages from the switch that wants to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

Configure one switch as the IGMP snooping querier in each VLAN that is supported on switches that use IGMP to report interest in IP multicast traffic.

You can configure a switch to generate IGMP queries on a VLAN regardless of whether or not IP multicast routing is enabled.

Information about IGMP Version 3 Support

IGMP Version 3 Support Overview

IGMP snooping supports IGMP version 3 (IGMPv3). IGMPv3 uses source-based filtering, which enables hosts and routers to specify which source addresses should be allowed or blocked for a specific multicast group. When you enable IGMPv3 snooping, the switch maintains IGMPv3 states based on messages it receives for a particular group in a particular VLAN and either allows or blocks traffic based on the following information in these messages:

- Source lists
- Allow (include) or block (exclude) filtering options

When a host wants to receives multicast traffic only from specific sources, it can send IGMPv3 joins with source filtering. For example, when host1 on port 3/11 sends join to group 224.1.2.3 from sources 10.1.1.1 and host2 on port 3/12 sends join to the same group but from a different source 20.1.1.1, the following entries are installed in forwarding table when IP-based lookup is configured:

```
vlan         mac/ip address                        LTL      ports
+----+----------------------------------------+------+----------------------
200        ( *,224.1.2.3)                       0x920
200        (10.1.1.1,224.1.2.3)                 0x93E    Gi3/11
200        (20.1.1.1,224.1.2.3)                 0x940    Gi3/12
```

The second entry constrain group traffic from source 10.1.1.1 to host1 only and the third entry constrain traffic from source 20.1.1.1 to Host2. The first entry drops group traffic from any other sources since there is no receiver interesting in other sources.

IGMPv3 Immediate-Leave Processing

IGMPv3 immediate-leave processing is active if explicit-host tracking is enabled. The **ip igmp snooping immediate-leave** command that enables IGMP version 2 immediate-leave processing does not affect IGMPv3 immediate-leave processing.

Immediate-leave processing with IGMPv3 is implemented by maintaining source-group based membership information in software while also allocating LTL indexes on a MAC GDA basis.

When immediate-leave processing is active, hosts send BLOCK_OLD_SOURCES{src-list} messages for a specific group when they no longer want to receive traffic from that source. When the switch receives such a message from a host, it parses the list of sources for that host for the given group. If this source list is exactly the same as the source list received in the leave message, the switch removes the host from the LTL index and stops forwarding this multicast group traffic to this host.

If the source lists do not match, the switch does not remove the host from the LTL index until the host is no longer interested in receiving traffic from any source.

Proxy Reporting

IGMP supports proxy reporting for IGMPv1 and IGMPv2 messages to handle group-specific queries. These queries are not sent downstream, but the switch does respond to them directly. When the switch receives a group-specific query, the switch terminates the query and sends an IGMP proxy report if there is a receiver for the group. There is no proxy reporting for IGMPv3 messages. For IGMPv3, a group-specific query or a group source-specific query is flooded to all VLAN member ports. The database for the IGMPv3 membership report is built based on the reports received.

Host reports responding to a specific query can be suppressed by the report suppression feature. Report suppression is supported for IGMPv1, IGMPv2, and IGMPv3 messages. With report suppression enabled (by default), when the switch receives a general query, the switch starts a suppression cycle for

reports from all hosts to each group or channel (S,G). Only the first report to the discovered multicast routers is forwarded; the rest of the reports are suppressed. For IGMPv1 and IGMPv2, the time of suppression is the report response time indicated in the general query message. For IGMPv3, suppression occurs for the entire general query interval.

Note The states are maintained only in software and used for explicit host tracking and statistics collection.

Explicit Host Tracking

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

- The port connected to the host
- The channels reported by the host
- The filter mode for each group reported by the host
- The list of sources for each group reported by the hosts
- The router filter mode of each group
- For each group, the list of hosts requesting the source

Note

- When explicit tracking is enabled and the switch is working in proxy-reporting mode, the router may not be able to track all the hosts behind a VLAN interface.

Default Settings for IGMP Snooping

None.

How to Configure IGMP Snooping

Note To use IGMP snooping, configure a Layer 3 interface in the subnet for multicast routing (see Chapter 6, "IPv4 Multicast Layer 3 Features") or enable the IGMP snooping querier in the subnet (see the "Enabling the IGMP Snooping Querier" section on page 7-9).

Enabling the IGMP Snooping Querier

Use the IGMP snooping querier to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed. To enable the IGMP snooping querier in a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip igmp snooping querier`	Enables the IGMP snooping querier globally.
Step 2	`Router(config)# vlan configuration` *vlan_ID*	Selects a VLAN.
Step 3	`Router(config-vlan-config)# ip igmp snooping querier address` *ip_address*	Assigns the IP address.
Step 4	`Router(config-vlan-config)# ip igmp snooping querier`	Enables the IGMP snooping querier on the VLAN.
Step 5	`Router(config-vlan-config)# end`	Exits configuration mode.

This example shows how to enable the IGMP snooping querier on VLAN 200 and verify the configuration:

```
Router(config)# ip igmp snooping querier
Router(config)# vlan configuration 200
Router(config-vlan-config)# ip igmp snooping querier address 10.1.1.1
Router(config-vlan-config)# igmp snooping querier
Router(config-vlan-config)# end
```

Enabling IGMP Snooping

Enabling IGMP Snooping Globally

To enable IGMP snooping globally, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip igmp snooping`	Enables IGMP snooping.
Step 2	`Router(config)# end`	Exits configuration mode.

This example shows how to enable IGMP snooping globally and verify the configuration:

```
Router(config)# ip igmp snooping
Router(config)# end
Router# show ip igmp interface vlan 200 | include globally
```

```
  IGMP snooping is globally enabled
Router#
```

Enabling IGMP Snooping in a VLAN

To enable IGMP snooping in a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan configuration vlan_ID`	Selects a VLAN.
Step 2	`Router(config-vlan-config)# ip igmp snooping`	Enables IGMP snooping.
Step 3	`Router(config-vlan-config)# end`	Exits configuration mode.

This example shows how to enable IGMP snooping on VLAN 25 and verify the configuration:

```
Router# vlan configuration 25
Router(config-vlan-config)# ip igmp snooping
Router(config-vlan-config)# end
Router# show ip igmp snooping vlan 25
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State    : Enabled
IGMPv3 snooping             : Enabled
Report suppression          : Disabled
EHT DB limit/count          : 100000/2
TCN solicit query           : Disabled
Robustness variable         : 2
Last member query count     : 3
Last member query interval  : 1000
Check TTL=1                 : No
Check Router-Alert-Option   : No

Vlan 25:
--------
IGMP snooping Admin State    : Enabled
IGMP snooping Oper State     : Enabled
IGMPv2 immediate leave       : Disabled
Explicit host tracking       : Enabled
Report suppression           : Enabled
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
EHT DB limit/count           : 100000/2
Check TTL=1                  : Yes
Check Router-Alert-Option    : Yes
Query Interval               : 100
Max Response Time            : 10000
Router#
```

Configuring the IGMP Snooping Lookup Method

To configure the IGMP snooping lookup method for a VLAN, perform this task:

Command	Purpose
`Router(config-vlan-config)# multicast snooping lookup {ip | mac}`	Configures the IGMP snooping lookup method for the VLAN. • Enter the **ip** keyword to use IP addresses to forward multicast traffic. • Enter the **mac** keyword to use destination MAC addresses to forward multicast traffic.

Note Changing the lookup mode is disruptive. Multicast forwarding is not optimal until all multicast entries are programmed with the new lookup mode. Also, if 32 IP addresses are mapped to a single MAC address, forwarding on the device might be suboptimal.

Configuring a Static Connection to a Multicast Receiver

To configure a static connection to a multicast receiver, perform this task:

Command	Purpose
`Router(config)# mac address-table static` *mac_addr* `vlan` *vlan_id* `interface` *type slot/port* `[disable-snooping]`	Configures a static connection to a multicast receiver.

When you configure a static connection, enter the **disable-snooping** keyword to prevent multicast traffic addressed to the statically configured multicast MAC address from also being sent to other ports in the same VLAN.

This example shows how to configure a static connection to a multicast receiver:

```
Router(config)# mac address-table static 0050.3e8d.6400 vlan 12 interface gigabitethernet
5/7
```

The above static mac command can be used when the lookup type in the VLAN is MAC-base. Irrespective of lookup type, the following commands can be used to configure static connection to a multicast receiver for a group or a group and from a specific source.

```
Router(config)# vlan configuration 200
Router(config-vlan-config)# ip igmp snooping static 224.1.2.3 interface g3/11
Router(config-vlan-config)# ip igmp snooping static 224.1.2.3 source 20.1.1.1 interface Gi3/12
```

Configuring a Multicast Router Port Statically

To configure a static connection to a multicast router, perform this task:

	Command	Purpose
Step 1	`Router(config-vlan-config)# ip igmp snooping mrouter interface` *type slot/port*	Configures a static connection to a multicast router.
Step 2	`Router(config-vlan-config)# end`	Exits configuration mode.

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

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

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

Configuring the IGMP Snooping Query Interval

You can configure the interval for which the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group.

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

To configure the interval for the IGMP snooping queries sent by the switch, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan configuration` *vlan_ID*	Selects a VLAN.
Step 2	`Router(config-vlan-config)# ip igmp snooping last-member-query-interval` *interval*	Configures the interval for the IGMP snooping queries sent by the switch. Default is 1 second. Valid range is 100 to 999 milliseconds.

This example shows how to configure the IGMP snooping query interval:

```
Router(config-vlan-config)# ip igmp snooping last-member-query-interval 200
Router(config-vlan-config)# exit
Router# show ip igmp interface vlan 200 | include last
  IGMP snooping last member query interval on this interface is 200 ms
```

Enabling IGMP Snooping Immediate-Leave Processing

Fast-leave configuration applies to IGMP version 2 hosts only. To enable IGMP snooping fast-leave processing in a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan configuration vlan_ID`	Selects a VLAN.
Step 2	`Router(config-vlan-config)# ip igmp snooping`	Enables IGMP snooping. This step is only necessary if IGMP snooping is not already enabled on this VLAN.
Step 3	`Router(config-vlan-config)# ip igmp snooping immediate-leave`	Enables IGMP immediate-leave processing in the VLAN.

This example shows how to enable IGMP snooping immediate-leave processing for IGMP version 2 hosts on the VLAN 200 interface, and how to verify the configuration:

```
Router# interface vlan 200
Router(config-vlan-config)# ip igmp snooping
Router(config-vlan-config)# ip igmp snooping immediate-leave
Configuring immediate leave on vlan 200
Router(config-vlan-config)# end
Router# show ip igmp interface vlan 200 | include immediate-leave
IGMP snooping immediate-leave is enabled on this interface
```

Configuring IGMPv3 Snooping Explicit Host Tracking

To enable IGMPv3 snooping explicit host tracking on a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan configuration vlan_ID`	Selects a VLAN.
Step 2	`Router(config-vlan-config)# ip igmp snooping explicit-tracking limit limit`	Enable IGMPv3 snooping explicit host tracking in a VLAN.

This example shows how to enable IGMPv3 snooping explicit host tracking:

```
Router(config-vlan-config)# ip igmp snooping explicit-tracking limit 400
Router# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State    : Enabled
IGMPv3 snooping             : Enabled
Report suppression          : Disabled
EHT DB limit/count          : 100000/2
TCN solicit query           : Disabled
Robustness variable         : 2
Last member query count     : 3
Last member query interval  : 1000
Check TTL=1                 : No
Check Router-Alert-Option   : No

Vlan 200:
--------
IGMP snooping Admin State  : Enabled
IGMP snooping Oper State   : Enabled
```

```
IGMPv2 immediate leave     : Disabled
Explicit host tracking     : Enabled
Report suppression         : Enabled
Robustness variable        : 2
Last member query count    : 2
Last member query interval : 1000
EHT DB limit/count         : 100000/2
Check TTL=1                : Yes
Check Router-Alert-Option  : Yes
Query Interval             : 100
Max Response Time          : 10000
Router(config-vlan-config)# ip igmp snooping static 224.1.2.3 source 10.1.1.1 interface Gi3/11
Router# show ip igmp snooping groups vlan 200
Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
Vlan       Group/source            Type      Version        Port List
------------------------------------------------------------------------
200        224.1.2.3                         v3
             /10.1.1.1              S                        Gi3/11
Router#
```

Displaying IGMP Snooping Information

Displaying Multicast Router Interfaces

When you enable IGMP snooping, the switch automatically learns to which interface the multicast routers are connected. To display multicast router interfaces, perform this task:

Command	Purpose
`Router# show ip igmp snooping vlan vlan_ID`	Displays multicast router interfaces.

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State    : Enabled
IGMPv3 snooping             : Enabled
Report suppression          : Disabled
EHT DB limit/count          : 100000/2
TCN solicit query           : Disabled
Robustness variable         : 2
Last member query count     : 3
Last member query interval  : 1000
Check TTL=1                 : No
Check Router-Alert-Option   : No

Vlan 200:
--------
IGMP snooping Admin State   : Enabled
IGMP snooping Oper State    : Enabled
IGMPv2 immediate leave      : Disabled
Explicit host tracking      : Enabled
```

```
Report suppression         : Enabled
Robustness variable        : 2
Last member query count    : 2
Last member query interval : 1000
EHT DB limit/count         : 100000/2
Check TTL=1                : Yes
Check Router-Alert-Option  : Yes
Query Interval             : 100
Max Response Time          : 10000
Router#
```

Displaying MAC Address Multicast Entries

To display MAC address multicast entries for a VLAN, perform this task:

Command	Purpose
Router# **show mac address-table multicast** *vlan_ID* [**count**]	Displays MAC address multicast entries for a VLAN.

This example shows how to display MAC address multicast entries for VLAN 1:

```
Router# show mac address-table multicast vlan 1
vlan   mac address     type    qos             ports
-----+---------------+--------+---+--------------------------------
  1  0100.5e02.0203  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0127  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0128  static   --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0001  static   --  Gi1/1,Gi2/1,Gi3/48,Router,Switch
Router#
```

This example shows how to display a total count of MAC address entries for a VLAN:

```
Router# show mac address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#
```

Displaying IGMP Snooping Information for a VLAN Interface

To display IGMP snooping information for a VLAN interface, perform this task:

Command	Purpose
Router# **show ip igmp interface** *vlan_ID*	Displays IGMP snooping information on a VLAN interface.

This example shows how to display IGMP snooping information on the VLAN 200 interface:

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
  Internet address is 43.0.0.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
```

```
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity:1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 43.0.0.1 (this system)
  IGMP querying router is 43.0.0.1 (this system)
  Multicast groups joined by this system (number of users):
      224.0.1.40(1)
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping immediate-leave is disabled and querier is disabled
  IGMP snooping explicit-tracking is enabled on this interface
  IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum