Configuring IPv4 IGMP Filtering and Router Guard

This chapter describes how IGMP traffic filtering and Router Guard are used to control the access of a port to IGMP traffic. Release 12.2(33)SXH and later releases support IGMP traffic filtering and Router Guard.

Note For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

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

The following sections describe IGMP filtering and Router Guard features for multicast hosts (receivers):

Understanding IGMP Filtering

These sections describe IGMP filtering:

IGMP Filtering Overview

IGMP snooping is a protocol that learns and maintains multicast group membership at the Layer 2 level. IGMP snooping looks at IGMP traffic to decide which ports should be allowed to receive multicast traffic from certain sources and for certain groups. This information is used to forward multicast traffic to only interested ports. The main benefit of IGMP snooping is to reduce flooding of packets. For information about IGMP snooping, see "Understanding IGMP Filtering" section on page 40-1.

IGMP filtering allows users to configure filters on a switch virtual interface (SVI), a per-port, or a per-port per-VLAN basis to control the propagation of IGMP traffic through the network. By managing the IGMP traffic, IGMP filtering provides the capability to manage IGMP snooping, which in turn controls the forwarding of multicast traffic.

When an IGMP packet is received, IGMP filtering uses the filters configured by the user to determine whether the IGMP packet should be discarded or allowed to be processed by the existing IGMP snooping code. With a IGMP version 1 or version 2 packet, the entire packet is discarded. With a IGMPv3 packet, the packet is rewritten to remove message elements that were denied by the filters.

The IGMP filtering feature is SSO compliant.

IGMP traffic filters control the access of a port to multicast traffic. Access can be restricted based on the following:

- Which multicast groups or channels can be joined on a port. Channels are joined by IGMPv3 hosts that specify both the group and the source of the multicast traffic.
- Maximum number of groups or channels allowed on a specific port or interface (regardless of the number of hosts requesting service).
- IGMP protocol versions (for example, disallow all IGMPv1 messages).

When you enter an IGMP filtering command, a user policy is applied to a Layer 3 SVI interface, a Layer 2 port, or a particular VLAN on a Layer 2 trunk port. The Layer 2 port may be an access port or a trunk port. The IGMP filtering features will work only if IGMP snooping is enabled (either on the interface or globally).

IGMP filtering is typically used in access switches connected to end-user devices in Ethernet-to-home deployment scenarios.

Note 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. For information about IGMP, see Chapter 37, "Understanding IPv4 Multicast Layer 3 Switching."

IGMP Filters

There are three different types of IGMP filters: IGMP group and channel access control, several IGMP groups and channels limit, and an IGMP minimum version. These filters are configurable and operate differently on different types of ports:

- Per SVI
- Per port
- Per VLAN basis on a trunk port

In the case of trunk ports, filters may also be configured separately for each of the different VLANs passing through that trunk port.

The following sections describe each type of filter in more detail:

IGMP Group and Channel Access Control

Filtering on the IGMP group or channel allows the user to control which IGMP groups or channels can be joined on a port or on a per VLAN basis on a trunk port.

To configure filtering on the IGMP group or channel use the following CLI command:

ip igmp snooping access-group *acl* [**vlan** *vlan_id*]

To allow or deny several groups or channels, you must configure multiple access control entries in the access control list. Depending on whether the ACL is configured as permit or deny, the corresponding group or channel is allowed or denied. The ACL specified may be either a simple or extended ACL.

Filtering by IGMP group or channel is configurable on a Layer 3 SVI as a default filter for all ports in access mode under that SVI and for the corresponding VLAN on all trunk ports carrying that VLAN. This filter is also configurable on a Layer 2 port. If the port is in access mode, this filter will override any default SVI filter. If the port is in trunk mode, this filter will act as a default for all VLANs on that trunk and will override the SVI filter for each corresponding VLAN.

The **vlan** keyword can apply the filter only to IGMP packets arriving on the specified Layer 2 VLAN if the port is a trunk port. This per-VLAN filter (configured using the **vlan** keyword) will override any interface level filter and any SVI filter for the same VLAN.

Number of IGMP Groups and Channels Limit

Limiting the number of IGMP groups or channels allows you to control how many IGMP groups or channels can be joined on a port or on a per-VLAN basis on a trunk port.

To limit the number of IGMP groups or channels, use the following interface command CLI:

ip igmp snooping limit *n* [**except** *acl*] [**vlan** *vlan_id*]

A maximum of *n* groups or channels are allowed on the port or interface. The **except** keyword allows you to specify groups or channels that are exempt from the configured limit. The ACL used with the **except** keyword may be either a simple or extended ACL.

If joins are received for (*,G1) and (S1,G1) on the same interface, these are counted as two separate joins. If the limit on an interface has been set to 2, and joins are received for (*,G1) and (S1,G1), all other joins (for groups or channels different from these two) will then be discarded.

This filter is configurable on a Layer 3 SVI as a default filter for all ports in access mode under that SVI and for the corresponding VLAN on all trunk ports carrying that VLAN. This filter is also configurable on a Layer 2 port. If the Layer 2 port is in access mode, this filter will override any default SVI filter. If the Layer 2 switch port is in trunk mode, this filter will act as a default for all VLANs on that trunk and will override the SVI filter for each corresponding VLAN. The **vlan** keyword allows the user to apply the filter only to IGMP packets arriving on the specified Layer 2 VLAN if the Layer 2 switch port is a trunk port. This per-VLAN filter, configured using the **vlan** keyword, will override any interface level filter and any SVI filter for the same VLAN.

IGMP Minimum Version

Filtering on the IGMP protocol allows you to configure the minimum version of IGMP hosts allowed on the SVI. For example, you may want to disallow all IGMPv1 hosts (such as, allow a minimum IGMP version of 2) or all IGMPv1 and IGMPv2 hosts (such as, allow a minimum IGMP version of 3). This filtering applies only to membership reports.

To configure filtering on the IGMP protocol, use the following CLI command:

ip igmp snooping minimum-version 2 | 3

This filter is only configurable on a Layer 3 SVI as a default filter for all ports in access mode under that SVI and for the corresponding VLAN on all trunk ports.

IGMP Filter Precedence

These sections describe the hierarchy of the different filters on various ports.

Access Mode

In access mode, filters can be configured on both the port and the SVI. When an IGMP packet is received on a port in access mode, the port filter is checked first. If the port filter exists, it is applied and the SVI filter is ignored. If no per-port filter exists, the SVI filter is used.

This hierarchy is applied separately for each type of filter. For example, a limit filter configured on the port overrides the default limit filter on the SVI, but has no affect on any of the other filters.

Trunk Mode

With ports in trunk mode, a filter can be configured for an SVI corresponding to one of the VLANs on the trunk port, another filter configured on the trunk port itself, and a third filter configured on one of the Layer 2 VLANs passing through the trunk. When an IGMP packet is received, the trunk-per-VLAN specific filter will be checked first. If this filter exists, it is applied. The main trunk port filter and SVI filter will be ignored. If no trunk-per-VLAN filter exists, the main trunk port filter will be used. If neither of these filters exist, the SVI filter for the VLAN will be used as a final default for ports in trunk mode.

Filter Hierarchy Example

This example shows the filter hierarchy. The following configuration of SVI VLAN 100 contains three access ports g1/1, g1/2, and g1/3:

VLAN 100:

```
Switch(config-if)# ip igmp snooping limit 20
```

Port g1/1:

```
Switch(config-if)# ip igmp snooping limit 35
```

Port g1/2:

```
Switch(config-if)# no limit filter
```

Port g1/3:

```
Switch(config-if)# no limit filter
```

In this example, the limit value for g1/1 is 35, the limit value for g1/2 is 20, and the limit value for g1/3 is also 20.

Displaying IGMP Filtering

The following sections describe how to display IGMP filtering:

- Displaying IGMP Filtering Configuration, page 40-5
- Displaying IGMP Filtering Statistics, page 40-6

Displaying IGMP Filtering Configuration

To display IGMP filtering rules, perform this task:

Command	Purpose
`Switch(config-if)# show ip igmp snooping filter interface` *interface-name* `[details]`	Displays the filters configured for the specified interface.

This example shows how to display the default filters configured on the SVI:

```
Router# show ip igmp snooping filter interface vlan 20
Access-Group: Channel1-Acl
Groups/Channels Limit:100 (Exception List: Channel6-Acl)
IGMP Minimum-Version:Not Configured
```

This example shows how to display the filters configured for all ports in access mode under this SVI and for all trunk ports carrying the corresponding VLAN:

```
Router# show ip igmp snooping filter interface g3/48
  Access-Group: Channel4-Acl
  Groups/Channels Limit:10 (Exception List: Channel3-Acl)
```

This example shows how to display the filters configured for all ports in access mode under this SVI:

```
Router# show ip igmp snooping filter interface vlan 20 detail
GigabitEthernet3/47 :
  Access-Group: Not Configured
  Groups/Channels Limit: Not Configured
GigabitEthernet3/48      :
  Access-Group: Channel4-ACL
  Groups/Channels Limit: 10     (Exception-list: Channel3-Acl)
```

This example shows how to display the default trunk port filters:

```
Router# show ip igmp snooping filter interface g3/46
  Access-Group: Channel1-Acl
  Groups/Channels Limit: 10 (Exception List: Channel3-Acl)
```

This example shows how to display the per-VLAN filters for all VLANs on this trunk:

```
Router# show ip igmp snooping filter interface g3/46 detail
Vlan 10  :
```

```
  Access-Group: Not Configured
  Groups/Channels Limit: Not Configured
Vlan 20  :
  Access-Group: Not Configured
        Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
```

This example shows how to display the per-VLAN filters for a specific VLAN on this trunk:

```
Router# show ip igmp snooping filter interface g3/46 vlan 20
  Access-Group: Not Configured
  Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
```

Note If the port is in the shutdown state, filter status will not be displayed because it cannot be determined whether the port is in trunk mode or access mode. In this situation, you can use the **show running-config interface** *xxxx* command to view the configuration.

Displaying IGMP Filtering Statistics

Statistics are maintained on an interface basis for ports in access mode and on a per-VLAN basis for ports in trunk mode.

To display IGMP filtering statistics, perform this task:

Command	Purpose
`Switch(config-if)# show ip igmp snooping filter interface` *interface-name* [**statistics**]	Displays the filtering statistic collected for the specified interface.

This example shows how to display statistics for each port in access mode under the SVI:

```
Router# show ip igmp snooping filter interface vlan 20 statistics
GigabitEthernet3/47       :
  IGMP Filters are not configured

GigabitEthernet3/48       :
  Access-group denied : 0
  Limit denied : 2
  Limit status : 0 active out of 2 max
  Minimum-version denied : 0
```

This example shows how to display statistics for a specific port in access mode:

```
Router# show ip igmp snooping filter interface g3/48 statistics
  Access-group denied : 0
  Limit denied : 2
  Limit status : 0 active out of 2 max
  Minimum-version denied : 0
```

This example shows how to display statistics for Gigabit Ethernet port 3/47 in access mode with no default SVI filter and no port filter:

```
Router# show ip igmp snooping filter interface g3/47 statistics
IGMP Filters are not configured
```

This example shows how to display statistics for all VLANs under a trunk:

```
Router# show ip igmp snooping filter interface g3/46 statistics
```

```
Vlan 10   :
IGMP Filters are not configured

Vlan 20   :
  Access-group denied : 0
  Limit denied : 0
  Minimum-version denied : 0
```

This example shows how to display statistics for a specific VLAN under a trunk:

```
Router# show ip igmp snooping filter interface g3/46 vlan 20 statistics
  Access-group denied : 0
  Limit denied : 0
  Minimum-version denied : 0
```

This example shows how to display statistics for a specific VLAN under a trunk port with no trunk and no VLAN filter:

```
Router# show ip igmp snooping filter interface g3/46 vlan 10 statistics
IGMP Filters are not configured
```

Note If the port is in the shutdown state, filter statistics will not be displayed because it cannot be determined whether the port is in trunk mode or access mode.

Clearing IGMP Filtering Statistics

To clear IGMP filtering statistics, perform one of these tasks:

Command	Purpose
`Router# clear ip igmp snooping filter statistics`	Clears IGMP filtering statistics for all access ports and for all VLANs on all trunk ports.
`Router# clear ip igmp snooping filter statistics interface` *interface_name*	Clears statistics for one particular access port or for all VLANs on one particular trunk port.
`Router# clear ip igmp snooping filter statistics interface` *interface_name* `vlan` *vlan_ID*	Clears statistics for one particular VLAN on a trunk port.

Understanding Router Guard

These sections describe Router Guard:

Router Guard Overview

The Router Guard feature allows you to designate a specified port only as a multicast host port and not as a multicast router port. Multicast router control packets received on this port are dropped.

Any port can become a multicast router port if the switch receives one of the multicast router control packets, such as IGMP general query, PIM hello, or CGMP hello. When a port becomes a multicast router port, all multicast traffic (both known and unknown source traffic) is sent to all multicast router ports. This cannot be prevented without Router Guard.

When configured, the Router Guard feature makes the specified port a host port only. The port is prevented from becoming a router port, even if a multicast router control packets are received.

In addition, any control packets normally received from multicast routers, such as IGMP queries and PIM joins, will also be discarded by this filter.

A Router Guard command applies a user policy to a Layer 3 SVI interface, a Layer 2 port, or a particular VLAN on a Layer 2 trunk port. The Layer 2 port may be an access port or a trunk port.

The Router Guard feature does not require IGMP snooping to be enabled.

Router Guard is implemented only for IPv4.

Router Guard is typically used in access switches connected to end-user boxes in Ethernet-to-home deployment scenarios.

The IPv4 multicast Router Guard feature is SSO-compliant.

The following packet types are discarded if they are received on a port that has Router Guard enabled:

- IGMP query messages
- IPv4 PIMv2 messages
- IGMP PIM messages (PIMv1)
- IGMP DVMRP messages
- RGMP messages
- CGMP messages

When these packets are discarded, statistics are updated indicating that packets are being dropped due to Router Guard.

Configuring Router Guard

The Router Guard feature can be configured globally and per-interface. Typically, the global configuration initiates Router Guard for all Layer 2 ports in the system. The per-interface configuration can then be used to override Router Guard for specific ports, for example, the ports where multicast routers are actually connected.

The following sections describe each type of configuration:

- Enabling Router Guard Globally, page 40-9
- Clearing Router Guard Statistics, page 40-9
- Disabling Router Guard on Ports, page 40-9

Enabling Router Guard Globally

To enable Router Guard globally, perform this task:

Command	Purpose
`Router# router-guard ip multicast switchports`	Enables Router Guard globally.

Clearing Router Guard Statistics

To clear Router Guard statistics, perform this task:

	Command	Purpose
Step 1	`Router# clear ip igmp snooping filter statistics interface interface_name`	Clears statistics for one particular access port or for all VLANs on one particular trunk port.
Step 2	`Router# clear ip igmp snooping filter statistics interface interface_name vlan vlan_id`	Clears statistics for one particular VLAN on a trunk port.

Disabling Router Guard on Ports

To disable Router Guard on a Layer 2 port to which a multicast router is connected, perform this task:

Command	Purpose
`Router(config-if)# no router-guard ip multicast [vlan vlan_id]`	Disables Router Guard on a Layer 2 port. **Note** The **vlan** keyword is effective only if the port is in trunk mode. You can use this keyword to override Router Guard only for specific VLANs on the trunk port.

This example shows how to allow multicast router messages on trunk port Gigabit Ethernet 3/46, VLAN 20:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/46
Router(config-if)# no router-guard ip multicast vlan 20
```

Displaying Router Guard Configurations

To display the global Router Guard configuration and the Router Guard configuration for a specific interface, perform these tasks:

Command	Purpose
`Router# show router-guard`	Displays the global Router Guard configuration.
`Router# show router-guard interface interface_name`	Displays the Router Guard configuration for a specific interface.

This example shows how to display the interface command output for a port in access mode with Router Guard not active:

```
Router# show router-guard interface g3/48
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Enabled on this interface
Packets denied:
  IGMP Queries:
  PIMv2 Messages:
  PIMv1 Messages:
  DVMRP Messages:
  RGMP Messages:
  CGMP Messages:
```

This example shows how to display the interface command output for a port in trunk mode:

```
Router# show router-guard interface g3/48
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Disabled on this interface
```

This example shows how to verify that a trunk port is carrying VLANs 10 and 20:

```
Router# show router-guard interface g3/46
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Default: Enabled for all VLANs on this interface
VLAN 10:
Enabled on this VLAN
Packets denied:
  IGMP Queries:
  PIMv2 Messages:
  PIMv1 Messages:
  DVMRP Messages:
  RGMP Messages:
  CGMP Messages:
VLAN 20 :
Disabled on this VLAN
```

Note If the port is in the shutdown state, the status will not be displayed because it cannot be determined whether the port is in trunk mode or access mode. You can use the **show running-config interface** *xxxx* command to display the Router Guard configuration.

Displaying Router Guard Interfaces

To display a list of all interfaces for which Router Guard is disabled, perform this task:

Command	Purpose

`Router# show router-guard interface`
`Router Guard for IP Multicast:`
`Globally enabled for all switchports`
 	
`Interfaces:`
`Gi3/46: Disabled on this port for VLANS: ALL`
	Displays a list of all interfaces for which Router Guard is disabled.

Clearing Router Guard Statistics

To clear Router Guard statistics, perform one of these tasks:

Command	Purpose
`Router(config)# clear router-guard ip multicast statistics`	Clears statistics for all access ports and for all VLANs on all trunk ports.
`Router(config)# clear router-guard ip multicast statistics interface interface_name`	Clears statistics for an access port and for all VLANs on a trunk port.
`Router(config)# clear router-guard ip multicast statistics interface interface_name vlan v`	Clears statistics for one particular VLAN on a trunk port.

This example shows how to clear statistics for one particular VLAN on a trunk port:

```
Router# clear router-guard ip multicast statistics interface interface_name vlan v
```

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