

# 11

## IPv4 Router Guard

---

- [Prerequisites for Router Guard, page 11-1](#)
- [Restrictions for Router Guard, page 11-1](#)
- [Information About Router Guard, page 11-1](#)
- [Default Settings for Router Guard, page 11-2](#)
- [How to Configure Router Guard, page 11-2](#)

**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](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.
- 

**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](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 Router Guard

None.

## Restrictions for Router Guard

None.

## Information About Router Guard

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.

Router Guard can be configured globally and per-interface. The global configuration initiates Router Guard for all Layer 2 ports, which can be modified with the interface configuration commands, for example, on ports where multicast routers are connected.

## Default Settings for Router Guard

None.

## How to Configure Router Guard

- [Enabling Router Guard Globally, page 11-3](#)
- [Disabling Router Guard on Ports, page 11-3](#)
- [Clearing Router Guard Statistics, page 11-3](#)
- [Displaying Router Guard Configuration, page 11-4](#)
- [Displaying Router Guard Interfaces, page 11-5](#)

## Enabling Router Guard Globally

To enable Router Guard globally, perform this task:

Command	Purpose
Router# <b>router-guard ip multicast switchports</b>	Enables Router Guard globally.

## 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)# <b>no router-guard ip multicast</b> [ <b>vlan</b> <i>vlan_id</i> ]	Disables Router Guard on a Layer 2 port.  <b>Note</b> The <b>vlan</b> 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
```

## Clearing Router Guard Statistics

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

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

# Verifying the Router Guard Configuration

- [Displaying Router Guard Configuration, page 11-4](#)
- [Displaying Router Guard Interfaces, page 11-5](#)

## Displaying Router Guard Configuration

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

Command	Purpose
Router# <b>show router-guard</b>	Displays the global Router Guard configuration.
Router# <b>show router-guard interface</b> <i>interface_name</i>	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 xxxxx** 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
<pre>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</pre>	Displays a list of all interfaces for which Router Guard is disabled.

**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](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

[Participate in the Technical Documentation Ideas forum](#)

