



CHAPTER 47

Configuring IP Source Guard

This chapter describes how to configure IP Source Guard. Cisco IOS Release 12.2(33)SXH and later releases support IP Source Guard.



Note

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, Release 12.2SX, at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_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

This chapter consists of these sections:

- [Overview of IP Source Guard, page 47-1](#)
- [Configuring IP Source Guard on the Switch, page 47-3](#)
- [Displaying IP Source Guard Information, page 47-4](#)
- [Displaying IP Source Binding Information, page 47-6](#)

Overview of IP Source Guard

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports.

Initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address. IP Source Guard is a port-based feature that automatically creates an implicit port access control list (PACL).

IP Source Guard Interaction with VLAN-Based Features

Use the **access-group mode** command to specify how IP Source Guard interacts with VLAN-based features (such as VACL and Cisco IOS ACL and RACL).

In prefer port mode, if IP Source Guard is configured on an interface, IP Source Guard overrides other VLAN-based features. If IP Source Guard is not configured on the interface, other VLAN-based features are merged in the ingress direction and applied on the interface.

In merge mode, IP Source Guard and VLAN-based features are merged in the ingress direction and applied on the interface. This is the default access-group mode.

Channel Ports

IP Source Guard is supported on the main Layer 2 channel interface but not on the port members. When IP Source Guard is applied on the main Layer 2 channel interface, it is applied to all the member ports in the channel.

Trunk Ports

IP Source Guard is not supported on trunk ports.

Layer 2 and Layer 3 Port Conversion

When an IP Source Guard policy is applied to a Layer 2 port, and then you change that port to be a Layer 3 port, the IP Source Guard policy no longer functions but is still present in the configuration. When the port is changed back to a Layer 2 port, IP Source Guard policy becomes effective again.

IP Source Guard and Voice VLAN

IP Source Guard is supported on a Layer 2 port that belongs to a voice VLAN. To configure the voice VLAN for the Layer 2 port, use the **switchport voice vlan** command. For IP Source Guard to be active on the voice VLAN, DHCP snooping must be enabled on the voice VLAN. In merge mode, the IP Source Guard feature is merged with VACL and Cisco IOS ACL configured on the access VLAN.

IP Source Guard and Web-Based Authentication

In releases earlier than Cisco IOS Release 12.2(33)SX12, configuring IP Source Guard and web-based authentication on the same interface is not supported.

In Cisco IOS Release 12.2(33)SX12 and later releases, you can configure IP Source Guard and web-based authentication on the same interface. If DHCP snooping is also enabled on the access VLAN, you must enter the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode to avoid conflicts between the two features. Other VLAN-based features are not supported when IP Source Guard and web-based authentication are combined.

IP Source Guard Restrictions

Because the IP Source Guard feature is supported only in hardware, IP Source Guard is not applied if there are insufficient hardware resources available. These hardware resources are shared by various other ACL features that are configured on the system. The following restrictions apply to IP Source Guard:

- Only supported on ingress Layer 2 ports.
- Only supported in hardware.
- Not applied to any traffic that is processed in software.
- Does not support filtering of traffic based on MAC address.
- Is not supported on private VLANs.

Configuring IP Source Guard on the Switch

To enable IP Source Guard, perform this task:

	Command	Purpose
Step 1	Router(config)# ip dhcp snooping	Enables DHCP snooping globally. You can use the no keyword to disable DHCP snooping.
Step 2	Router(config)# ip dhcp snooping vlan <i>number</i> [<i>number</i>]	Enables DHCP snooping on your VLANs.
Step 3	Router(config)# interface <i>interface-name</i>	Selects the interface to be configured.
Step 4	Router(config-if)# no ip dhcp snooping trust	Use the no keyword to configure the interface as untrusted.
Step 5	Router(config-if)# ip verify source vlan dhcp-snooping [port-security]	Enables IP Source Guard, source IP address filtering on the port. The following are the command parameters: <ul style="list-style-type: none"> • vlan applies the feature to only specific VLANs on the interface. The dhcp-snooping option applies the feature to all VLANs on the interface that have DHCP snooping enabled. • port-security enables MAC address filtering. This feature is currently not supported.
Step 6	Router(config-if)# exit	Returns to global configuration mode.
Step 7	Router(config)# ip source binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ip-address</i> interface <i>interface-name</i>	(Optional) Configures a static IP binding on the port.
Step 8	Router(config)# end	Exits configuration mode.
Step 9	Router# show ip verify source [interface <i>interface-name</i>]	Verifies the configuration.

**Note**

The static IP source binding can only be configured on a Layer 2 port. If you enter the **ip source binding vlan interface** command on a Layer 3 port, you receive this error message:

Static IP source binding can only be configured on switch port.

The **no** keyword deletes the corresponding IP source binding entry. This command requires an exact match of all the required parameters in order for the deletion to be successful.

This example shows how to enable per-Layer 2 port IP Source Guard on VLANs 10 through 20:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# ip dhcp snooping vlan 10 20
Router(config)# interface fa6/1
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 10
Router(config-if)# no ip dhcp snooping trust
Router(config-if)# ip verify source vlan dhcp-snooping
Router(config-if)# end
Router# show ip verify source interface f6/1
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----
Fa6/1     ip           active      10.0.0.1   -----
Fa6/1     ip           active      deny-all  11-20
Router#
```

The output shows that there is one valid DHCP binding to VLAN 10.

This example shows how to configure an interface to use prefer port mode:

```
Router# configure terminal
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# access-group mode prefer port
```

This example shows how to configure an interface to use merge mode:

```
Router# configure terminal
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# access-group mode merge
```

Displaying IP Source Guard Information

To display IP Source Guard PACL information for all interfaces on a switch, perform this task:

Command	Purpose
Router# show ip verify source [<i>interface interface-name</i>]	Displays IP Source Guard PACL information for all interfaces on a switch or for a specified interface.

This example shows that DHCP snooping is enabled on VLAN 10 through 20, interface fa6/1 is configured for IP filtering, and there is an existing IP address binding 10.0.01 on VLAN 10:

```
Router# show ip verify source interface fa6/1
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----
fa6/1     ip           active      10.0.0.1   -----
10
```

```
fa6/1      ip          active      deny-all      11-20
```

**Note**

The second entry shows that a default PACL (deny all IP traffic) is installed on the port for those snooping-enabled VLANs that do not have a valid IP source binding.

This example shows the displayed PACL information for a trusted port:

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
fa6/2      ip           inactive-trust-port
```

This example shows the displayed PACL information for a port in a VLAN not configured for DHCP snooping:

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
fa6/3      ip           inactive-no-snooping-vlan
```

This example shows the displayed PACL information for a port with multiple bindings configured for an IP/MAC filtering:

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
fa6/4      ip           active       10.0.0.2        aaaa.bbbb.cccc  10
fa6/4      ip           active       11.0.0.1        aaaa.bbbb.cccd  11
fa6/4      ip           active       deny-all        deny-all        12-20
```

This example shows the displayed PACL information for a port configured for IP/MAC filtering but not for port security:

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
fa6/5      ip           active       10.0.0.3        permit-all      10
fa6/5      ip           active       deny-all        permit-all      11-20
```

**Note**

The MAC address filter shows permit-all because port security is not enabled, so the MAC filter cannot apply to the port/VLAN and is effectively disabled. Always enable port security first.

This example shows an error message when you enter the **show ip verify source** command on a port that does not have an IP source filter mode configured:

```
Router# show ip verify source interface fa6/6
IP Source Guard is not configured on the interface fa6/6.
```

This example shows how to display all interfaces on the switch that have IP Source Guard enabled:

```
Router# show ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
fa6/1      ip           active       10.0.0.1        11-20            10
fa6/1      ip           active       deny-all        11-20            11-20
fa6/2      ip           inactive-trust-port
fa6/3      ip           inactive-no-snooping-vlan
fa6/4      ip           active       10.0.0.2        aaaa.bbbb.cccc  10
fa6/4      ip           active       11.0.0.1        aaaa.bbbb.cccd  11
fa6/4      ip           active       deny-all        deny-all        12-20
fa6/5      ip           active       10.0.0.3        permit-all      10
fa6/5      ip           active       deny-all        permit-all      11-20
```

Displaying IP Source Binding Information

To display all IP source bindings configured on all interfaces on a switch, perform this task:

Command	Purpose
<pre>Router# show ip source binding [ip-address] [mac-address] [dhcp-snooping static] [vlan vlan-id] [interface interface-name]</pre>	<p>Displays IP source bindings using the optional specified display filters.</p> <p>The dhcp-snooping filter displays all VLANs on the interface that have DHCP snooping enabled.</p>

This example shows how to display all IP source bindings configured on all interfaces on the switch.

```
Router# show ip source binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:02:B3:3F:3B:99  55.5.5.2      6522       dhcp-snooping  10    FastEthernet6/10
00:00:00:0A:00:0B  11.0.0.1      infinite    static         10    FastEthernet6/10
Router#
```

Table 47-1 describes the fields in the **show ip source binding** command output.

Table 47-1 *show ip source binding Command Output*

Field	Description
MAC Address	Client hardware MAC address
IP Address	Client IP address assigned from the DHCP server
Lease (seconds)	IP address lease time
Type	Binding type; static bindings configured from CLI to dynamic binding learned from DHCP snooping
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host



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