Configuring IP Source Guard

This chapter describes how to configure IP Source Guard on Cisco NX-OS devices.

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter includes the following sections:

Information About IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table.
- Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent spoofing attacks, in which an attacker uses the IP address of a valid host to gain unauthorized network access. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

You can enable IP Source Guard on Layer 2 interfaces that are not trusted by DHCP snooping. IP Source Guard supports interfaces that are configured to operate in access mode and trunk mode. When you initially enable IP Source Guard, all inbound IP traffic on the interface is blocked except for the following:

- DHCP packets, which DHCP snooping inspects and then forwards or drops, depending upon the results of inspecting the packet.
- IP traffic from static IP source entries that you have configured in the Cisco NX-OS device.

The device permits the IP traffic when DHCP snooping adds a binding table entry for the IP address and MAC address of an IP packet or when you have configured a static IP source entry.

The device drops IP packets when the IP address and MAC address of the packet do not have a binding table entry or a static IP source entry. For example, assume that the binding table contains the following entry:

```
MacAddress          IpAddress    LeaseSec   Type        VLAN      Interface
----------          ----------   ---------  ------      -------    ---------
00:02:B3:3F:3B:99  10.5.5.2       6943    dhcp-snooping  10      Ethernet2/3
```

If the device receives an IP packet with an IP address of 10.5.5.2, IP Source Guard forwards the packet only if the MAC address of the packet is 00:02:B3:3F:3B:99.

Licensing Requirements for IP Source Guard

This table shows the licensing requirements for IP Source Guard.

Product	License Requirement
Cisco DCNM	IP Source Guard requires a LAN Enterprise license. For an explanation of the Cisco DCNM licensing scheme and how to obtain and apply licenses, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
Cisco NX-OS	IP Source Guard requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites for IP Source Guard

The following prerequisites are required for using this feature on Cisco DCNM. For a full list of feature-specific prerequisites, see the platform-specific documentation.

- System-message logging levels for the IP Source Guard feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the .

Platform Support for IP Source Guard

The following platform supports this feature. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 3000 Series Switches	Cisco Nexus 3000 Series Switches Documentation
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 Series Switches Documentation

Configuring IP Source Guard

Enabling or Disabling IP Source Guard on a Layer 2 Interface

You can enable or disable IP Source Guard on a Layer 2 interface. By default, IP Source Guard is disabled on all interfaces.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ IP Source Guard**.
The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device whose interface you want to configure with IP Source Guard.
Slots on the selected device appear in the Summary pane.

Step 3 Double-click the slot whose interface you want to configure with IP Source Guard.
The Layer 2 interfaces on the selected slot appear in the Summary pane.

Step 4 Click the interface that you want to configure with IP Source Guard.
The Interface Configuration tab appears in the Details pane.

Step 5 From the Interface Configuration tab, do one of the following:

- To enable IP Source Guard on the interface, check **IP Source Guard**.
- To disable IP Source Guard on the interface, uncheck **IP Source Guard**.

Step 6 (Optional) From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

Related Topics

- Adding or Removing a Static IP Source Entry, page 4

Adding or Removing a Static IP Source Entry

You can add or remove a static IP source entry on a device. By default, there are no static IP source entries on a device.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ IP Source Guard**.
The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device that you want to configure with static source entries.
The Summary pane displays the Static Binding tab, which contains a table of static IP source entries, if any exist on the device.

Step 3 Click the **Static Binding** tab.

Step 4 To add a static IP source entry, follow these steps:

a) From the menu bar, choose **Actions ➤ Add Source Binding**.
A new row appears.

b) From the drop-down list, choose the VLAN that the binding is associated with.

c) Double-click the MAC Address field and enter the MAC address. Valid entries are in dotted hexadecimal format.

d) Double-click the IP Address field and enter the IPv4 address. Valid entries are in dotted decimal format.

Step 5 To delete a static IP source entry, follow these steps:

a) Click the entry that you want to delete.

b) From the menu bar, choose **Actions ➤ Delete Source Binding**.
A confirmation dialog box appears.

c) Click **Yes**.

Step 6 (Optional) From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

Related Topics

- Enabling or Disabling IP Source Guard on a Layer 2 Interface, page 3
- Displaying IP Source Guard Bindings, page 4

Displaying IP Source Guard Bindings

You can display static IP-MAC address bindings for a managed device.

Procedure

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > IP Source Guard**.

Step 2 The available devices appear in the Summary pane.

Step 3 From the Summary pane, click the device whose static IP-MAC address bindings you want to display.

Field Descriptions for IP Source Guard

Device: Static Binding Tab

Table 1: Device: Static Binding Tab

Figure	Description
VLAN	*Display only.* VLAN ID associated with the static DHCP binding.
MAC Address	*Display only.* MAC address of the static DHCP binding.
IP Address	*Display only.* IP address of the static DHCP binding.
Lease Expiry Time	*Display only.* Date and time when the DHCP IP address lease expires.

Interface: Interface Configuration Tab

Table 2: Device: Interface Configuration Tab

Figure	Description
Interface	*Display only.* Name of the Layer 2 interface.
Number of Static Bindings	*Display only.* Number of static DHCP bindings for the interface. By default, there are no static DHCP bindings.
IP Source Guard	Whether the IP Source Guard feature is enabled for the interface. By default, this check box is unchecked.

Additional References for IP Source Guard

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IP Source Guard

This table lists the release history for this feature.

Table 3: Feature History for IP Source Guard

Feature Name	Releases	Feature Information
IP Source Guard	5.2(1)	Added support for the Cisco Nexus 3000 Series Switches.
IP Source Guard	5.1(1)	No change from Release 5.0.
IP Source Guard	5.0(2)	No change from Release 4.2.
IP Source Guard	4.2(1)	No change from Release 4.1.