



CHAPTER 13

Configuring IP Source Guard

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

This chapter includes the following sections:

- [Information About IP Source Guard, page 13-1](#)
- [Licensing Requirements for IP Source Guard, page 13-2](#)
- [Prerequisites for IP Source Guard, page 13-2](#)
- [Guidelines and Limitations, page 13-2](#)
- [Configuring IP Source Guard, page 13-3](#)
- [Displaying IP Source Guard Bindings, page 13-5](#)
- [Field Descriptions for IP Source Guard, page 13-5](#)
- [Additional References, page 13-6](#)

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 attacks that rely on 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 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.

Send document comments to nexus7k-docfeedback@cisco.com.

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 forward the packet only if the MAC address of the packet is 00:02:B3:3F:3B:99.

Virtualization Support

The following information applies to IP Source Guard used in Virtual Device Contexts (VDCs):

- IP-MAC address bindings are unique per VDC. Bindings in one VDC do not affect IP Source Guard in other VDCs.
- NX-OS does not limit binding database size on a per-VDC basis.

Licensing Requirements for IP Source Guard

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	IP Source Guard requires a LAN Enterprise license. For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the <i>Cisco DCNM Licensing Guide</i> .
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 a complete explanation of the NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

Prerequisites for IP Source Guard

IP Source Guard has the following prerequisites:

- You should be familiar with DHCP snooping before you configure IP Source Guard.
- DHCP snooping is enabled (see the [“Configuring DHCP Snooping”](#) section on page 11-7).

Guidelines and Limitations

IP Source Guard has the following configuration guidelines and limitations:

- IP Source Guard limits IP traffic on an interface to only those sources that have an IP-MAC address binding table entry or static IP source entry. When you first enable IP Source Guard on an interface, you may experience disruption in IP traffic until the hosts on the interface receive a new IP address from a DHCP server.
- IP Source Guard is dependent upon DHCP snooping to build and maintain the IP-MAC address binding table or upon manual maintenance of static IP source entries.

Send document comments to nexus7k-docfeedback@cisco.com.

- For each device that you use DCNM to configure IP Source Guard, ensure that you configure the logging level for DHCP snooping to 6 (Informational) or a higher level. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

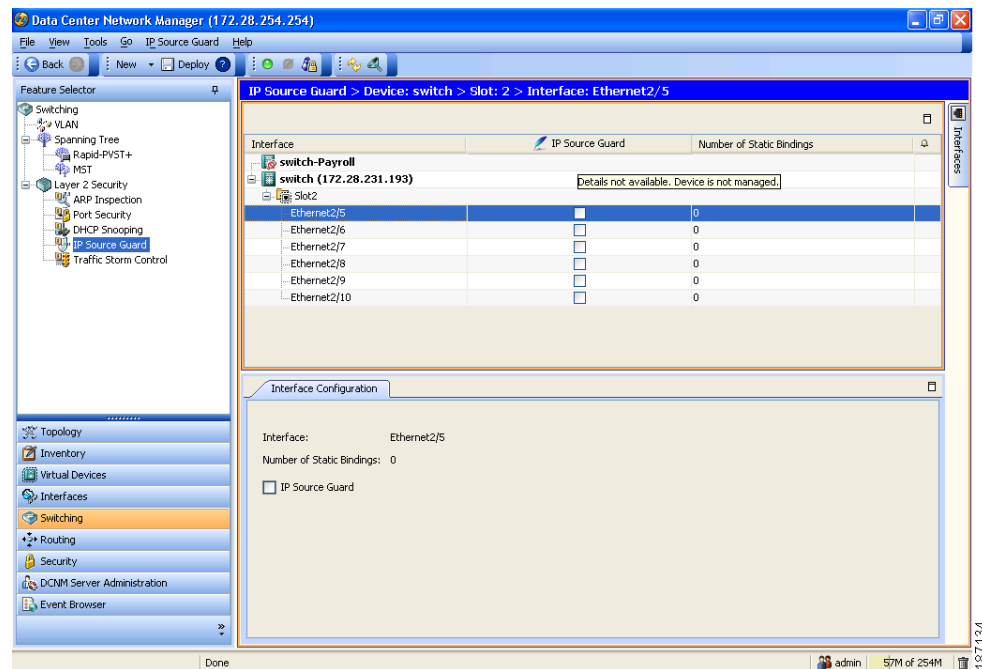
```
switch(config)# logging level dhcp 6
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

For more information about NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0*.

Configuring IP Source Guard

Figure 13-1 shows the IP Source Guard content pane.

Figure 13-1 IP Source Guard Content Pane



This section includes the following topics:

- [Enabling or Disabling IP Source Guard on a Layer 2 Interface, page 13-3](#)
- [Adding or Removing a Static IP Source Entry, page 13-4](#)

Enabling or Disabling IP Source Guard on a Layer 2 Interface

You can enable or disable IP Source Guard on a Layer 2 interface.

Send document comments to nexus7k-docfeedback@cisco.com.

BEFORE YOU BEGIN

By default, IP Source Guard is disabled on all interfaces.

Ensure that DHCP snooping is enabled. For more information, see the “[Enabling or Disabling the DHCP Snooping Feature](#)” section on page 11-8.

If you are enabling IP Source Guard, ensure that on the NX-OS device you configure the logging level for DHCP snooping to 6 (Informational) or a higher level. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

```
switch(config)# logging level dhcp 6
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

For more information about NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0*.

DETAILED STEPS

To enable or disable IP Source Guard on a Layer 2 interface, follow these steps:

-
- 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** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Adding or Removing a Static IP Source Entry

You can add or remove a static IP source entry on a device.

BEFORE YOU BEGIN

By default, there are no static IP source entries on a device.

DETAILED STEPS

To add or remove a static IP source entry, follow these steps:

Send document comments to nexus7k-docfeedback@cisco.com.

-
- 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:
- From the menu bar, choose **IP Source Guard > Adding Source Binding**.
 - A new row appears.
 - From the drop-down list, choose the VLAN that the binding is associated with.
 - Double-click the MAC Address field and enter the MAC address. Valid entries are in dotted hexadecimal format.
 - 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:
- Click the entry that you want to delete.
 - From the menu bar, choose **IP Source Guard > Delete Source Binding**.
A confirmation dialog box appears.
 - Click **Yes**.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Displaying IP Source Guard Bindings

To display static IP-MAC address bindings for a device, follow these steps:

-
- 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 whose static IP-MAC address bindings you want to display.
The Summary pane displays the Static Binding tab, which lists IP-MAC address bindings per VLAN.
-

Field Descriptions for IP Source Guard

This section includes the following topics:

- [Device: Static Binding Tab, page 13-6](#)
- [Interface: Interface Configuration Tab, page 13-6](#)

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

Device: Static Binding Tab

Table 13-1 Device: Static Binding Tab

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

Interface: Interface Configuration Tab

Table 13-2 Device: Interface Configuration Tab

Figure	Description
Interface	<i>Display only.</i> Name of the Layer 2 interface.
Number of Static Bindings	<i>Display only.</i> 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 additional information related to implementing IP Source Guard, see the following sections:

- [Related Documents, page 13-6](#)
- [Standards, page 13-6](#)

Related Documents

Related Topic	Document Title
Information About DHCP Snooping, page 11-1	<i>Cisco DCNM Security Configuration Guide, Release 4.0</i>

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.	—

Send document comments to nexus7k-docfeedback@cisco.com.

Send document comments to nexus7k-docfeedback@cisco.com.

Send document comments to nexus7k-docfeedback@cisco.com.

Send document comments to nexus7k-docfeedback@cisco.com.