

Configuring IP Source Guard

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

This chapter includes the following sections:

- IP source guard overview, on page 1
- Prerequisites for IP source guard, on page 2
- Recommendation for IP source guard configuration, on page 2
- Default settings for IP source guard, on page 3
- Configuring IP source guard, on page 3
- Displaying IP source guard bindings, on page 6
- Clearing IP source guard statistics, on page 6
- IP source guard configuration example, on page 6
- Additional references, on page 7

IP source guard overview

IP Source Guard is a filter that operates on a per interface basis.

IP traffic is permitted only if the IP address and MAC address of each packet match an entry from either the DHCP snooping binding table or a static IP source entry.

- 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 a spoofing attack, 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.

IP source guard architecture

You can enable IP Source Guard on Layer 2 interfaces that are not trusted by DHCP snooping. It supports interfaces operating in access mode and trunk mode. When you first enable IP Source Guard, the interface blocks all inbound IP traffic except:

- DHCP packets that DHCP snooping inspects and then forwards or drops, depending on the results of the inspection
- IP traffic from static IP source entries you have configured on the NX-OS device.

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

The device drops IP packets when neither the IP address nor the MAC address have a binding table entry or a static IP source entry.

For example, assume that the **show ip dhcp snooping binding** command displays this binding table entry:

```
MacAddress          IpAddress     LeaseSec    Type           VLAN    Interface
------------------  ----------    ---------   -------------  ----    ---------
00:00:5E:00:53:01   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 00:00:5E:00:53:01.

Prerequisites for IP source guard

IP Source Guard requires these prerequisites

- You must enable the DHCP feature and DHCP snooping before you can configure IP Source Guard. See Configuring DHCP .
- You must configure the ACL TCAM region size for IP Source Guard using the **hardware access-list tcam region ipsg** command. See Configure ACL TCAM region sizes .

Note By default, the ipsg region size is zero. Allocate enough entries to this region to store and enforce the SMAC–IP bindings.

Recommendation for IP source guard configuration

Use this reference to review recommendation for IP source guard configuration.

Recommendation for IP source guard configuration information

IP Source Guard has the following configuration guidelines and limitations:

- When you enable IP Source Guard on an interface, only sources with an IP-MAC address binding table entry or a static IP source entry can send IP traffic. You may notice a disruption in IP traffic until hosts on the interface receive a new IP address from a DHCP server.
- You must enable DHCP snooping to build and maintain the IP-MAC address binding table with IP Source Guard, or manually maintain static IP source entries.
- Do not use IP Source Guard on fabric extender (FEX) ports or generic expansion module (GEM) ports because it is not supported.
- Do not configure IP Source Guard on EoR, as it is not supported.
- Beginning with Cisco NX-OS Release 9.3(5), IP Source Guard is supported on Cisco Nexus 9364C-GX, Cisco Nexus 9316D-GX, and Cisco Nexus 93600CD-GX switches.

- You do not need to configure TCAM carving when you use IP Source Guard on Cisco Nexus 9300-X Cloud Scale Switches.
- If IPSG is enabled, port security can't be enabled on the interface.

Default settings for IP source guard

Use the table to see the default states and values for key IP Source Guard configuration parameters.

Table 1: Default IP source guard parameters

Parameters	Default
IP Source Guard	IP Source Guard is disabled on all interfaces.
IP source entries	There are no static or default IP source entries.

Configuring IP source guard

Use this reference to review configuring IP source guard.

Enable or disable IP source guard on a layer 2 interface

Configure IP Source Guard to control access based on valid IP address assignments.

By default, IP Source Guard is disabled. Enabling it prevents devices with spoofed IP addresses from communicating on the network.

Before you begin

- Ensure that Dynamic Host Configuration Protocol (DHCP) and DHCP snooping are enabled for your device.
- Confirm that the Access Control List (ACL) TCAM region size for IP Source Guard (IPSG) is configured.

Procedure

Step 1 Enter the global configuration mode using the **configure terminal** command.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Enter the interface configuration mode for the specified interface using **interface ethernet** *slot* / *port* command.

Example:

```
switch(config)#interface ethernet 2/3
switch(config-if)#
```

Step 3 Enable IP Source Guard on the interface using the [**no**] **ip verify source dhcp-snooping-vlan** command.

Example:

```
switch(config-if)#ip verify source dhcp-snooping-vlan
```

The **no** form of this command disables IP Source Guard on the interface.

Step 4 (Optional) Use the show running configuration command for DHCP snooping to display the IP Source Guard configuration using the **show running-config dhcp** command.

Example:

```
switch#show running-config dhcp
```

Step 5 (Optional) Use the copy running-config startup-config command to save the running configuration to the startup configuration using **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

IP Source Guard is enabled or disabled on the interface.

What to do next

Verify your configuration and monitor interface behavior to confirm that the interface operates as intended.

Add or remove a static IP source entry

Ensure your device uses accurate static IP-MAC bindings for DHCP snooping to improve device integrity and network security.

By default, no static IP source entries exist. Add entries to enhance security and prevent unauthorized DHCP assignments. Remove stale entries regularly to keep the bindings accurate.

Note Beginning with NX-OS 10.6(1), the system immediately displays an error message if you enter an invalid IP source binding configuration. Invalid entries include illegal MAC addresses or non-L2 interfaces. You see this error even when configuring through a candidate session or REST. This behavior is consistent with CLI direct configuration.

Follow these steps to add or remove a static IP source entry:

Procedure

Step 1 Enter the global configuration mode using the **configure terminal** command.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Create or delete the static IP binding for the current interface using the [**no**] **ip source binding** *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-type slot* / *port* command.

Example:

```
switch(config)#ip source binding 192.0.2.10 001f.28bd.0013 vlan 100 interface ethernet 2/3
```

Use the **no** form of this command to remove the static IP source entry.

Step 3 (Optional) Display current IP-MAC bindings, including static IP source entries, using the **show ip dhcp snooping binding** [**interface** *interface-type slot* / *port*] command.

Example:

```
switch#show ip dhcp snooping binding interface ethernet 2/3
```

All static entries are displayed with the term "static" in the Type column.

Step 4 (Optional) Save the running configuration to the startup configuration using the **copy running-config startup-config** command.

Example:

```
switch#copy running-config startup-config
```

After you make changes, the device updates its static IP source binding entries and retains them after a reboot.

What to do next

- Verify correct operation and security posture by reviewing the binding table.
- Remove obsolete entries as network topology changes.

Configure IP source guard on trunk ports

When IP Source Guard is configured on a port, the port drops traffic unless the TCAM has a DHCP snooping entry to allow it. If you enable IP Source Guard on trunk ports and want certain VLANs to bypass this check, specify the VLANs you want to exclude, even if those VLANs do not have DHCP snooping enabled.

Before you begin

Make sure that the DHCP feature and DHCP snooping are enabled.

Procedure

Step 1 Enter the global configuration mode using the **configure terminal** command.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Specify the list of VLANs to exclude from the DHCP snooping check for IP Source Guard on trunk ports using the [**no**] **ip dhcp snooping ipsg-excluded vlan** *vlan-list* command.

Example:

```
switch(config)#ip dhcp snooping ipsg-excluded vlan 1001-1256,3097
```

Step 3 (Optional) Display the excluded VLANs using the **show ip ver source** [**ethernet** *slot/port* | **port-channel** *channel-number*] command.

Example:

```
switch#show ip ver source
```

Step 4 (Optional) Copy the running configuration to the startup configuration using the **copy running-config startup-config** command.

Example:

```
switch#copy running-config startup-config
```

The specified VLANs are excluded from IP Source Guard checks on trunk ports.

What to do next

Verify that the configuration is correct and monitor the trunk ports for expected traffic flow.

Displaying IP source guard bindings

Use the **show ip ver source** [**ethernet** *slot/port* | **port-channel** *channel-number*] command to display the IP-MAC address bindings.

Clearing IP source guard statistics

To clear IP Source Guard statistics, use the commands in this table.

Table 2: Clear IP source guard statistics commands

Command	Purpose
clear access-list ipsg stats [**instance** *number* | **module** *number*]	Clears IP Source Guard statistics.

IP source guard configuration example

This example demonstrates how to create a static IP source entry and enable IP Source Guard on an interface.

```
ip source binding 192.0.2.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
 interface ethernet 2/3
no shutdown
ip verify source dhcp-snooping-vlan
show ip ver source

IP source guard excluded vlans:
-------------------------------------------------------
None
```

```
-----------------------------------
IP source guard is enabled on the following interfaces:
-----------------------------------------------------
ethernet2/3
```

Additional references

Use this reference to find additional references.

Reference documents for ACL TCAM regions and DHCP snooping

Use this reference to review reference documents for ACL TCAM regions and DHCP snooping.

Table 3: Reference documents for ACL TCAM regions and DHCP snooping

Related Topic	Links to Documentation
ACL TCAM regions	
DHCP and DHCP snooping	Configuring DHCP