



# 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](#)
- [Licensing Requirements for IP Source Guard, on page 2](#)
- [Prerequisites for IP Source Guard, on page 2](#)
- [Guidelines and Limitations for IP Source Guard, 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 7](#)
- [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
00:02: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 NX-OS	IP Source Guard requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

## 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 team region ipsg** command. See [Configuring 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.

## Guidelines and Limitations for IP Source Guard

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.
- IP Source Guard is not supported on fabric extender (FEX) ports or generic expansion module (GEM) ports.
- The following guidelines and limitations apply to the Cisco Nexus 9200 Series switches:
  - IPv6 adjacency is not formed with IPSG enabled on the incoming interface.
  - IPSG drops ARP packets at HSRP standby.
  - With DHCP snooping and IPSG enabled, if a binding entry exists for the host, traffic is forwarded to the host even without ARP.

## 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

### 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(config-if)# 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(config-if)# 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.

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(config)# 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(config)# 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(config)# 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(config)# 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                            |
|---------------------------------------------------------------------------------------|------------------------------------|
| <b>clear access-list ipsg stats</b> [ <i>instance number</i>   <b>module number</b> ] | 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

### Reference documents for ACL TCAM regions and DHCP snooping

| Related Topic          | Links to Documentation              |
|------------------------|-------------------------------------|
| ACL TCAM regions       | <a href="#">Configuring IP ACLs</a> |
| DHCP and DHCP snooping |                                     |

