Configuring IP Source Guard

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.

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 a source whose static IP entries are configured in the Cisco Nexus 1000V.

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 in the DHCP binding table.

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 **show ip dhcp snooping binding** command displays the following binding table entry:

```
MacAddress          IpAddress    LeaseSec   Type        VLAN      Interface
----------          ----------   ---------  ------      -------    ---------
00:02:B3:3F:3B:99  10.5.5.2       6943    dhcp-snooping  10      vEthernet3
```

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.

Prerequisites for IP Source Guard

- You should be familiar with DHCP snooping before you configure IP Source Guard.
- DHCP snooping is enabled.

Guidelines and Limitations for IP Source Guard

- 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 might experience disruption in the IP traffic until the hosts on the interface receive a new IP address from a DHCP server.
- When the IP Source Guard (IPSG) functionality is enabled on the Cisco Nexus 1000V switch and whenever a duplicate IP address is detected on a port, it is error-disabled.
- 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.
- For seamless IP Source Guard, Virtual Service Domain (VSD) service VM ports are trusted ports by default. If you configure these ports as untrusted, this setting is ignored.

Default Settings for IP Source Guard

Parameters	Default
IP Source Guard	Disabled on each interface.
IP source entries	None. No static or default IP source entries exist by default.

Configuring IP Source Guard Functionality

Enabling or Disabling IP Source Guard on a Layer 2 Interface

By default, IP Source Guard is disabled on all interfaces. You can configure IP Source Guard on either an interface or a port profile.

Before You Begin

Ensure that DHCP snooping is enabled.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you into global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Enters interface configuration mode, where interface-number is the vEthernet interface that you want to configure as trusted or untrusted for DHCP snooping.
Step 3	switch(config)# **port-profile** *profilename*	Places you in port profile configuration mode for the specified port profile.
Step 4	switch(config-if)# [**no**] **ip verify source dhcp-snooping-vlan**	Enables IP Source Guard on the interface. The **no** option disables IP Source Guard on the interface.
Step 5	switch(config-if)# **show ip verify source interface vethernet interface number**	(Optional) Displays the IP Source Guard configuration.
Step 6	switch(config-if)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

This example shows how to enable IP Source Guard on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip verify source dhcp-snooping-vlan
switch (config-if)# show ip verify source interface vethernet 3

IP source guard is  enabled on this interface.

Interface         Filter-mode            IP-address     Mac-address       Vlan
----------    -----------            ----------     -----------    ----
Vethernet3        active                  1.182.56.137   00:50:56:82:56:3e  1053
```

Verifying the IP Source Guard Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show running-config dhcp	Displays DHCP snooping configuration, including the IP Source Guard configuration.
show ip verify source	Displays IP-MAC address bindings.

Monitoring IP Source Guard Bindings

Use the following command to monitor IP Source Guard Bindings.

Command	Purpose
show ip verify source	Displays IP-MAC address bindings

Configuration Example for IP Source Guard

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

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface vethernet 3
switch(config)# interface Vethernet 3
switch(config)# ip verify source dhcp-snooping-vlan
switch(config-port-prof)# show ip verify source interface vethernet 3
Filter Mode (for static bindings): IP-MAC
IP source guard is  enabled on this interface.

Interface         Filter-mode             IP-address     Mac-address       Vlan
------      -----------             ----------     --------------    ----
Vethernet3        active              10.5.22.17     00:1f:28:bd:00:13  100
```

Feature History for IP Source Guard

This table only includes updates for those releases that have resulted in additions to the feature.

Feature Name	Releases	Feature Information
IP Source Guard	5.2(1)SM1(5.1)	This feature was introduced.