Configuring IP Source Guard

IP Source Guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings.

This chapter contains the following topics:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP Source Guard

IP Source Guard

You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor and you can enable IP source guard when DHCP snooping is enabled on an untrusted interface.

After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping.

The switch uses a source IP lookup table in hardware to bind IP addresses to ports. For IP and MAC filtering, a combination of source IP and source MAC lookups are used. IP traffic with a source IP address is the binding table is allowed, all other traffic is denied.

The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IPSG is supported only on Layer 2 ports, including access and trunk ports. You can configure IPSG with source IP address filtering or with source IP and MAC address filtering.

IP Source Guard for Static Hosts

Note Do not use IPSG (IP source guard) for static hosts on uplink ports or trunk ports.

IPSG for static hosts extends the IPSG capability to non-DHCP and static environments. The previous IPSG used the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. This security feature restricts IP traffic on nonrouted Layer 2 interfaces. It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings. The previous version of IPSG required a DHCP environment for IPSG to work.

IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IPSG for static hosts also supports dynamic hosts. If a dynamic host receives a DHCP-assigned IP address that is available in the IP DHCP snooping table, the same entry is learned by the IP device tracking table. In a stacked environment, when the master failover occurs, the IP source guard entries for static hosts attached to member ports are retained. When you enter the **show ip device tracking all** EXEC command, the IP device tracking table displays the entries as ACTIVE.

Note Some IP hosts with multiple network interfaces can inject some invalid packets into a network interface. The invalid packets contain the IP or MAC address for another network interface of the host as the source address. The invalid packets can cause IPSG for static hosts to connect to the host, to learn the invalid IP or MAC address bindings, and to reject the valid bindings. Consult the vender of the corresponding operating system and the network interface to prevent the host from injecting invalid packets.

IPSG for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP address. To resolve hosts that have moved or gone away for any reason, IPSG for static hosts leverages IP device tracking to age out dynamically learned IP address bindings. This feature can be used with DHCP snooping. Multiple bindings are established on a port that is connected to both DHCP and static hosts. For example, bindings are stored in both the device tracking database as well as in the DHCP snooping binding database.

IP Source Guard Configuration Guidelines

- You can configure static IP bindings only on nonrouted ports. If you enter the **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* global configuration command on a routed interface, this error message appears:

```
Static IP source binding can only be configured on switch port.
```

- When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.
- If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.

Note If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

- You can enable this feature when 802.1x port-based authentication is enabled.
- When you configure IP source guard smart logging, packets with a source address other than the specified address or an address learned by DHCP are denied, and the packet contents are sent to a NetFlow collector. If you configure this feature, make sure that smart logging is globally enabled.
- In a switch stack, if IP source guard is configured on a stack member interface and you remove the the configuration of that switch by entering the **no switch** *stack-member-number* **provision** global configuration command, the interface static bindings are removed from the binding table, but they are not removed from the running configuration. If you again provision the switch by entering the **switch** *stack-member-number* **provision** command, the binding is restored.

  To remove the binding from the running configuration, you must disable IP source guard before entering the **no switch provision** command. The configuration is also removed if the switch reloads while the interface is removed from the binding table.

How to Configure IP Source Guard

Enabling IP Source Guard

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **ip verify source** [**mac-check**]
4. **exit**
5. **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface to be configured, and enters interface configuration mode.
Step 3	**ip verify source** [**mac-check**] **Example:** `Switch(config-if)# ip verify source`	Enables IP source guard with source IP address filtering. (Optional) **mac-check—**Enables IP Source Guard with source IP address and MAC address filtering.
Step 4	**exit** **Example:** `Switch(config-if)# exit`	Returns to global configuration mode.
Step 5	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **Example:** `Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1`	Adds a static IP source binding. Enter this command for each static binding.

Step 6	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Enabling IP source guard with source IP and MAC filtering on VLANs 10 and 11

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# ip verify source
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface gigabitethernet
 1/0/1
```

```
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet
 1/0/1
Switch(config)# end
```

Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port

You must configure the **ip device tracking maximum** *limit-number* interface configuration command globally for IPSG for static hosts to work. If you only configure this command on a port without enabling IP device tracking globally or by setting an IP device tracking maximum on that interface, IPSG with static hosts rejects all the IP traffic from that interface.

SUMMARY STEPS

1. **configure terminal**
2. **ip device tracking**
3. **interface** *interface-id*
4. **switchport mode access**
5. **switchport access vlan** *vlan-id*
6. **ip verify source**[**tracking**] [**mac-check**]
7. **ip device tracking maximum** *number*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Turns on the IP host table, and globally enables IP device tracking.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Configures a port as access.
Step 5	**switchport access vlan** *vlan-id* **Example:** `Switch(config-if)# switchport access vlan 10`	Configures the VLAN for this port.
Step 6	**ip verify source**[**tracking**] [**mac-check**] **Example:** `Switch(config-if)# ip verify source tracking mac-check`	Enables IP source guard with source IP address filtering. (Optional) **tracking—**Enables IP source guard for static hosts. (Optional) **mac-check—**Enables MAC address filtering. The command **ip verify source tracking mac-check**enables IP source guard for static hosts with MAC address filtering.
Step 7	**ip device tracking maximum** *number* **Example:** `Switch(config-if)# ip device tracking maximum 8`	Establishes a maximum limit for the number of static IPs that the IP device tracking table allows on the port. The range is 1to 10. The maximum number is 10. **Note** You must configure the **ip device tracking maximum** *limit-number* interface configuration command.

Step 8	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Eight Examples

This example shows how to stop IPSG with static hosts on an interface.

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

This example shows how to enable IPSG with static hosts on a port.

```
Switch(config)# ip device tracking
Switch(config-if)# ip device tracking maximum 10
Switch(config-if)# ip verify source tracking
```

This example shows how to enable IPSG for static hosts with IP filters on a Layer 2 access port and to verify the valid IP bindings on the interface Gi1/0/3:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip trk       active       40.1.1.24                          10
Gi1/0/3      ip trk       active       40.1.1.20                          10
Gi1/0/3      ip trk       active       40.1.1.21                          10
```

This example shows how to enable IPSG for static hosts with IP-MAC filters on a Layer 2 access port, to verify the valid IP-MAC bindings on the interface Gi1/0/3, and to verify that the number of bindings on this interface has reached the maximum:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5

Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip trk       active       deny-all                            1
```

This example displays all IP or MAC binding entries for all interfaces. The CLI displays all active as well as inactive entries. When a host is learned on a interface, the new entry is marked as active. When the same host is disconnected from that interface and connected to a different interface, a new IP or MAC binding entry displays as active as soon as the host is detected. The old entry for this host on the previous interface is marked as INACTIVE.

```
Switch# show ip device tracking all
IP Device Tracking for wireless clients = Enabled
Global IP Device Tracking for wired clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
------------------------------------------------------------------------------------------

  IP Address     MAC Address    Vlan  Interface           Probe-Timeout       STATE
------------------------------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.9       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.10      0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.1       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.1       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.2       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.2       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.3       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.3       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.4       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.4       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
```

```
200.1.1.5       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.5       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.6       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.7       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
```

This example displays all active IP or MAC binding entries for all interfaces:

```
Switch# show ip device tracking all active
IP Device Tracking for wireless clients = Enabled
Global IP Device Tracking for wired clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
------------------------------------------------------------------------------------------

  IP Address     MAC Address   Vlan  Interface           Probe-Timeout      STATE
------------------------------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
```

This example displays all inactive IP or MAC binding entries for all interfaces. The host was first learned on GigabitEthernet 1/0/1 and then moved to GigabitEthernet 0/2. the IP or MAC binding entries learned on GigabitEthernet1/ 0/1 are marked as inactive.

```
Switch# show ip device tracking all inactive
IP Device Tracking for wireless clients = Enabled
Global IP Device Tracking for wired clients= Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
------------------------------------------------------------------------------------------

  IP Address     MAC Address   Vlan  Interface           Probe-Timeout      STATE
------------------------------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.9       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.10      0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.1       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.2       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.3       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.4       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.5       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.6       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.7       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
```

This example displays the count of all IP device tracking host entries for all interfaces:

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
---------------------------------------------------------------------
  Interface           Maximum Limit          Number of Entries
---------------------------------------------------------------------
Gi1/0/3                  5
```

Monitoring IP Source Guard

Table 1: Privileged EXEC show Commands

Command	Purpose
show ip verify source [**interface** *interface-id*]	Displays the IP source guard configuration on the switch or on a specific interface.
show ip device tracking { **all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *imac-address*}	Displays information about the entries in the IP device tracking table.

Table 2: Interface Configuration Commands

Command	Purpose
ip verify source tracking	Verifies the data source.

For detailed information about the fields in these displays, see the command reference for this release.

Additional References

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support