



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:

- [Information About IP Source Guard, on page 1](#)
- [How to Configure IP Source Guard, on page 3](#)
- [Monitoring IP Source Guard, on page 7](#)
- [Additional References, on page 8](#)

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 in 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 active switch 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 vendor 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.

- If you enable IP source guard with source IP and MAC address filtering, DHCP snooping and port security must be enabled on the interface. You must also enter the `ip dhcp snooping information option` global configuration command and ensure that the DHCP server supports option 82. When IP source guard is enabled with MAC address filtering, the DHCP host MAC address is not learned until the host is granted a lease. When forwarding packets from the server to the host, DHCP snooping uses option-82 data to identify the host port.
- When configuring IP source guard on interfaces on which a private VLAN is configured, port security is not supported.
- You can enable this feature when 802.1x port-based authentication is enabled.
- If the number of ternary content addressable memory (TCAM) entries exceeds the maximum, the CPU usage increases.
- 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 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. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `ip verify source [mac-check]`
5. Use one of the following:
 - `ip verify source`
 - `ip verify source port-security`
6. `exit`
7. `ip source binding mac-address vlan vlan-id ip-address interface interface-id`

8. `end`
9. `show running-config`
10. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Switch> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Switch# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>interface interface-id</code></p> <p>Example:</p> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	<p>Specifies the interface to be configured, and enters interface configuration mode.</p>
Step 4	<p><code>ip verify source [mac-check]</code></p> <p>Example:</p> <pre>Switch(config-if)# ip verify source</pre>	<p>Enables IP source guard with source IP address filtering.</p> <p>(Optional) mac-check—Enables IP Source Guard with source IP address and MAC address filtering.</p>
Step 5	<p>Use one of the following:</p> <ul style="list-style-type: none"> • <code>ip verify source</code> • <code>ip verify source port-security</code> <p>Example:</p> <pre>Switch(config-if)# ip verify source</pre> <p>or</p> <pre>Switch(config-if)# ip verify source port-security</pre>	<p>Enables IP source guard with source IP address filtering.</p> <p>Enables IP source guard with source IP and MAC address filtering.</p> <p>When you enable both IP source guard and port security by using the ip verify source port-security interface configuration command, there are two caveats:</p> <ul style="list-style-type: none"> • The DHCP server must support option 82, or the client is not assigned an IP address. • The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.
Step 6	<p><code>exit</code></p> <p>Example:</p>	<p>Returns to global configuration mode.</p>

	Command or Action	Purpose
	Switch(config-if) # exit	
Step 7	<p>ip source binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ip-address</i> interface <i>interface-id</i></p> <p>Example:</p> <pre>Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1</pre>	<p>Adds a static IP source binding.</p> <p>Enter this command for each static binding.</p>
Step 8	<p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 9	<p>show running-config</p> <p>Example:</p> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 10	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

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 IPSPG 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, IPSPG with static hosts rejects all the IP traffic from that interface.

SUMMARY STEPS

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

9. `switchport port-security`
10. `switchport port-security maximum value`
11. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Switch> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Switch# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>ip device tracking</code></p> <p>Example:</p> <pre>Switch(config)# ip device tracking</pre>	<p>Turns on the IP host table, and globally enables IP device tracking.</p>
Step 4	<p><code>interface interface-id</code></p> <p>Example:</p> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	<p>Enters interface configuration mode.</p>
Step 5	<p><code>switchport mode access</code></p> <p>Example:</p> <pre>Switch(config-if)# switchport mode access</pre>	<p>Configures a port as access.</p>
Step 6	<p><code>switchport access vlan vlan-id</code></p> <p>Example:</p> <pre>Switch(config-if)# switchport access vlan 10</pre>	<p>Configures the VLAN for this port.</p>
Step 7	<p><code>ip verify source[tracking] [mac-check]</code></p> <p>Example:</p> <pre>Switch(config-if)# ip verify source tracking mac-check</pre>	<p>Enables IP source guard with source IP address filtering.</p> <p>(Optional) tracking—Enables IP source guard for static hosts.</p> <p>(Optional) mac-check—Enables MAC address filtering.</p>

	Command or Action	Purpose
		The command ip verify source tracking mac-check enables IP source guard for static hosts with MAC address filtering.
Step 8	ip device tracking maximum <i>number</i> Example: <pre>Switch(config-if)# ip device tracking maximum 8</pre>	Establishes a maximum limit for the number of static IPs that the IP device tracking table allows on the port. The range is 1 to 10. The maximum number is 10. Note You must configure the ip device tracking maximum <i>limit-number</i> interface configuration command.
Step 9	switchport port-security	(Optional) Activate port security for this port.
Step 10	switchport port-security maximum <i>value</i>	(Optional) Establish a maximum of MAC addresses for this port.
Step 11	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.

Monitoring IP Source Guard

Table 1: Privileged EXEC show Commands

Command	Purpose
show ip verify source [interface <i>interface-id</i>]	Displays the IP source guard configuration on the switch or on a specific interface.
show ip device tracking { all interface <i>interface-id</i> ip <i>ip-address</i> mac <i>mac-address</i> }	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 the 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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support