IP Source Guard

- Feature history for IP Source Guard, on page 1
- IP Source Guard, on page 1
- IP Source Guard for static hosts, on page 2
- IP Source Guard configuration guidelines, on page 3
- Enable IP Source Guard, on page 3
- Configure IP Source Guard for static hosts on a Layer 2 access port, on page 4
- Monitoring IP Source Guard, on page 6

Feature history for IP Source Guard

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 17.18.1	IP Source Guard: IP Source Guard 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.	Cisco C9350 Series Smart Switches

IP Source Guard

IP Source Guard 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.

You can enable IP source guard when DHCP snooping is enabled. This ensures that IP traffic with a source IP address in the binding table is allowed, while all other traffic is denied.

The switch utilizes a source IP lookup table enabling both IP and MAC filtering through a combination of source IP and source MAC lookups. This table, known as the IP source binding table, contains bindings that are either learned by DHCP snooping or manually configured as static IP source bindings. Each entry in this table consists of an IP address, its associated MAC address, and its associated VLAN number.

IP source guard is supported on private VLAN access port and etherchannel but not on private VLAN trunk port. You have the capability to configure IP Source Guard with source IP address filtering or with source IP and MAC address filtering.

IP Source Guard for static hosts

Note Do not use IP Source Guard for static hosts on uplink ports or trunk ports.

A static host is a network device in a non-DHCP environment that:

- requires IP addresses to be manually assigned,
- extends IP Source Guard capabilities without relying on DHCP, and
- relies on IP device tracking-table entries to manage port ACLs.

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 by filtering traffic based on the DHCP snooping binding database and manually configured IP source bindings.

IP Source Guard for static hosts also supports dynamic hosts. If a dynamic host receives a DHCP-assigned IP address 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 device-tracking database** EXEC command, the IP device tracking table displays the entries as ACTIVE.

Note Some IP hosts with multiple network interfaces can inject invalid packets into the network. Invalid packets contain the IP or MAC address of another network interface as the source address. The invalid packets can cause IP Source Guard for static hosts to interact with the host, to learn the invalid IP or MAC address bindings, and to reject the valid bindings. Contact the vendor of the operating system and network interface to stop the host from injecting invalid packets.

IP Source Guard for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned via ARP and IP packets and stored in the device tracking database. If dynamically learned or statically configured IP addresses on a port reach their maximum, the hardware drops any packet with a new IP address.

To resolve hosts that have moved or gone away for any reason, IP Source Guard 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

- 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.
  ```

- Enable DHCP snooping on the access VLAN for the interface when enabling IP Source Guard with source IP address filtering.
- 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 active and you change DHCP snooping on a VLAN on the trunk interface, the switch might not filter traffic properly.

- You can enable this feature when 802.1x port-based authentication is 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. The binding is restored when you re-provision the switch by entering the **switch** *stack-member-number* **provision** command.

  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.

Enable IP Source Guard

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:**	Specifies the interface to be configured, and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)#` **`interface gigabitethernet 1/0/1`**	
Step 4	**ip verify source** [**mac-check**] **Example:** `Device(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 5	**exit** **Example:** `Device(config-if)#` **`exit`**	Exits interface configuration mode and returns to global configuration mode.
Step 6	**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id* **Example:** `Device(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 7	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and reutrns to privileged EXEC mode.

Configure IP Source Guard for static hosts on a Layer 2 access port

To ensure IP Source Guard works with static hosts, configure the **ip device tracking maximum** *limit-number* interface configuration command globally. In cases where 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, IP Source Guard with static hosts will reject all IP traffic from that interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>` **`enable`**	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip device tracking** **Example:** `Device(config)# ip device tracking`	Turns on the IP host table, and globally enables IP device tracking.
Step 4	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.
Step 5	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Configures a port as access.
Step 6	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 10`	Configures the VLAN for this port.
Step 7	**ip verify source**[**tracking**] [**mac-check**] **Example:** `Device(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. Use the **ip verify source tracking mac-check** command to enable IP Source Guard for static hosts with MAC address filtering.
Step 8	**ip device tracking maximum** *number* **Example:** `Device(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 9	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring IP Source Guard

Table 1: Commands to monitor IP Source Guard

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** *mac-address***}**	Displays information about the entries in the IP device tracking table.