Configuring IP Source Guard

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

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.ter
- 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 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.

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.

Related Topics

Enabling IP Source Guard, on page 4
Monitoring IP Source Guard, on page 16

Source IP Address Filtering

When IPSG is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

When a DHCP snooping binding or static IP source binding is added, changed, or deleted on an interface, the switch modifies the port ACL by using the IP source binding changes and re-applies the port ACL to the interface.

If you enable IPSG on an interface on which IP source bindings (dynamically learned by DHCP snooping or manually configured) are not configured, the switch creates and applies a port ACL that denies all IP traffic on the interface. If you disable IP source guard, the switch removes the port ACL from the interface.

Source IP and MAC Address Filtering

IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table.

When address filtering is enabled, the switch filters IP and non-IP traffic. If the source MAC address of an IP or non-IP packet matches a valid IP source binding, the switch forwards the packet. The switch drops all other types of packets except DHCP packets.

The switch uses port security to filter source MAC addresses. The interface can shut down when a port-security violation occurs.

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.

Related Topics

Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port, on page 7
Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port, on page 9
Configuring IP Source Guard for Static Hosts: Examples, on page 12
Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port: Examples, on page 15

Default IP Source Guard Configuration

By default, IP source guard is disabled.

How to Configure IP Source Guard

Enabling IP Source Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. Use one of the following:
   - `ip verify source[smartlog]`
   - **ip verify source port-security**
5. **exit**
6. **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*
7. **end**
8. **show ip verify source** [**interface** *interface-id*]

9. **show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *interface-id*] [**vlan** *vlan-id*]
10. **show running-config**
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface to be configured, and enters interface configuration mode.

Step 4	Use one of the following:
	• `ip verify source[smartlog]`
	• **ip verify source port-security**
	Example:
	`Switch(config-if)# ip verify source`
	or
	`Switch(config-if)# ip verify source port-security`
		Enables IP source guard with source IP address filtering.
		(Optional) Enter **smartlog** to configure the switch to send the contents of dropped packets to a NetFlow collector.
		Enables IP source guard with source IP and MAC address filtering.
		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:
		• 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 5	**exit** **Example:** `Switch(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 6	**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 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show ip verify source** [**interface** *interface-id*] **Example:** `Switch# show ip verify source interface gigabitethernet 1/0/1`	Verifies the IP source guard configuration.
Step 9	**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *interface-id*] [**vlan** *vlan-id*] **Example:** `Switch# show ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet 1/0/1`	Displays the IP source bindings on the switch, on a specific VLAN, or on a specific interface.
Step 10	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

IP Source Guard, on page 2
Monitoring IP Source Guard, on page 16

Configuring IP Source Guard for Static Hosts

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. This requirement also applies to IPSG with static hosts on a private VLAN host port.

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 port-security**
8. **ip device tracking maximum** *number*
9. **switchport port-security**
10. **switchport port-security maximum** *value*
11. **end**
12. **show ip verify source interface** *interface-id*
13. **show ip device tracking all** [**active** | **inactive**] **count**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Turns on the IP host table, and globally enables IP device tracking.

	Command or Action	Purpose
Step 4	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.
Step 5	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Configures a port as access.
Step 6	**switchport access vlan** *vlan-id* **Example:** `Switch(config-if)# switchport access vlan 10`	Configures the VLAN for this port.
Step 7	**ip verify source tracking port-security** **Example:** `Switch(config-if)# ip verify source tracking port-security`	Enables IPSG for static hosts with MAC address filtering. **Note** When you enable both IP source guard and port security by using the **ip verify source port-security** interface configuration command: • 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 8	**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 9	**switchport port-security**	(Optional) Activate port security for this port.
Step 10	**switchport port-security maximum** *value*	(Optional) Establish a maximum of MAC addresses for this port.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 12	**show ip verify source interface** *interface-id* **Example:** `Switch# show ip verify source interface gigabitethernet 1/0/1`	Verifies the configuration and display IPSG permit ACLs for static hosts.
Step 13	**show ip device tracking all** [**active** | **inactive**] **count** **Example:** `Switch# show ip device tracking all`	Verifies the configuration by displaying the IP-to-MAC binding for a given host on the switch interface. • **all active**—display only the active IP or MAC binding entries • **all inactive**—display only the inactive IP or MAC binding entries • **all**—display the active and inactive IP or MAC binding entries

Related Topics

IP Source Guard for Static Hosts, on page 3
Configuring IP Source Guard for Static Hosts: Examples, on page 12
Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port: Examples, on page 15

Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port

You must globally 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 setting an IP device tracking maximum on that interface, IPSG with static hosts will reject all the IP traffic from that interface. This requirement also applies to IPSG with static hosts on a Layer 2 access port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id1*
4. **private-vlan primary**
5. **exit**
6. **vlan** *vlan-id2*
7. **private-vlan isolated**
8. **exit**
9. **vlan** *vlan-id1*
10. **private-vlan association 201**
11. **exit**
12. **interface** *interface-id*
13. **switchport mode private-vlan host**
14. **switchport private-vlan host-association** *vlan-id1 vlan-id2*

15. **ip device tracking maximum** *number*
16. **ip verify source tracking** [**port-security**]
17. **end**
18. **show ip device tracking all**
19. **show ip verify source interface** *interface-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**vlan** *vlan-id1* **Example:** `Switch(config)# vlan 10`	Enters VLAN configuration mode.
Step 4	**private-vlan primary** **Example:** `Switch(config-vlan)# private-vlan primary`	Establishes a primary VLAN on a private VLAN port.
Step 5	**exit** **Example:** `Switch(config-vlan)# exit`	Exits VLAN configuration mode.
Step 6	**vlan** *vlan-id2* **Example:** `Switch(config)# vlan 20`	Enters configuration VLAN mode for another VLAN.
Step 7	**private-vlan isolated** **Example:**	Establishes an isolated VLAN on a private VLAN port.

	Command or Action	Purpose
	`Switch(config-vlan)# private-vlan isolated`	
Step 8	**exit** **Example:** `Switch(config-vlan)# exit`	Exits VLAN configuration mode.
Step 9	**vlan** *vlan-id1* **Example:** `Switch(config)# vlan 10`	Enters VLAN configuration mode.
Step 10	**private-vlan association 201** **Example:** `Switch(config-vlan)# private-vlan association 201`	Associates the VLAN on an isolated private VLAN port.
Step 11	**exit** **Example:** `Switch(config-vlan)# exit`	Exits VLAN configuration mode.
Step 12	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.
Step 13	**switchport mode private-vlan host** **Example:** `Switch(config-if)# switchport mode private-vlan host`	(Optional) Establishes a port as a private VLAN host.
Step 14	**switchport private-vlan host-association** *vlan-id1 vlan-id2* **Example:** `Switch(config-if)# switchport private-vlan host-association 10 20`	(Optional) Associates this port with the corresponding private VLAN.

	Command or Action	Purpose
Step 15	**ip device tracking maximum** *number* **Example:** `Switch(config-if)# ip device tracking maximum 8`	Establishes a maximum for the number of static IPs that the IP device tracking table allows on the port. The maximum is 10. **Note** You must globally configure the **ip device tracking maximum** *number* interface command for IPSG for static hosts to work.
Step 16	**ip verify source tracking** [**port-security**] **Example:** `Switch(config-if)# ip verify source tracking`	Activates IPSG for static hosts with MAC address filtering on this port.
Step 17	**end** **Example:** `Switch(config-if)# end`	Exits interface configuration mode.
Step 18	**show ip device tracking all** **Example:** `Switch# show ip device tracking all`	Verifies the configuration.
Step 19	**show ip verify source interface** *interface-id* **Example:** `Switch# show ip verify source interface gigabitethernet 1/0/1`	Verifies the IP source guard configuration. Display IPSG permit ACLs for static hosts.

Related Topics

IP Source Guard for Static Hosts, on page 3
Configuring IP Source Guard for Static Hosts: Examples, on page 12
Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port: Examples, on page 15

Configuration Examples for Configuring IP Source Guard for Static Hosts

Configuring IP Source Guard for Static Hosts: 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)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

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)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi1/0/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi1/0/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi1/0/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi1/0/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  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 = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              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 = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              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 = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              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
```

Related Topics

IP Source Guard for Static Hosts, on page 3
Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port, on page 7
Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port, on page 9

Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port: Examples

This example shows how to enable IPSG for static hosts with IP filters on a private VLAN host port:

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
------------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface                  STATE
------------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  GigabitEthernet1/0/3        ACTIVE
40.1.1.20       0000.0000.0305  200  GigabitEthernet1/0/3        ACTIVE
40.1.1.21       0000.0000.0306  200  GigabitEthernet1/0/3        ACTIVE
40.1.1.22       0000.0000.0307  200  GigabitEthernet1/0/3        ACTIVE
40.1.1.23       0000.0000.0308  200  GigabitEthernet1/0/3        ACTIVE
```

The output shows the five valid IP-MAC bindings that have been learned on the interface Fa0/3. For the private VLAN cases, the bindings are associated with primary VLAN ID. So, in this example, the primary VLAN ID, 200, is shown in the table.

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  -----
Gi1/0/3      ip trk       active       40.1.1.23                         200
Gi1/0/3      ip trk       active       40.1.1.24                         200
Gi1/0/3      ip trk       active       40.1.1.20                         200
Gi1/0/3      ip trk       active       40.1.1.21                         200
Gi1/0/3      ip trk       active       40.1.1.22                         200
Gi1/0/3      ip trk       active       40.1.1.23                         201
Gi1/0/3      ip trk       active       40.1.1.24                         201
Gi1/0/3      ip trk       active       40.1.1.20                         201
Gi1/0/3      ip trk       active       40.1.1.21                         201
Gi1/0/3      ip trk       active       40.1.1.22                         201
```

The output shows that the five valid IP-MAC bindings are on both the primary and secondary VLAN.

Related Topics

IP Source Guard for Static Hosts, on page 3
Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port, on page 7
Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port, on page 9

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.

Related Topics

IP Source Guard, on page 2
Enabling IP Source Guard, on page 4