CHAPTER 53

Configuring DHCP Snooping, IP Source Guard, and IPSG for Static Hosts

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping, IP source guard, and IP source guard (IPSG) for static hosts on Catalyst 4500 series switches. It provides guidelines, procedures, and configuration examples.

This chapter consists of the following major sections:

Note For complete syntax and usage information for the switch commands used in this chapter, see the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

If a command is not in the *Catalyst 4500 Series Switch Command Reference*, you can locate it in the Cisco IOS library. See the *Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

About DHCP Snooping

DHCP snooping is a DHCP security feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts such as a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

Note In order to enable DHCP snooping on a VLAN, you must enable DHCP snooping on the switch.

You can configure DHCP snooping for switches and VLANs. When you enable DHCP snooping on a switch, the interface acts as a Layer 2 bridge, intercepting and safeguarding DHCP messages going to a Layer 2 VLAN. When you enable DHCP snooping on a VLAN, the switch acts as a Layer 2 bridge within a VLAN domain.

This section includes these topics:

- Trusted and Untrusted Sources, page 53-2
- About the DHCP Snooping Database Agent, page 53-2
- Option 82 Data Insertion, page 53-4

Trusted and Untrusted Sources

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.

In an enterprise network, devices under your administrative control are trusted sources. These devices include the switches, routers and servers in your network. Any device beyond the firewall or outside your network is an untrusted source. Host ports are generally treated as untrusted sources.

In a service provider environment, any device that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In the Catalyst 4500 series switch, you indicate that a source is trusted by configuring the trust state of its connecting interface.

The default trust state of all interfaces is untrusted. You must configure DHCP server interfaces as trusted. You can also configure other interfaces as trusted if they connect to devices (such as switches or routers) inside your network. You usually do not configure host port interfaces as trusted.

Note For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces, as untrusted DHCP messages will be forwarded only to trusted interfaces.

About the DHCP Snooping Database Agent

To retain the bindings across switch reloads, you must use the DHCP snooping database agent. Without this agent, the bindings established by DHCP snooping are lost upon switch reload. Connectivity is lost as well.

The mechanism for the database agent stores the bindings in a file at a configured location. Upon reload, the switch reads the file to build the database for the bindings. The switch keeps the file current by writing to the file as the database changes.

The format of the file that contains the bindings is as follows:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

Each entry in the file is tagged with a checksum that is used to validate the entries whenever the file is read. The <initial-checksum> entry on the first line helps distinguish entries associated with the latest write from entries that are associated with a previous write.

it is a sample bindings file:

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
1.1.1.1 512 0001.0001.0005 3EBE2881 Gi1/1                              e5e1e733
1.1.1.1 512 0001.0001.0002 3EBE2881 Gi1/1                              4b3486ec
1.1.1.1 1536 0001.0001.0004 3EBE2881 Gi1/1                             f0e02872
1.1.1.1 1024 0001.0001.0003 3EBE2881 Gi1/1                             ac41adf9
1.1.1.1 1 0001.0001.0001 3EBE2881 Gi1/1                                34b3273e
END
```

Each entry holds an IP address, VLAN, MAC address, lease time (in hex), and the interface associated with a binding. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry consists of 72 bytes of data, followed by a space, followed by a checksum.

Upon bootup, when the calculated checksum equals the stored checksum, a switch reads entries from the file and adds the bindings to the DHCP snooping database. When the calculated checksum does not equal the stored checksum, the entry read from the file is ignored and so are all the entries following the failed entry. The switch also ignores all those entries from the file whose lease time has expired. (This situation is possible because the lease time might indicate an expired time.) An entry from the file is also ignored if the interface referred to in the entry no longer exists on the system or if it is a router port or a DHCP snooping-trusted interface.

When a switch learns of new bindings or when it loses some bindings, the switch writes the modified set of entries from the snooping database to the file. The writes are performed with a configurable delay to batch as many changes as possible before the actual write happens. Associated with each transfer is a timeout after which a transfer is aborted if it is not completed. These timers are referred to as the write delay and abort timeout.

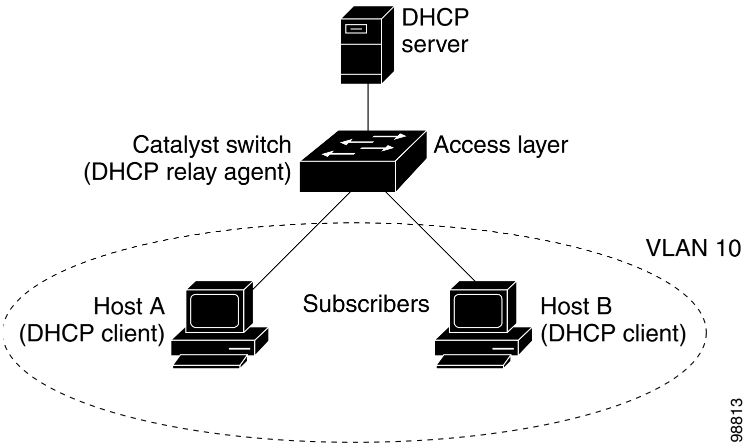
Option 82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP Option 82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

Note The DHCP Option 82 feature is supported only when DHCP snooping is globally enabled and on the VLANs to which subscriber devices using this feature are assigned.

Figure 53-1 is an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

Figure 53-1 DHCP Relay Agent in a Metropolitan Ethernet Network



When you enable the DHCP snooping information Option 82 on the switch, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the Option 82 information in the packet. By default, the remote ID suboption is the switch MAC address, and the circuit ID suboption is the port identifier, **vlan-mod-port**, from which the packet is received. Beginning with Cisco IOS Release 12.2(40)SG, you can configure the remote ID and circuit ID. For information on configuring these suboptions, see the "Enabling DHCP Snooping and Option 82" section on page 53-10.
- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the Option 82 field to the DHCP server.
- The DHCP server receives the packet. If the server is Option 82-capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. The DHCP server then echoes the Option 82 field in the DHCP reply.

- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the Option 82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the Option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

In the default suboption configuration, when the described sequence of events occurs, the values in these fields in Figure 53-2 do not change:

- Circuit ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit ID type
  - Length of the circuit ID type
- Remote ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Remote ID type
  - Length of the remote ID type

Figure 53-2 shows the packet formats for the remote ID suboption and the circuit ID suboption when the default suboption configuration is used. For the circuit ID suboption, the module number corresponds to the switch module number. The switch uses the packet formats when you globally enable DHCP snooping and enter the **ip dhcp snooping information option** global configuration command.

Figure 53-2 Suboption Packet Formats

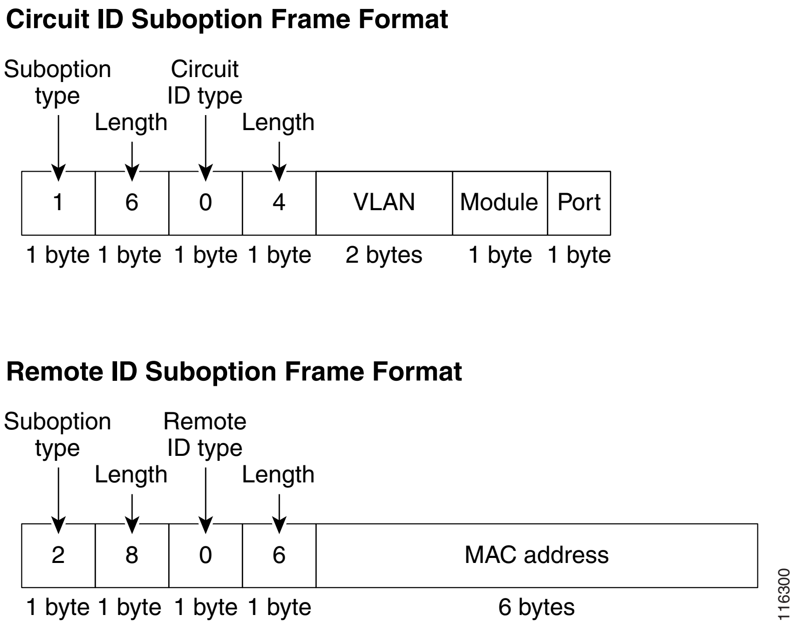
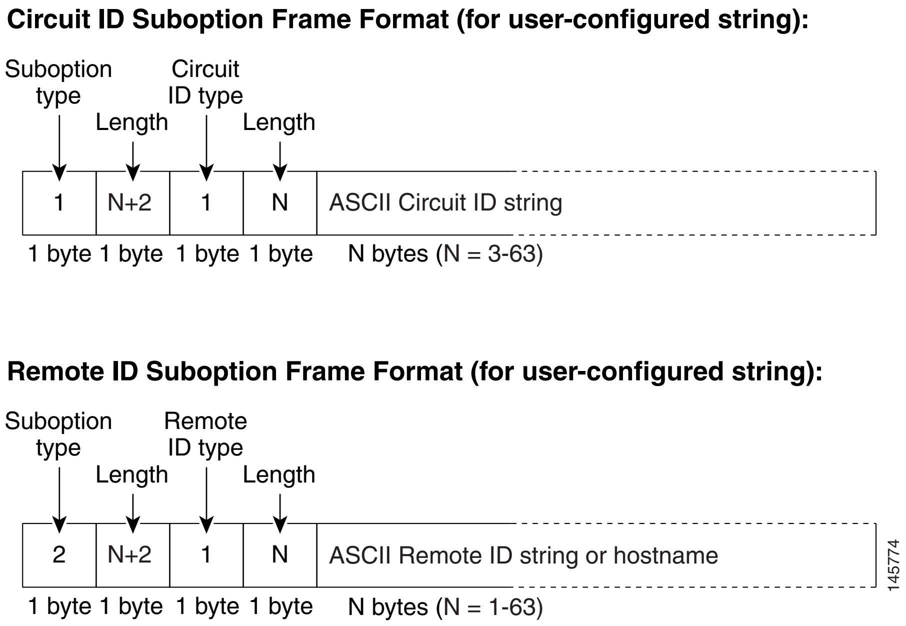


Figure 53-3 shows the packet formats for user-configured remote ID and circuit ID suboptions. The switch uses these packet formats when DHCP snooping is globally enabled and when the **ip dhcp snooping information option format remote-id** global configuration command and the **ip dhcp snooping vlan information option format-type circuit-id string** interface configuration command are entered.

The values for these fields in the packets change from the default values when you configure the remote ID and circuit ID suboptions:

- Circuit ID suboption fields
  - The circuit ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.
- Remote ID suboption fields
  - The remote ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.

Figure 53-3 User-Configured Suboption Packet Formats


Circuit ID Suboption Frame Format (for user-configured string):
Suboption type
Length
Circuit ID type
Length
1
N+2
1
N
ASCII Circuit ID string
1 byte 1 byte 1 byte 1 byte
N bytes (N = 3-63)
Remote ID Suboption Frame Format (for user-configured string):
Suboption type
Length
Remote ID type
Length
2
N+2
1
N
ASCII Remote ID string or hostname
1 byte 1 byte 1 byte 1 byte
N bytes (N = 1-63)
145774

Configuring DHCP Snooping

When you configure DHCP snooping on your switch, you are enabling the switch to differentiate untrusted interfaces from trusted interfaces. You must enable DHCP snooping globally before you can use DHCP snooping on a VLAN. You can enable DHCP snooping independently from other DHCP features.

These sections describe how to configure DHCP snooping:

- Default Configuration for DHCP Snooping, page 53-7
- Enabling DHCP Snooping, page 53-7

- Enabling DHCP Snooping on the Aggregation Switch, page 53-9
- Enabling DHCP Snooping and Option 82, page 53-10
- Enabling DHCP Snooping on Private VLAN, page 53-12
- Configuring DHCP Snooping on Private VLAN, page 53-12
- Configuring DHCP Snooping with an Ethernet Channel Group, page 53-12
- Enabling the DHCP Snooping Database Agent, page 53-13
- Limiting the Rate of Incoming DHCP Packets, page 53-13
- Configuration Examples for the Database Agent, page 53-15

Note For DHCP server configuration information, refer to "Configuring DHCP" in the *Cisco IOS IP and IP Routing Configuration Guide* at:

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html

Default Configuration for DHCP Snooping

DHCP snooping is disabled by default. Table 53-1 shows all the default configuration values for each DHCP snooping option.

Table 53-1 Default Configuration Values for DHCP Snooping

Option	Default Value/State
DHCP snooping	Disabled
DHCP snooping information option	Enabled
DHCP snooping information option allow-untrusted	Disabled
DHCP snooping limit rate	Infinite (functions as if rate limiting were disabled)
DHCP snooping trust	Untrusted
DHCP snooping vlan	Disabled

If you want to change the default configuration values, see the "Enabling DHCP Snooping" section.

Enabling DHCP Snooping

Note When DHCP snooping is enabled globally, DHCP requests are dropped until the ports are configured. Consequently, you should probably configure this feature during a maintenance window and not during production.

To enable DHCP snooping, perform this task:

	Command	Purpose
Step 1	Switch(config)# **ip dhcp snooping**	Enables DHCP snooping globally. You can use the **no** keyword to disable DHCP snooping.
Step 2	Switch(config)# **ip dhcp snooping vlan** *number* [*number*] | **vlan** {*vlan range*}]	Enables DHCP snooping on your VLAN or VLAN range.
Step 3	Switch(config)# **errdisable recovery** {**cause dhcp-rate-limit** | **interval** *interval*}	(Optional) Configures the amount of time required for recovery from a specified errdisable cause.
Step 4	Switch(config)# **errdisable detect cause dhcp-rate-limit** {**action shutdown vlan**}	(Optional) Enables per-VLAN errdisable detection. **Note** By default this command is enabled, and when a violation occurs the interface is shutdown.
Step 5	Switch(config-if)# **ip dhcp snooping trust**	Configures the interface as trusted or untrusted. You can use the **no** keyword to configure an interface to receive messages from an untrusted client.
Step 6	Switch(config-if)# **ip dhcp snooping limit rate** *rate*	Configures the number of DHCP packets per second (pps) that an interface can receive.[1]
Step 7	Switch(config)# **end**	Exits configuration mode.
Step 8	Switch# **show ip dhcp snooping**	Verifies the configuration.

[1] We recommend not configuring the untrusted interface rate limit to more than 100 packets per second. The recommended rate limit for each untrusted client is 15 packets per second. Normally, the rate limit applies to untrusted interfaces. If you want to set up rate limiting for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value. You should fine tune this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate of more than 1,000 packets per second.

You can configure DHCP snooping for a single VLAN or a range of VLANs. To configure a single VLAN, enter a single VLAN number. To configure a range of VLANs, enter a beginning and an ending VLAN number or a dash and range of VLANs.

The number of incoming DHCP packets is rate-limited to prevent a denial-of-service attack. When the rate of incoming DHCP packets exceeds the configured limit, the switch places the port in the errdisabled state. To prevent the port from shutting down, you can use the **errdisable detect cause dhcp-rate-limit action shutdown vlan** global configuration command to shut down just the offending VLAN on the port where the violation occurred.

When a secure port is in the errdisabled state, you can bring it out of this state automatically by configuring the **errdisable recovery cause dhcp-rate-limit** global configuration command or you can manually reenable it by entering the **shutdown** and **no shut down** interface configuration commands. If a port is in per-VLAN errdisable mode, you can also use **clear errdisable interface** *name* **vlan** *range* command to reenable the VLAN on the port.

This example shows how to enable DHCP snooping on VLAN 500 through 555:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
500,555
DHCP snooping is operational on following VLANs:
500,555
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
    circuit-id default format: vlan-mod-port
    remote-id: switch123 (string)
Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled DHCP
snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
 ------------------------     -------     ----------------
FastEthernet5/1              yes         100
  Custom circuit-ids:
    VLAN 555: customer-555
FastEthernet2/1              no          unlimited
  Custom circuit-ids:
    VLAN 500: customer-500

Switch#
```

The following configuration describes the DHCP snooping configuration steps if routing is defined on another Catalyst switch (for example, a Catalyst 6500 series switch):

```
// Trust the uplink gigabit Ethernet trunk port

interface range GigabitEthernet 1/1 – 2
switchport mode trunk
switchport trunk encapsulation dot1q
ip dhcp snooping trust

!

interface VLAN 14
ip address 10.33.234.1 255.255.254.0
ip helper-address 10.5.1.2
```

Note If you are enabling trunking on uplink gigabit interfaces, and the above routing configuration is defined on a Catalyst 6500 series switch, you must configure the “trust” relationship with downstream DHCP snooping (on a Catalyst 4500 series switch) which adds Option 82. On a Catalyst 6500 series switch, this task is accomplished with the **ip dhcp relay information trusted** VLAN configuration command.

Enabling DHCP Snooping on the Aggregation Switch

To enable DHCP snooping on an aggregation switch, configure the interface connecting to a downstream switch as a snooping untrusted port. If the downstream switch (or a device such as a DSLAM in the path between the aggregation switch and the DHCP clients) adds DHCP information Option 82 to the DHCP packets, the DHCP packets would be dropped on arriving on a snooping untrusted port. If you configure the **ip dhcp snooping information option allow-untrusted** global configuration command on the aggregation switch, the aggregation switch can accept DHCP requests with Option 82 information from any snooping untrusted port.

Enabling DHCP Snooping and Option 82

To enable DHCP snooping and Option 82 on the switch, perform the following steps:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(config)# **ip dhcp snooping**	Enables DHCP snooping globally.
Step 3	Switch(config)# **ip dhcp snooping vlan** *vlan-range*	Enables DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
Step 4	Switch(config)# **ip dhcp snooping information option**	Enables the switch to insert and remove DHCP relay information (Option 82 field) in forwarded DHCP request messages to the DHCP server. it is the default setting.
Step 5	Switch(config)# **ip dhcp snooping information option format remote-id [string** *ASCII-string* **|** hostname]	(Optional) Configures the remote ID suboption. You can configure the remote ID to be: • String of up to 63 ASCII characters (no spaces) • Configured hostname for the switch If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote ID configuration. The default remote ID is the switch MAC address.
Step 6	Switch(config)# **ip dhcp snooping information option allow-untrusted**	(Optional) If the switch is an aggregation switch connected to an edge switch, enables the switch to accept incoming DHCP snooping packets with Option 82 information from the edge switch. The default setting is disabled. **Note** Enter this command only on aggregation switches that are connected to trusted devices.
Step 7	Switch(config)# **interface** *interface-id*	Specifies the interface to be configured, and enter interface configuration mode.
Step 8	Switch(config-if)# **ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string*	(Optional) Configures the circuit ID suboption for the specified interface. Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094. The default circuit ID is the port identifier, in the format **vlan-mod-port.** You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces). Optional) Use the **override** keyword when you do not want the circuit-ID suboption inserted in TLV format to define subscriber information.

	Command	Purpose
Step 9	`Switch(config-if)# ip dhcp snooping trust`	(Optional) Configures the interface as trusted or untrusted. You can use the **no** keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.
Step 10	`Switch(config-if)# ip dhcp snooping limit rate rate`	(Optional) Configures the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured. **Note** We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one VLAN on which DHCP snooping is enabled.
Step 11	`Switch(config-if)# exit`	Returns to global configuration mode.
Step 12	`Switch(config)# ip dhcp snooping verify mac-address`	(Optional) Configures the switch to verify that the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.
Step 13	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 14	`Switch# show running-config`	Verifies your entries.
Step 15	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To disable DHCP snooping, use the **no ip dhcp snooping** global configuration command. To disable DHCP snooping on a VLAN or range of VLANs, use the **no ip dhcp snooping vlan** *vlan-range* global configuration command. To disable the insertion and removal of the Option 82 field, use the **no ip dhcp snooping information option** global configuration command. To configure an aggregation switch to drop incoming DHCP snooping packets with Option 82 information from an edge switch, use the **no ip dhcp snooping information option allow-untrusted** global configuration command.

This example shows how to enable DHCP snooping globally and on VLAN 10 and to configure a rate limit of 100 packets per second on a port:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

The following example shows how to enable DHCP snooping on VLAN 500 through 555 and option 82 circuit-id:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end
```

This example shows how to configure the Option 82 circuit-ID override suboption:

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

Enabling DHCP Snooping on Private VLAN

DHCP snooping can be enabled on private VLANs, which provide isolation between Layer 2 ports within the same VLAN. If DHCP snooping is enabled (or disabled), the configuration is propagated to both the primary VLAN and its associated secondary VLANs. You cannot enable (or disable) DHCP snooping on a primary VLAN without reflecting this configuration change on the secondary VLANs.

Configuring DHCP snooping on a secondary VLAN is still allowed, but it does not take effect if the associated primary VLAN is already configured. If the associated primary VLAN is configured, the effective DHCP snooping mode on the secondary VLAN is derived from the corresponding primary VLAN. Manually configuring DHCP snooping on a secondary VLAN causes the switch to issue this warning message:

```
DHCP Snooping configuration may not take effect on secondary vlan XXX
```

The **show ip dhcp snooping** command displays all VLANs (both primary and secondary) that have DHCP snooping enabled.

Configuring DHCP Snooping on Private VLAN

DHCP snooping, IPSG, and DAI are Layer 2-based security features that can be enabled and disabled on an individual VLAN, including auxiliary or voice VLAN. You need to enable DHCP snooping on a voice VLAN for a Cisco IP phone to function properly.

Configuring DHCP Snooping with an Ethernet Channel Group

When you configure DHCP snooping, you need to configure trunk interfaces that transmit DHCP packets as trusted interfaces by adding **ip dhcp snooping trust** to the physical interface configuration. However, if DHCP packets will be transmitted over an Ethernet channel group, you must configure **ip dhcp snooping trust** on the logical port channel interface, for example:

```
Switch# show run int port-channel50
Building configuration...

Current configuration : 150 bytes
!
interface Port-channel50
 switchport
 switchport trunk native vlan 4092
 switchport mode trunk
 switchport nonegotiate
 ip dhcp snooping trust
end

Switch#
```

Enabling the DHCP Snooping Database Agent

To configure the database agent, perform one or more of the following tasks:

Command	Purpose
Switch(config)# **ip dhcp snooping database {***url* | **write-delay *seconds*** | **timeout** *seconds***}** Switch(config)# **no ip dhcp snooping database [write-delay | timeout]**	(Required) Configures a URL for the database agent (or file) and the related timeout values.
Switch# **show ip dhcp snooping database [detail]**	(Optional) Displays the current operating state of the database agent and statistics associated with the transfers.
Switch# **clear ip dhcp snooping database statistics**	(Optional) Clears the statistics associated with the database agent.
Switch# **renew ip dhcp snooping database [validation none] [***url***]**	(Optional) Requests the read entries from a file at the given URL.
Switch# **ip dhcp snooping binding** *mac-addr* **vlan** *vlan ipaddr* **interface** *ifname* expiry *lease-in-seconds* Switch# **no ip dhcp snooping binding** *mac-addr* **vlan** *vlan ipaddr* **interface** *ifname*	(Optional) Adds or deletes bindings to the snooping database.

Note Because both NVRAM and bootflash have limited storage capacity, you should use TFTP or network-based files. If you use flash to store the database file, new updates (by the agent) result in the creation of new files (flash fills quickly). Moreover, because of the nature of the file system used on flash, a large number of files can cause slow access. When a file is stored in a remote location accessible through TFTP, an RPR or SSO standby supervisor engine can take over the binding list when a switchover occurs.

Note Network-based URLs (such as TFTP and FTP) require that you create an empty file at the configured URL before the switch can write the set of bindings for the first time.

Limiting the Rate of Incoming DHCP Packets

The switch CPU performs DHCP validation checks; therefore, the number of incoming DHCP packets is rate-limited to prevent a denial-of-service attack.

When the rate of incoming DHCP packets exceeds the configured limit, the switch places the port in the errdisabled state. The port remains in that state until you intervene or you enable errdisable recovery so that ports automatically emerge from this state after a specified timeout period.

Note Unless you explicitly configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip dhcp snooping limit rate** interface configuration command, the interface reverts to its default rate limit.

To prevent the port from shutting down, you can use the **errdisable detect cause dhcp-rate-limit action shutdown vlan** global configuration command to shut down just the offending VLAN on the port where the violation occurred.

To limit the rate of incoming DHCP packets, perform this task:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(config)# **errdisable detect cause dhcp-rate-limit** [**action shutdown vlan**]	Enables per-VLAN errdisable detection.
Step 3	Switch(config)# **interface** *interface-id*	Specifies the interface to be rate-limited, and enter interface configuration mode.
Step 4	Switch(config-if)# [**no**] **ip dhcp snooping limit** *rate*	Limits the rate of incoming DHCP requests and responses on the interface. The default rate is disabled.
Step 5	Switch(config-if)# **exit**	Returns to global configuration mode.
Step 6	Switch(config)# **errdisable recovery** {**cause dhcp-rate-limit** | **interval** *interval*}	(Optional) Enables error recovery from the DHCP errdisable state. By default, recovery is disabled, and the recovery interval is 300 seconds. For **interval** *interval*, specify the time in seconds to recover from the errdisable state. The range is 30 to 86400.
Step 7	Switch(config)# **exit**	Returns to privileged EXEC mode.
Step 8	Switch# **show interfaces status**	Verifies your settings.
Step 9	Switch# **show errdisable recovery**	Verifies your settings.
Step 10	Switch# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return to the default rate-limit configuration, use the **no ip dhcp-rate-limit** interface configuration command. To disable error recovery for DHCP inspection, use the **no errdisable recovery cause dhcp-rate-limit** global configuration command.

This example shows how to set an upper limit for the number of incoming packets (100 pps) and to specify a burst interval (1 second):

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface g3/31
Switch(config-if)# ip dhcp-rate-limit rate 100 burst interval 1
Switch(config-if)# exit
Switch(config)# errdisable recovery cause dhcp-rate-limit
Switch(config)# exit
Switch# show interfaces status

Port    Name               Status     Vlan       Duplex Speed Type
Te1/1                      connected  1          full   10G   10GBase-LR
Te1/2                      connected  vl-err-dis full   10G   10GBase-LR
```

```
SwitchB# show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Enabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

SwitchB#
1w2d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 101 packets received in 739 milliseconds on Gi3/31.
1w2d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/31, putting Gi3/31 in
err-disable state
SwitchB# show clock
*02:21:43.556 UTC Fri Feb 4 2005
SwitchB#
SwitchB# show interface g3/31 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi3/31                       err-disabled 100          auto   auto 10/100/1000-TX
SwitchB#
SwitchB#
1w2d: %PM-4-ERR_RECOVER: Attempting to recover from arp-inspection err-disable state on
Gi3/31
SwitchB# show interface g3/31 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi3/31                       connected    100        a-full  a-100 10/100/1000-TX
SwitchB# show clock
*02:27:40.336 UTC Fri Feb 4 2005
SwitchB#
```

Configuration Examples for the Database Agent

The following examples show how to configuration commands in the previous procedure:

Example 1: Enabling the Database Agent

The following example shows how to configure the DHCP snooping database agent to store the bindings at a given location and to view the configuration and operating state:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
```

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0

Switch#
```

The first three lines of output show the configured URL and related timer configuration values. The next three lines show the operating state and the amount of time left for expiry of write delay and abort timers.

Among the statistics shown in the output, startup failures indicate the number of attempts the read or create of the file has failed upon bootup.

Note Because the location is based off in the network, you must create a temporary file on the TFTP server. You can create a temporary file on a typical UNIX workstation by creating a 0 byte file "file" in the directory "directory" that can be referenced by the TFTP server daemon. With some server implementations on UNIX workstations, the file should be provided with full (777) permissions for write access to the file.

DHCP snooping bindings are keyed on the MAC address and VLAN combination. If an entry in the remote file has an entry for a given MAC address and VLAN set, for which the switch already has a binding, the entry from the remote file is ignored when the file is read. This condition is referred to as the binding collision.

An entry in a file may no longer be valid because the lease indicated by the entry may have expired by the time it is read. The expired leases counter indicates the number of bindings ignored because of this condition. The Invalid interfaces counter refers to the number of bindings that have been ignored when the interface referred by the entry either does not exist on the system or is a router or DHCP snooping trusted interface if it exists, when the read happened. Unsupported VLANs refers to the number of entries that have been ignored because the indicated VLAN is not supported on the system. The Parse failures counter provides the number of entries that have been ignored when the switch is unable to interpret the meaning of the entries from the file.

The switch maintains two sets of counters for these ignored bindings. One provides the counters for a read that has at least one binding ignored by at least one of these conditions. These counters are shown as the "Last ignored bindings counters." The total ignored bindings counters provides a sum of the number of bindings that have been ignored because of all the reads since the switch bootup. These two set of counters are cleared by the **clear** command. The total counter set may indicate the number of bindings that have been ignored since the last clear.

Example 2: Reading Binding Entries from a TFTP File

To manually read the entries from a TFTP file, perform this task:

	Command	Purpose
Step 1	`Switch#` **`show ip dhcp snooping database`**	Displays the DHCP snooping database agent statistics.
Step 2	`Switch#` **`renew ip dhcp snoop data`** *`url`*	Directs the switch to read the file from given URL.
Step 3	`Switch#` **`show ip dhcp snoop data`**	Displays the read status.
Step 4	`Switch#` **`show ip dhcp snoop bind`**	Verifies whether the bindings were read successfully.

it is an example of how to manually read entries from the tftp://10.1.1.1/directory/file:

```
Switch# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Switch#
Switch# renew ip dhcp snoop data tftp://10.1.1.1/directory/file
Loading directory/file from 10.1.1.1 (via GigabitEthernet1/1): !
[OK - 457 bytes]
Database downloaded successfully.

Switch#
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Read
succeeded.
Switch#
Switch# show ip dhcp snoop data
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
```

```
Last Succeded Time : 15:24:34 UTC Sun Jul 8 2001
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        1   Startup Failures :        0
Successful Transfers :        1   Failed Transfers :        0
Successful Reads     :        1   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Switch#
Switch# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:05   1.1.1.1          49810       dhcp-snooping  512   GigabitEthernet1/1
00:01:00:01:00:02   1.1.1.1          49810       dhcp-snooping  512   GigabitEthernet1/1
00:01:00:01:00:04   1.1.1.1          49810       dhcp-snooping  1536  GigabitEthernet1/1
00:01:00:01:00:03   1.1.1.1          49810       dhcp-snooping  1024  GigabitEthernet1/1
00:01:00:01:00:01   1.1.1.1          49810       dhcp-snooping  1     GigabitEthernet1/1
Switch#
Switch# clear ip dhcp snoop bind
Switch# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Switch#
```

Example 3: Adding Information to the DHCP Snooping Database

To manually add a binding to the DHCP snooping database, perform this task:

	Command	Purpose
Step 1	`Switch# show ip dhcp snooping binding`	Views the DHCP snooping database.
Step 2	`Switch# ip dhcp snooping binding` *binding-id* **vlan** *vlan-id* **interface** *interface* **expiry** *lease-time*	Adds the binding using the **ip dhcp snooping** EXEC command.
Step 3	`Switch# show ip dhcp snooping binding`	Checks the DHCP snooping database.

This example shows how to manually add a binding to the DHCP snooping database:

```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Switch#
Switch# ip dhcp snooping binding 1.1.1 vlan 1 1.1.1.1 interface gi1/1 expiry 1000

Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:01   1.1.1.1          992         dhcp-snooping  1     GigabitEthernet1/1
Switch#
```

Displaying DHCP Snooping Information

You can display a DHCP snooping binding table and configuration information for all interfaces on a switch.

Displaying a Binding Table

The DHCP snooping binding table for each switch contains binding entries that correspond to untrusted ports. The table does not contain information about hosts interconnected with a trusted port because each interconnected switch has its own DHCP snooping binding table.

This example shows how to display the DHCP snooping binding information for a switch:

```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6943        dhcp-snooping  10    FastEthernet6/10
Switch#
```

Table 53-2 describes the fields in the **show ip dhcp snooping binding** command output.

Table 53-2 show ip dhcp snooping binding Command Output

Field	Description
MAC Address	Client hardware MAC address
IP Address	Client IP address assigned from the DHCP server
Lease (seconds)	IP address lease time
Type	Binding type; dynamic binding learned by DHCP snooping or statically-configured binding.
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host

Displaying the DHCP Snooping Configuration

This example shows how to display the DHCP snooping configuration for a switch:

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
    10 30-40 100 200-220
Insertion of option 82 is enabled
Option82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface           Trusted        Rate limit (pps)
---------           -------        ----------------
FastEthernet2/1     yes            10
FastEthernet3/1     yes            none
GigabitEthernet1/1  no             20
Switch#
```

About IP Source Guard

The IP source guard feature is enabled on a DHCP snooping untrusted Layer 2 port. Initially, all IP traffic on the port is blocked except for DHCP packets that are captured by the DHCP snooping process. When a client receives a valid IP address from the DHCP server, or when you configure a static IP source binding, a per-port and VLAN access control list (VACL) is installed on the port. This process restricts the client IP traffic to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address.

Note If IP source guard is enabled on a trunk port with a large number of VLANs that have DHCP snooping enabled, you might exhaust ACL hardware resources, and some packets might be switched in software instead.

Note When IP source guard is enabled, you might want to designate an alternative scheme for ACL hardware programming. For more information, see the "TCAM Programming and ACLs" section in Chapter 54, "Configuring Network Security with ACLs".

Note When an interface is in down state, TCAMs are consumed for PACLs, but not for RACLs.

IP source guard supports the Layer 2 port only, including both access and trunk. For each untrusted Layer 2 port, there are two levels of IP traffic security filtering:

- Source IP address filter

  IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted.

  An IP source address filter is changed when a new IP source entry binding is created or deleted on the port. The port VACL is recalculated and reapplied in the hardware to reflect the IP source binding change. By default, if the IP filter is enabled without any IP source binding on the port, a default PVACL that denies all IP traffic is installed on the port. Similarly, when the IP filter is disabled, any IP source filter PVACL is removed from the interface.

- Source IP and MAC address filter

  IP traffic is filtered based on its source IP address as well as its MAC address; only IP traffic with source IP and MAC addresses matching the IP source binding entry are permitted.

Note When IP source guard is enabled in IP and MAC filtering mode, the DHCP snooping Option 82 must be enabled to ensure that the DHCP protocol works properly. Without Option 82 data, the switch cannot locate the client host port to forward the DHCP server reply. Instead, the DHCP server reply is dropped, and the client cannot obtain an IP address.

Configuring IP Source Guard

To enable IP source guard, perform this task:

	Command	Purpose
Step 1	`Switch(config)# ip dhcp snooping`	Enables DHCP snooping globally. You can use the **no** keyword to disable DHCP snooping.
Step 2	`Switch(config)# ip dhcp snooping vlan number [number]`	Enables DHCP snooping on your VLANs.

	Command	Purpose
Step 3	Switch(config-if)# **no ip dhcp snooping trust**	Configures the interface as trusted or untrusted. You can use the **no** keyword of to configure an interface to receive only messages from within the network.
Step 4	Switch(config-if)# **ip verify source vlan dhcp-snooping port-security**	Enables IP source guard, source IP, and source MAC address filtering on the port.
Step 5	Switch(config-if)# **switchport port-security limit rate invalid-source-mac N**	Enables security rate limiting for learned source MAC addresses on the port. **Note** This limit only applies to the port where IP source guard is enabled as filtering both IP and MAC addresses.
Step 6	Switch(config)# **ip source binding** *mac-address* **Vlan** *vlan-id ip-address* **interface** *interface-name*	Configures a static IP binding on the port.
Step 7	Switch(config)# **end**	Exits configuration mode.
Step 8	Switch# **show ip verify source interface** *interface-name*	Verifies the configuration.

If you want to stop IP source guard with static hosts on an interface, use the following commands in interface configuration submode:

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

If the **no ip device tracking** command is used in interface configuration submode, it actually runs in global configuration mode and causes IP device tracking to be disabled globally. Disabling IP device tracking globally causes IP source guard with static hosts to deny all IP traffic on interfaces using the **ip verify source tracking** [**port-security**] command.

Note The static IP source binding can only be configured on switch port. If you enter the **ip source binding vlan interface** command on a Layer 3 port, you receive this error message:

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

This example shows how to enable per-Layer 2 port IP source guard on VLAN 10 through 20:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface fa6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
```

```
Switch# show ip verify source interface f6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa6/1      ip-mac       active       10.0.0.1                            10
Fa6/1      ip-mac       active       deny-all                            11-20
Switch#
```

The output shows that there is one valid DHCP binding to VLAN 10.

Configuring IP Source Guard on Private VLANs

For IP source guard to be effective on PVLAN ports, you must enable DHCP snooping on primary VLANs. IP source guard on a primary VLAN is automatically propagated to a secondary VLAN. You can configure static IP source binding on a secondary VLAN, but it does not work. When manually configuring a static IP source binding on a secondary VLAN, you receive the following message:

```
IP source filter may not take effect on a secondary VLAN where IP source binding is
configured. If the private VLAN feature is enabled, IP source filter on the primary VLAN
will automatically propagate to all secondary VLAN.
```

Note IP Source Guard is supported on private VLAN host ports only.

Displaying IP Source Guard Information

You can display IP source guard PVACL information for all interfaces on a switch using the **show ip verify source** command, as the following examples show:

- This example shows displayed PVACLs if DHCP snooping is enabled on VLAN 10 through 20, if interface fa6/1 is configured for IP filtering, and if there is an existing IP address binding 10.0.01 on VLAN 10:

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/1      ip           active       10.0.0.1                         10
fa6/1      ip           active       deny-all                         11-20
```

Note The second entry shows that a default PVACL (deny all IP traffic) is installed on the port for those snooping-enabled VLANs that do not have a valid IP source binding.

- This example shows displayed PVACL for a trusted port:

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/2      ip           inactive-trust-port
```

- This example shows displayed PVACL for a port in a VLAN not configured for DHCP snooping:

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/3      ip           inactive-no-snooping-vlan
```

- This example shows displayed PVACLs for a port with multiple bindings configured for an IP-to-MAC filtering:

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip-mac       active       deny-all         deny-all        12-20
```

- This example shows displayed PVACLs for a port configured for IP-to-MAC filtering but not for port security:

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/5      ip-mac       active       10.0.0.3         permit-all      10
fa6/5      ip-mac       active       deny-all         permit-all      11-20
```

Note The MAC filter shows permit-all because port security is not enabled, so the MAC filter cannot apply to the port or VLAN and is effectively disabled. Always enable port security first.

- This example shows displayed error message when entering the **show ip verify source** command on a port that does not have an IP source filter mode configured:

```
IP Source Guard is not configured on the interface fa6/6.
```

You can also use the **show ip verify source** command to display all interfaces on the switch that have IP source guard enabled, as follows:

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/1      ip           active       10.0.0.1                         10
fa6/1      ip           active       deny-all                         11-20
fa6/2      ip           inactive-trust-port
fa6/3      ip           inactive-no-snooping-vlan
fa6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip-mac       active       deny-all         deny-all        12-20
fa6/5      ip-mac       active       10.0.0.3         permit-all      10
fa6/5      ip-mac       active       deny-all         permit-all      11-20
```

Displaying IP Source Binding Information

You can display all IP source bindings configured on all interfaces on a switch using the **show ip source binding** command.

```
Switch# show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6522        dhcp-snooping  10    FastEthernet6/10
00:00:00:0A:00:0B   11.0.0.1         infinite    static         10    FastEthernet6/10
Switch#
```

Table 53-3 describes the fields in the **show ip source binding** command output.

Table 53-3 show ip source binding Command Output

Field	Description
MAC Address	Client hardware MAC address
IP Address	Client IP address assigned from the DHCP server
Lease (seconds)	IP address lease time
Type	Binding type; static bindings configured from CLI to dynamic binding learned from DHCP snooping
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host

Configuring IP Source Guard for Static Hosts

Note IPSG for static hosts should not be used on uplink ports.

IP source guard (IPSG) for static hosts extends the IPSG capability to non-DHCP and static environments.

This section includes these topics:

- About IP Source Guard for Static Hosts, page 53-24
- Configuring IPSG for Static Hosts on a Layer 2 Access Port, page 53-25
- Configuring IPSG for Static Hosts on a PVLAN Host Port, page 53-28

About IP Source Guard for Static Hosts

The prior feature, IPSG, uses the entries created by the DHCP snooping feature to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. A DHCP environment is a prerequisite for IPSG to work. The IPSG for static hosts feature removes IPSG' dependency on DHCP. The switch creates static entries based on ARP requests or other IP packets and uses them to maintain the list of valid hosts for a given port. In addition, you can specify the number of hosts that would be allowed to send traffic to a given port. it is equivalent to port security at Layer 3.

Note Some IP hosts with multiple network interfaces may inject some invalid packets into a network interface. Those invalid packets contain the IP-to-MAC address for another network interface of that host as the source address. It may cause IPSG for static hosts in the switch, which connects to the host, to learn the invalid IP-to-MAC address bindings and reject the valid bindings. You should consult the vendor of the corresponding operating system and the network device of that host to prevent it from injecting invalid packets.

IPSG for static hosts initially learns IP-to-MAC bindings dynamically through an ACL-based snooping method. IP-to-MAC bindings are learned from static hosts by using ARP and IP packets and are stored using the device tracking database. Once the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum limit, any packet with a new IP address is dropped in hardware. To handle hosts that have moved or gone away for any reason, the IPSG for static hosts feature uses the IP device tracking functionality to age out dynamically learned IP address bindings. This feature can be used in conjunction with DHCP snooping. Multiple bindings will be established on a port that is connected to both DHCP and static hosts (that is, bindings will be stored in both the device tracking database as well as the DHCP snooping binding database).

Configuring IPSG for Static Hosts on a Layer 2 Access Port

You can configure IPSG for static hosts on a Layer 2 access port.

To enable IPSG for static hosts with IP filters on a Layer 2 access port, perform this task:

	Command	Purpose
Step 1	Switch(config)# **ip device tracking**	Turns on the IP host table.
Step 2	Switch(config)# **ip device tracking** [**probe** {**count** *count* | interval *interval*}]	(Optional) Configures these parameters for the IP device tracking table: • **count—**Number of times that the switch sends the ARP probe. The range is 1 to 5. The default is 3. • **interval—**Number of seconds that the switch waits for a response before resending the ARP probe. The range is 30 to 300 seconds. The default is 30 seconds.
Step 3	Switch(config)# **ip device tracking** [**probe** {*delay interval*}]	(Optional) Configures the optional probe delay parameter for the IP device tracking table: • **interval**—Number of seconds that the switch delays sending an ARP probe, triggered by link-up and ARP probe generation by the tracked device. The range is 1 to 120 seconds. The default is 0 seconds.
Step 4	Switch(config)# **interface fastEthernet** *a/b*	Enters IP configuration mode.
Step 5	Switch(config-if)# **switchport mode access**	Configures a port as access.
Step 6	Switch(config-if)# **switchport access vlan** *n*	Configures the VLAN for this port.
Step 7	Switch(config-if)# **ip device tracking maximum** *n*	Establishes a maximum limit for the bindings on this port. Upper bound for the maximum is 10.
Step 8	Switch(config-if)# **switchport port-security**	(Optional) Activates port security for this port.
Step 9	Switch(config-if)# **switchport port-security maximum** *n*	(Optional) Establishes a maximum number of MAC addresses for this port.
Step 10	Switch(config-if)# **ip verify source tracking** [**port-security**]	Activates IPSG for static hosts on this port.
Step 11	Switch(config-if)# **end**	Exits configuration interface mode.

	Command	Purpose
Step 12	`Switch# show ip verify source interface-name`	Verifies the configuration.
Step 13	`Switch# show ip device track all [active | inactive] count`	Verifies the configuration by displaying the IP-to-MAC binding for a given host on the switch interface. • **all active—**Displays only the active IP-to-MAC binding entries. • **all inactive—**Displays only the inactive IP-to-MAC binding entries. • **all**—Displays the active and inactive IP-to-MAC binding entries.

To stop IPSG with static hosts on an interface, use the following commands in interface configuration submode:

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

To enable IPSG with static hosts on a port, enter the following commands:

```
Switch(config)# ip device tracking ****enable IP device tracking globally
Switch(config)# ip device tracking max <n> ****set an IP device tracking maximum on int
Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on the port
```

Caution If you only configure the **ip verify source tracking [port-security]** interface configuration 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 issue also applies to IPSG with static hosts on a PVLAN host port.

This example shows how to enable IPSG for static hosts with IP filters on a Layer 2 access port and to verify the three valid IP bindings on the interface Fa4/3:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
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
---------  -----------  -----------  ---------------  -----------------  ----
Fa4/3      ip trk       active       40.1.1.24                           10
Fa4/3      ip trk       active       40.1.1.20                           10
Fa4/3      ip trk       active       40.1.1.21                           10
```

The following example shows how to enable IPSG for static hosts with IP MAC filters on a Layer 2 access port, to verify the five valid IP-MAC bindings on the interface Fa4/3, and to verify that the number of bindings on this interface has reached the maximum limit:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
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
---------  -----------  -----------  ---------------  -----------------  ----
Fa4/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Fa4/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Fa4/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Fa4/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Fa4/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1
```

The following example displays all IP-to-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 the current interface and connected to a different interface, a new IP-to-MAC binding entry is displayed as active as soon as the host is detected. The old entry for this host on the previous interface is now 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    GigabitEthernet3/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
```

The following example displays all active IP-to-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    GigabitEthernet4/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
```

The following example displays all inactive IP-to-MAC binding entries for all interfaces. The host was first learned on GigabitEthernet 3/1 then moved to GigabitEthernet 4/1. The IP-to-MAC binding entries learned on GigabitEthernet 3/1 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    GigabitEthernet3/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
```

The following example display 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
---------------------------------------------------------------------
Fa4/3                  5
```

Configuring IPSG for Static Hosts on a PVLAN Host Port

You can configure IPSG for static hosts on a PVLAN host port.

To enable IPSG for static hosts with IP filters on a PVLAN host port, perform this task:

	Command	Purpose
Step 1	Switch(config)# **vlan** *n1*	Enters configuration VLAN mode.
Step 2	Switch(config-vlan)# **private-vlan primary**	Establishes a primary VLAN on a PVLAN port.
Step 3	Switch(config-vlan)# **exit**	Exits VLAN configuration mode.
Step 4	Switch(config)# **vlan** *n2*	Enters configuration VLAN mode.
Step 5	Switch(config-vlan)# **private-vlan isolated**	Establishes an isolated VLAN on a PVLAN port.
Step 6	Switch(config-vlan)# **exit**	Exits VLAN configuration mode.
Step 7	Switch(config)# **vlan** *n1*	Enters configuration VLAN mode.
Step 8	Switch(config-vlan)# **private-vlan association 201**	Associates the VLAN on an isolated PVLAN port.
Step 9	Switch(config-vlan)# **exit**	Exits VLAN configuration mode.
Step 10	Switch(config)# **interface fastEthernet** *a/b*	Enters interface configuration mode.
Step 11	Switch(config-if)# **switchport mode private-vlan host**	(Optional) Establishes a port as a PVLAN host.
Step 12	Switch(config-if)# **switchport private-vlan host-association** a b	(Optional) Associates this port with the corresponding PVLAN.

	Command	Purpose
Step 13	`Switch(config-if)#` **`ip device tracking maximum`** *`n`*	Establishes a maximum limit for the bindings on this port.
Step 14	`Switch(config-if)#` **`ip verify source tracking`** `[`**`port-security`**`]`	Activates IPSG for static hosts on this port.
Step 15	`Switch(config-if)#` **`end`**	Exits configuration interface mode.
Step 16	`Switch#` **`show ip device tracking all`**	Verifies the configuration.
Step 17	`Switch#` **`show ip verify source`** *`interface-name`*	Verifies the configuration.

This example shows how to enable IPSG for static hosts with IP filters on a PVLAN 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)# int fastEthernet 4/3
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  FastEthernet4/3        ACTIVE
40.1.1.20       0000.0000.0305  200  FastEthernet4/3        ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet4/3        ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet4/3        ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet4/3        ACTIVE
```

The output shows the five valid IP-to-MAC bindings that have been learned on the interface Fa4/3. For the PVLAN, the bindings are associated with primary VLAN ID. 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
---------  -----------  -----------  ---------------  -----------------  ----
Fa4/3      ip trk       active       40.1.1.23                           200
Fa4/3      ip trk       active       40.1.1.24                           200
Fa4/3      ip trk       active       40.1.1.20                           200
Fa4/3      ip trk       active       40.1.1.21                           200
Fa4/3      ip trk       active       40.1.1.22                           200
Fa4/3      ip trk       active       40.1.1.23                           201
Fa4/3      ip trk       active       40.1.1.24                           201
Fa4/3      ip trk       active       40.1.1.20                           201
Fa4/3      ip trk       active       40.1.1.21                           201
Fa4/3      ip trk       active       40.1.1.22                           201
```

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