



# CHAPTER 19

## Configuring DHCP Features

This chapter describes how to configure DHCP snooping and the option-82 data insertion features on the Catalyst 3550 switch.



### Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release, and see the “DHCP Commands” section in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*.

This chapter consists of these sections:

- [Understanding DHCP Features, page 19-1](#)
- [Configuring DHCP Features, page 19-8](#)
- [Displaying DHCP Information, page 19-18](#)

## Understanding DHCP Features

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses.

The switch supports these DHCP features:

- [DHCP Server, page 19-2](#)
- [DHCP Relay Agent, page 19-2](#)
- [DHCP Snooping, page 19-2](#)
- [Option-82 Data Insertion, page 19-3](#)
- [Cisco IOS DHCP Server Database, page 19-7](#)
- [DHCP Snooping Binding Database, page 19-7](#)

For information about the DHCP client, see the “*Configuring DHCP*” section of the “*IP Addressing and Services*” section of the *Cisco IOS IP Configuration Guide, Release 12.2*.

## DHCP Server

The DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator.

## DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on egress interfaces.

## DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You can use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

**Note**

---

For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

---

An untrusted message is a message that is received from outside the network or firewall. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer's switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database contains the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not contain information regarding hosts interconnected with a trusted interface.

In a service-provider network, a trusted interface is connected to a port on a device in the same network. An untrusted interface is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCP OFFER, DHCP ACK, DHCP NAK, or DHCP REQUEST packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCP RELEASE or DHCP DECLINE broadcast message that contains a MAC address in the DHCP snooping binding table, but the interface information in the binding table does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes an relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.

If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When option-82 information is inserted by an edge switch in software releases earlier than Cisco IOS Release 12.1(22)EA3 or in Cisco IOS Release 12.2(25)SEA or later, you cannot configure DHCP snooping on an aggregation switch because the DHCP snooping bindings database is not properly populated. You also cannot configure IP source guard and dynamic Address Resolution Protocol (ARP) inspection on the switch unless you use static bindings or ARP access control lists (ACLs).

In Cisco IOS Release 12.1(22)EA3 and in Cisco IOS Release 12.2(25)SEA or later when an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the **ip dhcp snooping information option allow-untrusted** global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as dynamic ARP or IP source guard, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on ingress untrusted interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

## Option-82 Data Insertion

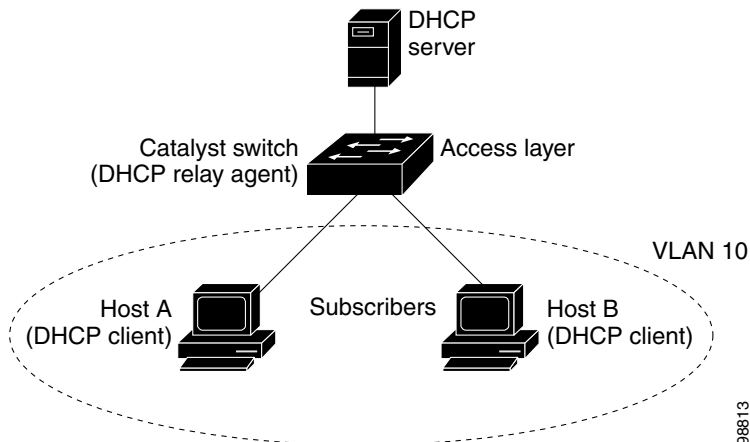
In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in 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

In Cisco IOS Release 12.1(19)EA1 or later, the DHCP option-82 feature is supported when DHCP snooping is enabled globally and on the VLANs to which subscriber devices using this feature are assigned. The switch also supports the DHCP option-82 feature when DHCP is disabled.

Figure 19-1 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 19-1 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 option-82 information contains the switch MAC address (the remote-ID suboption) and the port identifier, **vlan-mod-port** or **snmp-ifindex**, from which the packet is received (the circuit-ID suboption). Beginning with Cisco IOS Release 12.2(25)SEE, 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 19-15.
- If the IP address of the relay agent is configured, the switch adds the 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. Then the DHCP server 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. When the client and server are on the same subnet, the server broadcasts the reply. 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 of examples 1 and 2 in [Figure 19-2](#) 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

Example 3 in [Figure 19-2](#) shows the packet formats for user-configured remote-ID and circuit-ID suboptions. The switch uses these packet formats when you globally enable DHCP snooping and enter both 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.

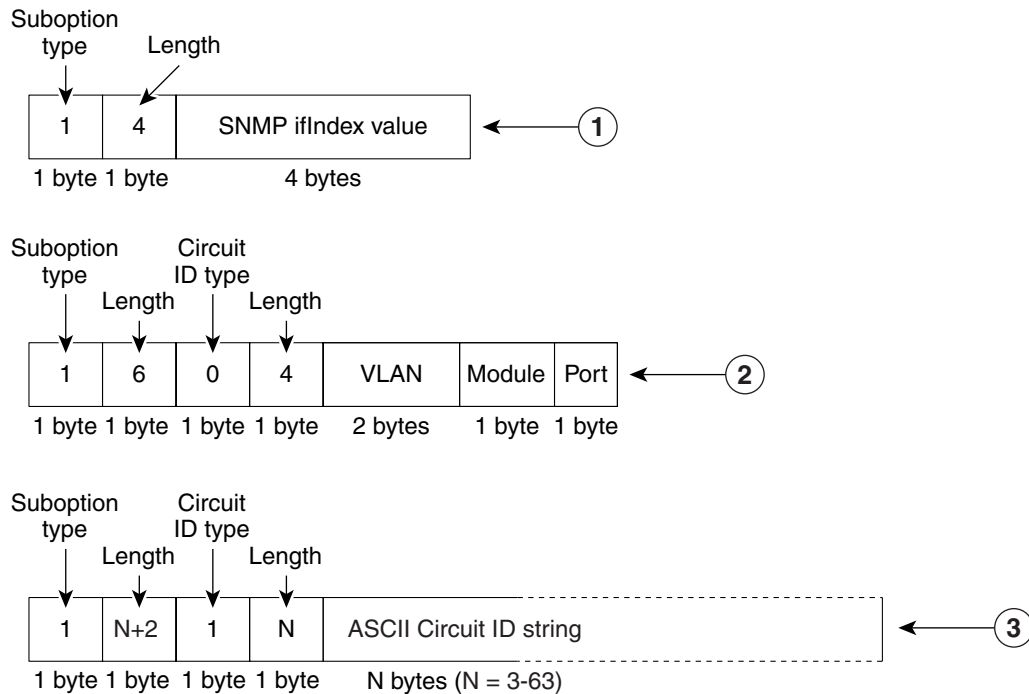
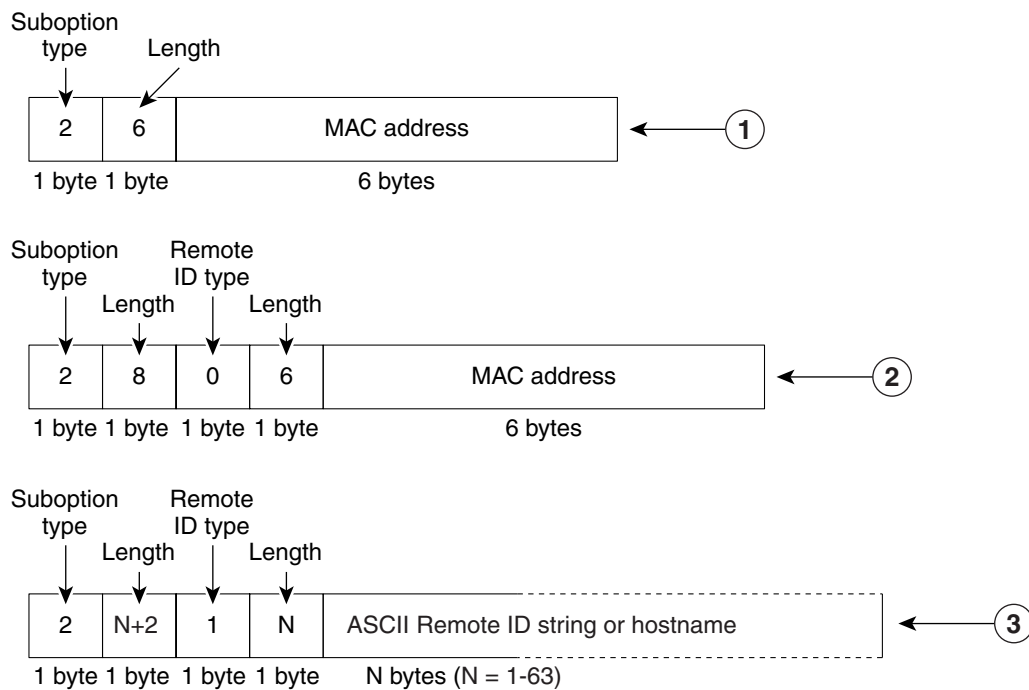
The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:

- 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.

When you globally enable DHCP snooping, and enter the **ip dhcp snooping information option** global configuration command, and do not configure the SNMP ifIndex format, the port numbers in the port field of the circuit-ID suboption start at 0. For example, on a Catalyst 3550-24 switch, port 0 is the Fast Ethernet 0/1 port, port 1 is the Fast Ethernet 0/2 port, port 2 is the Fast Ethernet 0/3 port, and so on. Port 24 is the Gigabit Interface Converter (GBIC)-based Gigabit module slot 0/1, and port 25 is the GBIC-based Gigabit module slot 0/2.

[Figure 19-2](#) shows the packet formats for the default and user-configured remote-ID suboption and circuit-ID suboption. For the circuit-ID suboption, the module field is always zero.

**Figure 19-2 Suboption Packet Formats****Circuit ID Suboption Frame Format****Remote ID Suboption Frame Format**

145775

|   |   |
|---|---|
| 1 | When you globally enable DHCP snooping, and enter the <b>ip dhcp relay information option</b> global configuration command, and enter the <b>ip dhcp snooping information option format snmp-ifindex</b> global configuration command, the switch uses these formats.                                       |
| 2 | When you globally enable DHCP snooping, and enter the <b>ip dhcp snooping information option</b> global configuration command, and the SNMP ifIndex format is not configured, the switch uses these formats.  |
| 3 | When you globally enable DHCP snooping, and enter the <b>ip dhcp snooping information option format remote-id</b> global configuration command, and enter the <b>ip dhcp snooping vlan information option format-type circuit-id string</b> interface configuration command, the switch uses these formats. |

## Cisco IOS DHCP Server Database

During the DHCP-based autoconfiguration process, the designated DHCP server uses the Cisco IOS DHCP server database. It has IP addresses, *address bindings*, and configuration parameters, such as the boot file.

An address binding is a mapping between an IP address and a MAC address of a host in the Cisco IOS DHCP server database. You can manually assign the client IP address, or the DHCP server can allocate an IP address from a DHCP address pool. For more information about manual and automatic address bindings, see the “Configuring DHCP” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*.

## DHCP Snooping Binding Database

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 8192 bindings.

Each database entry (*binding*) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. 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 is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DCHP spoofing attacks.

When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch updates the file when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file with bindings:

```
<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 value that the switch uses to verify the entries when it reads the file. The *initial-checksum* entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa1/0/4 584a38f0
END
```

When the switch starts and the calculated checksum value equals the stored checksum value, the switch reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The switch ignores an entry when one of these situations occurs:

- The switch reads the entry and the calculated checksum value does not equal the stored checksum value. The entry and the ones following it are ignored.
- An entry has an expired lease time (the switch might not remove a binding entry when the lease time expires).
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.

## Configuring DHCP Features

These sections describe how to configure DHCP snooping and option 82 on your switch:

- [Default DHCP Configuration, page 19-9](#)
- [DHCP Snooping Configuration Guidelines, page 19-9](#)
- [Upgrading from a Previous Software Release, page 19-10](#)
- [Configuring the DHCP Server, page 19-11](#)
- [Enabling Only the DHCP Relay Agent, page 19-11](#)
- [Enabling the DHCP Relay Agent and Option 82, page 19-11](#)
- [Validating the Relay Agent Information Option 82, page 19-12](#)
- [Configuring the Reforwarding Policy, page 19-12](#)
- [Specifying the Packet Forwarding Address, page 19-13](#)
- [Enabling DHCP Snooping and Option 82, page 19-15](#)
- [Enabling DHCP Snooping on Private VLANs, page 19-16](#)



- [Enabling the Cisco IOS DHCP Server Database, page 19-17](#)
- [Enabling the DHCP Snooping Binding Database Agent, page 19-17](#)

## Default DHCP Configuration

Table 19-1 shows the default DHCP configuration.

**Table 19-1**      **Default DHCP Configuration**

| Feature   | Default Setting   |
|---|---|
| DHCP server   | Enabled in Cisco IOS software, requires configuration <sup>1</sup>  |
| DHCP relay agent  | Enabled <sup>2</sup>  |
| DHCP packet forwarding address  | None configured   |
| Checking the relay agent information  | Enabled (invalid messages are dropped) <sup>2</sup>   |
| DHCP relay agent forwarding policy  | Replace the existing relay agent information <sup>2</sup>   |
| DHCP snooping enabled globally  | Disabled  |
| DHCP snooping information option  | Enabled   |
| DHCP snooping option to accept packets on untrusted ingress interfaces <sup>3</sup> | Disabled  |
| DHCP snooping limit rate  | None configured   |
| DHCP snooping trust   | Untrusted   |
| DHCP snooping VLAN  | Disabled  |
| DHCP snooping MAC address verification  | Enabled   |
| Cisco IOS DHCP server binding database  | Enabled in Cisco IOS software, requires configuration<br><br>The switch gets network addresses and configuration parameters only from a device configured as a DHCP server. |
| DHCP snooping binding database agent  | Enabled in Cisco IOS software, requires configuration<br><br>This feature is operational only when a destination is configured.   |

1. The switch responds to DHCP requests only if it is configured as a DHCP server.
2. The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
3. Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.

## DHCP Snooping Configuration Guidelines

These are the configuration guidelines for DHCP snooping.

- You must globally enable DHCP snooping on the switch.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.

- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- When you globally enable DHCP snooping on the switch, these Cisco IOS commands are not available until snooping is disabled. If you enter these commands, the switch returns an error message, and the configuration is not applied.
  - **ip dhcp relay information check** global configuration command
  - **ip dhcp relay information policy** global configuration command
  - **ip dhcp relay information trust-all** global configuration command
  - **ip dhcp relay information option** global configuration command
  - **ip dhcp relay information trusted** interface configuration command
- Before configuring the DHCP snooping information option on your switch, be sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.
- Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.
- If the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.
- If a switch port is connected to a DHCP server, configure a port as trusted by entering the **ip dhcp snooping trust** interface configuration command.
- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the **no ip dhcp snooping trust** interface configuration command.
- Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information

## Upgrading from a Previous Software Release

In Cisco IOS Release 12.1(19)EA1, the implementation for the option 82 Subscriber Identification changed from the previous release. The new option-82 format uses a different circuit-ID and remote-ID suboption, **vlan-mod-port**. The previous version uses the **snmp-ifindex** circuit ID and remote-ID suboption.

If you have option 82 configured on the switch and you upgrade to Cisco IOS Release 12.1(19)EA1 or later, the option 82 configuration is not affected. However, when you globally enable DHCP snooping on the switch by using the **ip dhcp snooping** global configuration command, the previous option 82 configuration is suspended, and the new option 82 format is applied. When you globally disable DHCP snooping on the switch, the previous option 82 configuration is re-enabled.

To provide for backward compatibility, you can select the previous option 82 format by using the **ip dhcp snooping information option format snmp-ifindex** global configuration command when you enable DHCP snooping. When DHCP snooping is globally enabled, option-82 information (in the selected format) is only inserted on snooped VLANs.

To use the previous version of option 82 without enabling DHCP snooping, see the [“Enabling the DHCP Relay Agent and Option 82” section on page 19-11](#) for instructions.

Beginning in Cisco IOS Release 12.2(25)SEE, you can configure a string of ASCII characters for the remote-ID and circuit-ID suboptions. For information on configuring these suboptions, see the [“Enabling DHCP Snooping and Option 82” section on page 19-15](#)

## Configuring the DHCP Server

The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured. These features are not operational.

For procedures to configure the switch as a DHCP server, see the “Configuring DHCP” section of the “IP addressing and Services” section of the *Cisco IOS IP Configuration Guide, Release 12.2*.

## Enabling Only the DHCP Relay Agent

Beginning in privileged EXEC mode, follow these steps to enable the DHCP relay agent on the switch:

|        | Command                                   | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b>                 | Enter global configuration mode.  |
| Step 2 | <b>service dhcp</b>                       | Enable the DHCP server and relay agent on your switch. By default, this feature is enabled. |
| Step 3 | <b>end</b>                                | Return to privileged EXEC mode.   |
| Step 4 | <b>show running-config</b>                | Verify your entries.  |
| Step 5 | <b>copy running-config startup-config</b> | (Optional) Save your entries in the configuration file.                                     |

To disable the DHCP server and relay agent, use the **no service dhcp** global configuration command.

## Enabling the DHCP Relay Agent and Option 82

In Cisco IOS Release 12.1(19)EA1, the implementation for the option 82 Subscriber Identification changed from the previous release. For more information about configuring the relay agent and option 82 when using DHCP snooping, see the [“Upgrading from a Previous Software Release” section on page 19-10](#).

Beginning in privileged EXEC mode, follow these steps to enable the DHCP relay agent and option 82 on the switch.

|        | Command                                 | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b>               | Enter global configuration mode.  |
| Step 2 | <b>service dhcp</b>                     | Enable the DHCP server and relay agent on your switch. By default, this feature is enabled.   |
| Step 3 | <b>ip dhcp relay information option</b> | Enable the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server.<br><br>By default, this feature is disabled. |

|        | Command                                   | Purpose   |
|--------|---|---|
| Step 4 | <b>end</b>                                | Return to privileged EXEC mode.                         |
| Step 5 | <b>show running-config</b>                | Verify your entries.                                    |
| Step 6 | <b>copy running-config startup-config</b> | (Optional) Save your entries in the configuration file. |

To disable the DHCP server and relay agent, use the **no service dhcp** global configuration command. To disable the insertion and removal of the option-82 field, use the **no ip dhcp relay information option** global configuration command.

## Validating the Relay Agent Information Option 82

By default, the switch verifies that the option-82 field in DHCP reply packet it receives from the DHCP server is valid. If an invalid message is received, the switch drops it. If a valid message is received, the switch removes the option-82 field and forwards the packet.

If you want to disable this feature, use the **no ip dhcp relay information check** global configuration command. When disabled, the switch does not validate the option-82 field for validity, but still removes the option from the packet and forwards it. (This feature is not available when DHCP snooping is enabled on the switch.)



### Note

If the switch receives a packet that contains the option-82 field from a DHCP client and the information checking feature is enabled, the switch drops the packet because it is invalid. However, in some instances, you might configure a client with the option-82 field. In this situation, you should disable the information-check feature so that the switch does not remove the option-82 field from the packet. You can configure the action that the switch takes when it receives a packet with existing option-82 information by using the **ip dhcp relay information policy** global configuration command. For more information, see the [“Configuring the Reforwarding Policy” section on page 19-12](#). (This feature is not available when DHCP snooping is enabled on the switch.)

## Configuring the Reforwarding Policy

By default, the reforwarding policy of the switch is to replace existing relay information in packets received from DHCP clients with switch DHCP relay information. If the default action is not suitable for your network configuration, you can use the **ip dhcp relay information policy {drop | keep | replace}** global configuration command to change it. (This feature is not available when DHCP snooping is enabled on the switch.)



### Note

To ensure the correct operation of the reforwarding policy, make sure to disable the relay agent information check by using the **no ip dhcp relay information check** global configuration command.

Beginning in privileged EXEC mode, follow these steps to change the action of the reforwarding policy.

|        | Command   | Purpose  |
|--------|---|--|
| Step 1 | <b>configure terminal</b>                                       | Enter global configuration mode.   |
| Step 2 | <b>ip dhcp relay information policy {drop   keep   replace}</b> | Configure the reforwarding policy. The default is to replace (overwrite) existing information with switch DHCP relay information. <ul style="list-style-type: none"> <li>Use the <b>drop</b> keyword if you want the switch to discard messages with existing relay information if the option-82 information is also present.</li> <li>Use the <b>keep</b> keyword if you want the switch to retain the existing relay information.</li> </ul> |
| Step 3 | <b>end</b>  | Return to privileged EXEC mode.  |
| Step 4 | <b>show running-config</b>                                      | Verify your entries.   |
| Step 5 | <b>copy running-config startup-config</b>                       | (Optional) Save your entries in the configuration file.  |

To return to the default reforwarding policy, use the **no ip dhcp relay information policy** global configuration command.

## Specifying the Packet Forwarding Address

A DHCP relay agent is any device that forwards DHCP packets between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are transparently switched between networks. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface.

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the switch with the **ip helper-address** *address* interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the **ip helper-address** command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address. This procedure is optional.

|        | Command   | Purpose   |
|--------|---|---|
| Step 1 | <b>configure terminal</b>                       | Enter global configuration mode.  |
| Step 2 | <b>interface vlan</b> <i>vlan-id</i>            | Enter a VLAN ID to create a switch virtual interface, and enter interface configuration mode. |
| Step 3 | <b>ip address</b> <i>ip-address subnet-mask</i> | Configure the interface with an IP address and an IP subnet.                                  |

|         | Command  | Purpose   |
|---------|--|---|
| Step 4  | <b>ip helper-address</b> <i>address</i>  | Specify the DHCP packet forwarding address.<br><br>The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests.<br><br>If you have multiple servers, you can configure one helper address for each server. |
| Step 5  | <b>exit</b>  | Return to global configuration mode.  |
| Step 6  | <b>interface range</b> <i>port-range</i><br><br>or<br><b>interface</b> <i>interface-id</i> | Configure multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode.<br><br>or<br>Configure a single physical port that is connected to the DHCP client, and enter interface configuration mode.   |
| Step 7  | <b>switchport mode access</b>  | Define the VLAN membership mode for the port.   |
| Step 8  | <b>switchport access vlan</b> <i>vlan-id</i>   | Assign the ports to the same VLAN as configured in Step 2.  |
| Step 9  | <b>end</b>   | Return to privileged EXEC mode.   |
| Step 10 | <b>show running-config</b>   | Verify your entries.  |
| Step 11 | <b>copy running-config startup-config</b>  | (Optional) Save your entries in the configuration file.   |

To remove the DHCP packet forwarding address, use the **no ip helper-address** *address* interface configuration command.

This example shows how to enable the DHCP server, the relay agent, and the insertion and removal of the DHCP relay information (option 82). It creates a switch virtual interface with VLAN ID 10, assigns it an IP address, and specifies the DHCP packet forwarding address of 30.0.0.2 (DHCP server address). Two interfaces (Gigabit Ethernet 0/1 and 0/2) that connect to the DHCP clients are configured as static access ports in VLAN 10 (see [Figure 19-1 on page 19-4](#)):

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# service dhcp
Switch(config)# ip dhcp relay information option
Switch(config)# interface vlan 10
Switch(config-if)# ip address 10.0.0.1 255.0.0.0
Switch(config-if)# ip helper-address 30.0.0.2
Switch(config-if)# exit
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

## Enabling DHCP Snooping and Option 82

Beginning in privileged EXEC mode, follow these steps to enable DHCP snooping on the switch.

|        | Command  | Purpose  |
|--------|--|--|
| Step 1 | <b>configure terminal</b>  | Enter global configuration mode.   |
| Step 2 | <b>ip dhcp snooping</b>  | Enable DHCP snooping globally.   |
| Step 3 | <b>ip dhcp snooping vlan</b> <i>vlan-range</i>   | Enable DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094.<br><br>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 | <b>ip dhcp snooping information option</b>   | Enable the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. The default is enabled.   |
| Step 5 | <b>ip dhcp snooping information option format snmp-ifindex</b>   | (Optional) Specify <b>ip dhcp snooping information option format snmp-ifindex</b> to select an alternate format for the circuit-ID and remote-ID suboption of the option 82 feature. See the <a href="#">“Upgrading from a Previous Software Release”</a> section on page 19-10 for more information.<br><br>The default setting is <b>no ip dhcp snooping information option format snmp-ifindex</b> .                          |
| Step 6 | <b>ip dhcp snooping information option format remote-id</b> [ <i>string ASCII-string</i>   <i>hostname</i> ]         | (Optional) Configure the remote-ID suboption.<br><br>You can configure the remote ID to be: <ul style="list-style-type: none"> <li>• String of up to 63 ASCII characters (no spaces)</li> <li>• Configured hostname for the switch</li> </ul> <b>Note</b> If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration.<br><br>The default remote ID is the switch MAC address. |
| Step 7 | <b>ip dhcp snooping information option allow-untrusted</b>   | (Optional) If the switch is an aggregation switch connected to an edge switch, enable the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch.<br><br>The default is disabled.<br><br><b>Note</b> You must only enter this command on aggregation switches that are connected to trusted devices.  |
| Step 8 | <b>interface</b> <i>interface-id</i>   | Specify the interface to be configured, and enter interface configuration mode.  |
| Step 9 | <b>ip dhcp snooping vlan</b> <i>vlan</i> <b>information option format-type circuit-id</b> <i>string ASCII-string</i> | (Optional) Configure the circuit-ID suboption for the specified interface.<br><br>Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094.<br><br>You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces).<br><br>The default circuit ID is the port identifier, in the format <b>vlan-mod-port</b> .  |

|         | Command  | Purpose  |
|---------|--|--|
| Step 10 | <b>ip dhcp snooping trust</b>                  | (Optional) Configure the interface as trusted or untrusted. You can use the <b>no</b> keyword to configure an interface to receive messages from an untrusted client. The default is untrusted.  |
| Step 11 | <b>ip dhcp snooping limit rate</b> <i>rate</i> | (Optional) Configure the number of DHCP packets per second than an interface can receive. The range is 1 to 4294967294. The default is no rate limit configured.<br><br><b>Note</b> 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 12 | <b>exit</b>                                    | Return to global configuration mode.   |
| Step 13 | <b>ip dhcp snooping verify mac-address</b>     | (Optional) Configure 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 14 | <b>end</b>                                     | Return to privileged EXEC mode.  |
| Step 15 | <b>show running-config</b>                     | Verify your entries.   |
| Step 16 | <b>copy running-config startup-config</b>      | (Optional) Save 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-id* 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 Fast Ethernet port 0/1:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface fastethernet0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

## Enabling DHCP Snooping on Private VLANs

You can enable DHCP snooping on private VLANs. If DHCP snooping is enabled, the configuration is propagated to both a primary VLAN and its associated secondary VLANs. If DHCP snooping is enabled on the primary VLAN, it is also configured on the secondary VLANs.



If DHCP snooping is already configured on the primary VLAN and you configure DHCP snooping with different settings on a secondary VLAN, the configuration for the secondary VLAN does not take effect. You must configure DHCP snooping on the primary VLAN. If DHCP snooping is not configured on the primary VLAN, this message appears when you are configuring DHCP snooping on the secondary VLAN, such as VLAN 200:

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take
effect on secondary vlan 200. DHCP Snooping configuration on secondary vlan is derived
from its primary vlan.
```

The **show ip dhcp snooping** privileged EXEC command output shows all VLANs, including primary and secondary private VLANs, on which DHCP snooping is enabled.

## Enabling the Cisco IOS DHCP Server Database

For procedures to enable and configure the Cisco IOS DHCP server database, see the “DHCP Configuration Task List” section in the “Configuring DHCP” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*.

## Enabling the DHCP Snooping Binding Database Agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the switch.

|        | Command   | Purpose  |
|--------|---|--|
| Step 1 | <b>configure terminal</b>   | Enter global configuration mode.   |
| Step 2 | <b>ip dhcp snooping database</b><br>{ <b>flash:</b> filename  <br><b>ftp:</b> //user:password@host/filename  <br><b>http:</b> //[[username:password]@]<br>{hostname   host-ip}[/directory]<br>/image-name.tar  <br><b>rtp:</b> //user@host/filename } | Specify the URL for the database agent or the binding file by using one of these forms: <ul style="list-style-type: none"> <li>• <b>flash:</b>filename</li> <li>• <b>ftp:</b>//user:password@host/filename</li> <li>• <b>http:</b>//[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</li> <li>• <b>rtp:</b>//user@host/filename</li> <li>• <b>tftp:</b>//host/filename</li> </ul> |
| Step 3 | <b>ip dhcp snooping database timeout</b><br>seconds   | Specify (in seconds) how long to wait for the database transfer to finish before stopping.<br><br>The range is 0 to 86400. Use 0 for an infinite duration. The default is 300 seconds (5 minutes).   |
| Step 4 | <b>ip dhcp snooping database write-delay</b><br>seconds   | Specify the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).   |
| Step 5 | <b>end</b>  | Return to privileged EXEC mode.  |

|        | Command   | Purpose  |
|--------|---|--|
| Step 6 | <b>ip dhcp snooping binding</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> <b>ip-address</b> <b>interface</b> <i>interface-id</i> <b>expiry</b> <i>seconds</i> | (Optional) Add binding entries to the DHCP snooping binding database. The <i>vlan-id</i> range is from 1 to 4904. The <i>seconds</i> range is from 1 to 4294967295.<br><br>Enter this command for each entry that you add.<br><br><b>Note</b> Use this command when you are testing or debugging the switch. |
| Step 7 | <b>show ip dhcp snooping database</b> [detail]  | Display the status and statistics of the DHCP snooping binding database agent.   |
| Step 8 | <b>copy running-config startup-config</b>   | (Optional) Save your entries in the configuration file.  |

To stop using the database agent and binding files, use the **no ip dhcp snooping database** global configuration command. To reset the timeout or delay values, use the **ip dhcp snooping database timeout** *seconds* or the **ip dhcp snooping database write-delay** *seconds* global configuration command.

To clear the statistics of the DHCP snooping binding database agent, use the **clear ip dhcp snooping database statistics** privileged EXEC command. To renew the database, use the **renew ip dhcp snooping database** privileged EXEC command.

To delete binding entries from the DHCP snooping binding database, use the **no ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* **ip-address** **interface** *interface-id* privileged EXEC command. Enter this command for each entry that you want to delete.

## Displaying DHCP Information

To display the DHCP snooping information, use one or more of the privileged EXEC commands in [Table 19-2](#):

**Table 19-2** Commands for Displaying DHCP Information

| Command                               | Purpose   |
|---------------------------------------|---|
| <b>show ip dhcp snooping</b>          | Displays the DHCP snooping configuration for a switch.  |
| <b>show ip dhcp snooping binding</b>  | Displays only the dynamically configured bindings in the DHCP snooping binding database. <sup>1</sup> |
| <b>show ip dhcp snooping database</b> | Displays the DHCP snooping binding database status and statistics.                                    |
| <b>show running-config</b>            | Displays the status of the insertion and removal of the DHCP option-82 field on all interfaces.       |

1. If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the manually configured bindings.

# Understanding IP Source Guard

IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface, except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

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.

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

## Source IP Address Filtering

When IP source guard 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 using the IP source binding changes, and re-applies the port ACL to the interface.

If you enable IP source guard 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

When IP source guard is enabled with this option, 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 IP source guard with source IP and MAC 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.

# Configuring IP Source Guard

This section describes how to configure IP source guard on your switch.

- [Default IP Source Guard Configuration, page 19-20](#)
- [IP Source Guard Configuration Guidelines, page 19-20](#)
- [Enabling IP Source Guard, page 19-21](#)
- [Displaying IP Source Guard Information, page 19-22](#)

## Default IP Source Guard Configuration

By default, IP source guard is disabled.

## IP Source Guard Configuration Guidelines

These are the configuration guides for IP source guard:

- 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 a VLAN, DHCP snooping must be enabled on the access VLAN to which the interface belongs.
- 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.

- When IP source guard with source IP and MAC address filtering is enabled, DHCP snooping and port security must be enabled on the interface.
- When configuring IP source guard on interfaces on which a private VLAN is configured, port security is not supported.
- IP source guard is not supported on EtherChannels.
- You can enable this feature when IEEE 802.1x port-based authentication is enabled.
- If the number of ternary content addressable memory (TCAM) entries exceeds the maximum available, the CPU usage increases.

## Enabling IP Source Guard

Beginning in privileged EXEC mode, follow these steps to enable and configure IP source guard on an interface.

|        | Command   | Purpose  |
|--------|---|--|
| Step 1 | <b>configure terminal</b>   | Enter global configuration mode.   |
| Step 2 | <b>interface</b> <i>interface-id</i>  | Specify the interface to be configured, and enter interface configuration mode.  |
| Step 3 | <b>ip verify source</b><br>or<br><b>ip verify source port-security</b>  | <p>Enable IP source guard with source IP address filtering.</p> <p>Enable IP source guard with source IP and MAC address filtering.</p> <p><b>Note</b> When you enable both IP Source Guard and Port Security, using the <b>ip verify source port-security</b> interface configuration command, there are two caveats:</p> <ul style="list-style-type: none"> <li>• The DHCP server must support option 82, or the client is not assigned an IP address.</li> <li>• 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.</li> </ul> |
| Step 4 | <b>exit</b>   | Return to global configuration mode.   |
| Step 5 | <b>ip source binding</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> <i>ip-address</i> <b>interface</b> <i>interface-id</i>   | <p>Add a static IP source binding.</p> <p>Enter this command for each static binding.</p>  |
| Step 6 | <b>end</b>  | Return to privileged EXEC mode.  |
| Step 7 | <b>show ip verify source</b> [ <b>interface</b> <i>interface-id</i> ]   | Display the IP source guard configuration for all interfaces or for a specific interface.  |
| Step 8 | <b>show ip source binding</b> [ <i>ip-address</i> ] [ <i>mac-address</i> ] [ <b>dhcp-snooping</b>   <b>static</b> ] [ <b>interface</b> <i>interface-id</i> ] [ <b>vlan</b> <i>vlan-id</i> ] | Display the IP source bindings on the switch, on a specific VLAN, or on a specific interface.  |
| Step 9 | <b>copy running-config startup-config</b>   | (Optional) Save your entries in the configuration file.  |

To disable IP source guard with source IP address filtering, use the **no ip verify source** interface configuration command.

To delete a static IP source binding entry, use the **no ip source global** configuration command.

This example shows how to enable IP source guard with source IP and MAC filtering on VLANs 10 and 11:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
Switch(config)# end
```

# Displaying IP Source Guard Information

To display the IP source guard information, use one or more of the privileged EXEC commands in [Table 19-3](#):

**Table 19-3**      *Commands for Displaying IP Source Guard Information*

| Command                       | Purpose  |
|-------------------------------|--|
| <b>show ip source binding</b> | Display the IP source bindings on a switch.              |
| <b>show ip verify source</b>  | Display the IP source guard configuration on the switch. |