



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 18-1](#)
- [/Configuring DHCP Features, page 18-6](#)
- [Displaying DHCP Information, page 18-13](#)

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 18-2](#)
- [DHCP Relay Agent, page 18-2](#)
- [DHCP Snooping, page 18-2](#)
- [Option-82 Data Insertion, page 18-3](#)

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 can forward 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 DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY 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 DHCPRELEASE or DHCPDECLINE 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 a 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.

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.

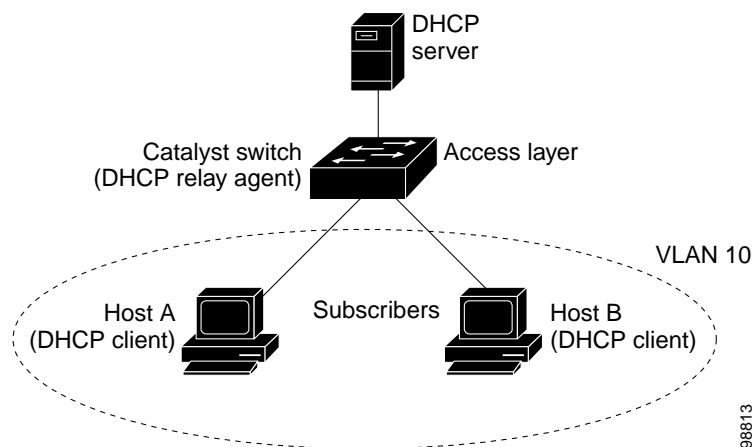


Note

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 18-1 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 18-1 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. 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).
- 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.

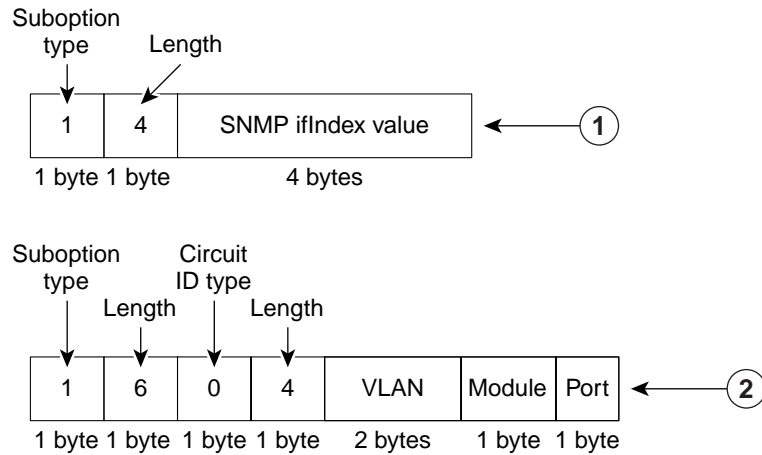
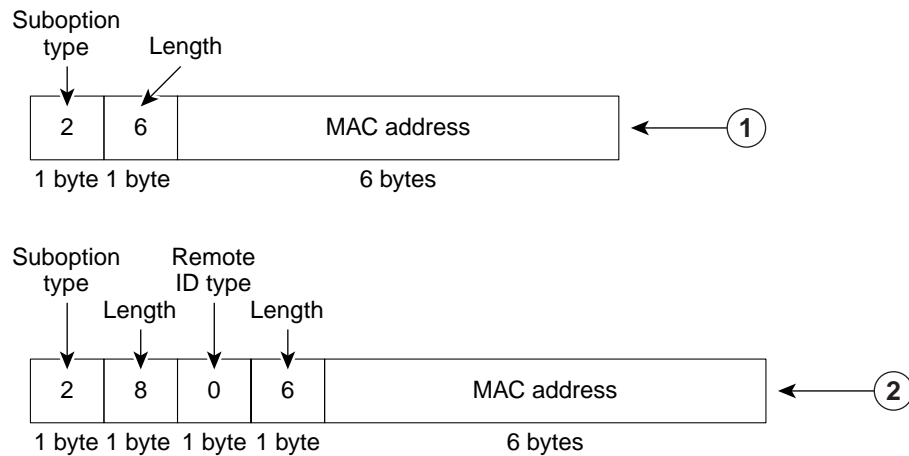
When the previously described sequence of events occurs, the values in these fields in [Figure 18-2](#) do not change:

- 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 circuit ID type

When DHCP snooping is globally enabled, the **ip dhcp snooping information option** global configuration command is entered, and the SNMP ifIndex format is not configured, 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 18-2](#) shows the packet formats for the remote ID suboption and the circuit ID suboption. For the circuit ID suboption, the module field is always zero.

Figure 18-2 Suboption Packet Formats

Circuit ID Suboption Frame Format**Remote ID Suboption Frame Format**

- | | |
|---|--|
| 1 | The switch uses these formats when DHCP snooping is globally enabled, the ip dhcp relay information option global configuration command is entered, and the ip dhcp snooping information option format snmp-ifindex global configuration command is entered. |
| 2 | The switch uses these formats when DHCP snooping is globally enabled, the ip dhcp snooping information option global configuration command is entered, and the SNMP ifIndex format is not configured. |

116301

Configuring DHCP Features

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

- [Default DHCP Configuration, page 18-6](#)
- [DHCP Snooping Configuration Guidelines, page 18-6](#)
- [Upgrading from a Previous Software Release, page 18-7](#)
- [Configuring the DHCP Server, page 18-8](#)
- [Enabling Only the DHCP Relay Agent, page 18-8](#)
- [Enabling the DHCP Relay Agent and Option 82, page 18-8](#)
- [Validating the Relay Agent Information Option 82, page 18-9](#)
- [Configuring the Reforwarding Policy, page 18-9](#)
- [Specifying the Packet Forwarding Address, page 18-10](#)
- [Enabling DHCP Snooping and Option 82, page 18-11](#)

Default DHCP Configuration

Table 18-1 shows the default DHCP configuration.

Table 18-1 Default DHCP Configuration

Feature	Default Setting
DHCP server	Enabled ¹
DHCP relay agent	Enabled ²
DHCP packet forwarding address	None configured
Checking the relay agent information	Enabled (invalid messages are dropped) ²
DHCP relay agent forwarding policy	Replace the existing relay agent information ²
DHCP snooping enabled globally	Disabled
DHCP snooping information option	Enabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping VLAN	Disabled
DHCP snooping MAC address verification	Enabled

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.

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.

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 18-8 for instructions.

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	configure terminal	Enter global configuration mode.
Step 2	service dhcp	Enable the DHCP server and relay agent on your switch. By default, this feature is enabled.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(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 18-7](#).

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	service dhcp	Enable the DHCP server and relay agent on your switch. By default, this feature is enabled.
Step 3	ip dhcp relay information option	Enable the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. By default, this feature is disabled.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(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 18-9](#). (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	configure terminal	Enter global configuration mode.
Step 2	ip dhcp relay information policy {drop keep replace}	Configure the reforwarding policy. The default is to replace (overwrite) existing information with switch DHCP relay information. <ul style="list-style-type: none"> Use the drop keyword if you want the switch to discard messages with existing relay information if the option-82 information is also present. Use the keep keyword if you want the switch to retain the existing relay information.

	Command	Purpose
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(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	configure terminal	Enter global configuration mode.
Step 2	interface vlan <i>vlan-id</i>	Enter interface configuration mode, and create a switch virtual interface.
Step 3	ip address <i>ip-address subnet-mask</i>	Configure the interface with an IP address and an IP subnet.
Step 4	ip helper-address <i>address</i>	Specify the DHCP packet forwarding address. 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. If you have multiple servers, you can configure one helper address for each server.
Step 5	exit	Return to global configuration mode.
Step 6	interface range <i>port-range</i> or interface <i>interface-id</i>	Configure multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. Configure a single physical port that is connected to the DHCP client, and enter interface configuration mode.
Step 7	switchport mode access	Define the VLAN membership mode for the port.
Step 8	switchport access vlan <i>vlan-id</i>	Assign the ports to the same VLAN as configured in Step 2.
Step 9	end	Return to privileged EXEC mode.

	Command	Purpose
Step 10	show running-config	Verify your entries.
Step 11	copy running-config startup-config	(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 18-1 on page 18-3](#)):

```
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	configure terminal	Enter global configuration mode.
Step 2	ip dhcp snooping	Enable DHCP snooping globally.
Step 3	ip dhcp snooping vlan <i>vlan-range</i>	Enable 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	ip dhcp snooping information option	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	ip dhcp snooping information option format snmp-ifindex	(Optional) Specify ip dhcp snooping information option format snmp-ifindex to select an alternate format for the circuit ID and remote ID suboption of the option 82 feature. See the “Upgrading from a Previous Software Release” section on page 18-7 for more information. The default setting is no ip dhcp snooping information option format snmp-ifindex .

	Command	Purpose
Step 6	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to be configured.
Step 7	ip dhcp snooping trust	(Optional) Configure 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 is untrusted.
Step 8	ip dhcp snooping limit rate <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. 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 9	ip dhcp snooping verify mac-address	(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 10	end	Return to privileged EXEC mode.
Step 11	show running-config	Verify your entries.
Step 12	copy running-config startup-config	(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.

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
```

Displaying DHCP Information

To display the DHCP snooping information, use one or more of the privileged EXEC commands in [Table 18-2](#):

Table 18-2 Commands for Displaying DHCP Information

Command	Purpose
show ip dhcp snooping	Displays the DHCP snooping configuration for a switch
show ip dhcp snooping binding	Displays only the dynamically configured bindings in the DHCP snooping binding database. ¹
show running-config	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.

