



## Configuring DHCP Features

---

This chapter describes how to configure DHCP snooping and the option-82 data insertion features on the Catalyst 2970 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 18-5](#)
- [Displaying DHCP Snooping Information, page 18-8](#)

## 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, also referred to as a DHCP snooping binding table. For more information about this database, see the [“Displaying DHCP Snooping Information” section on page 18-8](#).

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You 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 DHCP 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 has 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 have 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 the 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 has a MAC address in the DHCP snooping binding database, but the interface information in the binding database 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.

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 12.2(25)SEA, you cannot configure DHCP snooping on an aggregation switch because the DHCP snooping bindings database will not be 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 12.2(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 allowed-trust** 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 DHCP snooping 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.

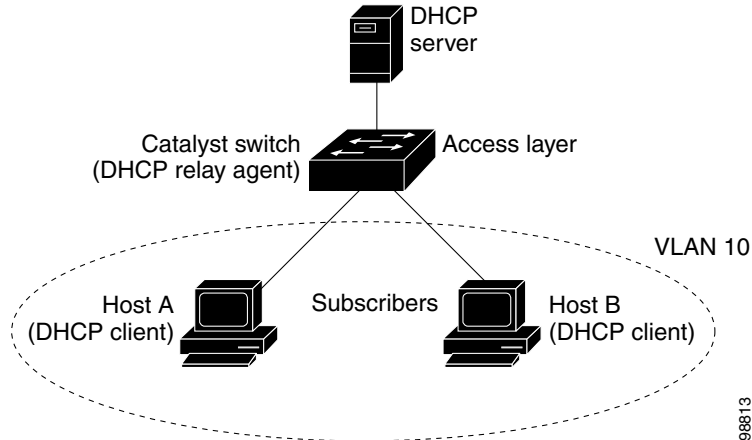


### Note

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

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 is the switch MAC address (the remote ID suboption) and the port identifier, **vlan-mod-port**, from which the packet is received (the circuit ID suboption).
- 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. 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. 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:

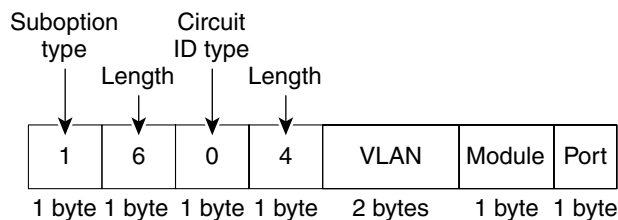
- Circuit ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit ID type
  - Length of the circuit ID type
- Remote ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Remote ID type
  - Length of the circuit ID type

In the port field of the circuit ID suboption, the port numbers start at 3. For example, on a Catalyst 2970-24TS switch, port 3 is the Fast Ethernet 0/1 port, port 4 is the Fast Ethernet 0/2 port, port 5 is the Fast Ethernet 0/3 port, and so on. Port 27 is the small form-factor pluggable (SFP) module slot 0/1, port 28 is the SFP module slot 0/2, and so on.

Figure 18-2 shows the packet formats for the remote ID suboption and the circuit ID suboption. For the circuit ID suboption, the module number corresponds to the switch number in the stack. The switch uses the packet formats when DHCP snooping is globally enabled and when the **ip dhcp snooping information option** global configuration command is entered.

**Figure 18-2 Suboption Packet Formats**

#### Circuit ID Suboption Frame Format



#### Remote ID Suboption Frame Format



## Configuring DHCP Features

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

- [Default DHCP Configuration, page 18-5](#)
- [DHCP Snooping Configuration Guidelines, page 18-6](#)
- [Enabling DHCP Snooping and Option 82, page 18-7](#)

## Default DHCP Configuration

Table 18-1 shows the default DHCP configuration.

**Table 18-1 Default DHCP Configuration**

Feature	Default Setting
DHCP server	Enabled <sup>1</sup>
DHCP relay agent	Enabled <sup>2</sup>

**Table 18-1** Default DHCP Configuration (continued)

Feature	Default Setting
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

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 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.
- 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 allowed-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.

## 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.  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 allowed-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.  The default is disabled.  <b>Note</b> You must enter this command only on aggregation switches that are connected to trusted devices.
Step 6	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the interface to be configured.
Step 7	<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 8	<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 2048. The default is no rate limit configured.  <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 9	<b>exit</b>	Return to global configuration mode.
Step 10	<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.

	Command	Purpose
Step 11	<b>end</b>	Return to privileged EXEC mode.
Step 12	<b>show running-config</b>	Verify your entries.
Step 13	<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-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 allowed-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 gigabitethernet0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

## Displaying DHCP Snooping 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
<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, also referred to as a binding table. <sup>1</sup>

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



**Note**

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