



Configuring DHCP Features

This chapter describes how to configure DHCP snooping and the option-82 data insertion features on the Catalyst 2950 or Catalyst 2955 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 “*IP Addressing and Services*” section in the *Cisco IOS IP and IP Routing Command Reference, Release 12.1*.

This chapter consists of these sections:

- [Understanding DHCP Features, page 19-1](#)
- [Configuring DHCP Features, page 19-5](#)
- [Displaying DHCP Information, page 19-8](#)

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 19-2](#)
- [DHCP Relay Agent, page 19-2](#)
- [DHCP Snooping, page 19-2](#)
- [Option-82 Data Insertion, page 19-3](#)

For information about the DHCP client, see the “*IP Addressing and Services*” section in the *Cisco IOS IP and IP Routing Configuration Guide, Release 12.1*.

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.

**Note**

The DHCP server feature is only available on Catalyst 2955 switches.

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 LEASE QUERY 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 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.

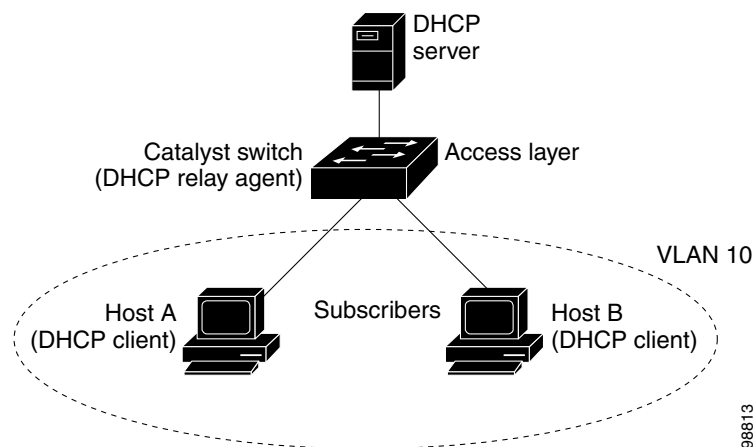


Note

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. 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:

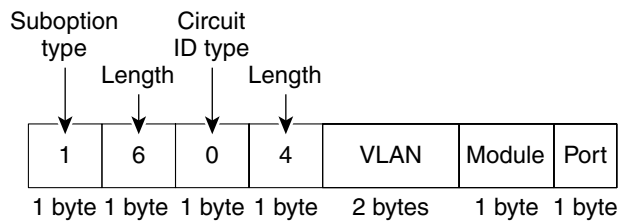
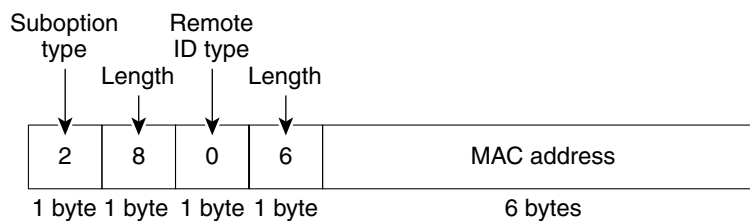
- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, **vlan-mod-port**, from which the packet is received (the circuit ID suboption).
- If the IP address of the relay agent is configured, the switch adds 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 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 circuit ID type

The port numbers in the port field of the circuit ID suboption start at 0. For example, on a Catalyst 2950G-24-EI 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 remote ID suboption and the circuit ID suboption. 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. 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**

116300

Configuring DHCP Features

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

- [Default DHCP Configuration, page 19-5](#)
- [DHCP Snooping Configuration Guidelines, page 19-6](#)
- [Configuring the DHCP Server, page 19-6](#)
- [Enabling DHCP Snooping and Option 82, page 19-6](#)

Default DHCP Configuration

Table 19-1 shows the default DHCP configuration.

Table 19-1 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 |

Table 19-1 Default DHCP Configuration (continued)

| Feature | Default Setting |
|--------------------------|-----------------|
| DHCP snooping limit rate | None configured |
| DHCP snooping trust | Untrusted |
| DHCP snooping VLAN | Disabled |

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.
- 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.

Configuring the DHCP Server

The Catalyst 2955 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 and IP Routing Configuration Guide, Release 12.1*.

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. |

| | Command | Purpose |
|---------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 | interface <i>interface-id</i> | Enter interface configuration mode, and specify the interface to be configured. |
| Step 6 | 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 7 | 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 8 | end | Return to privileged EXEC mode. |
| Step 9 | show running-config | Verify your entries. |
| Step 10 | 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 19-1](#):

Figure 19-3 *Commands for Displaying DHCP Information*

| Command | Purpose |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <code>show ip dhcp snooping</code> | Displays the DHCP snooping configuration for a switch |
| <code>show ip dhcp snooping binding</code> | Displays only the dynamically configured bindings in the DHCP snooping binding database. ¹ |

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