CHAPTER 19

Configuring DHCP Features

This chapter describes how to configure Dynamic Host Configuration Protocol (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 refer to the "*IP Addressing and Services*" section in the *Cisco IOS IP and IP Routing Command Reference for Release 12.1*.

This chapter consists of these sections:

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.

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 table. An untrusted message is a message that is received from outside the network or firewall that can cause traffic attacks within your network.

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

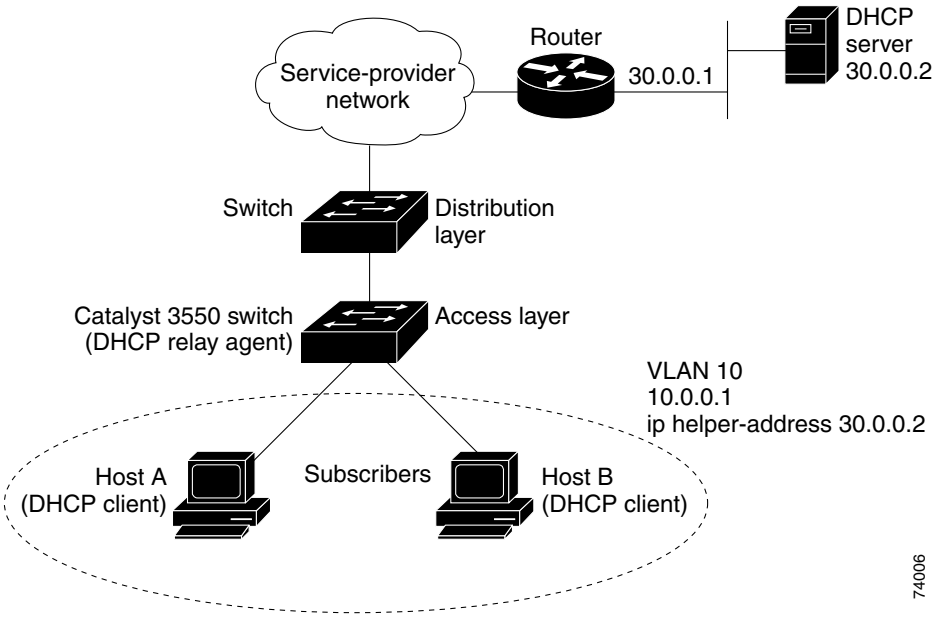
DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

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 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.

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 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).
- 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 a 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.

Configuring DHCP Features

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

Default DHCP Configuration

Table 19-1 shows the default DHCP configuration.

Table 19-1 Default DHCP Configuration

Feature	Default Setting
DHCP snooping enabled globally	Disabled
DHCP snooping information option	Enabled
DHCP relay information option	Enabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping VLAN	Disabled

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.

- 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 information option 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 or configure DHCP options for devices.
  - If your switch is the DHCP server, see the "Configuring the DHCP Server" section on page 4-5 for more information.
  - If your DHCP server is a Cisco device, refer to the "IP Addressing and Services" section in the "Configuring DHCP" chapter of the *Cisco IOS IP and IP Routing Configuration Guide for Release 12.1*. Otherwise, refer to the documentation that shipped with the server.

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 19-6 for instructions.

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** *vlan-id* [*vlan-id*]	Enable DHCP snooping on a VLAN or range of VLANs. You can specify a single VLAN identified by VLAN ID number or a start and end VLAN ID to specify a range of VLANs. The range is 1 to 4094.
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 19-4 for more information. The default setting is **no ip dhcp snooping information option format snmp-ifindex**.
Step 6	**interface** *interface-id*	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** *rate*	(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. Normally, the rate limit applies to untrusted interfaces. If you configure rate limiting for trusted interfaces, you will need to adjust the rate limit to a higher value because trusted interfaces might aggregate DHCP traffic in the switch.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**show running-config**	Verify your entries.
Step 11	**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
```

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 19-4.

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 19-7. (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. • 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.
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** *vlan-id*	Enter interface configuration mode, and create a switch virtual interface.
Step 3	**ip address** *ip-address subnet-mask*	Configure the interface with an IP address and an IP subnet.
Step 4	**ip helper-address** *address*	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** *port-range* or **interface** *interface-id*	Configure multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. or 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** *vlan-id*	Assign the ports to the same VLAN as configured in Step 2.
Step 9	**end**	Return to privileged EXEC mode.
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 19-1 on page 19-2):

```
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
```

Displaying DHCP Information

You can display a DHCP snooping binding table and configuration information for all interfaces on a switch. To display the status of the insertion and removal of the DHCP option-82 field on all interfaces, use the **show running-config** privideged EXEC command.

Displaying a Binding Table

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

This example shows how to display the DHCP snooping binding entries for a switch.

```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type     VLAN  Interface
------------------  ---------------  ----------  -------  ----  --------------------
00:30:94:C2:EF:35   41.0.0.51        286         dynamic  41    FastEthernet0/3
00:D0:B7:1B:35:DE   41.0.0.52        237         dynamic  41    FastEthernet0/3
00:00:00:00:00:01   40.0.0.46        286         dynamic  40    FastEthernet0/9
00:00:00:00:00:03   42.0.0.33        286         dynamic  42    FastEthernet0/9
00:00:00:00:00:02   41.0.0.53        286         dynamic  41    FastEthernet0/9
```

Table 19-2 describes the fields in the **show ip dhcp snooping binding** command output.

Table 19-2 show ip dhcp snooping binding Command Output

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

Displaying the DHCP Snooping Configuration

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

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/5              yes         unlimited
FastEthernet0/7              yes         unlimited
FastEthernet0/3              no          5000
FastEthernet0/5              yes         unlimited
FastEthernet0/7              yes         unlimited
FastEthernet0/5              yes         unlimited
FastEthernet0/7              yes         unlimited
```