CHAPTER 11

Configuring DHCP Snooping

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on an NX-OS device.

This chapter includes the following sections:

- Information About DHCP Snooping, page 11-1
- Licensing Requirements for DHCP Snooping, page 11-5
- Prerequisites for DHCP Snooping, page 11-6
- Guidelines and Limitations, page 11-6
- Configuring DHCP Snooping, page 11-7
- Displaying DHCP Bindings, page 11-16
- Field Descriptions for DHCP Snooping, page 11-16
- Additional References, page 11-18

Information About DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Uses the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

Dynamic ARP inspection (DAI) and IP Source Guard also use information stored in the DHCP snooping binding database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

This section includes the following topics:

- Trusted and Untrusted Sources, page 11-2
- DHCP Snooping Binding Database, page 11-2
- DHCP Relay Agent, page 11-2
- Packet Validation, page 11-3

- DHCP Snooping Option-82 Data Insertion, page 11-3
- Virtualization Support for DHCP Snooping, page 11-5

Trusted and Untrusted Sources

You can configure whether DHCP snooping trusts traffic sources. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, DHCP snooping filters messages from untrusted sources.

In an enterprise network, a trusted source is a device that is under your administrative control. These devices include the switches, routers, and servers in the network. Any device beyond the firewall or outside the network is an untrusted source. Generally, host ports are treated as untrusted sources.

In a service provider environment, any device that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In the NX-OS device, you indicate that a source is trusted by configuring the trust state of its connecting interface.

The default trust state of all interfaces is untrusted. You must configure DHCP server interfaces as trusted. You can also configure other interfaces as trusted if they connect to devices (such as switches or routers) inside your network. You usually do not configure host port interfaces as trusted.

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

DHCP Snooping Binding Database

Using information extracted from intercepted DHCP messages, DHCP snooping dynamically builds and maintains a database. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces.

Note The DHCP snooping binding database is also referred to as the DHCP snooping binding table.

DHCP snooping updates the database when the device receives specific DHCP messages. For example, the feature adds an entry to the database when the device receives a DHCPACK message from the server. The feature removes the entry in the database when the IP address lease expires or the device receives a DHCPRELEASE message from the host.

Each entry in the DHCP snooping binding database includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.

DHCP Relay Agent

You can configure the device to run a DHCP relay agent, which forwards DHCP packets between clients and servers. This feature is useful when clients and servers are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched

between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

Packet Validation

The device validates DHCP packets received on the untrusted interfaces of VLANs that have DHCP snooping enabled. The device forwards the DHCP packet unless any of the following conditions occur (in which case the packet is dropped):

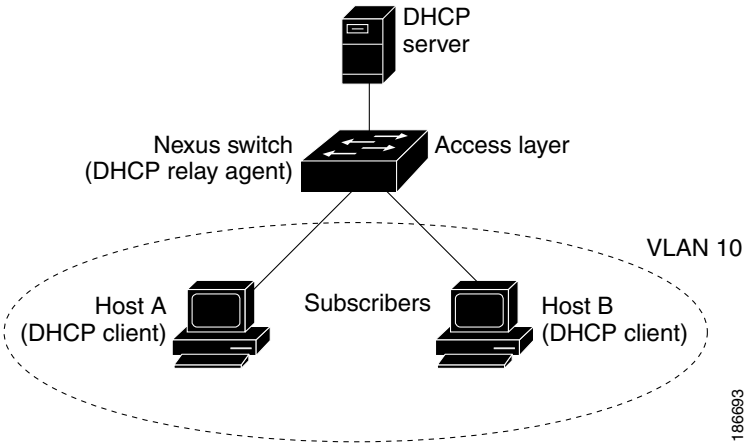
- The device receives a DHCP response packet (such as DHCPACK, DHCPNAK, or DHCPOFFER packet) on an untrusted interface.
- The device receives a packet on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match. This check is performed only if the DHCP snooping MAC address verification option is turned on.
- The device receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.
- The device receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0.

DHCP Snooping 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 you enable option 82, the device identifies a subscriber device that connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can connect to the same port on the access device and are uniquely identified.

Figure 11-1 shows an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the device 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 is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

Figure 11-1 DHCP Relay Agent in a Metropolitan Ethernet Network



When you enable option 82 on the NX-OS device, the following sequence of events occurs:

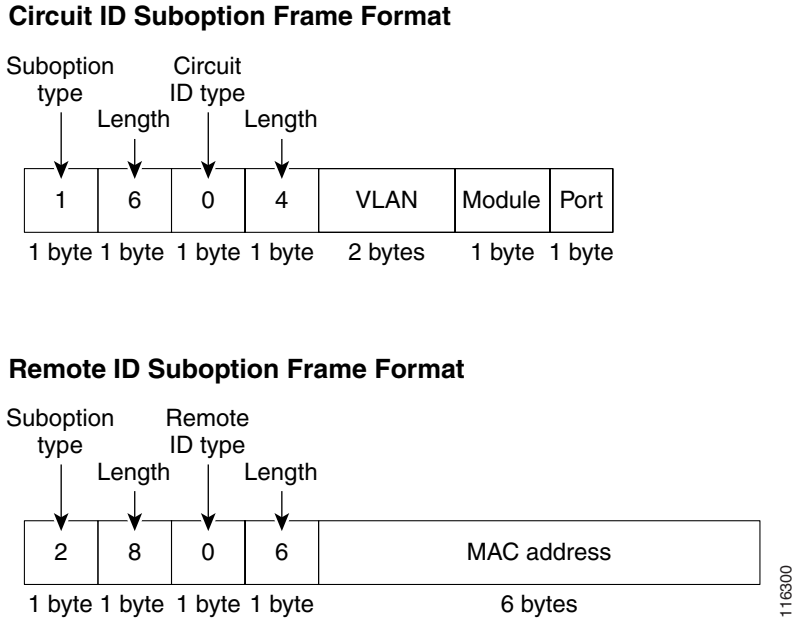
1. The host (DHCP client) generates a DHCP request and broadcasts it on the network.
2. When the NX-OS device receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the device MAC address (the remote ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit ID suboption).
3. The device adds the IP address of the relay agent to the DHCP packet.
4. The device forwards the DHCP request that includes the option-82 field to the DHCP server.
5. 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. The DHCP server echoes the option-82 field in the DHCP reply.
6. The DHCP server unicasts the reply to the NX-OS device if the request was relayed to the server by the device. The NX-OS device verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The NX-OS device removes the option-82 field and forwards the packet to the interface that connects to the DHCP client that sent the DHCP request.

If the previously described sequence of events occurs, the following values (see Figure 11-2) 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

Figure 11-2 shows the packet formats for the remote ID suboption and the circuit ID suboption. The NX-OS device uses the packet formats when you globally enable DHCP snooping and when you enable option-82 data insertion and removal. For the circuit ID suboption, the module field is the slot number of the module.

Figure 11-2 Suboption Packet Formats



Virtualization Support for DHCP Snooping

The following information applies to DHCP snooping used in Virtual Device Contexts (VDCs):

- DHCP snooping binding databases are unique per VDC. Bindings in one VDC do not affect DHCP snooping in other VDCs.
- The system does not limit binding database size on a per-VDC basis.

Licensing Requirements for DHCP Snooping

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	DHCP snooping requires a LAN Enterprise license. For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the *Cisco DCNM Licensing Guide.*
NX-OS	DHCP snooping requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0.*

Prerequisites for DHCP Snooping

DHCP snooping has the following prerequisites:

- You must be familiar with DHCP to configure DHCP snooping.

Guidelines and Limitations

DHCP snooping has the following configuration guidelines and limitations:

- When you use the **feature dhcp** command to enable the DHCP snooping feature, there is a delay of approximately 30 seconds before the I/O modules receive DHCP snooping or DAI configuration. This delay occurs regardless of the method that you use to change from a configuration with DHCP snooping disabled to a configuration with DHCP snooping enabled. For example, if you use the Rollback feature to revert to a configuration that enables DHCP snooping, the I/O modules receive DHCP snooping and DAI configuration approximately 30 seconds after you complete the rollback.
- The DHCP snooping database can store 2000 bindings.
- DHCP snooping is not active until you enable the feature, enable DHCP snooping globally, and enable DHCP snooping on at least one VLAN.
- Before globally enabling DHCP snooping on the device, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- Access-control list (ACL) statistics are not supported if the DHCP snooping feature is enabled.
- For each device that you use DCNM to configure DHCP snooping, ensure that you configure the logging level for DHCP snooping to 6 (Informational) or a higher level. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

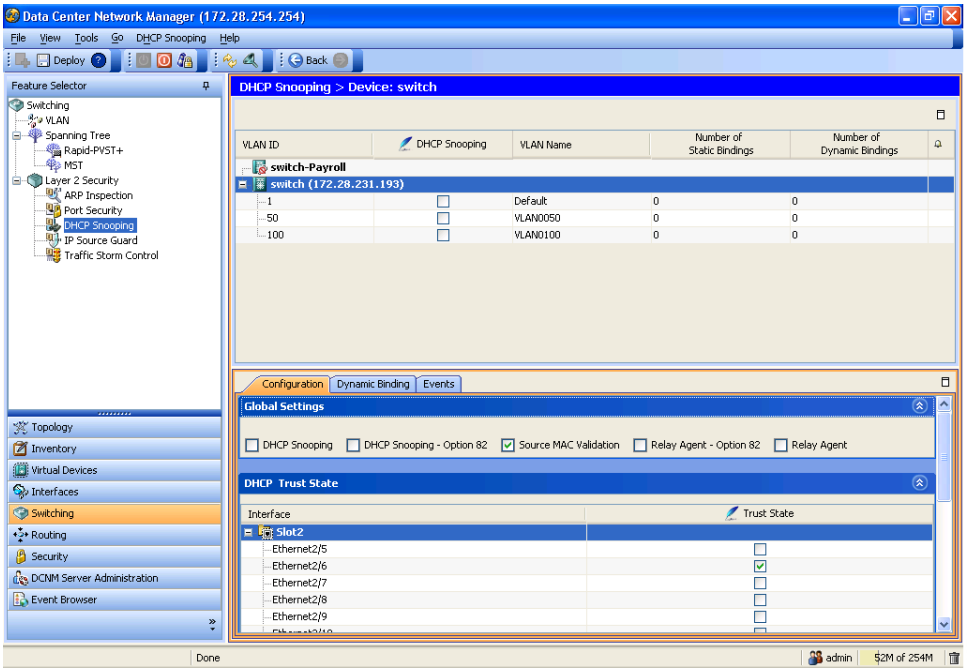
```
switch(config)# logging level dhcp 6
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

  For more information about NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0*.

Configuring DHCP Snooping

Figure 11-3 shows the DHCP Snooping content pane.

Figure 11-3 DHCP Snooping Content Pane



This section includes the following topics:

- Minimum DHCP Snooping Configuration, page 11-7
- Enabling or Disabling the DHCP Snooping Feature, page 11-8
- Enabling or Disabling DHCP Snooping Globally, page 11-9
- Enabling or Disabling DHCP Snooping on a VLAN, page 11-10
- Enabling or Disabling DHCP Snooping MAC Address Verification, page 11-10
- Enabling or Disabling Option-82 Data Insertion and Removal, page 11-11
- Configuring a Layer 2 Interface as Trusted or Untrusted, page 11-12
- Enabling or Disabling the DHCP Relay Agent, page 11-12
- Enabling or Disabling Option 82 for the DHCP Relay Agent, page 11-13
- Configuring a DHCP Server Address on a Layer 3 Ethernet Interface, page 11-14
- Configuring a DHCP Server Address on a Port Channel, page 11-14
- Configuring a DHCP Server Address on a VLAN Interface, page 11-15

Minimum DHCP Snooping Configuration

The minimum configuration for DHCP snooping is as follows:

Step 1 Enable the DHCP snooping feature. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

When the DHCP snooping feature is disabled, you cannot configure DHCP snooping.

Step 2 Enable DHCP snooping globally. For more information, see the "Enabling or Disabling DHCP Snooping Globally" section on page 11-9.

Step 3 Enable DHCP snooping on at least one VLAN. For more information, see the "Enabling or Disabling DHCP Snooping on a VLAN" section on page 11-10.

By default, DHCP snooping is disabled on all VLANs.

Step 4 Ensure that the DHCP server is connected to the device using a trusted interface. For more information, see the "Configuring a Layer 2 Interface as Trusted or Untrusted" section on page 11-12.

Step 5 (Optional) Enable the DHCP relay agent. For more information, see the "Enabling or Disabling the DHCP Relay Agent" section on page 11-12.

Step 6 (Optional) Configure an interface with the IP address of the DHCP server. For more information, see one of the following topics:

- Configuring a DHCP Server Address on a Layer 3 Ethernet Interface, page 11-14
- Configuring a DHCP Server Address on a Port Channel, page 11-14
- Configuring a DHCP Server Address on a VLAN Interface, page 11-15

Enabling or Disabling the DHCP Snooping Feature

You can enable or disable the DHCP snooping feature on the device. By default, DHCP snooping is disabled.

BEFORE YOU BEGIN

If you disable the DHCP snooping feature, all DHCP snooping configuration is lost. If you want to turn off DHCP snooping and preserve the DHCP snooping configuration, disable DHCP globally. For more information, see the "Enabling or Disabling DHCP Snooping Globally" section on page 11-9.

If you enable DHCP snooping, ensure that you configure the logging level for DHCP snooping to 6 (Informational) or a higher level on the NX-OS device. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

```
switch(config)# logging level dhcp 6
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

For more information about NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0*.

DETAILED STEPS

To enable or disable the DHCP snooping feature on the device, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to enable or disable DHCP snooping.

Step 3 Do one of the following:

- To enable DHCP snooping, from the menu bar, choose **DHCP Snooping > Enable DHCP Snooping Service**.

  In the Details pane, the Global Settings and DHCP Rate Limiting sections appear on the Configuration tab.
- To disable DHCP snooping, from the menu bar, choose **DHCP Snooping > Disable DHCP Snooping Service**.

  In the Details pane, the Enable DHCP Snooping service link appears on the Configuration tab.

Step 4 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Enabling or Disabling DHCP Snooping Globally

You can enable or disable the DHCP snooping globally on the device.

BEFORE YOU BEGIN

By default, DHCP snooping is globally disabled.

Ensure that you have enabled the DHCP snooping feature. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

Globally disabling DHCP snooping stops the device from performing any DHCP snooping or relaying DHCP messages. It preserves DCHP snooping configuration.

DETAILED STEPS

To enable or disable DHCP snooping globally on the device, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to enable or disable DHCP snooping globally.

Step 3 From the Details pane, click the **Configuration** tab and expand the **Global Settings** section, if necessary.

Step 4 Do one of the following:

- To enable DCHP snooping globally, check **DHCP Snooping**.
- To disable DCHP snooping globally, uncheck **DHCP Snooping**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Enabling or Disabling DHCP Snooping on a VLAN

You can enable or disable DHCP snooping on one or more VLANs.

BEFORE YOU BEGIN

By default, DHCP snooping is disabled on all VLANs.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To enable or disable DHCP snooping on a VLAN, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device on which you want to enable or disable per-VLAN DHCP snooping.

The VLANs for the device that you double-clicked appear in the Summary pane.

Step 3 Click the VLAN that you want to configure with DHCP snooping.

In the Details pane, the DHCP VLAN Details tab appears.

Step 4 Do one of the following:

- To enable DHCP snooping on a VLAN, on the DHCP VLAN Details tab, check **DHCP Snooping**.
- To disable per-VLAN DHCP snooping, on the DHCP VLAN Details tab, uncheck **DHCP Snooping**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Enabling or Disabling DHCP Snooping MAC Address Verification

You can enable or disable DHCP snooping MAC address verification. If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet.

BEFORE YOU BEGIN

MAC address verification is enabled by default.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To enable or disable DHCP snooping MAC address verification, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to enable or disable DHCP snooping MAC address verification.

Step 3 From the Details pane, click the **Configuration** tab and expand the **Global Settings** section, if necessary.

Step 4 Do one of the following:

- To enable MAC address verification, check **Source MAC Validation**.
- To disable MAC address verification, uncheck **Source MAC Validation**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Enabling or Disabling Option-82 Data Insertion and Removal

You can enable or disable the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.

Note You must separately configure the DHCP relay agent to support option 82. For more information, see the "Enabling or Disabling Option 82 for the DHCP Relay Agent" section on page 11-13.

BEFORE YOU BEGIN

By default, the device does not include option-82 information in DHCP packets.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To enable or disable Option-82 data insertion and removal, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to enable or disable option-82 data insertion and removal.

Step 3 From the Details pane, click the **Configuration** tab and expand the **Global Settings** section, if necessary.

Step 4 Do one of the following:

- To enable option-82 data insertion and removal, check **DHCP Snooping - Option 82**.
- To disable option-82 data insertion and removal, uncheck **DHCP Snooping - Option 82**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring a Layer 2 Interface as Trusted or Untrusted

You can configure whether an interface is a trusted or untrusted source of DHCP messages. You can configure this on interfaces operating in any the following port modes:

- Access
- Trunk
- Private VLAN Host
- Private VLAN Promiscuous

BEFORE YOU BEGIN

By default, all interfaces are untrusted.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To configure an interface as trusted or untrusted, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to configure an interface trust state.

Step 3 From the Details pane, click the **Configuration** tab and expand the **DHCP Rate Limiting** section, if necessary.

Step 4 From the DHCP Rate Limiting section, expand the slot that contains the interface that you want to configure, if necessary.

The Layer 2 interfaces on the slot appear in the Details pane. For each interface, a check box in the Trust State column indicates whether the device trusts the interface.

Step 5 For each interface whose trust state you want to configure, do one of the following:

- To make the interface a trusted interface, check the check box in the Trust State column.
- To make the interface an untrusted interface, uncheck the check box in the Trust State column.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Enabling or Disabling the DHCP Relay Agent

You can enable or disable the DHCP relay agent.

BEFORE YOU BEGIN

By default, the DHCP relay agent is disabled.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To enable or disable the DHCP relay agent, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to enable or disable option-82 data insertion and removal.

Step 3 From the Details pane, click the **Configuration** tab and expand the **Global Settings** section, if necessary.

Step 4 Do one of the following:

- To enable the DHCP relay agent, check **Relay Agent**.
- To disable the DHCP relay agent, uncheck **Relay Agent**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Enabling or Disabling Option 82 for the DHCP Relay Agent

You can enable or disable the device to insert and remove option-82 information on DHCP packets forwarded by the relay agent.

BEFORE YOU BEGIN

By default, the DHCP relay agent does not include option-82 information in DHCP packets.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To enable or disable option 82 for the DHCP relay agent, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to enable or disable option-82 data insertion and removal.

Step 3 From the Details pane, click the **Configuration** tab and expand the **Global Settings** section, if necessary.

Step 4 Do one of the following:

- To enable option 82 for the relay agent, check **Relay Agent - Option 82**.
- To disable option 82 for the relay agent, uncheck **Relay Agent - Option 82**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring a DHCP Server Address on a Layer 3 Ethernet Interface

You can configure a DHCP server IP address on a Layer 3 Ethernet interface or subinterface. A Layer 3 Ethernet interface is an interface that is operating in routed port mode. When an inbound DHCP BOOTREQUEST packet arrives on a port that is a member of the port channel, the relay agent forwards the packet to the IP address specified.

BEFORE YOU BEGIN

By default, there is no DHCP server IP address configured on a Layer 3 interface.

Ensure that the DHCP server is correctly configured.

Determine the IP address of the DHCP server.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To configure a DHCP server IP address on a Layer 3 Ethernet interface or subinterface, follow these steps:

Step 1 From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device that has the interface that you want to configure.

Available slots on the device appear in the Summary pane.

Step 3 Double-click the slot that has the interface that you want to configure.

Available interfaces on the slot appear in the Summary pane.

Step 4 Double-click the interface that you want to configure or that has the subinterface that you want to configure.

The Port Details tab appears in the Details pane.

Step 5 (Optional) Click the subinterface that you want to configure.

Step 6 From the Details pane, click the **Port Details** tab and expand the **Port Mode Settings** section, if necessary.

Step 7 In the Port Mode Settings section, in the Helper area, right-click and choose **Add Helper IP**.

Step 8 Enter the IPv4 address of the DHCP server.

Step 9 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring a DHCP Server Address on a Port Channel

You can configure a DHCP server IP address on a port channel. When an inbound DHCP BOOTREQUEST packet arrives on a port that is a member of the port channel, the relay agent forwards the packet to the IP address specified.

BEFORE YOU BEGIN

By default, there is no DHCP server IP address configured on a port channel.

Ensure that the DHCP server is correctly configured.

Determine the IP address of the DHCP server.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To configure a DHCP server IP address on a port channel, follow these steps:

Step 1 From the Feature Selector pane, choose **Interfaces > Logical > Port Channel**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device that has the port channel that you want to configure.

Available port channels on the device appear in the Summary pane.

Step 3 Click the channel ID of the port channel that you want to configure.

The Port Channel Advanced Settings tab appears in the Details pane.

Step 4 From the Details pane, click the **Port Channel Advanced Settings** tab and expand the **IP Address Settings** section, if necessary.

Step 5 In the IP Address Settings section, in the Helper area, right-click and choose **Add Helper IP**.

Step 6 Enter the IPv4 address of the DHCP server.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring a DHCP Server Address on a VLAN Interface

You can configure a DHCP server IP address on a VLAN interface (sometimes referred to as a switched virtual interface or SVI). When an inbound DHCP BOOTREQUEST packet arrives on the VLAN interface, the relay agent forwards the packet to the IP address specified.

BEFORE YOU BEGIN

By default, there is no DHCP server IP address configured on a VLAN interface.

Ensure that the DHCP server is correctly configured.

Determine the IP address of the DHCP server.

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 11-8.

DETAILED STEPS

To configure a DHCP server IP address on a VLAN interface, follow these steps:

Step 1 From the Feature Selector pane, choose **Interfaces > Logical > VLAN Network Interface**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device that has the interface that you want to configure.

Available VLAN interfaces on the device appear in the Summary pane.

Step 3 Click the VLAN ID of the VLAN interface that you want to configure.

The Details tab appears in the Details pane.

Step 4 From the Details pane, click the **Details** tab and expand the **IP Address Settings** section, if necessary.

Step 5 In the IP Address Settings section, in the Helper area, right-click and choose **Add Helper IP**.

Step 6 Enter the IPv4 address of the DHCP server.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Displaying DHCP Bindings

To display DHCP bindings for a device, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Layer 2 Security > DHCP Snooping**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device.

The Dynamic Binding tab appears in the Details pane.

Step 3 Double-click the slot that has the interface.

Step 4 From the Details pane, click the **Dynamic Binding** tab.

The Dynamic Binding tab displays a table that lists the DHCP bindings per VLAN.

Field Descriptions for DHCP Snooping

This section includes the following topics:

- Device: Configuration Tab, page 11-17
- Device: Configuration: Global Settings Section, page 11-17
- Device: Configuration: DHCP Trust State Section, page 11-17
- Device: Dynamic Binding Tab, page 11-18
- VLAN: DHCP VLAN Details Tab, page 11-18

Device: Configuration Tab

Table 11-1 Device: Configuration Tab

Field	Description
Enable DHCP Snooping service	Link that enables the DHCP snooping feature globally on the device. This link appears only when DHCP snooping is not enabled on the selected device. By default, DHCP snooping is not enabled.

Device: Configuration: Global Settings Section

Table 11-2 Device: Configuration: Global Settings Section

Figure	Description
DHCP Snooping	Whether DHCP snooping is enabled globally on the device. By default, this check box is unchecked.
DHCP Snooping - Option 82	Whether option-82 data insertion and removal is enabled on the device. By default, this check box is unchecked.
Source MAC Validation	Whether MAC address verification is enabled for DHCP snooping. When this check box is checked, the device verifies that in packets received on an untrusted interface, the source MAC address and the DHCP client hardware address match. If they do not, the device drops the packet. By default, this check box is unchecked.
Relay Agent - Option 82	Whether option-82 data insertion and removal by the DHCP relay agent is enabled on the device. By default, this check box is unchecked.
Relay Agent	Whether the DHCP relay agent is enabled on the device. By default, this check box is unchecked.

Device: Configuration: DHCP Trust State Section

Table 11-3 Device: Configuration: DHCP Trust State Section

Figure	Description
Interface	*Display only.* Name of the Layer 2 interface or the name of the slot containing Layer 2 interfaces.
Trust State	Whether the interface is trusted. When this check box is checked, the device does not trust DHCP sources on the interface. By default, this check box is unchecked.

Device: Dynamic Binding Tab

Table 11-4 Device: Dynamic Binding Tab

Figure	Description
VLAN	*Display only.* VLAN ID associated with the dynamic DHCP binding.
MAC Address	*Display only.* MAC address of the dynamic DHCP binding.
IP Address	*Display only.* IP address of the dynamic DHCP binding.
Lease Expiry Time	*Display only.* Date and time when the DHCP IP address lease expires.

VLAN: DHCP VLAN Details Tab

Table 11-5 VLAN: DHCP VLAN Details Tab

Figure	Description
VLAN	*Display only.* ID number of the VLAN.
VLAN Name	*Display only.* Name assigned to the VLAN. By default, VLAN 1 is named Default and all other VLANs are named by combining “VLAN” the four-digit VLAN ID. For example, the default VLAN name for VLAN 50 is VLAN0050.
Number of Static Bindings	*Display only.* By default, the number of static bindings is zero (0).
Number of Dynamic Bindings	*Display only.* By default, the number of dynamic bindings is zero (0).
DHCP Snooping	Whether DHCP snooping is enabled for the VLAN. By default, this check box is unchecked.
DHCP Operational State	*Display only.* Whether DHCP snooping is active on the interface.

Additional References

For additional information related to implementing DHCP snooping, see the following sections:

- Related Documents, page 11-19
- Standards, page 11-19

Related Documents

Related Topic	Document Title
IP Source Guard	Information About IP Source Guard, page 13-1
Dynamic ARP Inspection	Information About DAI, page 12-1

Standards

Standards	Title
RFC-2131	*Dynamic Host Configuration Protocol* (http://tools.ietf.org/html/rfc2131)
RFC-3046	*DHCP Relay Agent Information Option* (http://tools.ietf.org/html/rfc3046)