



# Configuring DHCP

---

This chapter describes how to configure the Dynamic Host Configuration Protocol (DHCP) on a Cisco NX-OS device.

This chapter includes the following sections:

- [Finding Feature Information, on page 1](#)
- [Information About DHCP Snooping, on page 2](#)
- [Information About the DHCP Relay Agent, on page 6](#)
- [Information About the DHCPv6 Relay Agent, on page 9](#)
- [Virtualization Support for DHCP, on page 9](#)
- [Prerequisites for DHCP, on page 9](#)
- [Guidelines and Limitations for DHCP, on page 9](#)
- [Default Settings for DHCP, on page 11](#)
- [Configuring DHCP, on page 12](#)
- [Configuring DHCPv6, on page 33](#)
- [Verifying the DHCP Configuration, on page 38](#)
- [Displaying DHCP Bindings, on page 38](#)
- [Clearing the DHCP Snooping Binding Database, on page 38](#)
- [Clearing DHCP Relay Statistics, on page 39](#)
- [Clearing DHCPv6 Relay Statistics, on page 40](#)
- [Monitoring DHCP, on page 40](#)
- [Additional References for DHCP, on page 40](#)
- [Feature History for DHCP, on page 41](#)

## Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter or the Feature History table in this chapter.

# 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.

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

## 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 Cisco 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.

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

You can remove entries from the binding database by using the **clear ip dhcp snooping binding** command.

#### Related Topics

[Clearing the DHCP Snooping Binding Database](#), on page 38

## DHCP Snooping in a vPC Environment

A virtual port channel (vPC) allows two Cisco NX-OS switches to appear as a single logical port channel to a third device. The third device can be a switch, server, or any other networking device that supports port channels.

In a typical vPC environment, DHCP requests can reach one vPC peer switch and the responses can reach the other vPC peer switch, resulting in a partial DHCP (IP-MAC) binding entry in one switch and no binding entry in the other switch. As a result, DHCP snooping and associated features such as dynamic ARP inspection (DAI) and IP Source Guard are disrupted. Beginning with Cisco NX-OS Release 5.1, this issue is addressed by using Cisco Fabric Service over Ethernet (CFSoE) distribution to ensure that all DHCP packets (requests and responses) appear on both switches, which helps in creating and maintaining the same binding entry on both switches for all clients behind the vPC link.

CFSoE distribution also allows only one switch to forward the DHCP requests and responses on the vPC link. In non-vPC environments, both switches forward the DHCP packets.

## Synchronizing DHCP Snooping Binding Entries

The dynamic DHCP binding entries should be synchronized in the following scenarios:

- When the remote vPC is online, all the binding entries for that vPC link should be synchronized with the peer.
- When DHCP snooping is enabled on the peer switch, the dynamic binding entries for all vPC links should be synchronized with the peer.

## 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 a DHCPACK, DHCPNAK, or DHCP OFFER 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.

In addition, you can enable strict validation of DHCP packets, which checks the options field of DHCP packets, including the “magic cookie” value in the first four bytes of the options field. By default, strict validation is disabled. When you enable it, by using the **ip dhcp packet strict-validation** command, if DHCP snooping processes a packet that has an invalid options field, it drops the packet.

#### Related Topics

[Enabling or Disabling Strict DHCP Packet Validation](#), on page 17

## DHCP Snooping Option 82 Data Insertion

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.

When you enable Option 82 on the Cisco 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 Cisco 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). For hosts behind the port channel, the circuit ID is filled with the if\_index of the port channel.




---

**Note** For vPC peer switches, the remote ID suboption contains the vPC switch MAC address, which is unique in both switches. This MAC address is computed with the vPC domain ID. The Option 82 information is inserted at the switch where the DHCP request is first received before it is forwarded to the other vPC peer switch.

---

3. The device forwards the DHCP request that includes the Option 82 field to the DHCP server.
4. 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.
5. The DHCP server sends the reply to the Cisco NX-OS device. The Cisco NX-OS device verifies that it originally inserted the Option 82 data by inspecting the remote ID and possibly the circuit ID fields. The Cisco 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 do not change:

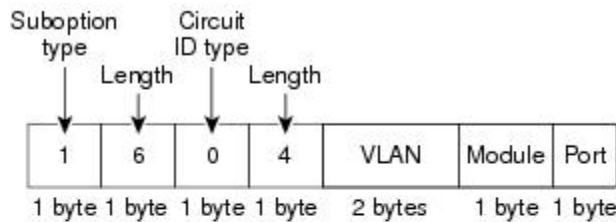
- Circuit ID suboption fields

- 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

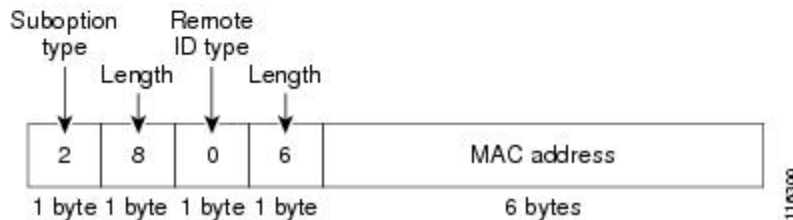
**Figure 1: Suboption Packet Formats**

This figure shows the packet formats for the remote ID suboption and the circuit ID suboption. The Cisco 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.

**Circuit ID Suboption Frame Format**



**Remote ID Suboption Frame Format**

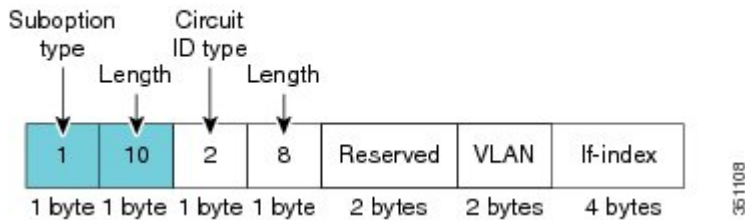


**Figure 2: Circuit ID Suboption Frame Format for Regular and vPC Interfaces**

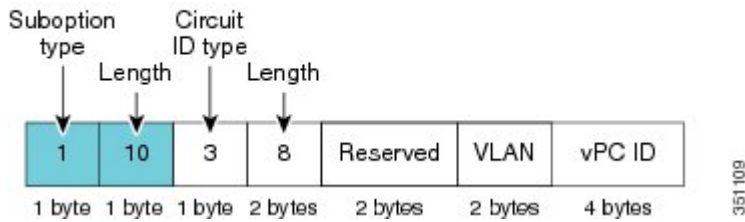
Beginning with Cisco NX-OS Release 6.2(2), a new circuit ID format is used when Option 82 is enabled in DHCP snooping. The new circuit ID format is used by default and cannot be disabled. However, you might need to configure the DHCP server for the new circuit ID format if it was using the old Option 82 format for IP address allocation. These figures show the new default circuit ID format that is used for regular interfaces and vPC interfaces when Option 82 is enabled for DHCP snooping.

The enhanced Option 82 format improves DHCP packet processing. For vPC and vPC+ interfaces, the new format assigns vPC peers a unique circuit ID in case some are configured with different port channel numbers.

### Circuit ID Suboption Frame Format (Regular Interface)



### Circuit ID Suboption Frame Format (vPC/vPC+ Interface)



## Information About the DHCP Relay Agent

### 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 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 (Option 82) 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.

After you enable Option 82, the device uses the binary ifindex format by default. If needed, you can change the Option 82 setting to use an encoded string format instead.



**Note** When the device relays a DHCP request that already includes Option 82 information, the device forwards the request with the original Option 82 information without altering it.

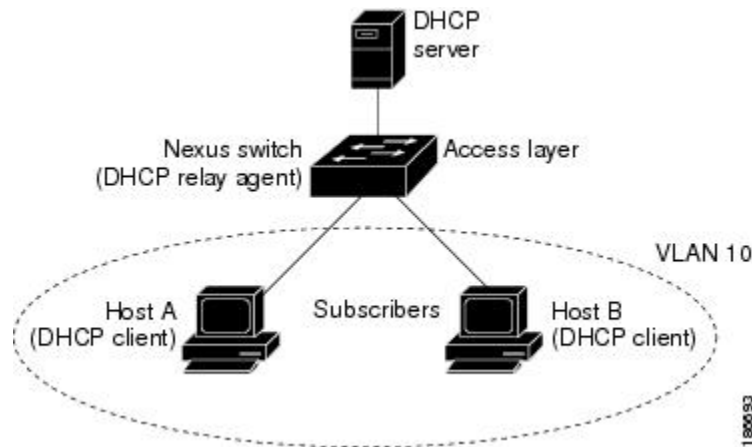
### DHCP Relay Agent Option 82

You can enable the device to insert and remove Option 82 information on DHCP packets that are forwarded by the relay agent.

*Figure 3: DHCP Relay Agent in a Metropolitan Ethernet Network*

This figure 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.



When you enable Option 82 for the DHCP relay agent on the Cisco 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 Cisco 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). In DHCP relay, the circuit ID is filled with the if\_index of the SVI or Layer 3 interface on which DHCP relay is configured.




---

**Note** For vPC peer devices, the remote ID suboption contains the vPC device MAC address, which is unique in both devices. This MAC address is computed with the vPC domain ID. The Option 82 information is inserted at the device where the DHCP request is first received before it is forwarded to the other vPC peer device.

---

3. When **dhcp relay source interface** *interface* is configured the device adds the configured source interface IP address as giaddr to the DHCP packet if source interface vrf is same as that of DHCP server VRF, otherwise IP address of the interface through which the server is reachable will be used as giaddr.
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 Cisco NX-OS device if the request was relayed to the server by the device. The Cisco NX-OS device verifies that it originally inserted the Option 82 data by inspecting the remote ID and possibly the circuit ID fields. The Cisco 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.

## VRF Support for the DHCP Relay Agent

You can configure the DHCP relay agent to forward DHCP broadcast messages from clients in a virtual routing and forwarding (VRF) instance to DHCP servers in a different VRF. By using a single DHCP server to provide DHCP support to clients in multiple VRFs, you can conserve IP addresses by using a single IP address pool rather than one for each VRF. For general information about VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Enabling VRF support for the DHCP relay agent requires that you enable Option 82 for the DHCP relay agent.

If a DHCP request arrives on an interface that you have configured with a DHCP relay address and VRF information, and the address of the DHCP server belongs to a network on an interface that is a member of a different VRF, the device inserts Option 82 information in the request and forwards it to the DHCP server in the server VRF. The Option 82 information includes the following:

### VPN identifier

Name of the VRF that the interface that receives the DHCP request is a member of.

### Link selection

Subnet address of the interface that receives the DHCP request. When DHCP smart relay is enabled, the link selection is filled with the subnet of the active giaddr.

### Server identifier override

IP address of the interface that receives the DHCP request. When DHCP smart relay is enabled, the server identifier is filled with the active giaddr.



#### Note

The DHCP server must support the VPN identifier, link selection, and server identifier override options.

When the device receives the DHCP response message, it strips off the Option 82 information and forwards the response to the DHCP client in the client VRF.

### Related Topics

[Enabling or Disabling VRF Support for the DHCP Relay Agent](#), on page 27

## DHCP Smart Relay Agent

When the DHCP relay agent receives broadcast DHCP request packets from a host, it sets giaddr to the primary address of the inbound interface and forwards the packets to the server. The server allocates IP addresses from the giaddr subnet pool until the pool is exhausted and ignores further requests.

Beginning with Cisco NX-OS Release 5.2, you can configure the DHCP smart relay agent to allocate IP addresses from the secondary IP address subnet pool if the first subnet pool is exhausted or the server ignores further requests. This enhancement is useful if the number of hosts is greater than the number of IP addresses in the pool or if multiple subnets are configured on an interface using secondary addresses.

### Related Topics

[Enabling or Disabling DHCP Smart Relay Globally](#), on page 31

[Enabling or Disabling DHCP Smart Relay on a Layer 3 Interface](#), on page 32



# Information About the DHCPv6 Relay Agent

## DHCPv6 Relay Agent

You can configure the device to run a DHCPv6 relay agent, which forwards DHCPv6 packets between clients and servers. This feature is useful when clients and servers are not on the same physical subnet. Relay agents receive DHCPv6 messages and then generate a new DHCPv6 message to send out on another interface. The relay agent sets the gateway address (giaddr field of the DHCPv6 packet) and forwards it to the DHCPv6 server.

## VRF Support for the DHCPv6 Relay Agent

You can configure the DHCPv6 relay agent to forward DHCPv6 broadcast messages from clients in a virtual routing and forwarding (VRF) instance to DHCPv6 servers in a different VRF. By using a single DHCPv6 server to provide DHCP support to clients in multiple VRFs, you can conserve IP addresses by using a single IP address pool rather than one for each VRF. For general information about VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

## Virtualization Support for DHCP

The following information applies to DHCP 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 the binding database size on a per-VDC basis.
- The DHCP smart relay agent can be configured independently in default and nondefault VDCs.

## Prerequisites for DHCP

DHCP has the following prerequisite:

- You should be familiar with DHCP before you configure DHCP snooping or the DHCP relay agent.

## Guidelines and Limitations for DHCP

DHCP has the following configuration guidelines and limitations:

- If you are using both the Unicast reverse Packeting Forwarding (uRFP) strict mode in your client vPC VLANs and the First Hop Redundancy Protocol (FHRP) with the DHCP relay feature, the DHCP requests are sourced from the physical egress IP address interface (not the FHRP VIP) by default. Consequently, if your DHCP server is not on a directly connected subnet and you have multiple ECMP routes back to your vPC pair, some packets might land on the neighbor switch instead of the originating switch and be

dropped by RFP. This behavior is expected. To avoid this scenario, perform one of the following workarounds:

- Use the uRFP loose mode, not uRFP strict.
- Configure static routes for the interface address on the affected FHRP interfaces and redistribute the static routes into IGP.
- Using the **ip dhcp relay source-interface** *interface-name* command, you can configure a different interface as the source interface. This command is used for DHCP relay in VPN and in non-VPN environments. The dhcp relay information option with vpn sub-option must be enabled for this command configuration to work. To enable VRF support for the DHCP relay agent, use the **ip dhcp relay information option vpn** command. For more details about the **ip dhcp relay information option vpn** command, see the [Cisco Nexus 7000 Series Security Command Reference](#).
- For Cisco NX-OS Release 6.2 and later releases, you must enable the insertion of Option 82 information for DHCP packets to support the highest DHCP snooping scale.
- After System Switchover, DHCP Global stats show incorrect values as they are not stored in PSS and get erased. Updating stats in PSS during packet path will affect scale.
- If you use DHCP relay where DHCP clients and servers are in different VRF instances, use only one DHCP server within a VRF.
- 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.
- DHCP snooping does not work with DHCP relay configured on the same nexus device.
- If a VLAN ACL (VACL) is configured on a VLAN that you are configuring with DHCP snooping, ensure that the VACL permits DHCP traffic between DHCP servers and DHCP hosts. When both DHCP snooping and DHCP relay are enabled on a VLAN and the SVI of that VLAN, DHCP relay takes precedence.
- If an ingress router ACL is configured on a Layer 3 interface that you are configuring with a DHCP server address, ensure that the router ACL permits DHCP traffic between DHCP servers and DHCP hosts.
- Access-control list (ACL) statistics are not supported if the DHCP snooping feature is enabled.
- Make sure that the DHCP configuration is synchronized across the devices in a vPC link. Otherwise, a run-time error can occur, resulting in dropped packets.
- Beginning with Cisco NX-OS Release 5.1, DHCP snooping is supported with FabricPath. Follow these guidelines when enabling DHCP snooping in a FabricPath network:
  - DHCP snooping should be enabled on CE-FabricPath boundary devices.
  - DHCP snooping is enabled on all access layer devices to secure the network at the access layer itself.
  - DHCP does not learn any binding entries on ports in FabricPath mode as users should have enabled DHCP snooping on all access layer devices. As a result, when DAI is enabled, ARP packets received on FabricPath ports are allowed.
  - IPSG cannot be enabled on ports in FabricPath mode.




---

**Note** For more information on FabricPath, see the *Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*.

---

- DHCP smart relay and DHCP subnet broadcast support are limited to the first 100 IP addresses of the interface on which they are enabled.
- You must configure a helper address on the interface in order to use DHCP smart relay and DHCP subnet broadcast support.
- In a vPC environment with DHCP smart relay enabled, the subnet of the primary and secondary addresses of an interface should be the same on both Cisco NX-OS devices.
- Before using POAP, make sure that DHCP snooping is enabled and firewall rules are set to block unintended or malicious DHCP servers.
- When you configure DHCPv6 server addresses on an interface, a destination interface cannot be used with global IPv6 addresses.




---

**Note** For DHCP configuration limits, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.

---

## Default Settings for DHCP

This table lists the default settings for DHCP parameters.

**Table 1: Default DHCP Parameters**

Parameters	Default
DHCP feature	Disabled
DHCP snooping	Disabled
DHCP snooping on VLANs	Disabled
DHCP snooping MAC address verification	Enabled
DHCP snooping Option 82 support	Disabled
DHCP snooping trust	Untrusted
DHCP relay agent	Enabled
DHCPv6 relay agent	Enabled
Lightweight DHCPv6 Relay Agent	Disabled
UDP Relay feature	Disabled

Parameters	Default
VRF support for the DHCP relay agent	Disabled
VRF support for the DHCPv6 relay agent	Disabled
DHCP relay sub-option type cisco	Disabled
DHCPv6 relay option type cisco	Disabled
DHCP Option 82 for relay agent	Disabled
Subnet broadcast support for the DHCP relay agent	Disabled
DHCP smart relay agent	Disabled
DHCP server IP address	None

# Configuring DHCP

## Minimum DHCP Configuration

- 
- Step 1** Enable the DHCP feature.  
When the DHCP feature is disabled, you cannot configure DHCP snooping.
- Step 2** Enable DHCP snooping globally.
- Step 3** Enable DHCP snooping on at least one VLAN.  
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.
- Step 5** (Optional) If DHCP servers and clients are in different VRF instances, do the following:
- a) Enable Option 82 for the DHCP relay agent.
  - b) Enable VRF support for the DHCP relay agent.
- Step 6** (Optional) Configure an interface with the IP address of the DHCP server.

---

### Related Topics

- [Enabling or Disabling the DHCP Feature](#), on page 13
- [Enabling or Disabling DHCP Snooping Globally](#), on page 13
- [Enabling or Disabling DHCP Snooping on a VLAN](#), on page 14
- [Configuring an Interface as Trusted or Untrusted](#), on page 18
- [Enabling or Disabling the DHCP Relay Agent](#), on page 23
- [Enabling or Disabling Option 82 for the DHCP Relay Agent](#), on page 26
- [Configuring DHCP Server Addresses on an Interface](#), on page 29
- [Enabling or Disabling VRF Support for the DHCP Relay Agent](#), on page 27

## Enabling or Disabling the DHCP Feature

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

When the DHCP feature is disabled, you cannot configure DHCP snooping, the DHCP relay agent, or any of the features that depend on DHCP, such as dynamic ARP inspection and IP Source Guard. In addition, all DHCP, dynamic ARP inspection, and IP Source Guard configuration is removed from the device.

### SUMMARY STEPS

1. `config t`
2. `[no] feature dhcp`
3. (Optional) `show running-config dhcp`
4. (Optional) `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>config t</b> <b>Example:</b> <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.
Step 2	<b>[no] feature dhcp</b> <b>Example:</b> <pre>switch(config)# feature dhcp</pre>	Enables the DHCP feature. The <b>no</b> option disables the DHCP feature and erases all DHCP configuration.
Step 3	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <pre>switch(config)# show running-config dhcp</pre>	Displays the DHCP configuration.
Step 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

#### Related Topics

[Enabling or Disabling DHCP Snooping Globally](#), on page 13

## Enabling or Disabling DHCP Snooping Globally

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

#### Before you begin

Ensure that you have enabled the DHCP feature.

**SUMMARY STEPS**

1. **config t**
2. **[no] ip dhcp snooping**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>config t</b> <b>Example:</b> switch# config t switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip dhcp snooping</b> <b>Example:</b> switch(config)# ip dhcp snooping	Enables DHCP snooping globally. The <b>no</b> option disables DHCP snooping.
<b>Step 3</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling or Disabling the DHCP Feature](#), on page 13

**Enabling or Disabling DHCP Snooping on a VLAN**

You can enable or disable DHCP snooping on one or more VLANs. By default, DHCP snooping is disabled on all VLANs.

**Before you begin**

Ensure that the DHCP feature is enabled.



**Note** If a VACL is configured on a VLAN that you are configuring with DHCP snooping, ensure that the VACL permits DHCP traffic between DHCP servers and DHCP hosts.

**SUMMARY STEPS**

1. **config t**
2. **[no] ip dhcp snooping vlan *vlan-list***

3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>config t</b> <b>Example:</b> <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.
Step 2	<b>[no] ip dhcp snooping vlan <i>vlan-list</i></b> <b>Example:</b> <pre>switch(config)# ip dhcp snooping vlan 100,200,250-252</pre>	Enables DHCP snooping on the VLANs specified by <i>vlan-list</i> . The <b>no</b> option disables DHCP snooping on the VLANs specified.
Step 3	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <pre>switch(config)# show running-config dhcp</pre>	Displays the DHCP configuration.
Step 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

#### Related Topics

[Enabling or Disabling the DHCP Feature](#), on page 13

## 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. MAC address verification is enabled by default.

#### Before you begin

Ensure that the DHCP feature is enabled.

#### SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp snooping verify mac-address**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b> <b>Example:</b> switch# config t switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip dhcp snooping verify mac-address</b> <b>Example:</b> switch(config)# ip dhcp snooping verify mac-address	Enables DHCP snooping MAC address verification. The <b>no</b> option disables MAC address verification.
<b>Step 3</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Related Topics

[Enabling or Disabling the DHCP Feature](#), on page 13

## 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. By default, the device does not include Option 82 information in DHCP packets.



**Note** DHCP relay agent support for Option 82 is configured separately.



**Note** To support a higher DHCP pps scale, you must enable the insertion of Option 82 information for DHCP packets.

### Before you begin

Ensure that the DHCP feature is enabled.

## SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp snooping information option**
3. (Optional) **show running-config dhcp**



#### 4. (Optional) `copy running-config startup-config`

##### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>config t</b> <b>Example:</b> <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.
Step 2	<b>[no] ip dhcp snooping information option</b> <b>Example:</b> <pre>switch(config)# ip dhcp snooping information option</pre>	Enables the insertion and removal of Option 82 information for DHCP packets. The <b>no</b> option disables the insertion and removal of Option 82 information.
Step 3	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <pre>switch(config)# show running-config dhcp</pre>	Displays the DHCP configuration.
Step 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

##### Related Topics

[Enabling or Disabling the DHCP Feature](#), on page 13

[Enabling or Disabling Option 82 for the DHCP Relay Agent](#), on page 26

## Enabling or Disabling Strict DHCP Packet Validation

You can enable or disable the strict validation of DHCP packets. By default, strict validation of DHCP packets is disabled.

##### SUMMARY STEPS

1. `config t`
2. `[no] ip dhcp packet strict-validation`
3. (Optional) `show running-config dhcp`
4. (Optional) `copy running-config startup-config`

##### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>config t</b> <b>Example:</b> <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>[no] ip dhcp packet strict-validation</b> <b>Example:</b> switch(config)# ip dhcp packet strict-validation	Enables the strict validation of DHCP packets. The <b>no</b> option disables strict DHCP packet validation.
<b>Step 3</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Configuring an Interface as Trusted or Untrusted

You can configure whether an interface is a trusted or untrusted source of DHCP messages. By default, all interfaces are untrusted. You can configure DHCP trust on the following types of interfaces:

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces

### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the interface is configured as a Layer 2 interface.

### SUMMARY STEPS

1. **config t**
2. Do one of the following options:
  - **interface ethernet** *slot/port*
  - **interface port-channel** *channel-number*
3. **[no] ip dhcp snooping trust**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b> <b>Example:</b> switch# config t switch(config)#	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	Do one of the following options: <ul style="list-style-type: none"> <li>• <b>interface ethernet</b> <i>slot/port</i></li> <li>• <b>interface port-channel</b> <i>channel-number</i></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• Enters interface configuration mode, where <i>slot/port</i> is the Layer 2 Ethernet interface that you want to configure as trusted or untrusted for DHCP snooping.</li> <li>• Enters interface configuration mode, where <i>slot/port</i> is the Layer 2 port-channel interface that you want to configure as trusted or untrusted for DHCP snooping.</li> </ul>
<b>Step 3</b>	<b>[no] ip dhcp snooping trust</b> <b>Example:</b> <pre>switch(config-if)# ip dhcp snooping trust</pre>	Configures the interface as a trusted interface for DHCP snooping. The <b>no</b> option configures the port as an untrusted interface.
<b>Step 4</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <pre>switch(config-if)# show running-config dhcp</pre>	Displays the DHCP configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

#### Related Topics

[Enabling or Disabling the DHCP Feature](#), on page 13

## Enabling or Disabling DHCP Relay Trusted Port Functionality

You can enable or disable the DHCP relay trusted port functionality. By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the DHCP relay agent will not discard the packet. If the **ip dhcp relay information option trust** command is configured globally, the DHCP relay agent will discard the packet if the gateway address is set to all zeros.

#### Before you begin

Ensure that the DHCP feature is enabled.

#### SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp relay information option trust**
3. (Optional) **show ip dhcp relay**
4. (Optional) **show ip dhcp relay information trusted-sources**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b> <b>Example:</b> switch# config terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip dhcp relay information option trust</b> <b>Example:</b> switch(config)# ip dhcp relay information option trust	Enables the DHCP relay trusted port functionality. The <b>no</b> option disables this functionality.
<b>Step 3</b>	(Optional) <b>show ip dhcp relay</b> <b>Example:</b> switch(config)# show ip dhcp relay	Displays the DHCP relay configuration.
<b>Step 4</b>	(Optional) <b>show ip dhcp relay information trusted-sources</b> <b>Example:</b> switch(config)# show ip dhcp relay information trusted-sources	Displays the DHCP relay trusted ports configuration.
<b>Step 5</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Configuring an Interface as a DHCP Relay Trusted or Untrusted Port

You can configure whether a Layer 3 interface is a DHCP relay trusted or untrusted interface. By default, all interfaces are untrusted. You can configure DHCP relay trust on the following types of interfaces:

- Layer 3 Ethernet interfaces and sub-interfaces
- Layer 3 port-channel interfaces
- Interface VLAN

### Before you begin

Ensure that the DHCP feature is enabled.

## SUMMARY STEPS

1. **config t**

2. Do one of the following options:
  - **interface ethernet** *slot/port.[number]*
  - **interface port-channel** *channel-number.[subchannel-id]*
  - **interface vlan** *vlan-id*
3. **[no] ip dhcp relay information trusted**
4. **show ip dhcp relay information trusted-sources**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>config t</b> <b>Example:</b> <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.
Step 2	Do one of the following options: <ul style="list-style-type: none"> <li>• <b>interface ethernet</b> <i>slot/port.[number]</i></li> <li>• <b>interface port-channel</b> <i>channel-number.[subchannel-id]</i></li> <li>• <b>interface vlan</b> <i>vlan-id</i></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• Enters interface configuration mode, where <i>slot/port</i> is the Layer 3 Ethernet interface that you want to configure as trusted or untrusted.</li> <li>• Enters interface configuration mode, where <i>channel-number</i> is the Layer 3 port-channel interface that you want to configure as trusted or untrusted.</li> <li>• Enters interface configuration mode, where <i>vlan-id</i> is the VLAN interface that you want to configure as trusted or untrusted.</li> </ul>
Step 3	<b>[no] ip dhcp relay information trusted</b> <b>Example:</b> <pre>switch(config-if)# ip dhcp relay information trusted</pre>	Configures the interface as a trusted interface for DHCP relay agent information. The <b>no</b> option configures the port as an untrusted interface.  <b>Note</b> For any L3 interface, if the interface is configured as trusted either through global command or interface-level command, the interface is considered as a trusted interface. Hence, when the trusted-port command is enabled at Global level, any L3 interface cannot be considered as untrusted irrespective of the interface-level configuration.
Step 4	<b>show ip dhcp relay information trusted-sources</b> <b>Example:</b> <pre>switch(config-if)# show ip dhcp relay information trusted-sources</pre>	Displays the DHCP relay trusted ports configuration.
Step 5	(Optional) <b>show running-config dhcp</b> <b>Example:</b>	Displays the DHCP configuration.

	Command or Action	Purpose
	<code>switch(config-if)# show running-config dhcp</code>	
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config-if)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Configuring all Interfaces as Trusted or Untrusted

You can configure all Layer 3 interfaces as DHCP relay trusted or untrusted interfaces. By default, all interfaces are untrusted. You can configure DHCP relay trust on the following types of interfaces:

- Layer 3 Ethernet interfaces and sub-interfaces
- Layer 3 port-channel interfaces
- Interface VLAN

When you enable the **ip dhcp relay information trust-all** command, any Layer 3 interface cannot be considered as untrusted irrespective of the interface-level configuration.

### Before you begin

Ensure that the DHCP feature is enabled.

### SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp relay information trust-all**
3. **show ip dhcp relay information trusted-sources**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b> <b>Example:</b> <code>switch# config t</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip dhcp relay information trust-all</b> <b>Example:</b> <code>switch(config)# ip dhcp relay information trust-all</code>	Configures the interfaces as trusted sources of DHCP messages. The <b>no</b> option configures the ports as untrusted interfaces.
<b>Step 3</b>	<b>show ip dhcp relay information trusted-sources</b> <b>Example:</b>	Displays the DHCP relay trusted ports configuration.

	Command or Action	Purpose
	<code>switch(config)# show ip dhcp relay information trusted-sources</code>	
<b>Step 4</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	Displays the DHCP configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Enabling or Disabling the DHCP Relay Agent

You can enable or disable the DHCP relay agent. By default, the DHCP relay agent is enabled.

### Before you begin

Ensure that the DHCP feature is enabled.

### SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp relay**
3. (Optional) **show ip dhcp relay**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b> <b>Example:</b> <code>switch# config t</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip dhcp relay</b> <b>Example:</b> <code>switch(config)# ip dhcp relay</code>	Enables the DHCP relay agent. The <b>no</b> option disables the relay agent.
<b>Step 3</b>	(Optional) <b>show ip dhcp relay</b> <b>Example:</b> <code>switch(config)# show ip dhcp relay</code>	Displays the DHCP relay configuration.
<b>Step 4</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	Displays the DHCP configuration.

	Command or Action	Purpose
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling or Disabling the DHCP Feature](#), on page 13

## Enabling or Disabling the DHCP Relay Source Interface

You can enable or disable the DHCP relay source interface. You can configure a different interface as the source of the DHCP relay agent.

**Before you begin**

Ensure that the DHCP feature is enabled.

**SUMMARY STEPS**

1. **configure terminal**
2. **[no] ip dhcp relay source-interface *interface-name***
3. **[no] ip dhcp relay information option vpn**
4. **interface *interface-name***
5. **[no] ip dhcp relay address *ip address use-vrf vrf-name***
6. (Optional) **show ip dhcp relay source-interface**
7. (Optional) **show running-config dhcp**
8. (Optional) **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip dhcp relay source-interface <i>interface-name</i></b>  <b>Example:</b> switch(config)# ip dhcp relay source-interface Ethernet1/1	Enables the DHCP relay source interface. You can configure a different interface as the source of the DHCP relay agent. The <b>no</b> option disables the relay source interface.  The source interface's IP address will be used as the source address in the DHCP packet, only when the source interface and the DHCP server are in the same VRF. If not in same VRF, IP address of any other interface (through which server will be reachable) will be used.



	Command or Action	Purpose
Step 3	<p><b>[no] ip dhcp relay information option vpn</b></p> <p><b>Example:</b></p> <pre>switch(config)# ip dhcp relay information option vpn</pre>	<p>Enables VRF support for the DHCP relay agent. The no option disables the VRF support.</p> <p>The VPN option will be added in option-82 only when the server and the client are in the different VRF.</p> <p>Three sub-options get added in the information option of the relayed packet only when the server and client are in different VRFs.</p> <p>Sub-option 151 - VRF Name / VPN ID: this indicates the VRF information of the client.</p> <p>Sub-option 11 - Server ID override: this indicates the client subnet gateway.</p> <p>Sub-option 5 - Link Selection: provides the client subnet address.</p> <p>When the client and server are in different VRFs, the DHCP server address configuration must have <b>use-vrf vrf-name</b> for the DHCP relay to work.</p>
Step 4	<p><b>interface interface-name</b></p> <p><b>Example:</b></p> <pre>switch(config)# interface ethernet 1/3</pre>	Configures the interface and enters interface configuration mode.
Step 5	<p><b>[no] ip dhcp relay address ip address use-vrf vrf-name</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# ip dhcp relay address 10.43.87.132 use-vrf testA</pre>	<p>Configures an IP address for a DHCP server to which the relay agent forwards the packets received on this interface.</p> <p>The <b>use-vrf</b> option specifies the virtual routing and forwarding instance (VRF) that the DHCP server is within, where the vrf-name argument is the name of the VRF. The VRF membership of the interface connected to the DHCP server determines the VRF that the DHCP is within.</p> <p>The source interface's IP address will be used as the source address only when the source interface and the server are in the same VRF.</p>
Step 6	<p>(Optional) <b>show ip dhcp relay source-interface</b></p> <p><b>Example:</b></p> <pre>switch(config)# show ip dhcp relay source-interface</pre>	Displays the DHCP relay source-interface configuration.
Step 7	<p>(Optional) <b>show running-config dhcp</b></p> <p><b>Example:</b></p> <pre>switch(config)# show running-config dhcp</pre>	Displays the DHCP configuration.
Step 8	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 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.

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

### SUMMARY STEPS

1. **configure terminal**
2. **[no] ip dhcp relay**
3. **[no] ip dhcp relay information option**
4. (Optional) **show ip dhcp relay**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip dhcp relay</b> <b>Example:</b> switch(config)# ip dhcp relay	Enables the DHCP relay feature. The <b>no</b> option disables this behavior.
<b>Step 3</b>	<b>[no] ip dhcp relay information option</b> <b>Example:</b> switch(config)# ip dhcp relay information option	Enables the DHCP relay agent to insert and remove Option 82 information on the packets that it forwards. The Option 82 information is in binary ifindex format by default. The <b>no</b> option disables this behavior.
<b>Step 4</b>	(Optional) <b>show ip dhcp relay</b> <b>Example:</b> switch(config)# show ip dhcp relay	Displays the DHCP relay configuration.
<b>Step 5</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

## Enabling or Disabling VRF Support for the DHCP Relay Agent

You can configure the device to support the relaying of DHCP requests that arrive on an interface in one VRF to a DHCP server in a different VRF instance.

### Before you begin

You must enable Option 82 for the DHCP relay agent.

### SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp relay information option vpn**
3. **[no] ip dhcp relay sub-option type cisco**
4. (Optional) **show ip dhcp relay**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>config t</b>  <b>Example:</b> switch# config t switch(config)#	Enters global configuration mode.
Step 2	<b>[no] ip dhcp relay information option vpn</b>  <b>Example:</b> switch(config)# ip dhcp relay information option vpn	Enables VRF support for the DHCP relay agent. The <b>no</b> option disables this behavior.
Step 3	<b>[no] ip dhcp relay sub-option type cisco</b>  <b>Example:</b> switch(config)# ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent Option 82 suboptions. The <b>no</b> option causes DHCP to use RFC numbers 5, 11, and 151 for the link selection, server ID override, and VRF name/VPN ID suboptions.
Step 4	(Optional) <b>show ip dhcp relay</b>  <b>Example:</b> switch(config)# show ip dhcp relay	Displays the DHCP relay configuration.
Step 5	(Optional) <b>show running-config dhcp</b>  <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
Step 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b>	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	<code>switch(config)# copy running-config startup-config</code>	

**Related Topics**

[Enabling or Disabling Option 82 for the DHCP Relay Agent](#), on page 26

[VRF Support for the DHCP Relay Agent](#), on page 8

## Enabling or Disabling Subnet Broadcast Support for the DHCP Relay Agent on a Layer 3 Interface

You can configure the device to support the relaying of DHCP packets from clients to a subnet broadcast IP address. When this feature is enabled, the VLAN ACLs (VACLs) accept IP broadcast packets and all subnet broadcast (primary subnet broadcast as well as secondary subnet broadcast) packets.

**Before you begin**

Ensure that the DHCP feature is enabled.

Ensure that the DHCP relay agent is enabled.

**SUMMARY STEPS**

1. `config t`
2. `interface interface slot/port`
3. `[no] ip dhcp relay subnet-broadcast`
4. `exit`
5. `exit`
6. (Optional) `show ip dhcp relay`
7. (Optional) `show running-config dhcp`
8. (Optional) `copy running-config startup-config`

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b>  <b>Example:</b> <code>switch# config t</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<b>interface interface slot/port</b>  <b>Example:</b> <code>switch(config)# interface ethernet 2/2</code> <code>switch(config-if)#</code>	Enters interface configuration mode, where <i>slot/port</i> is the interface for which you want to enable or disable subnet broadcast support for the DHCP relay agent.
<b>Step 3</b>	<b>[no] ip dhcp relay subnet-broadcast</b>  <b>Example:</b> <code>switch(config-if)# ip dhcp relay subnet-broadcast</code>	Enables subnet broadcast support for the DHCP relay agent. The <b>no</b> option disables this behavior.

	Command or Action	Purpose
Step 4	<b>exit</b> <b>Example:</b> <pre>switch(config-if)# exit switch(config)#</pre>	Exits interface configuration mode.
Step 5	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 6	(Optional) <b>show ip dhcp relay</b> <b>Example:</b> <pre>switch# show ip dhcp relay</pre>	Displays the DHCP relay configuration.
Step 7	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <pre>switch# show running-config dhcp</pre>	Displays the DHCP configuration.
Step 8	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Configuring DHCP Server Addresses on an Interface

You can configure DHCP server IP addresses on an interface. When an inbound DHCP BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCP server IP addresses specified. The relay agent forwards replies from all DHCP servers to the host that sent the request.

### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP server is correctly configured.

Determine the IP address for each DHCP server that you want to configure on the interface.

If the DHCP server is in a different VRF instance than the interface, ensure that you have enabled VRF support.



#### Note

If an ingress router ACL is configured on an interface that you are configuring with a DHCP server address, ensure that the router ACL permits DHCP traffic between DHCP servers and DHCP hosts.

### SUMMARY STEPS

1. **config t**
2. Do one of the following options:

- **interface ethernet** *slot/port*[. *number*]
  - **interface vlan** *vlan-id*
  - **interface port-channel** *channel-id*[. *subchannel-id*]
3. **ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*]
  4. (Optional) **show ip dhcp relay address**
  5. (Optional) **show running-config dhcp**
  6. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b> <b>Example:</b> <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	Do one of the following options: <ul style="list-style-type: none"> <li>• <b>interface ethernet</b> <i>slot/port</i>[. <i>number</i>]</li> <li>• <b>interface vlan</b> <i>vlan-id</i></li> <li>• <b>interface port-channel</b> <i>channel-id</i>[. <i>subchannel-id</i>]</li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• Enters interface configuration mode, where <i>slot/port</i> is the physical Ethernet interface that you want to configure with a DHCP server IP address. If you want to configure a subinterface, include the <i>number</i> argument to specify the subinterface number.</li> <li>• Enters interface configuration mode, where <i>vlan-id</i> is the ID of the VLAN that you want to configure with a DHCP server IP address.</li> <li>• Enters interface configuration mode, where <i>channel-id</i> is the ID of the port channel that you want to configure with a DHCP server IP address. If you want to configure a subchannel, include the <i>subchannel-id</i> argument to specify the subchannel ID.</li> </ul>
<b>Step 3</b>	<b>ip dhcp relay address</b> <i>IP-address</i> [ <b>use-vrf</b> <i>vrf-name</i> ] <b>Example:</b> <pre>switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red</pre>	Configures an IP address for a DHCP server to which the relay agent forwards BOOTREQUEST packets received on this interface.  To configure more than one IP address, use the <b>ip dhcp relay address</b> command once per address.
<b>Step 4</b>	(Optional) <b>show ip dhcp relay address</b> <b>Example:</b> <pre>switch(config-if)# show ip dhcp relay address</pre>	Displays all the configured DHCP server addresses.
<b>Step 5</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <pre>switch(config-if)# show running-config dhcp</pre>	Displays the DHCP configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b>	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	<code>switch(config-if)# copy running-config startup-config</code>	

### Related Topics

[Enabling or Disabling the DHCP Feature](#), on page 13

## Enabling or Disabling DHCP Smart Relay Globally

You can enable or disable DHCP smart relay globally on the device.

### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP relay agent is enabled.

### SUMMARY STEPS

1. `config t`
2. `[no] ip dhcp smart-relay global`
3. (Optional) `show ip dhcp relay`
4. (Optional) `show running-config dhcp`
5. (Optional) `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<code>config t</code> <b>Example:</b> <code>switch# config t</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<code>[no] ip dhcp smart-relay global</code> <b>Example:</b> <code>switch(config)# ip dhcp smart-relay global</code>	Enables DHCP smart relay globally. The <b>no</b> option disables DHCP smart relay.
<b>Step 3</b>	(Optional) <code>show ip dhcp relay</code> <b>Example:</b> <code>switch(config)# show ip dhcp relay</code>	Displays the DHCP smart relay configuration.
<b>Step 4</b>	(Optional) <code>show running-config dhcp</code> <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	Displays the DHCP configuration.
<b>Step 5</b>	(Optional) <code>copy running-config startup-config</code> <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Enabling or Disabling DHCP Smart Relay on a Layer 3 Interface

You can enable or disable DHCP smart relay on Layer 3 interfaces.

### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP relay agent is enabled.

### SUMMARY STEPS

1. **config t**
2. **interface** *interface slot/port*
3. **[no] ip dhcp smart-relay**
4. **exit**
5. **exit**
6. (Optional) **show ip dhcp relay**
7. (Optional) **show running-config dhcp**
8. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b>  <b>Example:</b> switch# config t switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>interface slot/port</i>  <b>Example:</b> switch(config)# interface ethernet 2/3 switch(config-if)#	Enters interface configuration mode, where <i>slot/port</i> is the interface for which you want to enable or disable DHCP smart relay.
<b>Step 3</b>	<b>[no] ip dhcp smart-relay</b>  <b>Example:</b> switch(config-if)# ip dhcp smart-relay	Enables DHCP smart relay on the interface. The <b>no</b> option disables DHCP smart relay on the interface.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> switch(config-if)# exit switch(config)#	Exits interface configuration mode.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> switch(config)# exit switch#	Exits global configuration mode.



	Command or Action	Purpose
Step 6	(Optional) <b>show ip dhcp relay</b> <b>Example:</b> switch# show ip dhcp relay	Displays the DHCP smart relay configuration.
Step 7	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch# show running-config dhcp	Displays the DHCP configuration.
Step 8	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Configuring DHCPv6

### Enabling or Disabling the DHCPv6 Relay Agent

You can enable or disable the DHCPv6 relay agent. By default, the DHCPv6 relay agent is enabled.

#### Before you begin

Ensure that the DHCP feature is enabled.

#### SUMMARY STEPS

1. **configure terminal**
2. **[no] ipv6 dhcp relay**
3. (Optional) **show ipv6 dhcp relay [interface interface]**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	<b>[no] ipv6 dhcp relay</b> <b>Example:</b> switch(config)# ipv6 dhcp relay	Enables the DHCPv6 relay agent. The <b>no</b> option disables the relay agent.

	Command or Action	Purpose
<b>Step 3</b>	(Optional) <b>show ipv6 dhcp relay</b> [ <i>interface interface</i> ] <b>Example:</b> switch(config)# show ipv6 dhcp relay	Displays the DHCPv6 relay configuration.
<b>Step 4</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Enabling or Disabling VRF Support for the DHCPv6 Relay Agent

You can configure the device to support the relaying of DHCPv6 requests that arrive on an interface in one VRF to a DHCPv6 server in a different VRF.

### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCPv6 relay agent is enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **[no] ipv6 dhcp relay option vpn**
3. **[no] ipv6 dhcp relay option type cisco**
4. (Optional) **show ipv6 dhcp relay** [*interface interface*]
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ipv6 dhcp relay option vpn</b> <b>Example:</b> switch(config)# ipv6 dhcp relay option vpn	Enables VRF support for the DHCPv6 relay agent. The <b>no</b> option disables this behavior.

	Command or Action	Purpose
Step 3	<b>[no] ipv6 dhcp relay option type cisco</b> <b>Example:</b> switch(config)# ipv6 dhcp relay option type cisco	Causes the DHCPv6 relay agent to insert virtual subnet selection (VSS) details as part of the vendor-specific option. The <b>no</b> option causes the DHCPv6 relay agent to insert VSS details as part of the VSS option (68), which is defined in RFC-6607. This command is useful when you want to use DHCPv6 servers that do not support RFC-6607 but allocate IPv6 addresses based on the client VRF name.
Step 4	(Optional) <b>show ipv6 dhcp relay [interface interface]</b> <b>Example:</b> switch(config)# show ipv6 dhcp relay	Displays the DHCPv6 relay configuration.
Step 5	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
Step 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Configuring DHCPv6 Server Addresses on an Interface

You can configure DHCPv6 server IP addresses on an interface. When an inbound DHCP BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCPv6 server IP addresses specified. The relay agent forwards replies from all DHCPv6 servers to the host that sent the request.

### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCPv6 server is correctly configured.

Determine the IP address for each DHCPv6 server that you want to configure on the interface.

If the DHCPv6 server is in a different VRF than the interface, ensure that you have enabled VRF support.



**Note** If an ingress router ACL is configured on an interface that you are configuring with a DHCPv6 server address, ensure that the router ACL permits DHCP traffic between DHCPv6 servers and DHCP hosts.

### SUMMARY STEPS

1. **config t**
2. Do one of the following options:
  - **interface ethernet** *slot/port*[. *number*]
  - **interface port-channel** *channel-id*[. *subchannel-id*]

3. **[no] ipv6 dhcp relay address** *IPv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*]
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>config t</b> <b>Example:</b> <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	Do one of the following options: <ul style="list-style-type: none"> <li>• <b>interface ethernet</b> <i>slot/port</i>[. <i>number</i>]</li> <li>• <b>interface port-channel</b> <i>channel-id</i>[. <i>subchannel-id</i>]</li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• Enters interface configuration mode, where <i>slot/port</i> is the physical Ethernet interface that you want to configure with a DHCPv6 server IP address. If you want to configure a subinterface, include the <i>number</i> argument to specify the subinterface number.</li> <li>• Enters interface configuration mode, where <i>channel-id</i> is the ID of the port channel that you want to configure with a DHCPv6 server IP address. If you want to configure a subchannel, include the <i>subchannel-id</i> argument to specify the subchannel ID.</li> </ul>
<b>Step 3</b>	<b>[no] ipv6 dhcp relay address</b> <i>IPv6-address</i> [ <b>use-vrf</b> <i>vrf-name</i> ] [ <b>interface</b> <i>interface</i> ] <b>Example:</b> <pre>switch(config-if)# ipv6 dhcp relay address FF02:1::FF0E:8C6C use-vrf red</pre>	Configures an IP address for a DHCPv6 server to which the relay agent forwards BOOTREQUEST packets received on this interface.  Use the <b>use-vrf</b> option to specify the VRF name of the server if it is in a different VRF and the other argument <i>interface</i> is used to specify the output interface for the destination.  The server address can either be a link-scoped unicast or multicast address or a global or site-local unicast or multicast address. The <b>interface</b> option is mandatory for a link-scoped server address and multicast address. It is not allowed for a global or site-scoped server address.  To configure more than one IP address, use the <b>ipv6 dhcp relay address</b> command once per address.
<b>Step 4</b>	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <pre>switch(config-if)# show running-config dhcp</pre>	Displays the DHCPv6 configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Configuring the DHCPv6 Relay Source Interface

You can configure the source interface for the DHCPv6 relay agent. By default, the DHCPv6 relay agent uses the relay agent address as the source address of the outgoing packet. Configuring the source interface enables you to use a more stable address (such as the loopback interface address) as the source address of relayed messages.

### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCPv6 relay agent is enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **[no] ipv6 dhcp relay source-interface *interface***
3. (Optional) **show ipv6 dhcp relay [interface *interface*]**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ipv6 dhcp relay source-interface <i>interface</i></b>  <b>Example:</b> switch(config)# ipv6 dhcp relay source-interface loopback 2	Configures the source interface for the DHCPv6 relay agent.  <b>Note</b> The DHCPv6 relay source interface can be configured globally, per interface, or both. When both the global and interface levels are configured, the interface-level configuration overrides the global configuration.
<b>Step 3</b>	(Optional) <b>show ipv6 dhcp relay [interface <i>interface</i>]</b>  <b>Example:</b> switch(config)# show ipv6 dhcp relay	Displays the DHCPv6 relay configuration.
<b>Step 4</b>	(Optional) <b>show running-config dhcp</b>  <b>Example:</b> switch(config)# show running-config dhcp	Displays the DHCP configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Verifying the DHCP Configuration

To display DHCP configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
<code>show running-config dhcp [all]</code>	Displays the DHCP configuration in the running configuration.
<code>show ip dhcp relay</code>	Displays the DHCP relay configuration.
<code>show ipv6 dhcp relay [interface interface]</code>	Displays the DHCPv6 relay global or interface-level configuration.
<code>show ip dhcp relay address</code>	Displays all the DHCP server addresses configured on the device.
<code>show ip dhcp snooping</code>	Displays general information about DHCP snooping.
<code>show startup-config dhcp [all]</code>	Displays the DHCP configuration in the startup configuration.

## Displaying DHCP Bindings

Use the `show ip dhcp snooping binding` command to display the DHCP binding table. For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

## Clearing the DHCP Snooping Binding Database

You can remove entries from the DHCP snooping binding database, including a single entry, all entries associated with an interface, or all entries in the database.

### Before you begin

Ensure that the DHCP feature is enabled.

### SUMMARY STEPS

1. (Optional) `clear ip dhcp snooping binding`
2. (Optional) `clear ip dhcp snooping binding interface ethernet slot/port[.subinterface-number]`
3. (Optional) `clear ip dhcp snooping binding interface port-channel channel-number[.subchannel-number]`
4. (Optional) `clear ip dhcp snooping binding vlan vlan-id mac mac-address ip ip-address interface {ethernet slot/port[.subinterface-number] | port-channel channel-number[.subchannel-number]}`

5. (Optional) **show ip dhcp snooping binding**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>clear ip dhcp snooping binding</b> <b>Example:</b> switch# clear ip dhcp snooping binding	Clears all entries from the DHCP snooping binding database.
<b>Step 2</b>	(Optional) <b>clear ip dhcp snooping binding interface ethernet slot/port[.subinterface-number]</b> <b>Example:</b> switch# clear ip dhcp snooping binding interface ethernet 1/4	Clears entries associated with a specific Ethernet interface from the DHCP snooping binding database.
<b>Step 3</b>	(Optional) <b>clear ip dhcp snooping binding interface port-channel channel-number[.subchannel-number]</b> <b>Example:</b> switch# clear ip dhcp snooping binding interface port-channel 72	Clears entries associated with a specific port-channel interface from the DHCP snooping binding database.
<b>Step 4</b>	(Optional) <b>clear ip dhcp snooping binding vlan vlan-id mac mac-address ip ip-address interface {ethernet slot/port[.subinterface-number]   port-channel channel-number[.subchannel-number] }</b> <b>Example:</b> switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11	Clears a single, specific entry from the DHCP snooping binding database.
<b>Step 5</b>	(Optional) <b>show ip dhcp snooping binding</b> <b>Example:</b> switch# show ip dhcp snooping binding	Displays the DHCP snooping binding database.

## Related Topics

[Enabling or Disabling the DHCP Feature](#), on page 13

## Clearing DHCP Relay Statistics

Use the **clear ip dhcp relay statistics** command to clear the global DHCP relay statistics.

Use the **clear ip dhcp relay statistics interface interface** command to clear the DHCP relay statistics for a particular interface.

## Clearing DHCPv6 Relay Statistics

Use the **clear ipv6 dhcp relay statistics** command to clear the global DHCPv6 relay statistics.

Use the **clear ipv6 dhcp relay statistics interface** *interface* command to clear the DHCPv6 relay statistics for a particular interface.

## Monitoring DHCP

Use the **show ip dhcp snooping statistics** command to monitor DHCP snooping.

Use the **show ip dhcp relay statistics [interface** *interface*] command to monitor DHCP relay statistics at the global or interface level.

Use the (Optional) **show ip dhcp snooping statistics vlan [vlan-id] interface [ethernet|port-channel][id]** command to know the exact statistics about snooping statistics per interface under a vlan.

Use the **show ipv6 dhcp relay statistics [interface** *interface*] command to monitor DHCPv6 relay statistics at the global or interface level.



### Note

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

## Additional References for DHCP

### Related Documents

Related Topic	Document Title
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference</i>
VRFs and Layer 3 virtualization	<i>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide</i>
vPCs	<i>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide</i>

### Standards

Standards	Title
RFC-2131	Dynamic Host Configuration Protocol
RFC-3046	DHCP Relay Agent Information Option



Standards	Title
RFC-6607	Virtual Subnet Selection Options for DHCPv4 and DHCPv6

## Feature History for DHCP

This table lists the release history for this feature.

**Table 2: Feature History for DHCP**

Feature Name	Releases	Feature Information
IP DHCP Relay Source Interface	8.2(3)	Added support for the DHCP relay source interface.
DHCP	6.2(2)	Added support for the DHCPv6 relay agent.
DHCP	6.2(2)	Added a new default circuit ID format that is used when Option 82 is enabled for DHCP snooping.
DHCP	6.0(1)	No change from Release 5.2.
DHCP	5.2(1)	Added support for DHCP smart relay.
DHCP	5.2(1)	Added subnet broadcast support for the DHCP relay agent.
DHCP	5.1(1)	Optimized DHCP snooping to work in a vPC environment.
DHCP	5.0(2)	Modified the DHCP relay agent to support VRFs, added the <b>ip dhcp relay information option vpn</b> command, and modified the <b>ip dhcp relay address</b> command to add the <b>use-vrf vrf-name</b> option.

Feature Name	Releases	Feature Information
DHCP	5.0(2)	Added the <b>ip dhcp relay sub-option type cisco</b> command to enable DHCP to use Cisco proprietary numbers 150, 152, and 151 for the link selection, server ID override, and VRF name/VPN ID relay agent Option 82 suboptions.
DHCP	4.2(1)	Deprecated the <b>service dhcp</b> command and replaced it with the <b>ip dhcp relay</b> command.