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:

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.

Note The interfaces which are connected to the client side are considered as un-trusted, even if trust state is configured.

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.

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, a 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. 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 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.

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.

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-ifindex (for non-vPCs) or vlan-vpcid (for vPCs), from which the packet is received (the circuit ID suboption).

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.

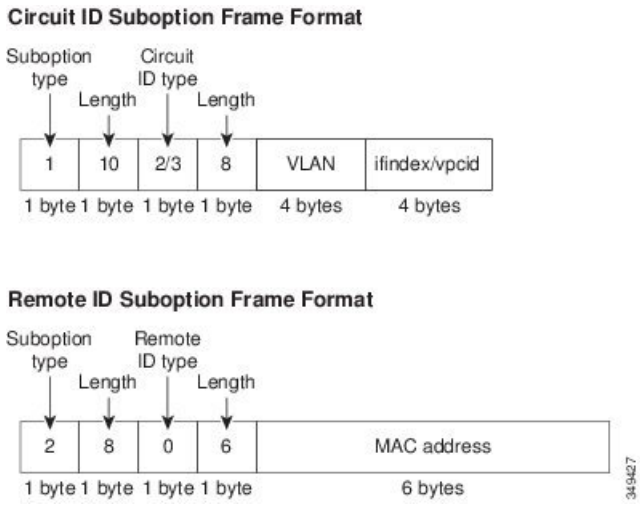
If the previously described sequence of events occurs, the following values do not change:

- 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

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.

Figure 1: Suboption Packet Formats



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.

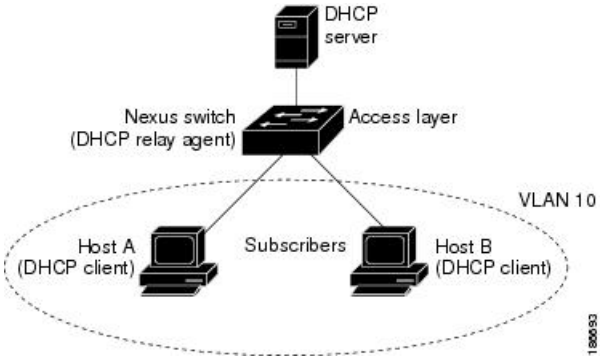
Note When the device relays a DHCP request that already includes Option 82 information, the device forwards the request with the original Option 82 information without altering it.

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 2: 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.

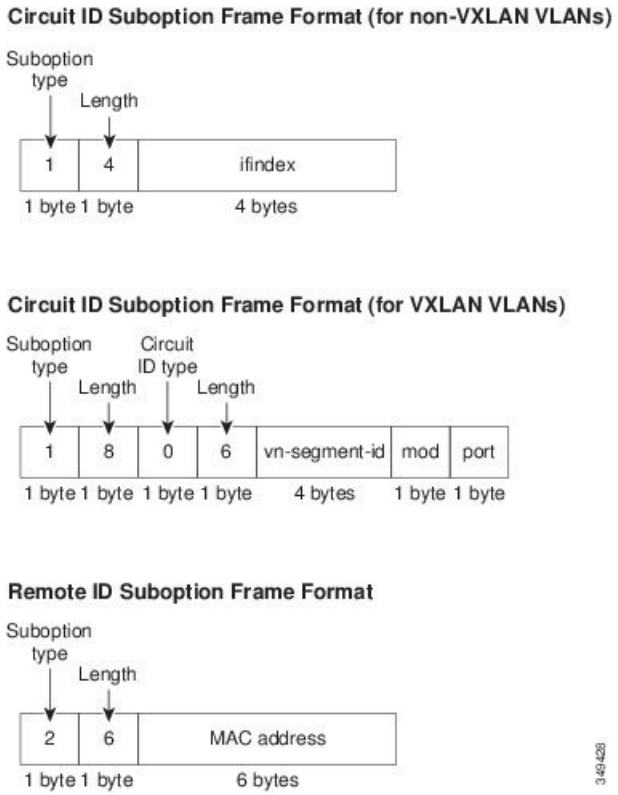


When you enable Option 82 for the DHCP relay agent on the Cisco NX-OS device, the following sequence of events occurs:

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 ifindex (for non-VXLAN VLANs) or vn-segment-id-mod-port (for VXLAN VLANs), from which the packet is received (the circuit ID suboption). In DHCP relay, the circuit ID is filled with the ifindex of the SVI or Layer 3 interface on which DHCP relay is configured.
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 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.

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

Figure 3: Suboption Packet Formats



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 9000 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 DCHP 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.

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.

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.

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 9000 Series NX-OS Unicast Routing Configuration Guide*.

About DHCP Client

The DHCP client feature enables the configuration of an IPv4 or IPv6 address on an interface. Interfaces can include routed ports, the management port, and switch virtual interfaces (SVIs).

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:

- For secure POAP, make sure that DHCP snooping is enabled and firewall rules are set to block unintended or malicious DHCP servers.
- Cisco Nexus 9000 Series switches do not support the relaying of bootp packets. However, the switches do support bootp packets that are Layer 2 switched.
- DHCP subnet broadcast is not supported.
- You must enable the insertion of Option 82 information for DHCP packets to support the highest DHCP snooping scale.
- Before you globally enable 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 should not be followed by DHCP relay in the network (DHCP snooping does not work when the DHCP relay is configured on the same Cisco Nexus device).
- The **ip dhcp snooping** command is not supported on Cisco Nexus 9500 platform switches with N9K-X9636C-R, N9K-X9636C-RX, and N9K-X9636Q-R line cards and Cisco Nexus 34180YC switches.
- DHCP snooping is not supported on VXLAN VLANs.
- DHCP snooping supports multiple IP addresses with the same MAC address and VLAN in static binding entries.
- VXLAN supports DHCP relay when the DHCP server is reachable through a default VRF.
- If a VLAN ACL (VACL) is configured on a VLAN that you are configuring with DHCP snooping, make sure 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, make sure that the router ACL permits DHCP traffic between DHCP servers and DHCP hosts.
- If you use DHCP relay where DHCP clients and servers are in different VRFs, use only one DHCP server within a VRF.
- 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 switches in a vPC link. Otherwise, a run-time error can occur, resulting in dropped packets.

- DHCP Smart Relay is limited to the first 100 IP addresses of the interface on which it is enabled.
- You must configure a helper address on the interface in order to use DHCP smart relay.
- If DHCP Smart Relay is enabled in a vPC environment, primary interface IP addresses should share a subnet between the peers. Secondary interface IP addresses should also share a subnet between the peers.
- When you configure DHCPv6 server addresses on an interface, a destination interface cannot be used with global IPv6 addresses.
- DHCPv6-PD Routes will not be generated when a DHCPv6 client initiates a Rebind. Existing IAPD entries for the client will be refreshed, but not created. For IAPD route creation, a full Solicit, Advertise, Request, Reply must be seen by the DHCPv6 Relay agent.
- If you use DHCP relay on an unnumbered interface, you must configure the switch to insert option 82.
- DHCPv6 Prefix Delegation Routes are not generated when Option 14 **Rapid Commit** is present. A full Solicit, Advertise, Request, Reply sequence is needed to generate an IAPD route.
- The following guidelines and limitations apply to the DHCP client feature:
  - You can configure multiple SVIs, but each interface VLAN should be in a different subnet. The DHCP client feature cannot configure different IP addresses with the same subnet on different interface VLANs on the same device.
  - DHCP client and DHCP relay are not supported on the same switch.
  - DHCP client is not supported for Layer 3 subinterfaces.
  - DHCP client is supported on the Cisco Nexus 9300 Series switches and the Cisco Nexus 9500 Series switches.
  - DHCP client is not supported on Cisco Nexus 9500 platform switches with N9K-X9636C-R, N9K-X9636C-RX, N9K-X9636Q-R, and N9K-X96136YC-R line cards.
- Beginning with Cisco NX-OS Release 9.3(3), DHCP snooping and DHCP relay is supported on Cisco Nexus 9364C-GX, Cisco Nexus 9316D-GX, and Cisco Nexus 93600CD-GX switches.

Note For DHCP configuration limits, see the *Cisco Nexus 9000 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

Parameters	Default
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
VRF support for the DHCP relay agent	Disabled
VRF support for the DHCPv6 relay agent	Disabled
DHCP Option 82 for relay agent	Disabled
DHCP smart relay agent	Disabled
DHCP server IP address	None

Configuring DHCP

Minimum DHCP Configuration

Procedure

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 Make sure that the DHCP server is connected to the device using a trusted interface.

Step 5 (Optional) Enable the DHCP relay agent.

Step 6 (Optional) If DHCP servers and clients are in different VRFs, do the following:

a) Enable Option 82 for the DHCP relay agent.
b) Enable VRF support for the DHCP relay agent.

Step 7 (Optional) Configure an interface with the IP address of the DHCP server.

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 the DHCP relay agent, DHCP snooping, or any of the features that depend on DHCP. In addition, all DHCP configuration is removed from the device.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature dhcp** **Example:** `switch(config)# feature dhcp`	Enables the DHCP feature. The **no** option disables the DHCP feature and erases all DHCP configuration.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring DHCP Snooping

Enabling or Disabling DHCP Snooping Globally

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

Before you begin

Make sure that you have enabled the DHCP feature.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	[**no**] **ip dhcp snooping** **Example:** `switch(config)# ip dhcp snooping`	Enables DHCP snooping globally. The **no** form of this command disables DHCP snooping.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

Make sure that the DHCP feature is enabled.

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping vlan** *vlan-list* **Example:** `switch(config)# ip dhcp snooping vlan 100,200,250-252`	Enables DHCP snooping on the VLANs specified by *vlan-list*. The **no** form of this command disables DHCP snooping on the VLANs specified.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

Make sure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping verify mac-address** **Example:** `switch(config)# ip dhcp snooping verify mac-address`	Enables DHCP snooping MAC address verification. The **no** form of this command disables MAC address verification.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

Note You must add Option82 as specified in the format string in the command configuration.

- The length of the Option82 string increases based on the length of the format string.
- The circuit-id must include the ascii value of the format string.

Before you begin

Make sure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping information option** **Example:** `switch(config)# ip dhcp snooping information option`	Enables the insertion and removal of Option 82 information for DHCP packets. The **no** form of this command disables the insertion and removal of Option 82 information.

Step 3	(Optional) [**no**] **ip dhcp option82 sub-option circuit-id** *format_type string format*
	Example:
	`switch(config)# ip dhcp snooping sub-option circuit-id format-type string format`
	Example:
	`switch(config)# ip dhcp snooping sub-option circuit-id format-type string format?`
	`WORD Format string (Max Size 64)`
		Configures Option 82 as follows:
		• If you do not specify *format-type*, the *circuit-id* displays the incoming port, for example, *ethernet1/1*.
		• If you specify format <*word*>, the *circuit-id* displays the specified word
		• If you specify *%h* instead of <*word*>, the *circuit-id* displays the host name.
		• If you specify *%p* instead of <*word*>, the *circuit-id* displays the port name.

	Command or Action	Purpose
		• If you specify *%h:%p* instead of *<word>*, the *circuit-id* displays both host and port name. **Note** The *no* option disables this behavior.

Step 4	**interface** *interface slot/port*
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Enters the interface configuration mode, where slot/port is the interface where you want to enable or disable snooping.

Step 5	(Optional) **ip dhcp option82 sub-option circuit-id**
	Example:
	`switch(config-if)# ip dhcp option82 sub-option circuit-id?`
	`WORD Format string (Max Size 64)`
	Example:
	`switch(config-if)# ip dhcp option82 sub-option circuit-id test`
	`switch(config-if)#`
		Configures Option 82 at the interface.
		Note This command is not supported at SVI and Sub-Interface.
		Note The *no* option disables this behavior

Step 6	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 7	(Optional) **show ip dhcp option82 info interface** *intf_name*	Displays the DHCP configuration. It shows whether option82 is enabled or disabled on that interface and the transmitted packets for an interface that is option82 enabled.
Step 8	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp packet strict-validation** **Example:** `switch(config)# ip dhcp packet strict-validation`	Enables the strict validation of DHCP packets. The **no** form of this command disables strict DHCP packet validation.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `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

Make sure that the DHCP feature is enabled.

Make sure that the interface is configured as a Layer 2 interface.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Do one of the following options: • **interface ethernet** *slot*/*port* • **interface port-channel** *channel-number*	• Enters interface configuration mode, where *slot*/*port* is the Layer 2 Ethernet interface that you want to configure as trusted or untrusted for DHCP snooping.

	Command or Action	Purpose

	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		• Enters interface configuration mode, where *slot*/*port* is the Layer 2 port-channel interface that you want to configure as trusted or untrusted for DHCP snooping.

Step 3	[**no**] **ip dhcp snooping trust** **Example:** `switch(config-if)# ip dhcp snooping trust`	Configures the interface as a trusted interface for DHCP snooping. The **no** form of this command configures the port as an untrusted interface.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

Make sure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay information option trust** **Example:** `switch(config)# ip dhcp relay information option trust`	Enables the DHCP relay trusted port functionality. The **no** form of this command disables this functionality.
Step 3	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.

	Command or Action	Purpose
Step 4	(Optional) **show ip dhcp relay information trusted-sources** **Example:** `switch(config)# show ip dhcp relay information trusted-sources`	Displays the DHCP relay trusted ports configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `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 subinterfaces
- Layer 3 port-channel interfaces

Before you begin

Make sure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** [**ethernet** *slot/port*[*.number*] | **port-channel** *channel-number*]
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode, where *slot/port* is the Layer 3 Ethernet interface that you want to configure as trusted or untrusted or *channel-number* is the Layer 3 port-channel interface that you want to configure as trusted or untrusted.

Step 3	[**no**] **ip dhcp relay information trusted** **Example:** `switch(config-if)# ip dhcp relay information trusted`	Configures the interface as a trusted interface for DHCP relay agent information. The **no** form of this command configures the port as an untrusted interface.

	Command or Action	Purpose
		Note For any Layer 3 interface, if the interface is configured as trusted either through a global command or an interface-level command, the interface is considered as a trusted interface. Hence, when the trusted-port command is enabled at the global level, any Layer 3 interface cannot be considered as untrusted irrespective of the interface-level configuration.
Step 4	(Optional) **show ip dhcp relay information trusted-sources** **Example:** `switch(config-if)# show ip dhcp relay information trusted-sources`	Displays the DHCP relay trusted ports configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	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 subinterfaces
- Layer 3 port-channel interfaces

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

Make sure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay information trust-all** **Example:** `switch(config)# ip dhcp relay information trust-all`	Configures the interfaces as trusted sources of DHCP messages. The **no** form of this command configures the ports as untrusted interfaces.
Step 3	(Optional) **show ip dhcp relay information trusted-sources** **Example:** `switch(config)# show ip dhcp relay information trusted-sources`	Displays the DHCP relay trusted ports configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay** **Example:**	Enables the DHCP relay agent. The **no** option disables the DHCP relay agent.

	Command or Action	Purpose
	`switch(config)# ip dhcp relay`	
Step 3	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.

Before you begin

Ensure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **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 **no** option disables this behavior.
Step 3	(Optional) switch(config)# [**no**] **ip dhcp relay sub-option circuit-id customized**	Programs Option 82 with the VLAN + slot + port format. This command is applicable only for SVIs. The **no** option disables this behavior.
Step 4	(Optional) switch(config)# [**no**] **ip dhcp relay sub-option circuit-id format-type string**	Configures Option 82 to use encoded string format instead of the default binary ifindex format. The **no** option disables this behavior. For VLANs and SVIs:

	Command or Action	Purpose
		• When this command and the **ip dhcp relay sub-option circuit-id customized** command are both configured, the **ip dhcp relay sub-option circuit-id format-type string** command is programmed. • When the **ip dhcp relay sub-option circuit-id format-type string** command is removed, the **ip dhcp relay sub-option circuit-id customized** command is programmed. • When both commands are removed, the ifindex is programmed. For other interfaces, if the **ip dhcp relay sub-option circuit-id format-type string** command is configured, it is used. Otherwise, the default ifindex is programmed.
Step 5	(Optional) switch(config)# **show ip dhcp relay**	Displays the DHCP relay configuration.
Step 6	(Optional) switch(config)# **show running-config dhcp**	Displays the DHCP configuration.
Step 7	(Optional) 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.

Before you begin

You must enable Option 82 for the DHCP relay agent.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay information option vpn** **Example:**	Enables VRF support for the DHCP relay agent. The **no** option disables this behavior.

	Command or Action	Purpose
	`switch(config)# ip dhcp relay information option vpn`	
Step 3	[**no**] **ip dhcp relay sub-option type cisco** **Example:** `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 **no** 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) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Disabling the Server Identifier Override Option

Beginning with Cisco NX-OS Release 9.3(3), you can disable the server identifier override option. This option is added by default in DHCP Option 82 packets for a DHCP relay VPN configuration or source interface configuration.

Before you begin

You must enable Option 82 for the DHCP relay agent.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **ip dhcp relay information option server-id-override-disable** **Example:**	Disables the server identifier override option in DHCP Option 82 packets.

	Command or Action	Purpose
	`switch(config)# ip dhcp relay information option server-id-override-disable`	**Note** You can use the **no** form of this command to re-enable the server identifier override option.

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 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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Do one of the following options:
	• **interface ethernet** *slot*/*port*[**.***number*]
	• **interface vlan** *vlan-id*
	• **interface port-channel** *channel-id*[.*subchannel-id*]
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• Enters interface configuration mode, where *slot*/*port* 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 *number* argument to specify the subinterface number.
		Note Port-channel subinterfaces are supported only in Cisco NX-OS Releases 6.1(2)I3(3) and 6.1(2)I3(3a). They are not supported in Cisco NX-OS Release 9.2(1).

	Command or Action	Purpose
		• Enters interface configuration mode, where *vlan-id* is the ID of the VLAN that you want to configure with a DHCP server IP address. • Enters interface configuration mode, where *channel-id* 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 *subchannel-id* argument to specify the subchannel ID.
Step 3	**ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*] **Example:** `switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red`	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 **ip dhcp relay address** command once per address.
Step 4	(Optional) **show ip dhcp relay address** **Example:** `switch(config-if)# show ip dhcp relay address`	Displays all the configured DHCP server addresses.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the DHCP Relay Source Interface

You can configure the source interface for the DHCP relay agent. By default, the DHCP 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. When DHCP relay source 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.

Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP relay agent is enabled.

Ensure CLI dhcp relay information option and ip dhcp relay information option vpn are enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay source-interface** *interface* **Example:** `switch(config)# ip dhcp relay source-interface loopback 2`	Configures the source interface for the DHCP relay agent. **Note** The DHCP 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.
Step 3	(Optional) **show ip dhcp relay** [**interface** *interface*] **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp smart-relay global** **Example:** `switch(config)# ip dhcp smart-relay global`	Enables DHCP smart relay globally. The **no** form of this command disables DHCP smart relay.
Step 3	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP smart relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface** *interface slot/port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Enters interface configuration mode, where *slot/port* is the interface for which you want to enable or disable DHCP smart relay.

Step 3	[**no**] **ip dhcp smart-relay** **Example:** `switch(config-if)# ip dhcp smart-relay`	Enables DHCP smart relay on the interface. The **no** form of this command disables DHCP smart relay on the interface.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 6	(Optional) **show ip dhcp relay** **Example:** `switch# show ip dhcp relay`	Displays the DHCP smart relay configuration.
Step 7	(Optional) **show running-config dhcp** **Example:** `switch# show running-config dhcp`	Displays the DHCP configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring DHCP Relay Subnet-Selection

If an interface includes both, a primary and a secondary IP address, then by default the DHCP relay uses the primary subnet to request the IP address allocation from the server. You must enable DHCP smart relay if you want the DHCP relay to use the secondary IP address. With smart relay enabled, DHCP relay first requests the IP address in the primary subnet. If it fails to get the IP address in the primary subnet, it requests the IP address of the secondary subnet. The IP address of the secondary subnet is not chosen by default.

With the introduction of the DHCP relay subnet selection feature, you have an option to choose the IP address of either the primary or the secondary subnet based on your requirements. When you configure the DHCP relay subnet selection, the DHCP relayed packet includes the subnet that is used in subnet-selection for a source and relay agent. If there is a VPN or a source interface option, the option 82 link selection is updated with the configured subnet.

The DHCP Smart relay and the subnet-selection configuration are mutually exclusive at the interface level. If DHCP Smart relay is enabled globally and the subnet-selection is configured on the interface level, then the interface configuration takes precedence.

With the DHCP VPN or the source interface option, the DHCP server must use the option 82 link-selection to assign the IP address.

Before you begin

Ensure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface vlan** *vlan-id*
	Example:
	`switch(config)#interface vlan 3`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	**ip dhcp relay subnet-selection** *ip address* **Example:** `switch(config-if)#ip dhcp relay subnet-selection 20.20.21.1`	Configures the DHCP relay subnet-selection for the specified IP address.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	[**no**] **ipv6 dhcp relay** **Example:** `switch(config)# ipv6 dhcp relay`	Enables the DHCPv6 relay agent. The **no** option disables the relay agent.
Step 3	(Optional) **show ipv6 dhcp relay** [**interface** *interface*] **Example:** `switch(config)# show ipv6 dhcp relay`	Displays the DHCPv6 relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ipv6 dhcp relay option vpn** **Example:** `switch(config)# ipv6 dhcp relay option vpn`	Enables VRF support for the DHCPv6 relay agent. The **no** option disables this behavior.
Step 3	[**no**] **ipv6 dhcp relay option type cisco** **Example:**	Causes the DHCPv6 relay agent to insert virtual subnet selection (VSS) details as part of the vendor-specific option. The **no** option causes

	Command or Action	Purpose
	`switch(config)# ipv6 dhcp relay option type cisco`	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) **show ipv6 dhcp relay** [**interface** *interface*] **Example:** `switch(config)# show ipv6 dhcp relay`	Displays the DHCPv6 relay configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	Do one of the following options:
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-id*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• Enters interface configuration mode, where *slot*/*port* is the physical Ethernet interface that you want to configure with a DHCPv6 server IP address.
		• Enters interface configuration mode, where *channel-id* is the ID of the port channel that you want to configure with a DHCPv6 server IP address.

Step 3	[**no**] **ipv6 dhcp relay address** *IPv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*] **Example:** `switch(config-if)# ipv6 dhcp relay address FF02:1::FF0E:8C6C use-vrf red`	Configures an IP address for a DHCPv6 server to which the relay agent forwards BOOTREQUEST packets received on this interface. Use the **use-vrf** option to specify the VRF name of the server if it is in a different VRF and the other argument interface 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 **interface** 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 **ipv6 dhcp relay address** command once per address.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the DHCPv6 configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling DHCPv6 Option 79

Beginning with Cisco NX-OS Release 9.3(3), you can enable the use of the DHCPv6 client's link-layer address through Option 79. When you enable this feature, the switch adds Option 79 with relay forward packets, and the IPv6 client's link-layer address is inserted into the Options field of the DHCPv6 packet.

This feature is supported for both regular DHCPv6 and DHCPv6 with VXLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 2	**ipv6 dhcp relay option79** **Example:** `switch(config)# ipv6 dhcp relay option79`	Enables the DHCP relay forward packets that are transmitted from the relay server to the DHCP server to carry the DHCPv6 host's link-layer address. This command affects the transmitted relay forward packets only.

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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ipv6 dhcp relay source-interface** *interface* **Example:**	Configures the source interface for the DHCPv6 relay agent.

	Command or Action	Purpose
	`switch(config)# ipv6 dhcp relay source-interface loopback 2`	**Note** 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.
Step 3	(Optional) **show ipv6 dhcp relay** [**interface** *interface*] **Example:** `switch(config)# show ipv6 dhcp relay`	Displays the DHCPv6 relay configuration.
Step 4	(Optional) **show running-config dhcp show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring IPv6 RA Guard

You can configure the IPv6 router advertisement (RA) guard feature for Cisco Nexus 9200, 9300, and 9300-EX Series switches and the N9K-X9732C-EX line card. This feature is used to drop all incoming IPv6 RA packets on a Layer 2 interface.

Before you begin

You must enable DHCP (using the **feature dhcp** command).

To enable DHCP relay on any interface, you must disable DHCP on interfaces that have an IPv4 or IPv6 address assigned using DHCP (dynamic IP addressing).

Make sure that both PTP (**feature ptp**) and NV overlay (**feature nv overlay**) are not already configured. A dynamic ifacl label is reserved when these features are configured. However, only two dynamic ifacl label bits are available. If both of these features are already configured, a dynamic ifacl label will not be available for IPv6 RA guard, and the feature cannot be enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**interface** *interface slot/port*
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	[**no**] **ipv6 nd raguard** **Example:** `switch(config-if)# ipv6 nd raguard`	Enables the IPv6 RA guard feature on the specified interface.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling DHCP Client

You can use the DHCP client feature to enable the configuration of an IPv4 or IPv6 address on an interface. Interfaces can include routed ports, the management port, and switch virtual interfaces (SVIs). Layer 3 subinterfaces are not supported.

Note DHCP client is independent of the DHCP relay and DHCP snooping processes, so it does not require that the **feature dhcp** command be enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Do one of the following options:
	• **interface ethernet** *slot/port*
	• **interface mgmt 0**
	• **interface vlan** *vlan-id*
	Example:
	`switch(config)# interface vlan 3`
	`switch(config-if)#`
		• Enters interface configuration mode, where *slot/port* is the physical Ethernet interface for which you want to enable the DHCP client feature.
		• Enters interface configuration mode and specifies the management interface as the interface for which you want to enable the DHCP client feature.

	Command or Action	Purpose
		• Enters interface configuration mode, where *vlan-id* is the ID of the VLAN for which you want to enable the DHCP client feature.
Step 3	**ipv6 address use-link-local-only** **Example:** `switch(config-if)# ipv6 address use-link-local-only`	You must enter this command before assigning an IPv6 address to the interface in the next step. This command is not required if you will assign an IPv4 address to the interface.
Step 4	[**no**] {**ip** | **ipv6**} **address dhcp** **Example:** `switch(config-if)# ip address dhcp`	Assigns an IPv4 or IPv6 address to the interface. The **no** form of this command releases the IP address.
Step 5	(Optional) Do one of the following options: • **show running-config interface ethernet** *slot/port* • **show running-config interface mgmt 0** • **show running-config interface vlan** *vlan-id* **Example:** `switch(config-if)# show running-config interface vlan 3`	Displays the IPv4 or IPv6 address assigned to the interface in the running configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration. Only the {**ip** | **ipv6**} **address dhcp** command is saved. The assigned IP address is not saved even though it shows in the running configuration.

Configuring UDP Relay

About UDP Relay

By default, routers do not forward broadcast packets. You must configure routers if you want to forward broadcast packets. You can use the UDP relay feature to relay broadcasts destined for UDP ports except DHCPv4 port numbers 67 and 68. The UDP relay feature is also known as the IP Helper feature.

Us the **ip forward-protocol udp** command to enable the UDP relay feature. By default, the UDP relay feature is disabled.

To forward a packet, configure IP address object groups with the forwarding destination IP addresses or network addresses and then associate the IP address object groups with the L3 interfaces.

The UDP relay feature is supported on the following types of Layer 3 interfaces:

- Physical port
- Interface VLAN (SVI)
- L3 port channel
- L3 subinterfaces

Guidelines and Limitations for UDP Relay

UDP relay has the following guidelines and limitations:

- Beginning with Cisco NX-OS Release 9.3(5), UDP relay is supported on Cisco Nexus 9200, 9332C, 9364C, 9300-EX, 9300-FX/FX2/FXP platform switches, and Cisco Nexus 9500 platform switches with -EX/FX line cards.
- The UDP port must be in the range of 1 to 65565.
- Any L3 or SVI interface can be associated with a maximum of one object group. Therefore, any interface can be associated with a maximum of 300 UDP relay IP addresses.
- The UDP relay feature supports seven UDP ports.
- The objet-group name can be maximum of 64 alpha-numeric characters.
- DHCP and UDP relay cannot co-exist.
- Subnet broadcast is not supported.

Configuring UDP Relay

Before you begin

Ensure that you have enabled the DHCP feature.

Procedure

Step 1 **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **[no] ip forward-protocol udp**

Example:

```
switch(config)# ip forward-protocol udp
```

Enables the UDP relay feature. By default, the UDP relay feature is disabled. However, it is enabled on the predefined set of UDP ports.

Step 3 (Optional) **[no] ip forward-protocol udp** *udp-port-number*

Example:

```
switch(config)# ip forward-protocol udp 1
```

Enable the UDP relay feature on the non-default UDP ports.

Note You can enable or disable UDP forwarding for any UDP port in the range 1 to 65565 except the DHCP ports.

Step 4 **[no] object-group udp relay ip addres** *object-group-name*

Example:

```
switch(config)# ip forward-protocol udp relay ip address relay1
```

Configures the destination IP addresses to which the packets are forwarded.

Note For each entry that you want to create, use the **host** command to specify a single host, or omit the **host** command to specify a network of hosts.

Step 5 **[no] {host** *host-addr*| *network-addr network-mask*| *network-addr/mask-length*}

Example:

```
switch(config)# host 2.1.2.2 30.1.1.1 255.255.255.0 10.1.1.1./24
```

Configure an object group that consists of destination IP addresses to which the packets are forwarded

Note For each entry that you want to create, use the **host** command to specify a single host, or omit the **host** command to specify a network of hosts.

Step 6 **exit**

Example:

```
switch(config-udp-group)# exit
```

Exists the interface configuration mode.

Step 7 **interface ethernet** *slot/port*

Example:

```
switch(config)# interface ethernet 1/1
```

Associates the object froup with a Layer 3 interface.

Note The L3 interface can be a physical port, interface VLAN (SVI), L3 port channel, or L3 subinterfaces.

Step 8 **ip udp relay addrgroup** *object-group-name*

Example:

```
switch(config-if)# ip udp relay addrgroup group1
```

Associates an object group to the interface.

Step 9 **exit**

Example:

```
switch(config-if)# exit
```

Exists the interface configuration mode.

Configuration Example for UDP Relay

The following example shows a running configuration to configure UDP relay.

Configuring UDP Relay

This example shows a running configuration to configure the UDP relay feature.

```
configure terminal
 feature dhcp
 ip forward-protocol udp
 object-group udp relay ip address <udprelay1>
   host <20.1.2.2>
   <30.1.1.1> <255.255.255.0>
   <10.1.1.1/24>
   exit
 interface ethernet <e1/1>
  ip udp relay addrgroup <udprelay1>
  exit
```

Verifying the UDP Relay Configuration

To display UDP relay configuration information, perform one of the following tasks:

Command	Purpose
show ip udp relay	Displays the UDP replay configuration.
show ip udp relay interface [{ *interface-type* | *interface-range}]*	Displays the interface level attributes.
show ip udp relay object-group	Displays all configured UDP relay object-groups and the associated IP addresses.
show ip udp relay object-group *object-group-name*	Displays the object-group and the associated IP addresses.

Verifying the DHCP Configuration

To display DHCP configuration information, perform one of the following tasks:

Command	Purpose
show ip dhcp relay	Displays the DHCP relay configuration.
show ipv6 dhcp relay [**interface** *interface*]	Displays the DHCPv6 relay global or interface-level configuration.
show ip dhcp relay address	Displays all the DHCP server addresses configured on the device.

Command	Purpose
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp [**all**]	Displays the DHCP configuration in the running configuration. **Note** The **show running-config dhcp** command displays the **ip dhcp relay** and the **ipv6 dhcp relay** commands, although these are configured by default.
show running-config interface {**ethernet** *slot/port* | **mgmt 0** | **vlan** *vlan-id*}	Displays the IPv4 or IPv6 address assigned to the interface when DHCP client is enabled.
show startup-config dhcp [**all**]	Displays the DHCP configuration in the startup configuration.

Displaying IPv6 RA Guard Statistics

To display IPv6 RA guard statistics, perform one of the following tasks:

Command	Purpose
show ipv6 raguard statistics	Displays IPv6-related RA guard statistics.

The following example shows sample statistics:

```
switch# show ipv6 raguard statistics
-------------------------------------
Interface     Rx         Drops
------------- ---------- ------------
Ethernet1/53  4561102    4561102
```

Displaying DHCP Snooping Bindings

Use the **show ip dhcp snooping binding** [*ip-address* | *mac-address* | **dynamic** | **static** | **vlan** *vlan-id* | **interface** *interface-type interface-number*] command to display all entries from the DHCP snooping binding database.

```
MacAddress        IpAddress LeaseSec Type   VLAN Interface
----------------- --------- -------- ------ ---- ------------
0f:00:60:b3:23:33 10.3.2.2  infinite static 13   Ethernet2/46
0f:00:60:b3:23:35 10.2.2.2  infinite static 100  Ethernet2/10
```

Clearing the DHCP Snooping Binding Database

Use the **clear ip dhcp snooping binding** command to clear all entries from the DHCP snooping binding database.

Use the **clear ip dhcp snooping binding interface ethernet** *slot/port* command to clear entries associated with a specific Ethernet interface from the DHCP snooping binding database.

Use the **clear ip dhcp snooping binding interface port-channel** *channel-number* command to clear entries associated with a specific port-channel interface from the DHCP snooping binding database.

Use the **clear ip dhcp snooping binding vlan** *vlan-id* [**mac** *mac-address* **ip** *ip-address* **interface** {**ethernet** *slot /port* | **port-channel** *channel-number*}] command to clear a single specific VLAN entry from the DHCP snooping binding database.

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

Clearing DHCP Snooping Statistics

Use the **clear ip dhcp snooping statistics** [**vlan** *vlan-id*] command to clear the DHCP snooping statistics.

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.

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

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.

Configuration Examples for DHCP

This example shows how to enable DHCP snooping on two VLANs, with Option 82 support enabled and Ethernet interface 2/5 trusted because the DHCP server is connected to that interface:

```
feature dhcp
ip dhcp snooping
ip dhcp snooping information option

interface ethernet 2/5
  ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```

This example shows how to enable the DHCP relay agent and configure the DHCP server IP address for Ethernet interface 2/3, where the DHCP server IP address is 10.132.7.120 and the DHCP server is in the VRF instance named red:

```
feature dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn

interface ethernet 2/3
  ip dhcp relay address 10.132.7.120 use-vrf red
```

This example shows how to enable and use the DHCP smart relay agent. In this example, the device forwards the DHCP broadcast packets received on Ethernet interface 2/2 to the DHCP server (10.55.11.3), inserting 192.168.100.1 in the giaddr field. If the DHCP server has a pool configured for the 192.168.100.0/24 network, it responds. If the server does not respond, the device sends two more requests using 192.168.100.1 in the giaddr field. If the device still does not receive a response, it starts using 172.16.31.254 in the giaddr field instead.

```
feature dhcp
ip dhcp relay
ip dhcp smart-relay global

interface ethernet 2/2
  ip address 192.168.100.1/24
  ip address 172.16.31.254/24 secondary
  ip dhcp relay address 10.55.11.3
```

Configuration Examples for DHCP Client

The following example shows how the DHCP client feature can be used to assign an IPv4 address to a VLAN interface:

```
switch# configure terminal
switch(config)# interface vlan 7
switch(config-if)# no shutdown
switch(config-if)# ip address dhcp
switch(config-if)# show running-config interface vlan 7
interface Vlan7
no shutdown
ip address dhcp
```

Additional References for DHCP

Related Documents

Related Topic	Document Title
Dynamic ARP inspection (DAI)	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*
IP Source Guard	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*
vPCs	*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*
VRFs and Layer 3 virtualization	*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
RFC 2131	Dynamic Host Configuration Protocol (https://datatracker.ietf.org/doc/html/rfc2131)
RFC 3046	DHCP Relay Agent Information Option (https://datatracker.ietf.org/doc/html/rfc3046)
RFC 6607	Virtual Subnet Selection Options for DHCPv4 and DHCPv6 (https://datatracker.ietf.org/doc/html/rfc6607)
RFC 6939	Client Link-Layer Address Option in DHCPv6 (https://datatracker.ietf.org/doc/html/rfc6939)