



Implementing DHCP

This module describes the concepts and tasks you will use to configure Dynamic Host Configuration Protocol (DHCP).

- [Introduction to DHCP Relay, on page 1](#)
- [Prerequisites for Configuring DHCP Relay Agent, on page 2](#)
- [Limitations for DHCP Relay Feature , on page 2](#)
- [How to Configure and Enable DHCP Relay Agent, on page 2](#)
- [Implementing DHCP Snooping, on page 14](#)
- [Configure DHCPv6 Relay Source Address, on page 21](#)
- [DHCP Client, on page 23](#)

Introduction to DHCP Relay

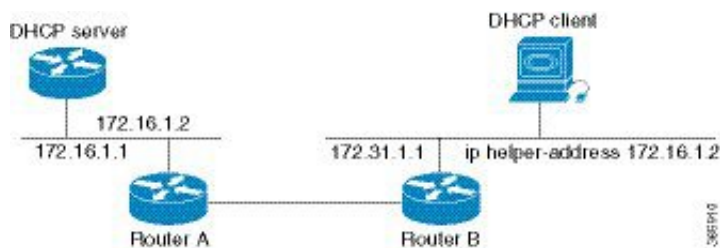
A DHCP relay agent is a host that forwards DHCP packets between clients and servers that do not reside on a shared physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router where the IP datagrams switch between networks transparently.

DHCP clients use User Datagram Protocol (UDP) broadcasts to send DHCPDISCOVER messages when they lack information about the network to which they belong.

If a client is on a network segment that does not include a server, the network segment needs a relay agent. Presence of the relay agent ensures that DHCP packets reach the servers on another network segment. Routers do not forward UDP broadcast packets, because most routers are not configured to forward broadcast traffic. You can configure a DHCP relay agent to forward DHCP packets to a remote server. You can configure a DHCP relay profile on the DHCP relay agent and configure one or more helper addresses in it. You can assign the profile to an interface or a VRF.

The following figure demonstrates the process. The DHCP client broadcasts a request for an IP address and other configuration parameters on its local LAN. Acting as a DHCP relay agent, Router B picks up the broadcast. It changes the destination address to the DHCP server's address and sends the message out on another interface. The relay agent inserts the IP address of the interface, which receives the DHCP client's packets, into the gateway address (giaddr) field of the DHCP packet. The giaddr enables the DHCP server to determine which subnet receives the offer and identify the appropriate IP address range. The relay agent unicasts the messages to the server address, in this case 172.16.1.2 (which is specified by the helper address in the relay profile).

Figure 1: Forwarding UDP Broadcasts to a DHCP Server Using a Helper Address



Prerequisites for Configuring DHCP Relay Agent

The following are the prerequisites to configure a DHCP relay agent:

- You must be in a user group that is associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect that a user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- A configured and running DHCP client and DHCP server.
- Connectivity between the relay agent and DHCP server

Limitations for DHCP Relay Feature

The limitations for implementing DHCP relay feature are as follows:

- DHCP relay profile does not support multicast addresses. The **helper-address** command in a DHCP relay profile submode supports a global unicast IP address only as the helper address.
- Relay agents add only interface-id and remote-id DHCP option code while forwarding the packet to a DHCP server.



Note DHCP relay profile submode does not support the configuration of DHCP option code.

How to Configure and Enable DHCP Relay Agent

This section contains the following tasks:

Configuring and Enabling the DHCP Relay Agent

Configuration Example

```
Router# configure
/* Enters the global configuration mode */
```

```

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile r1 relay
/* Enables DHCP relay profile */

Router(config-dhcpv4-relay-profile)# helper-address vrf A 10.10.7.1 giaddr 10.10.7.2
Router(config-dhcpv4-relay-profile)# broadcast-flag policy check
/* Configures VRF addresses for forwarding UDP broadcasts, including DHCP. */

Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
/* Inserts the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST
messages to a DHCP server. */

Router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
/* (Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets
that have an existing relay information option and the giaddr set to zero. */

Router(config-dhcpv4-relay-profile)# exit
Router(config-dhcpv4)# interface BVI 1 relay profile r1
Router(config-dhcpv4)# commit
/* Configures DHCP relay on a BVI interface and commits the configuration */

```

Running Configuration

```

Router#show running-config
Tue May 23 10:56:14.463 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Tue May 23 10:56:08 2017 by annseque
!
dhcp ipv4
  vrf vrf1 relay profile client
  profile r1 relay
    helper-address vrf A 10.10.7.1 giaddr 10.10.7.2
    broadcast-flag policy check
    relay information option vpn
    relay information option vpn-mode rfc
    relay information option allow-untrusted
!

```

Enabling a DHCP Relay Agent on an Interface

This section describes how to enable the Cisco IOS XR DHCP relay agent on an interface.

Configuration Example

The DHCP relay agent is disabled by default.

```

Router#configure

Router(config)#dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)#interface HundredGigE 0/2/0/2 relay profile client
/* Attaches a relay profile to an interface.

```

To disable the DHCP relay on the interface, use the 'no interface HundredGigE 0/2/0/2 none' command. */

```
Router(config-dhcpv4-if)#commit
```

Running Configuration

```
Router#show running-config dhcp ipv4
dhcp ipv4
interface HundredGigE 0/2/0/2 relay profile client
!
```

Disabling DHCP Relay on an Interface

This task describes how to disable the DHCP relay on an interface by using the **no** keyword on the interface.

```
Router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# no interface type name relay profile profile-nameRouter(config-dhcpv6)#
no interface type name none
Router(config-dhcpv6-if)# commit
```

Configuring and Enabling DHCP Relay Agent with DHCP MAC Address Verification

This section discusses how to configure and enable DHCP Relay Agent with DHCP MAC address verification.

Configuration Example

```
Router# configure

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile client relay
/* Enables DHCP relay profile */

Router(config-dhcpv4)# client-mac-mismatch action drop
/* Enables MAC address verification. If MAC address in the DHCPv4 protocol header does not
match the L2 header source MAC address in the DHCPv4 relay profile,
the frame is dropped */

Router(config-dhcpv4-relay-profile)# relay information option
/* Inserts the DHCP relay agent information option (option-82 field) in forwarded
BOOTREQUEST messages to a DHCP server. */

Router(config-dhcpv4-relay-profile)# relay information check
/* (Optional) Configures DHCP to check the validity of the relay agent information
option in forwarded BOOTREPLY messages. */

Router(config-dhcpv4-relay-profile)# relay information policy drop
/* (Optional) Configures the reforwarding policy for a DHCP relay agent;
that is, whether the relay agent will drop or keep (using the 'keep' keyword)
the relay information. */

Router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
/* (Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets that have
an existing
```

```

relay information option and the giaddr set to zero. */

Router(config-dhcpv4-relay-profile)# giaddr policy drop
/* Drops the packet that has an existing nonzero giaddr value. Use the 'replace' keyword
   to replace the existing giaddr value with a value that it generates (the default behavior).
   */

Router(config-dhcpv4-relay-profile)# helper-address vrf vrf1 10.1.1.1
/* Forwards UDP broadcasts, including DHCP. */

Router(config-dhcpv4-relay-profile)# commit

Router(config-dhcpv4-relay-profile)# exit
Router(config-dhcpv4)# vrf vrf1 relay profile client
Router(config-dhcpv4)# commit
/* Configures DHCP Relay on a VRF and commits the entire configuration. */

```

Running Configuration

Confirm your configuration.

```

Router# show run
Thu May 11 09:00:57.839 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Thu May 11 09:00:54 2017 by annseque
!
dhcp ipv4
vrf vrf1 relay profile client
profile client relay
client-mac-match action drop
helper-address vrf vrf1 10.1.1.1
giaddr policy drop
relay information check
relay information option
relay information policy drop
relay information option allow-untrusted
!
!

```

DHCP MAC Address Verification

Use the following show command to check if DHCP MAC addresses are verified on the router.

```

Router# show dhcp ipv4 relay statistics raw all
packet_drop_mac_mismatch          :          0

```

The output validates the verified DHCP MAC address of the packets is verified.

Configuring the DHCPv6 (Stateless) Relay Agent

Use the following steps:

- To specify a destination address for client messages.
- To enable DHCP IPv6 relay service on the interface.

Configuration Example

To configure the DHCPv6 (stateless) relay agent, you must complete the following configurations:

1. Enable the DHCP IPv6 configuration mode.
2. Configure the DHCPv6 relay profile.
3. Configure helper addresses.
4. Specify the interface for the relay profile.

Configuration

```
/* Enter the global configuration mode, and then enter the DHCP IPv6 configuration mode */
Router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile test relay
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:1::1
Router(config-dhcpv6-relay-profile)# !
Router(config-dhcpv6-relay-profile)# interface TenGigE0/0/0/0 relay profile test
Router(config-dhcpv6)# !
```

Enabling DHCP Relay on a VRF

This task describes how to enable DHCP relay on a VRF.

```
/CPU0:router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# vrf vrf-name relay profile profile-name
Router(config-dhcpv6-if)# commit
```

Configure a DHCP Relay Profile with Multiple Helper Addresses

You can configure up to 16 helper IPv4 and IPv6 addresses for a DHCPv4 or DHCPv6 relay profile.

1. Enter the DHCPv4 or DHCPv6 configuration mode.

```
Router(config)# dhcp ipv6
```

2. Configure the DHCPv4 or DHCPv6 relay profile.

```
Router(config-dhcpv6)# profile helper relay
```

3. Configure helper addresses.



Note You can configure up to 16 IPv4 and IPv6 addresses.

```
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:1:1::2
```

4. Confirm your configuration.

```
Router(config-dhcpv6-relay-profile)# show configuration
```

```
!! IOS XR Configuration 0.0.0
dhcp ipv6
```

```

profile helper relay
  helper-address vrf default 2001:1:1::2
!
!
end

```

5. Commit your configuration.

```
Router(config-dhcpv6-relay-profile)# commit
```

6. Exit the configuration mode and verify the configured helper addresses.

```
Router# show dhcp ipv6 relay profile name helper
```

```

Profile: helper
Helper Addresses:
    2001:1:1::2, vrf default
Information Option: Disabled
Information Option Allow Untrusted: Disabled
Information Option VPN: Disabled
Information Option VPN Mode: RFC
Information Option Policy: Replace
Information Option Check: Disabled
GIADDR Policy: Keep
Broadcast-flag Policy: Ignore
VRF References:
Interface References:

```

You have successfully configured the DHCPv6 relay helper address.

DHCP Relay Agent Notification for Prefix Delegation

DHCP relay agent notification for prefix delegation allows the router working as a DHCPv6 relay agent to find prefix delegation options. The notifications allow you to review the contents of a DHCP RELAY-REPLY packet that is sent to the client. When the relay agent finds the prefix delegation option, it extracts the information about the delegated prefix. After extracting the information, the relay agent inserts an IPv4 or IPv6 subscriber route matching the prefix delegation information onto the relay agent. A relay agent forwards future packets that are destined to that prefix based on the information that is contained in the prefix delegation.

The relay agent automatically does the subscriber route management.

The IPv4 or IPv6 routes are added when the relay agent relays a RELAY-REPLY packet. The IPv4 or IPv6 routes are deleted when the prefix delegation lease time expires or the relay agent receives a release message. An IPv4 or IPv6 subscriber route in the routing table of the relay agent is updated when the prefix delegation lease time is extended.

This feature leaves an IPv4 or IPv6 route on the routing table of the relay agent. This registered IPv4 or IPv6 address allows a unicast reverse packet forwarding (uRPF) to work by allowing the router doing the reverse lookup. The reverse lookup enables you to confirm that the IPv4 or IPv6 address on the relay agent is not malformed or spoofed. The IPv6 route in the routing table of the relay agent can be redistributed to other routing protocols to advertise the subnets to other nodes. When the client sends a DHCP_DECLINE message, the routes are removed.

Configuring Relay Agent Option 82 Per Ethernet Flow Points

Table 1: Feature History Table

Feature Name	Release	Description
Option 82 support in DHCP packets	Release 25.1.1	<p>Introduced in this release on: Modular Systems (8800 [LC ASIC: P100]) (select variants only*)</p> <p>By utilizing DHCP Relay Agent Option 82 functionality, you can now enhance the network security by ensuring that DHCP allocates network addresses only to trusted sources. This reduces the risk of unauthorized devices gaining network access. You can achieve this by assigning Option 82 circuit ID and Remote ID per Ethernet Flow Points (EFP) or per ingress Layer 2 interface in the DHCP packet.</p> <p>*This feature is supported on:</p> <ul style="list-style-type: none"> • 88-LC1-52Y8H-EM • 88-LC1-12TH24FH-E

In forwarded BOOTREQUEST messages to a DHCP server, you can configure the relay agent to insert Option 82 suboptions in the DHCP packet. The Option 82 suboptions available for configuration are Circuit ID and Remote ID. When a DHCP relay profile is attached to a Bridge Virtual Interface (BVI), you can assign the Option 82 circuit ID and Remote ID per Ethernet Flow Points (EFP) or per ingress Layer 2 interface. The relay agent then sends the DHCP packet to the server with the included Option 82 Circuit ID or Remote ID. DHCP Relay Agent Option 82 provides security when DHCP is used to allocate network addresses. Thus, you can enable the DHCP relay agent to prevent DHCP client requests from untrusted sources.

Benefits of Configuring Relay Agent Option 82

The benefits of configuring relay agent Option 82 are:

- Option 82 allows for better tracking of where DHCP requests originate, making it easier to manage and troubleshoot network connections.
- By identifying the origin of DHCP requests, network resources such as IP addresses can be allocated more efficiently and appropriately based on the source location.

Configuration Example

Follow the steps to configure a Layer 2 interface with relay agent Option 82 suboptions, Circuit ID and Remote ID:

```
/* Configure DHCP for IPv4 and enter the DHCPv4 configuration submode. */
Router# configure
Router(config)# dhcp ipv4

/* Enable DHCP relay profile. */
Router(config-dhcpv4)# profile bvi1_profile relay

/* Configure VRF addresses for forwarding UDP broadcasts, including DHCP. */
Router(config-dhcpv4-relay-profile)# helper-address 192.0.2.1

/* Insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST
```



```

    messages to a DHCP server. */
Router(config-dhcpv4-relay-profile)# relay information option
Router(config-dhcpv4-relay-profile)# exit

/* Enable DHCP for IPv4 on a BVI interface and attach the profile as the relay profile for
the BVI interface. */
Router(config-dhcpv4)# interface BVI1 relay profile bv1_profile

/* Enable the DHCP relay agent to add Option 82 Circuit ID field in ascii or hex format per
EFP to the DHCP packet. */
Router(config-dhcpv4)# interface Bundle-Ether50.103 relay information option circuit-id
format-type ascii 110

/* Enable the DHCP relay agent to add Option 82 Remote ID field in ascii or hex format per
EFP to the DHCP packet. */
Router(config-dhcpv4)# interface Bundle-Ether50.103 relay information option remote-id
format-type ascii 110
Router(config-dhcpv4)# commit

```

Running Configuration

```

Router# show running-config dhcp ipv4
Wed Jan 27 11:20:19.842 UTC
dhcp ipv4
  profile bv1_profile relay
    helper-address vrf default 192.0.2.1
    relay information option
  !
  interface BVI1 relay profile bv1_profile
  interface Bundle-Ether50.103 relay information option circuit-id format-type ascii 110
  interface Bundle-Ether50.103 relay information option remote-id format-type ascii 110
  !

```

DHCPv6 Relay Over BVI for IANA Address Allocation

DHCPv6 relay agents relay all packets that are coming from DHCPv6 clients over the access-interfaces toward external DHCPv6 servers. DHCPv6 relay agents request IP addresses (::/128) through IANA allocation for the DHCPv6 clients. DHCPv6 relay agents also receive response packets from the DHCPv6 servers and forward the packets toward DHCPv6 clients over BVI interfaces. DHCPv6 relay agents act as stateless, by default, for DHCPv6 clients. DHCPv6 clients do not maintain any DHCPv6 binding and respective route entry for the allocated IP addresses. You can enable a DHCPv6 client to get a particular IPv6 address assigned by the DHCPv6 server over a Bridge Virtual Interface (BVI) through Internet Assigned Numbers Authority (IANA) address allocation. Therefore, the DHCPv6 relay agent acts as a stateful relay agents and maintains DHCPv6 binding and respective route entry for the allocated IPv6 addresses.

Restrictions

- You can configure up to 500 client sessions over a BVI interface for DHCP relay.
- You can configure up to 8 DHCPv6 server addresses for each DHCPv6 relay profile.

Configuration Example

To configure DHCPv6 Relay Over BVI for IANA Address Allocation, use the following steps.

1. Enter the interface configuration mode and configure a BVI interface.
2. Assign an IPv6 address to the BVI interface.

3. Route the L2 access interface to the L3 BVI interface of the relay agent.
4. Enter the DHCP IPv6 configuration mode and then create a DHCP IPv6 Stateful relay profile.
5. Attach the relay profile to a server address.
6. Configure a stateful relay agent by enabling route allocation through IANA.
7. Attach the BVI Interface to the DHCPv6 relay profile.

Configuration

```

/* Enter the interface configuration mode and configure a BVI interface. */
Router# configure
Router(config)# interface BVI1

Assign an IPv6 address to the BVI interface.
Router(config-if)# ipv6 address 2001:db8::2/64
Router(config-if)# commit
Router(config-if)# exit

/* Route the L2 access interface to the L3 BVI interface of the relay agent. */
Router(config)# l2vpn bridge group 1
Router(config-l2vpn-bg)# bridge-domain 1
Router(config-l2vpn-bg-bd)# interface hundredGigE 0/0/0/1.100
Router(config-l2vpn-bg-bd-ac)# commit
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# routed interface BVI1
Router(config-l2vpn-bg-bd)# exit
Router(config-l2vpn-bg)# exit
Router(config-l2vpn)# exit
Router(config)#

/* Enter the DHCP IPv6 configuration mode and then create a DHCP IPv6 Stateful relay profile.
*/
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile RELAY1 relay

/* Attach the relay profile to a server address. */
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:DB8::1

/* Configure a stateful relay agent by enabling route allocation through IANA. */
Router(config-dhcpv6-relay-profile)# iana-route-add
Router(config-dhcpv6-relay-profile)# exit

/* Attach the BVI Interface to the DHCPv6 relay profile. */
Router(config-dhcpv6-relay-profile)# interface BVI1 relay profile RELAY1
Router(config-dhcpv6-relay-profile)# commit

```

Running Configuration

```

Router# show running configuration
interface BVI1
  ipv6 address 2001:db8::2/64
!
l2vpn
  bridge group 1
    bridge-domain 1

```



```
Lifetime: 600 secs (00:10:00)
Expiration: 439 secs (00:07:19)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE
```

Use the following command to verify that a unique IPv6 address is assigned to a client due to IANA allocation:

```
Router# show route ipv6
Mon Oct 21 06:16:43.617 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
        U - per-user static route, o - ODR, L - local, G - DAGR, l - LISP
        A - access/subscriber, a - Application route
        M - mobile route, r - RPL, t - Traffic Engineering, (!) - FRR Backup path

Gateway of last resort is not set

A    2000::/64
      [1/0] via fe80::1, 00:00:37, BVI700
A    2000::1/128
      [1/0] via fe80::210:94ff:fe00:8, 00:00:12, BVI700
C    2007:3019::/64 is directly connected,
      00:00:37, Loopback1
L    2007:3019::1/128 is directly connected,
      00:00:37, Loopback1
C    7001:6018::/64 is directly connected,
      00:00:37, BVI700
L    7001:6018::1/128 is directly connected,
      00:00:37, BVI700
C    7001:6019::/64 is directly connected,
      00:00:37, TenGigE0/0/0/2.2
L    7001:6019::1/128 is directly connected,
      00:00:37, TenGigE0/0/0/2.2
```

Configuring the Relay Agent Information Feature

You can configure the DHCP relay agent information option. A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, the relay information from the previous relay agent is replaced (using the replace option).

Configuration

Use the following steps to configure the DHCP relay agent information option:

1. Enter DHCP IPv4 configuration submode.
2. Enter DHCP IPv4 profile relay submode.
3. Configure the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server.

**Note**

- This option is injected by the relay agent while forwarding client-originated DHCP packets to the server. Servers recognizing this option can use the information to implement IP address or other parameter assignment policies. When replying, the DHCP server echoes the option back to the relay agent. The relay agent removes the option before forwarding the reply to the client.
- The relay agent information is organized as a single DHCP option that contains one or more suboptions. These options contain the information known by the relay agent. The supported suboptions are:
 - Remote ID
 - Circuit ID
- This function is disabled by default. The port field of the default circuit-ID denotes the configured bundle-ID of the bundle. If circuit IDs require that bundles be unique, and because the port field is 8 bits, the low-order 8 bits of configured bundle IDs must be unique. To achieve this, configure bundle-IDs within the range from 0 to 255.

4. (Optional) Configure DHCP to check the validity of the relay agent information option in forwarded BOOTREPLY messages.

**Note**

- If an invalid message is received, the relay agent drops the message. If a valid message is received, the relay agent removes the relay agent information option field and forwards the packet.
- By default, DHCP does not check the validity of the relay agent information option field in DHCP reply packets, received from the DHCP server.

5. (Optional) Configure the reforwarding policy for a DHCP relay agent; that is, whether the relay agent will drop or keep the relay information.

**Note**

By default, the DHCP relay agent replaces the relay information option.

6. (Optional) Configure the DHCP IPv4 Relay not to discard BOOTREQUEST packets that have an existing relay information option and the giaddr set to zero.

Configuration Example

```

/* Enter DHCP IPv4 configuration submode. */
Router# Configure
Router(config)# dhcp ipv4

/* Enter DHCP IPv4 profile relay submode. */
Router(config-dhcpv4)# profile RELAY relay

/* Configure the system to insert the DHCP relay agent information option. */
Router(config-dhcpv4-relay-profile)# relay information option

/* (Optional) Configure DHCP to check the validity of the relay agent information option.
```

```

*/
Router(config-dhcpv4-relay-profile)# relay information check

/* (Optional) Configure the reforwarding policy for a DHCP relay agent. */
Router(config)# dhcp ipv4 profile TEST relay relay information policy drop
Router(config)# commit

```

Configuring Relay Agent Giaddr Policy

You can configure the DHCP relay agent's processing capabilities for the BOOTREQUEST packets that already contain a nonzero giaddr attribute. Use the `giaddr policy replace` command to replace the existing giaddr value with a value that it generates. Use the `giaddr policy drop` command to drop the packet that has an existing nonzero giaddr value.

Configuration

To configure a relay agent giaddr policy, use the following steps:

- Enter the DHCP IPv4 configuration submode.
- Enter the relay profile submode.
- Configure the giaddr policy.

Configuration Example

```

/* Enter the DHCP IPv4 configuration submode. */
Router# configure
Router(config)# dhcp ipv4

/* Enter the relay profile submode. */
Router(config-dhcpv4)# profile client relay

/* Configure the giaddr policy. */
Router(config-dhcpv4-relay-profile)# giaddr policy drop
Router(config-dhcpv4-relay-profile)# commit

```

Implementing DHCP Snooping

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
DHCP Snooping	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) This feature is supported on: <ul style="list-style-type: none"> • 8011-4G24Y4H-I

Feature Name	Release Information	Feature Description
DHCP Snooping	Release 24.4.1	<p>Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*)</p> <p>DHCP snooping enhances network security and prevents unauthorized or malicious DHCP servers from distributing IP addresses. By maintaining a whitelist of approved servers, DHCP snooping ensures that only trusted DHCP messages are processed. This feature safeguards against IP address spoofing and man-in-the-middle attacks by inspecting and filtering DHCP packets. This reliable security measure integrates seamlessly with existing network configurations, offering robust protection for your network infrastructure while maintaining efficient IP address management.</p> <p>*This feature support is now extended to Cisco 8712-MOD-M routers.</p>

Prerequisites for Configuring DHCP Snooping

The following prerequisites are required example shows how to configure DHCP IPv4 snooping relay agent broadcast flag policy:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- A Cisco 8000 Series Router running Cisco IOS XR software.
- A configured and running DHCP client and DHCP server.

Information about DHCP Snooping

DHCP Snooping features are focused on the edge of the aggregation network. Security features are applied at the first point of entry for subscribers. Relay agent information option information is used to identify the subscriber's line, which is either the DSL line to the subscriber's home or the first port in the aggregation network.

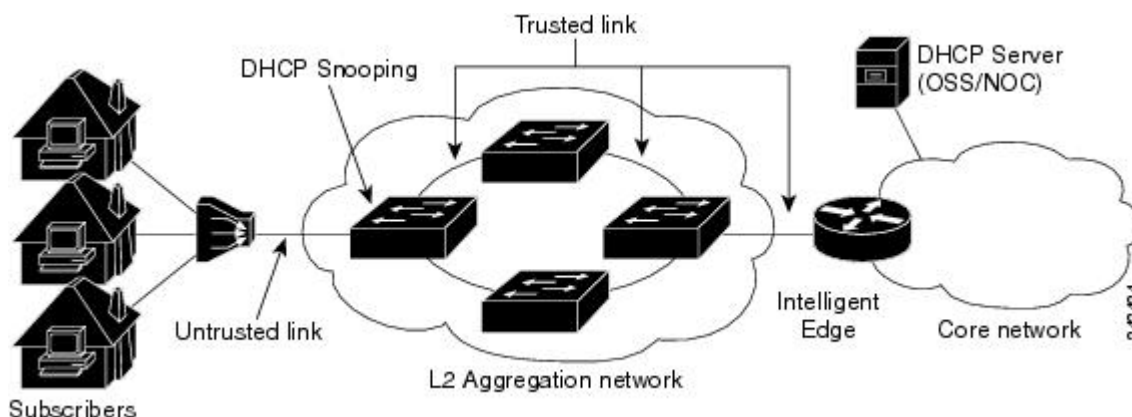
The central concept for DHCP snooping is that of trusted and untrusted links. A trusted link is one providing secure access for traffic on that link. On an untrusted link, subscriber identity and subscriber traffic cannot be determined. DHCP snooping runs on untrusted links to provide subscriber identity. [Figure 2: DHCP Snooping in an Aggregation Network, on page 16](#) shows an aggregation network. The link from the DSLAM to the aggregation network is untrusted and is the point of presence for DHCP snooping. The links connecting the switches in the aggregation network and the link from the aggregation network to the intelligent edge is considered trusted.



Note

Enabling both DHCP relay on a BVI and DHCP snooping in a bridge domain that has a BVI can result in duplicate DHCP messages from the DHCP client to the DHCP server.

Figure 2: DHCP Snooping in an Aggregation Network



Trusted and Untrusted Ports

On trusted ports, DHCP BOOTREQUEST packets are forwarded by DHCP snooping. The client's address lease is not tracked and the client is not bound to the port. DHCP BOOTREPLY packets are forwarded.

When the first DHCP BOOTREQUEST packet from a client is received on an untrusted port, DHCP snooping binds the client to the bridge port and tracks the clients's address lease. When that address lease expires, the client is deleted from the database and is unbound from the bridge port. Packets from this client received on this bridge port are processed and forwarded as long as the binding exists. Packets that are received on another bridge port from this client are dropped while the binding exists. DHCP snooping only forwards DHCP BOOTREPLY packets for this client on the bridge port that the client is bound to. DHCP BOOTREPLY packets that are received on untrusted ports are not forwarded.

DHCP Snooping in a Bridge Domain

To enable DHCP snooping in a bridge domain, there must be at least two profiles, a trusted profile and an untrusted profile. The untrusted profile is assigned to the client-facing ports, and the trusted profile is assigned to the server-facing ports. In most cases, there are many client facing ports and few server-facing ports. The simplest example is two ports, a client-facing port and a server-facing port, with an untrusted profile explicitly assigned to the client-facing port and a trusted profile assigned to the server-facing port.

Assigning Profiles to a Bridge Domain

Because there are normally many client-facing ports and a small number of server-facing ports, the operator assigns the untrusted profile to the bridge domain. This configuration effectively assigns an untrusted profile to every port in the bridge domain. This action saves the operator from explicitly assigning the untrusted profile to all of the client-facing ports. Because there also must be server-facing ports that have trusted DHCP snooping profiles, in order for DHCP snooping to function properly, this untrusted DHCP snooping profile assignment is overridden to server-facing ports by specifically configuring trusted DHCP snooping profiles on the server-facing ports. For ports in the bridge domain that do not require DHCP snooping, all should have the **none** profile assigned to them to disable DHCP snooping on those ports.

Relay Information Options

You can configure a DHCP snooping profile to insert the relay information option (option 82) into DHCP client packets only when it is assigned to a client port. The **relay information option allow-untrusted** command addresses what to do with DHCP client packets when there is a null giaddr and a relay-information

option already in the client packet when it is received. This is a different condition than a DHCP snooping trusted/untrusted port. The **relay information option allow-untrusted** command determines how the DHCP snooping application handles untrusted relay information options.

How to Configure DHCP Snooping

This section contains the following tasks:

Enabling DHCP Snooping in a Bridge Domain

The following configuration creates two ports, a client-facing port and a server-facing port. In Step 1 through Step 8, an untrusted DHCP snooping profile is assigned to the client bridge port and trusted DHCP snooping profile is assigned to the server bridge port. In Step 9 through Step 18, an untrusted DHCP snooping profile is assigned to the bridge domain and trusted DHCP snooping profiles are assigned to server bridge ports.

Procedure

Step 1 Enter the DHCP IPv4 profile configuration submode using the **dhcp ipv4** command.

Example:

```
Router(config)# dhcp ipv4
```

Step 2 Configure an untrusted DHCP snooping profile for the client port using the **profile *untrusted-profile-name* snoop** command.

Example:

```
Router(config-dhcpv4)# profile untrustedClientProfile snoop
```

Step 3 Exit the DHCP IPv4 profile configuration mode using the **exit** command.

Example:

```
Router(config-dhcpv4)# exit
```

Step 4 Enable DHCP for IPv4 and enters DHCP IPv4 profile configuration mode using the **dhcp ipv4** command.

Example:

```
Router(config)# dhcp ipv4
```

Step 5 Configure a trusted DHCP snooping profile for the server port using the **profile *profile-name* snoop** command.

Example:

```
Router(config-dhcpv4)# profile trustedServerProfile snoop
```

Step 6 Configure a DHCP snoop profile to be trusted using the **trusted** command.

Example:

```
Router(config-dhcpv4)# trusted
```

Step 7 Exit the DHCP IPv4 profile configuration mode using the **exit** command.

Example:

```
Router(config-dhcv4)# exit
```

Step 8 Enter the l2vpn configuration mode using the **l2vpn** command.

Example:

```
Router(config)# l2vpn
```

Step 9 Create a bridge group to contain bridge domains and enter l2vpn bridge group configuration submode using the **bridge group group-name** command.

Example:

```
Router(config-l2vpn)# bridge group ccc
```

Step 10 Establish a bridge domain using the **bridge-domain bridge-domain-name** command.

Example:

```
Router(config-l2vpn-bg)# bridge-domain ddd
```

Step 11 Identify the interface using the **interface type interface-path-id** command.

Example:

```
Router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/0
```

Step 12 Attach an untrusted DHCP snoop profile to the bridge port using the **dhcp ipv4 snoop profile untrusted-profile-name** command.

Example:

```
Router(config-l2vpn-bg-bd-ac)# dhcp ipv4 snoop profile untrustedClientProfile
```

Step 13 Identify the interface using the **interface type interface-path-id** command.

Example:

```
Router(config-l2vpn-bg-bd-ac)# gigabitethernet 0/1/0/1
```

Step 14 Attache a trusted DHCP snoop profile to the bridge port using the **dhcp ipv4 snoop profile trusted-profile-name** command.

Example:

```
Router(config-l2vpn-bg-bd-ac)# dhcp ipv4 snoop profile trustedServerProfile
```

Step 15 Exit the l2vpn bridge group bridge-domain interface configuration submode using the **exit** command.

Example:

```
Router(config-l2vpn-bg-bd-ac)# exit
```

Step 16 Exit the l2vpn bridge group bridge-domain configuration submode using the **exit** command.

Example:

```
Router(config-l2vpn-bg-bd) # exit
```

Step 17 Commit the configuration changes on the router.

Example:

```
Router(config) # commit
```

Disabling DHCP Snooping on a Specific Bridge Port

The following configuration enables DHCP to snoop packets on all bridge ports in the bridge domain ISP1 except for bridge port GigabitEthernet 0/1/0/1 and GigabitEthernet 0/1/0/2. DHCP snooping is disabled on bridge port GigabitEthernet 0/1/0/1. Bridge port GigabitEthernet 0/1/0/2 is the trusted port that connects to the server. In this example, no additional features are enabled, so only DHCP snooping is running.

Procedure

Step 1 Enter l2vpn configuration submode using the **l2vpn** command.

Example:

```
Router(config) # l2vpn
```

Step 2 Create a bridge group to contain bridge domains and enter l2vpn bridge group configuration submode using the **bridge group group-name** command.

Example:

```
Router(config-l2vpn) # bridge group GRP1
```

Step 3 Establish a bridge domain and enter l2vpn bridge group bridge-domain configuration submode. **bridge-domain bridge-domain-name**

Example:

```
Router(config-l2vpn-bg) # bridge-domain ISP1
```

Step 4 Attach the untrusted DHCP snooping profile to the bridge domain using the **dhcp ipv4 snoop profile profile-name** command.

Example:

```
Router(config-l2vpn-bg-bd) # dhcp ipv4 snoop profile untrustedClientProfile
```

Step 5 Identify an interface and enter l2vpn bridge group bridge-domain interface configuration submode using the **interface type interface-path-id** command.

Example:

```
Router(config-l2vpn-bg-bd) # interface gigabitethernet 0/1/0/1
```

Step 6 Disable DHCP snooping on the port using the **dhcp ipv4 none** command.

Example:

```
Router(config-l2vpn-bg-bd-if)# dhcp ipv4 none
```

Step 7 Identify an interface and enter l2vpn bridge group bridge-domain interface configuration submode using the **interface type interface-path-id** command.

Example:

```
Router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/2
```

Step 8 Attach the trusted DHCP snooping profile to a port using the **dhcp ipv4 snoop profile profile-name** command.

Example:

```
Router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile trustedServerProfile
```

Step 9 Exit l2vpn bridge-domain bridge group interface configuration submode using the **exit** command.

Example:

```
Router(config-l2vpn-bd-bg)# exit
```

Step 10 Exit l2vpn bridge-domain submode using the **exit** command.

Example:

```
Router(config-l2vpn-bg)# exit
```

Step 11 Commit the configuration changes on the router.

Example:

```
Router(config)# commit
```

Using the Relay Information Option

This task shows how to use the relay information commands to insert the relay information option (option 82) into DHCP client packets and forward DHCP packets with untrusted relay information options.

Procedure

Step 1 Enter the DHCP IPv4 profile configuration submode using the **dhcp ipv4** command.

Example:

```
Router# config
Router(config)# dhcp ipv4
```

Step 2 Configure an untrusted DHCP snooping profile for the client port using the **profile profile-name snoop** command.

Example:

```
Router(config-dhcpv4)# profile untrustedClientProfile snoop
```

- Step 3** Enable the system to insert the DHCP relay information option field in forwarded BOOTREQUEST messages to a DHCP server using the **relay information option** command.

Example:

```
Router(config-dhcpv4-snoop-profile)# relay information option
```

- Step 4** Commit the configuration changes on the router.

Example:

```
Router(config-dhcpv4-snoop-profile)# commit
```

Configure DHCPv6 Relay Source Address

Table 3: Feature History Table

Feature Name	Release Information	Feature Description
Configure DHCPv6 relay source address	Release 25.1.1	<p>Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100])</p> <p>You can now select an IPv6 address from the configured relay source-interface to be used as the source address for forwarding packets to a server. By selecting a fixed source address, the need to frequently update firewall rules when new, lower-value IPv6 addresses are added is minimized.</p> <p>Previously, the router automatically used the lowest numbered IPv6 address configured on that interface as the source address.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> The <i>dhcpv6 relay source address</i> variable is introduced in the helper-address (ipv6) command. <p>YANG Data Model: Cisco-IOS-XR-ipv6-new-dhcpv6d-cfg.yang (see GitHub, YANG Data Models Navigator)</p>

The feature introduces the capability to select a specific IPv6 address from the configured relay source-interface to be used as the source address for forwarding packets to the server. Previously, the system would automatically use the lowest numbered IPv6 address configured on that interface as the source address. This prior behavior required you to update the firewall rules whenever new IPv6 addresses of lower value were added to a DHCPv6 enabled interface.

Benefits of Configuring DHCPv6 Relay Source Address

The benefits of configuring DHCPv6 relay source address are:

- Flexibility – You can now choose a specific IPv6 address from the relay source-interface, allowing more control over which address is used for packet forwarding.
- Reduced firewall updates – By selecting a fixed source address, the need to frequently update firewall rules when new, lower-value IPv6 addresses are added is minimized.
- Enhanced security – With a stable relay source address, security policies can be more consistently applied, reducing the risk of misconfigurations.
- Improved troubleshooting – Having a predictable relay source address makes it easier to track and troubleshoot network traffic issues.

Configuration Guidelines and Restrictions for Configuring DHCPv6 Relay Source Address

These restrictions and guidelines apply if you configure DHCPv6 relay source address:

- Removing the configured DHCPv6 relay source-interface IP disables the feature and retains the old behaviour of automatically using the lowest numbered IPv6 address configured on that interface as the source address.
- You can configure the DHCPv6 relay source address under **helper-address** and in the **source-interface** as well.

Configuration Example

The following section details the configuration for DHCPv6 relay source address:

```
/* Enter the global configuration mode, and then enter the DHCP IPv6 configuration mode */
Router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile test relay
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2011::3 TenGigE0/0/0/0 1001::10
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2011::4
Router(config-dhcpv6-relay-profile)# source-interface TenGigE0/1/0/0 1001::1
Router(config-dhcpv6-relay-profile)# !
Router(config-dhcpv6-relay-profile)# interface Bundle-Ether1 relay profile test
Router(config-dhcpv6-relay-profile)# commit
Router(config-dhcpv6)# !
```

In this example, when a packet is received on the profile **relay test**, the router:

- The address **1001::10**, specified as the DHCPv6 relay source address, on interface **TenGigE0/0/0/0** is used to send packets to server **2011::3**.
- The address **1001::1**, specified as the DHCPv6 relay source address, on interface **TenGigE0/1/0/0** is used to send packets to server **2011::4**.



Note To disable this feature, use the **no** form of the command.

Running Configuration

To verify the DHCPv6 relay source address configuration:

```
Router#show running-config interface TenGigE0/0/0/0
Wed Jan 15 17:48:09.635 UTC
dhcp ipv6
profile test relay
  helper-address vrf default 2011::3 TenGigE0/0/0/0 1001::10
  helper-address vrf default 2011::4
  source-interface TenGigE0/1/0/0 1001::1
!
interface Bundle-Ether1 relay profile test
```

DHCP Client

Table 4: Feature History Table

Feature Name	Release	Description
Support for DHCP client	Release 25.1.1	<p>Introduced in this release on: Modular Systems (8800 [LC ASIC: P100]) (select variants only*)</p> <p>This release introduces the Dynamic Host Configuration Protocol (DHCP) client functionality. DHCP client is crucial for efficiently managing IP address allocation in a network. It enables router interfaces to dynamically obtain server information for DHCPv4 or DHCPv6, and ensures that the configuration responses are sent to the appropriate Layer 2 addresses. This process ensures that each device on the network receives the correct configuration data.</p> <p>*This feature is supported on:</p> <ul style="list-style-type: none"> • 88-LC1-52Y8H-EM • 88-LC1-12TH24FH-E

The Dynamic Host Configuration Protocol (DHCP) client functionality allows the router interfaces to dynamically acquire the IPv4 or DHCPv4 or DHCPv6 server information and forward responses to the correct Layer 2 address, ensuring that each device receives the appropriate configuration information.

DHCP can allocate IP addresses only for a specified duration, known as the lease period. If a client needs to retain an IP address for a longer period beyond the lease period, the lease period must be renewed before the IP address expires. The client renews the lease period based on the server's configuration by unicasting a REQUEST message to the server's IP address. Upon receiving the REQUEST, the server responds with an ACK message, extending the client's lease period as specified in the ACK.

Configuration Guideline for DHCP Clients

Either DHCPv4, DHCPv6, static IPv4, or static IPv6 can be configured on an interface.

Enabling DHCP Client on an Interface

The DHCPv4 or DHCPv6 client can be enabled at an interface level. The DHCP component receives a notification when DHCPv4 or DHCPv6 is enabled or disabled on an interface.

```
Router# configure
Router(config)# interface bvi
Router(config)# interface bvi_interface_name ipv6 address dhcp
```

You can configure DHCPv6 client on BVI interfaces. You can configure different DHCPv6 client options to differentiate between clients as required. The different DHCPv6 client options are also configured to differentiate how a DHCPv6 client communicates with a DHCPv6 server. The different DHCPv6 client options that can be configured are:

- **DUID:** If the DUID DHCPv6 client option is configured on an interface, DHCPv6 client communicates with the DHCPv6 server through the link layer address.
- **Rapid Commit:** If the Rapid Commit DHCPv6 client option is configured on an interface, DHCPv6 client can obtain configuration parameters from the DHCPv6 server through a rapid two-step exchange (solicit and reply) instead of the default four-step exchange (solicit, advertise, request, and reply).
- **DHCP Options:** The various other DHCPv6 options that can be configured on a DHCPv6 client are:
 - **Option 15:** Option 15 is also known as the User Class option and it is used by a DHCPv6 client to identify the type or category of users or applications it represents.
 - **Option 16:** Option 16 is also known as the Vendor ID option and it is used by a DHCPv6 a client to identify the vendor that manufactured the hardware on which the client is running.
 - **Option 23:** Option 23 is also known as the Domain name Server (DNS) option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver can send DNS queries.
 - **Option 24:** Option 24 is also known as the Domain List option and it specifies the domain search list that the client uses to resolve hostnames with the DNS.
- **DHCP Timers:** This option is used to set different timer value for DHCP client configurations. The various DHCP timer options are:
 - **Release-timeout:** It is used to set retransmission timeout value for the initial release message.
 - **Req-max-rt:** It is used to set the maximum retransmission timeout value for the request message.
 - **Req-timeout:** It is used to set the initial request timeout value of the request message.
 - **Sol-max-delay:** It is used to set the maximum delay time of the first solicit message.
 - **Sol-max-rt:** It is used to set the maximum solicit retransmission time.
 - **Sol-time-out:** It is used to set the initial timeout value of the solicit message.

Configuration Example

You can use the following steps to configure DHCPv6 client on a BVI interface:

```
/* Enter the interface configuration mode, and then configure a BVI interface. */
Router# configure
Router(config)# interface BVI 1
```



```
/* Enter the DHCPv6 client configuration mode, and then enter the DHCPv6 client mode. */
Router(config)# ipv6 address dhcp
Router(config)# commit
```

Verification

To verify the DHCPv6 client mode, use the `show dhcp ipv6 client` command:

```
Router# show dhcp ipv6 client
Interface name IPv6 Address State Lease Time Rem
-----
BVI1 2001::1:2/128 BOUND 2591973
```

Associated Commands

- `ipv6 address dhcp-client-options`
- `clear dhcp ipv6 client`
- `show dhcp ipv6 client`
- `show dhcp ipv4 client`
- `show tech-support dhcp ipv6 client`

