DHCPv6 Options Support

This module describes the Dynamic Host Control Protocol Version 6 (DHCPv6) Relay Agent, DHCPv6 Interface-ID, Lightweight DHCPv6 Relay Agent (LRDA), and CAPWAP Access Controller DHCP Option 52 features.

This module consists of these sections:

- Restrictions for DHCPv6 Options Support, page 61-1
- Information About DHCPv6 Options Support, page 61-2
- How to Configure DHCPv6 Options Support, page 61-5
- Configuration Examples for DHCPv6 Options Support, page 61-9
- Additional References for DHCPv6 Options Support, page 61-10
- Feature Information for DHCPv6 Options Support, page 61-12

Note For complete syntax and usage information for the switch commands used in this chapter, see publications at this location:

Cisco IOS Command Reference Guides for the Catalyst 4500 Series Switch

If a command is not in the *Catalyst 4500 Series Switch Command Reference*, you can locate it in the Cisco IOS library, at this location:

Cisco IOS Master Command List, All Releases

Restrictions for DHCPv6 Options Support

The following restrictions apply to the Lightweight DHCPv6 Relay Agent (LDRA) feature:

- An interface or port cannot be configured as both client facing and server facing at the same time.
- Access nodes implementing LDRA do not support IPv6 control or routing.
- Unlike a DHCPv6 relay agent, an LDRA does not implement any IPv6 control functions (like Internet Control Message Protocol Version 6 [ICMPv6] functions), nor does it have any routing capability in the node.

Information About DHCPv6 Options Support

- DHCPv6 Relay Agent Overview, page 61-2
- DHCPv6 Relay Options: Remote-ID, page 61-2
- DHCPv6 Interface-ID, page 61-3
- Lightweight DHCPv6 Relay Agent, page 61-3
- Interoperability between DHCPv6 Relay Agents and LDRA, page 61-3
- LDRA for VLANs and Interfaces, page 61-4
- CAPWAP Access Controller DHCPv6 Option, page 61-4

DHCPv6 Relay Agent Overview

A DHCPv6 relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet.

A DHCPv6 relay agent, which may reside on the client's link, is used to relay messages between the client and the server. The DHCPv6 relay agent operation is transparent to the client. A DHCPv6 client locates a DHCPv6 server using a reserved, link-scoped multicast address. For direct communication between the DHCPv6 client and the DHCPv6 server, both of them must be attached to the same link. However, in some situations where ease of management, economy, or scalability is a concern, it is desirable to allow a DHCPv6 client to send a message to a DHCPv6 server that is not connected to the same link.

DHCPv6 Relay Options: Remote-ID

The DHCPv6 Remote ID Option feature adds the remote identification (remote-ID) option to relayed (RELAY-FORWARD) DHCPv6 packets.

The remote-ID option provides information to the DHCPv6 server, which includes port information, the system's DHCP Unique Identifier (DUID), and the virtual LAN (VLAN) ID. This information can be used to uniquely identify both the relay and the port on the relay through which the client packet arrived. The DHCPv6 server uses this information to select parameters specific to a particular user, host, or subscriber modem.

The addition of the remote-ID option to the RELAY-FORWARD packet occurs automatically and no user configuration is necessary.

The DHCPv6 server does not need to echo the remote-ID option in the RELAY-REPLY packet. The Internet Assigned Numbers Authority (IANA) has assigned the DHCPv6 option code 37 for the relay agent remote-ID option.

If the remote-ID option is included in the RELAY-REPLY packet, the option is removed from the packet before it is relayed to the client.

DHCPv6 Interface-ID

The interface-ID option is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet. If a relay agent receives a RELAY-REPLY message with an interface-ID option, the message is relayed to the client through the interface identified by the option.

The server must copy the interface-ID option from the RELAY-FORWARD message into the RELAY-REPLY message the server sends to the relay agent in response to the RELAY-FORWARD message. This option must not appear in any message except a RELAY-FORWARD or a RELAY-REPLY message.

Servers can use the interface-ID for parameter assignment policies. The interface-ID must be considered as an opaque value, with policies based on exact match only; that is, interface-ID must not be internally parsed by the server. The interface-ID value for an interface must be stable and remain unchanged, for example, after the relay agent is restarted; if the interface-ID changes, a server will not be able to use it reliably in parameter assignment policies.

Lightweight DHCPv6 Relay Agent

The Lightweight DHCPv6 Relay Agent feature allows relay agent information to be inserted by an access node that performs a link-layer bridging (non-routing) function. Lightweight DHCPv6 Relay Agent (LDRA) functionality can be implemented in existing access nodes, such as DSL access multiplexers (DSLAMs) and Ethernet switches, that do not support IPv6 control or routing functions. LDRA is used to insert relay-agent options in DHCPv6 message exchanges primarily to identify client-facing interfaces. LDRA functionality can be enabled on an interface and a VLAN.

An LDRA device or interface has the following features:

- Maintains interoperability with existing DHCPv6 relay agents and servers.
- Is functionally the equivalent of a Layer 2 relay agent, without routing capabilities.

Note LDRA is a device or interface on which LDRA functionality is configured.

Background

A variety of different link-layer network topologies exist for the aggregation of IPv6 nodes into one or more devices. In Layer 2 aggregation networks (IEEE 802.1D bridging or similar) that have many nodes on a single link, a DHCPv6 server or DHCP relay agent normally does not recognize how a DHCP client is attached to a network. LDRA allows relay-agent information, including the Interface-ID option, to be inserted by the access node so that the information may be used by the DHCPv6 server for client identification.

Interoperability between DHCPv6 Relay Agents and LDRA

DHCPv6 relay agents are used to forward DHCPv6 messages between a client and a server when the client and server are not on the same IPv6 link. A DHCPv6 relay agent also adds an interface ID option in the upstream DHCPv6 message (from client-to-server) to identify the interface on which the client is connected. This information is used by the DHCPv6 relay agent while forwarding the downstream DHCPv6 message to the DHCPv6 client. The DHCPv6 relay agent is implemented alongside the routing functionality on the common node.

To maintain interoperability with existing DHCP relays and servers, LDRA implements the same message types (RELAY-FORWARD and RELAY-REPLY) as a DHCPv6 relay agent. LDRA allows relay-agent information to be inserted by an access node that performs a link-layer bridging (that is, non-routing) function. The LDRA resides on the same IPv6 link as the client and a DHCPv6 relay agent or server.

LDRA for VLANs and Interfaces

You can configure LDRA on VLANs and interfaces. LDRA is not enabled by default. You must enable it on the VLAN or interface first.

In a typical deployment, a majority of the interfaces or ports on a device are client facing. In such a scenario, you can configure LDRA functionality on the VLAN. When you configure LDRA on a VLAN, the functionality is configured on all ports or interfaces within the VLAN. Instead of configuring LDRA functionality individually on interfaces and ports within a VLAN, you can configure LDRA on the entire VLAN. As a result, all ports or interfaces associated with the VLAN will be configured as client facing.

You can also configure LDRA functionality on a specific interface or port. An interface or port can be configured as client-facing trusted, client-facing untrusted, or server facing.

The LDRA configuration on a VLAN has to be configured as trusted or untrusted. An LDRA must implement a configuration setting for all client-facing interfaces, marking them as trusted or as untrusted.

By default, any interface that is configured as client facing will be configured as an untrusted interface. When a client-facing interface is deemed untrusted, LDRA will discard any message of type RELAY-FORWARD received from the client-facing interface.

CAPWAP Access Controller DHCPv6 Option

The Control And Provisioning of Wireless Access Points (CAPWAP) protocol allows lightweight access points to use DHCPv6 to discover a Wireless Controller to which it can connect. CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.

Wireless access points use the DHCPv6 option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary Wireless Controllers.

Both stateless and stateful DHCPv6 addressing modes are supported. In stateless mode, access points obtain IPv6 address using the Stateless Address AutoConfiguration (SLAAC), while additional network information (not obtained from router advertisements) is obtained from a DHCPv6 server. In stateful mode, access points obtain both IPv6 addressing and additional network information exclusively from the DHCPv6 server. In both modes, a DHCPv6 server is required to provide option 52 if Wireless Controller discovery using DHCPv6 is required.

How to Configure DHCPv6 Options Support

- Configuring the DHCPv6 Relay Agent, page 61-5
- Configuring LDRA Functionality on a VLAN, page 61-5
- Configuring LDRA Functionality on an Interface, page 61-6
- Verifying the LRDA Configuration, page 61-7
- Verifying the LRDA Configuration, page 61-7

Configuring the DHCPv6 Relay Agent

	Command or Action	Purpose
Step 1	`Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# interface type number`	Configures an interface and enters interface configuration mode.
Step 4	`Device(config-if)# ipv6 dhcp relay destination ipv6-address [interface-type interface-number]`	Specifies a destination address to which client packets are forwarded and enables the DHCPv6 relay service on the interface.
Step 5	`Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring LDRA Functionality on a VLAN

	Command or Action	Purpose
Step 1	`Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# ipv6 dhcp-ldra {enable | disable | remote-id}`	Enables LDRA functionality globally. **Note** You must enable the LDRA functionality in global configuration mode before configuring it on an interface.
Step 4	`Device(config)# vlan configuration vlan-number`	Specifies a VLAN number and enters VLAN configuration mode.

	Command or Action	Purpose
Step 5	`Device(config-vlan-config)# ipv6 dhcp ldra attach-policy {client-facing-trusted | client-facing-untrusted}`	Enables the LDRA functionality on a specified VLAN. • The **client-facing-trusted** keyword configures all ports or interfaces associated with the VLAN as client facing, trusted ports. • The **client-facing-untrusted** keyword configures all ports or interfaces associated with the VLAN as client facing, untrusted ports.
Step 6	`Device(config-vlan-config)# exit`	Exits VLAN configuration mode and returns to global configuration mode.
Step 7	`Device(config)# interface type number`	Configures an interface and enters interface configuration mode.
Step 8	`Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 9	`Device(config-if)# switchport access vlan vlan-number`	Specifies that an interface operates in the specified VLAN instead of the default VLAN in interface configuration mode.
Step 10	`Device(config-if)# ipv6 dhcp-ldra attach-policy {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}`	Enables LDRA functionality on a specified interface or port. • The **server-facing** keyword specifies an interface or port as server facing.
Step 11	`Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring LDRA Functionality on an Interface

	Command or Action	Purpose
Step 1	`Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# ipv6 dhcp-ldra {enable | disable | remote-id}`	Enables LDRA functionality globally. **Note** You must enable the LDRA functionality in global configuration mode before configuring it on an interface.
Step 4	`Device(config)# interface type number`	Configures an interface and enters interface configuration mode.
Step 5	`Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 6	`Device(config-if# ipv6 dhcp ldra interface-id interface-id`	Configures LDRA interface ID on a port or an interface.
Step 7	`Device(config-if)# end`	Exits VLAN configuration mode and returns to privileged EXEC mode.

Verifying the LRDA Configuration

Step 1 **show ipv6 dhcp interface**

Displays DHCPv6 interface information.

Example:

```
Device# show ipv6 dhcp interface

GigabitEthernet0/1 is in relay mode
 Relay destinations:
  3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
Serial3/0 is in relay mode
 Relay destinations:
  3FFB:C00:C18:6:A8BB:CCFF:FE03:2600
  FE80::A8BB:CCFF:FE03:2801 on Serial3/0
  FF05::1:3
```

Step 2 **show ipv6 dhcp-ldra**

Displays LDRA configuration details. The fields in the example given below are self-explanatory.

Example:

```
Device# show ipv6 dhcp-ldra
DHCPv6 LDRA is Enabled.
DHCPv6 LDRA policy: client-facing-disable
       Target: none
DHCPv6 LDRA policy: client-facing-trusted
       Target: vlan 5
DHCPv6 LDRA policy: client-facing-untrusted
       Target: none
DHCPv6 LDRA policy: server-facing
       Target: Gi1/0/7
```

Step 3 **show ipv6 dhcp-ldra statistics**

Displays LDRA configuration statistics before and after initiating a DHCP session. The fields in the examples below are self-explanatory.

Example:

```
Device# show ipv6 dhcp-ldra statistics

           DHCPv6 LDRA client facing statistics.
Messages received 2
Messages sent 2
Messages discarded 0
Messages Received
SOLICIT 1
REQUEST 1
Messages Sent
RELAY-FORWARD 2
           DHCPv6 LDRA server facing statistics.
Messages received 2
Messages sent 2
Messages discarded 0
Messages Received
RELAY-REPLY 2
Messages Sent
```

```
ADVERTISE 1
REPLY 1
```

Step 4 **debug ipv6 dhcp-ldra all**

Enables all LDRA debugging flows. The fields in the example below are self-explanatory.

Example:

```
Device# debug ipv6 dhcp-ldra all

05:44:10: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:10: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1 to
FF02::1:2.
05:44:10:
05:44:10:
05:44:10:
05:44:10:
05:44:10: 0003000010015F906981B
05:44:10: option ORO(6), len 4
05:44:10: DNS-SERVERS,DOMAIN-LIST
05:44:10: option IA-NA(3), len 12
05:44:10: IAID 0x00040001, T1 0, T2 0
05:44:10: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:10: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
!
!
!
```

Configuring CAPWAP Access Points

	Command or Action	Purpose
Step 1	`Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Device# configure terminal`	Enters global configuration mode.
Step 3	`Device(config)# ipv6 dhcp pool` *poolname*	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	`Device(config-dhcpv6)# capwap-ac address` *ipv6-address*	Configures CAPWAP access controller address.
Step 5	`Device(config-dhcpv6)# end`	Exits DHCPv6 pool mode and returns to privileged EXEC mode.

Configuration Examples for DHCPv6 Options Support

- Example: Configuring the DHCPv6 Relay Agent, page 61-9
- Example: Configuring LDRA Functionality on a VLAN, page 61-9
- Example: Configuring LDRA Functionality on an Interface, page 61-9
- Example: Configuring CAPWAP Access Points, page 61-10

Example: Configuring the DHCPv6 Relay Agent

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1
Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 gigabitethernet
0/1
Device(config-if)# end
```

Example: Configuring LDRA Functionality on a VLAN

The following example shows how to configure Lightweight DHCPv6 Relay Agent (LDRA) on a VLAN numbered 5.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# vlan configuration 5
Device(config-vlan-config)# ipv6 dhcp ldra attach-policy client-facing-trusted
Device(config-vlan-config)# exit
Device(config)# interface gigabitethernet 0/0
Device(config-if)# switchport
Device(config-if)# switchport access vlan 5
Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0
Device(config-if)# switchport
Device(config-if)# switchport access vlan 5
Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing
Device(config-if)# end
```

Example: Configuring LDRA Functionality on an Interface

In the following example, LDRA is configured on the interfaces GigabitEthernet 0/0:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# interface gigabitethernet 0/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra interface-id 2
Device(config-if)# end
```

Example: Configuring CAPWAP Access Points

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# capwap-ac address 2001:DB8::1
Device(config-dhcpv6)# end
Device#
```

Additional References for DHCPv6 Options Support

Related Documents

Related Topic	Document Titl1
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Catalyst 4500 commands	*Cisco IOS Command Reference Guides for the Catalyst 4500 Series Switch*

Standards and RFCs

Standard/RFC	Title
RFC 3315	*Dynamic Host Configuration Protocol for IPv6*
RFC 4649	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*
RFC 5417	*Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option*
RFC 6221	*Lightweight DHCPv6 Relay Agent*

MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCPv6 Options Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for DHCPv6 Options Support

Feature Name	Releases	Feature Information
CAPWAP Access Controller DHCP Option 52	Cisco IOS Release 15.2(5)E2	The Control And Provisioning of Wireless Access Points (CAPWAP) protocol allows Lightweight Access Points to use DHCPv6 to discover a Wireless Controller to which it can connect.
DHCPv6 Interface-ID	Cisco IOS Release 15.2(5)E2	The interface-ID option is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet.
DHCPv6 Relay Agent	Cisco IOS Release 15.2(5)E2	A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and server.