DHCPv6Relay—LightweightDHCPv6RelayAgent

The DHCPv6 Relay—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 DHCP version 6 (DHCPv6) message exchanges primarily to identify client-facing interfaces. LDRA functionality can be enabled on an interface and on 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Prerequisites for DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

- You must understand DHCP and the functions of DHCP version 6 (DHCPv6) relay agents.

Restrictions for DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

- An interface or port cannot be configured as both client facing and server facing at the same time.
- Access nodes implementing Lightweight DHCPv6 Relay Agent (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 Relay—Lightweight DHCPv6 Relay Agent

Background

A variety of different link-layer network topologies exist for the aggregation of IPv6 nodes into one or more routers. In Layer 2 aggregation networks (IEEE 802.1D bridging or similar) that have many nodes on a single link, a DHCP version 6 (DHCPv6) server or DHCP relay agent normally does not recognize how a DHCP client is attached to a network. Lightweight DHCPv6 Relay Agent (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

DHCP version 6 (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 identifier 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, Lightweight DHCPv6 Relay Agent (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 (i.e., 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 Lightweight DHCPv6 Relay Agent (LDRA) functionality on the VLAN. When you configure LDRA functionality on a VLAN, the functionality is configured on all the ports or interfaces within the VLAN. Instead of configuring LDRA functionality individually on the interfaces and ports within a VLAN, you can configure LDRA on the entire VLAN. As a result, all the ports or interfaces associated with the VLAN will be configured as client facing.

Note The LDRA configuration on a VLAN has to be configured as trusted or untrusted.

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.

Note 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.

How to Configure a Lightweight DHCPv6 Relay Agent

Configuring LDRA Functionality on a VLAN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-ldra** {**enable** | **disable**}
4. **vlan configuration** *vlan-number*
5. **ipv6 dhcp ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted**}
6. **exit**
7. **interface** *type number*
8. **switchport**
9. **switchport access vlan** *vlan-number*
10. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
11. **exit**
12. **interface** *type number*
13. **switchport**
14. **switchport access vlan** *vlan-number*
15. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**ipv6 dhcp-ldra** {**enable** | **disable**}
	Example:
	`Device(config)# ipv6 dhcp-ldra enable`
		Enables LDRA functionality globally.
		Note You need to enable LDRA functionality in global configuration mode before configuring it on a VLAN.

Step 4	**vlan configuration** *vlan-number* **Example:** `Device(config)# vlan configuration 5`	Specifies a VLAN number and enters into VLAN configuration mode.

Step 5	**ipv6 dhcp ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted**}
	Example:
	`Device (config-vlan-config)# ipv6 dhcp ldra attach-policy client-facing-trusted`
		Enables LDRA functionality on a specified VLAN.
		Note The **client-facing-trusted** keyword configures all the ports or interfaces associated with the VLAN as client facing, trusted ports. The **client-facing-untrusted** keyword configures all the ports or interfaces associated with the VLAN as client facing, untrusted ports.

Step 6	**exit** **Example:** `Device (config-vlan-config)# exit`	Exits VLAN configuration mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 8	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 9	**switchport access vlan** *vlan-number* **Example:** `Device(config-if)# switchport access vlan 5`	Specifies that an interface operates in VLAN 5 instead of the default VLAN in the interface configuration mode.

Step 10	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted`
		Enables LDRA functionality on a specified interface or port.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 11	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 12	**interface** *type number* **Example:** `Device(config)# interface ethernet 1/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 13	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 14	**switchport access vlan** *vlan-number* **Example:** `Device(config-if)# switchport access vlan 5`	Specifies that an interface operates in VLAN 5 instead of the default VLAN in the interface configuration mode.

Step 15	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing`
		Enables the LDRA functionality on the specified interface.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 16	**end**
	Example:
	`Device(config-if)# end`
		Exits VLAN configuration mode and returns to user EXEC mode.

Configuring LDRA Functionality on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-ldra** {**enable** | **disable**}
4. **interface** *type number*
5. **switchport**
6. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
7. **exit**
8. **interface** *type number*
9. **switchport**
10. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**ipv6 dhcp-ldra** {**enable** | **disable**}
	Example:
	`Device(config)# ipv6 dhcp-ldra enable`
		Enables LDRA functionality globally.
		Note You need to enable LDRA functionality in global configuration mode before configuring it on an interface.

Step 4	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 5	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.

	Command or Action	Purpose

Step 6	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted`
		Enables LDRA functionality on a specified interface or port.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface ethernet 1/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 9	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.

Step 10	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing`
		Enables the LDRA functionality on the specified interface.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 11	**end**
	Example:
	`Device (config-if)# end`
		Exits interface configuration mode and returns to user EXEC mode.

Verifying and Troubleshooting LDRA

SUMMARY STEPS

1. **show ipv6 dhcp-ldra**
2. **show ipv6 dhcp-ldra statistics**
3. **debug ipv6 dhcp-ldra all**

DETAILED STEPS

Step 1 **show ipv6 dhcp-ldra**

This command 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 2 **show ipv6 dhcp-ldra statistics**

This command 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 0
 Messages sent 0
 Messages discarded 0

           DHCPv6 LDRA server facing statistics.
 Messages received 0
 Messages sent 0
 Messages discarded 0

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 facingstatistics.
 Messages received 2
 Messages sent 2
 Messages discarded 0
 Messages Received
 RELAY-REPLY 2
 Messages Sent
 ADVERTISE 1
 REPLY 1
```

Step 3 **debug ipv6 dhcp-ldra all**

This command 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:   type SOLICIT(1), xid 8035955
05:44:10:   option ELAPSED-TIME(8), len 2
05:44:10:     elapsed-time 0
05:44:10:   option CLIENTID(1), len 10
05:44:10:     000300010015F906981B
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.
05:44:10:   type RELAY-FORWARD(12), hop 0
05:44:10:   link ::
05:44:10:   peer 2001:DB8:1::1
05:44:10:   option RELAY-MSG(9), len 48
05:44:10:     type SOLICIT(1), xid 8035955
05:44:10:     option ELAPSED-TIME(8), len 2
05:44:10:       elapsed-time 0
05:44:10:     option CLIENTID(1), len 10
05:44:10:       000300010015F906981B
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:   option INTERFACE-ID(18), len 7
05:44:10:     0x4769312F302F33
05:44:10:   option REMOTEID(37), len 22
05:44:10:     0x000000090200130000050000A00030001588D09F89A00
05:44:11: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:11: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1
 to FF02::1:2.
05:44:11:   type SOLICIT(1), xid 8035955
05:44:11:   option ELAPSED-TIME(8), len 2
05:44:11:     elapsed-time 0
05:44:11:   option CLIENTID(1), len 10
05:44:11:     000300010015F906981B
05:44:11:   option ORO(6), len 4
05:44:11:     DNS-SERVERS,DOMAIN-LIST
05:44:11:   option IA-NA(3), len 12
05:44:11:     IAID 0x00040001, T1 0, T2 0
05:44:11: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:11: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
05:44:11:   type RELAY-FORWARD(12), hop 0
```

```
05:44:11:   link ::
05:44:11:   peer 2001:DB8:1::1
05:44:11:   option RELAY-MSG(9), len 48
05:44:11:     type SOLICIT(1), xid 8035955
05:44:11:     option ELAPSED-TIME(8), len 2
05:44:11:       elapsed-time 0
05:44:11:     option CLIENTID(1), len 10
05:44:11:       000300010015F906981B
05:44:11:     option ORO(6), len 4
05:44:11:       DNS-SERVERS,DOMAIN-LIST
05:44:11:     option IA-NA(3), len 12
05:44:11:       IAID 0x00040001, T1 0, T2 0
05:44:11:   option INTERFACE-ID(18), len 7
05:44:11:     0x4769312F302F33
05:44:11:   option REMOTEID(37), len 22
05:44:11:     0x000000090200130000050000A00030001588D09F89A00
05:44:13: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:13: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1
 to FF02::1:2.
05:44:13:   type SOLICIT(1), xid 8035955
05:44:13:   option ELAPSED-TIME(8), len 2
05:44:13:     elapsed-time 0
05:44:13:   option CLIENTID(1), len 10
05:44:13:     000300010015F906981B
05:44:13:   option ORO(6), len 4
05:44:13:     DNS-SERVERS,DOMAIN-LIST
05:44:13:   option IA-NA(3), len 12
05:44:13:     IAID 0x00040001, T1 0, T2 0
05:44:13: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:13: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
05:44:13:   type RELAY-FORWARD(12), hop 0
05:44:13:   link ::
05:44:13:   peer 2001:DB8:1::1
05:44:13:   option RELAY-MSG(9), len 48
05:44:13:     type SOLICIT(1), xid 8035955
05:44:13:     option ELAPSED-TIME(8), len 2
05:44:13:       elapsed-time 0
05:44:13:     option CLIENTID(1), len 10
05:44:13:       000300010015F906981B
05:44:13:     option ORO(6), len 4
05:44:13:       DNS-SERVERS,DOMAIN-LIST
05:44:13:     option IA-NA(3), len 12
05:44:13:       IAID 0x00040001, T1 0, T2 0
05:44:13:   option INTERFACE-ID(18), len 7
05:44:13:     0x4769312F302F33
05:44:13:   option REMOTEID(37), len 22
05:44:13:     0x000000090200130000050000A00030001588D09F89A00
05:44:17: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:17: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1
 to FF02::1:2.
05:44:17:   type SOLICIT(1), xid 8035955
05:44:17:   option ELAPSED-TIME(8), len 2
05:44:17:     elapsed-time 0
05:44:17:   option CLIENTID(1), len 10
05:44:17:     000300010015F906981B
05:44:17:   option ORO(6), len 4
05:44:17:     DNS-SERVERS,DOMAIN-LIST
05:44:17:   option IA-NA(3), len 12
05:44:17:     IAID 0x00040001, T1 0, T2 0
```

```
05:44:17: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:17: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
05:44:17:   type RELAY-FORWARD(12), hop 0
05:44:17:   link ::
05:44:17:   peer 2001:DB8:1::1
05:44:17:   option RELAY-MSG(9), len 48
05:44:17:     type SOLICIT(1), xid 8035955
05:44:17:     option ELAPSED-TIME(8), len 2
05:44:17:       elapsed-time 0
05:44:17:     option CLIENTID(1), len 10
05:44:17:       000300010015F906981B
05:44:17:     option ORO(6), len 4
05:44:17:       DNS-SERVERS,DOMAIN-LIST
05:44:17:     option IA-NA(3), len 12
05:44:17:       IAID 0x00040001, T1 0, T2 0
05:44:17:   option INTERFACE-ID(18), len 7
05:44:17:     0x4769312F302F33
05:44:17:   option REMOTEID(37), len 22
05:44:17:     0x00000009020013000005000A00030001588D09F89A00
```

Configuration Examples for a Lightweight DHCPv6 Relay Agent

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 ethernet 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 ethernet 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 ethernet 0/0 and ethernet 1/0:

```
Device> enable
Device # configure terminal
```

```
Device(config)# ipv6 dhcp-ldra enable
Device(config)# interface ethernet 0/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted
Device(config-if)# exit
Device(config)# interface ethernet 1/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing
Device(config-if)# end
```

Additional References for DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

Related Documents

Related Topic	Document Title
Configuring the DHCPv6 Relay Agent	*IP Addressing: DHCP Configuration Guide*
Cisco IOS commands	Cisco IOS Master Command List, All Releases
DHCP commands	Cisco IOS IP Addressing Services Command Reference
DHCP conceptual information	*DHCP Overview module in the IP Addressing: DHCP Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 6221	*Lightweight DHCPv6 Relay Agent*

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 Relay—Lightweight DHCPv6 Relay Agent

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 Lightweight DHCPv6 Relay Agent

Feature Name	Releases	Feature Information
DHCPv6 Relay—Lightweight DHCPv6 Relay Agent	15.1(2)E	The DHCPv6 Relay—Lightweight DHCPv6 Relay Agent feature allows relay agent information to be inserted by an access node that performs a link-layer bridging function. The following commands were introduced or modified: **clear ipv6 dhcp-ldra statistics**, **debug ipv6 dhcp-ldra**, **ipv6 dhcp ldra attach-policy**, **ipv6 dhcp-ldra**, **ipv6 dhcp-ldra attach-policy**, **show ipv6 dhcp-ldra**.

Glossary

Access Node —A device that combines many interfaces onto one link. An access node is not IP-aware in a data path.

Client facing —An interface on an access node that carries traffic towards a DHCPv6 client.

LDRA—Lightweight DHCPv6 Relay Agent. An interface or device on which LDRA functionality is configured (or that supports LDRA functionality.)

LDRA function—A function on an access node that intercepts DHCP messages between clients and servers.

Link—A communication facility or medium over which nodes can communicate at the link layer.

Link-local address—An IP address having only local scope that can be used to reach neighboring nodes attached to the same link. Every interface has a link-local address, which is defined by the address prefix fe80::/10.

Network-facing—An interface on an access node that carries traffic towards a DHCPv6 server.

Relay Agent—A node that acts as an intermediary to deliver DHCP messages between clients and servers.