Internet Engineering Task Force (IETF)
Request for Comments: 6221
Updates: 3315
Category: Standards Track
ISSN: 2070-1721

D. Miles, Ed.
S. Ooghe
Alcatel-Lucent
W. Dec
Cisco Systems
S. Krishnan
A. Kavanagh
Ericsson

May 2011

Lightweight DHCPv6 Relay Agent

Abstract

This document proposes a Lightweight DHCPv6 Relay Agent (LDRA) that is used to insert relay agent options in DHCPv6 message exchanges identifying client-facing interfaces. The LDRA can be implemented in existing access nodes (such as Digital Subscriber Link Access Multiplexers (DSLAMs) and Ethernet switches) that do not support IPv6 control or routing functions.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6221.

Table of Contents

1. Introduction

DHCPv6 Relay Agents [RFC3315] are deployed to forward DHCPv6 messages between clients and servers when they are not on the same IPv6 link and are often implemented alongside a routing function in a common node. A Lightweight 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. An LDRA resides on the same IPv6 link as the client and a DHCPv6 Relay Agent or server, and is functionally the equivalent of the Layer 2 Relay Agent proposed for DHCPv4 operation in [L2RA].

Unlike a DHCPv6 Relay Agent specified in [RFC3315], an LDRA does not implement any IPv6 control functions (e.g., ICMPv6) or have any routing capability in the node.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. 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 DHCPv6 server or DHCP Relay Agent would normally be unaware of how a DHCP client is attached to the network. The LDRA allows Relay Agent Information, including the Interface-ID option [RFC3315], to be inserted by the access node so that it may be used by the DHCPv6 server for client identification. A typical application in a broadband service provider could be equivalent to a Layer 2 DHCP Relay Agent as described in the Broadband Forum TR-101 report [TR-101] and in [L2RA].

3. Terminology

Access Node	A device that combines many interfaces onto one link. An access node is not IP-aware in the data path.
Address	An IP layer identifier for an interface or set of interfaces.
Client-facing	An interface on the access node that carries traffic towards the DHCPv6 client.

Host	A non-routing IPv6 node that is participating in a DHCPv6 message exchange.
IP	Internet Protocol Version 6 (IPv6).
LDRA	Lightweight DHCPv6 Relay Agent.
Lightweight Relay Agent	A function on the access node that intercepts DHCP messages between clients and servers. The function exists as a bump in the wire on the IP link.
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, indicated by having the address prefix fe80::/10, that can be used to reach neighbouring nodes attached to the same link. Every interface has a link-local address.
Network-facing	An interface on the access node that carries traffic towards the DHCPv6 server(s).
Node	A device that implements IPv6.
Router	A node that forwards packets not directly addressed to itself.
Relay Agent	A node that acts as an intermediary to deliver DHCP messages between clients and servers and being on the same link as the client.
Unspecified address	An IPv6 address that is comprised entirely of zeros.

4. Server Considerations

This document updates the behaviour specified in Section 11 of DHCP for IPv6 [RFC3315]. RFC 3315 states, in part:

> If the server receives the message from a forwarding relay agent, then the client is on the same link as the one to which the interface, identified by the link-address field in the message from the relay agent, is attached.

DHCP server implementations conforming to this specification MUST, for the purposes of address selection, ignore any link-address field whose value is zero. In the above text from RFC 3315, "link-address" refers to both the link-address field of the Relay-Forward message, and the link-address fields in any Relay-Forward messages that may be nested within the Relay-Forward message.

5. Message Format

The Lightweight DHCPv6 Relay Agent (LDRA) exchanges DHCP messages between clients and servers using the message formats established in [RFC3315].

To maintain interoperability with existing DHCP relays and servers, the message format is unchanged from [RFC3315]. The LDRA implements the same message types as a normal DHCPv6 Relay Agent. They are:

- Relay-Forward Messages
- Relay-Reply Messages

5.1. Relay-Forward Message

The Relay-Forward message is created by any DHCPv6 Relay Agent, including an LDRA, to forward messages between clients and servers or other relay agents. These messages are built as specified in [RFC3315].

The Relay-Forward message contains relay agent parameters that identify the client-facing interface on which any reply messages should be forwarded. These parameters are link-address, peer-address, and Interface-ID. The link-address parameter MUST be set to the unspecified address. The peer-address parameter MUST be set as specified in Section 6.1. The Interface-ID Relay Agent option MUST be included in the Relay-Forward message. The LDRA MAY insert additional relay agent options.

5.2. Relay-Reply Message

The Relay-Reply message is constructed by a DHCPv6 server to send parameters to a DHCP client when a relay agent is present between the server and the client. The Relay-Reply message may be sent after an initial Relay-Forward message as the parameters link-address, peer-address, and Interface-ID, as well as the relay agent's IP address, are learnt from the Relay-Forward message.

The server MUST include the Interface-ID option in the Relay-Reply Message to indicate to the LDRA the interface on which the decapsulated message should be forwarded.

5.3. Mandatory DHCP Options

Parameters are exchanged between the DHCP client, Relay Agent, and server through the use of DHCP options. There is a set of mandatory DHCP options that MUST be included by the LDRA in all Relay-Forward messages. These are the:

- Relay-Message Option
- Interface-ID Option

5.3.1. Relay-Message Option

A DHCPv6 Relay Agent relays messages between clients and servers or other relay agents through Relay-Forward and Relay-Reply message types. The original client DHCP message (i.e., the packet payload, excluding UDP and IP headers) is encapsulated in a Relay Message option [RFC3315].

If a Relay-Message would exceed the MTU of the outgoing interface, it MUST be discarded, and an error condition SHOULD be logged.

5.3.2. Interface-ID Option

The LDRA MUST include the Interface-ID option [RFC3315] in all Relay-Forward messages. When an LDRA receives a Relay-Reply message with an Interface-ID option present and link-address unspecified, the LDRA MUST relay the decapsulated message to the client on the interface identified in the Interface-ID option.

Servers MAY use the Interface-ID for parameter assignment policies. The format of the Interface-ID is outside the scope of this contribution. The Interface-ID SHOULD be considered an opaque value; i.e., the server SHOULD NOT try to parse the contents of the Interface-ID option. The LDRA SHOULD use the same Interface-ID value

for a given interface, and this value SHOULD be retained across restarts. This is because if the Interface-ID changes, a server will not be able to use it reliably in parameter assignment policies.

6. Agent Behaviour

The LDRA MUST have each of its interfaces configured as either client-facing or network-facing. The LDRA uses the notion of client-facing and network-facing interfaces to process DHCPv6 messages.

6.1. Relaying a Client Message

The LDRA MUST intercept and process all IP traffic received on any client-facing interface that has:

- destination IP address set to All_DHCP_Relay_Agents_and_Servers (ff02::1:2);
- protocol type UDP; and
- destination port 547.

The LDRA MUST also prevent the original message from being forwarded on the network-facing interface.

The lightweight relay agent adds any other options it is configured or required to include in the Relay-Forward message. The LDRA MUST set the link-address field of the Relay-Forward message to the Unspecified Address (::) and MUST include the Interface-ID option in all DHCP Relay-Forward messages.

If the message received on the client-facing interface is a Relay-Forward message, the LDRA MUST set the hop-count field in the newly created Relay-Forward message to the value of the hop-count field in the received message, incremented by 1 as specified in [RFC3315].

The LDRA MUST copy the IP destination and link-layer destination addresses from the client-originated message into the IP destination address and link-layer destination address of the Relay-Forward message.

The LDRA MUST copy the IP source address from the client-originated message into the peer-address field of the Relay-Forward message. The LDRA MUST copy the link-layer source address from the client-originated message into the link-layer source address of the Relay-Forward message.

6.1.1. Client Message Validation

On receipt of a DHCP message on a client-facing interface, the LDRA MUST discard a message if it is of one of the following message types:

- ADVERTISE (2)
- REPLY (7)
- RECONFIGURE (10)
- RELAY-REPL (13)

Options contained in the DHCPv6 message MUST NOT be validated by the LDRA, making it the responsibility of the DHCP server to check message option validity and allow new options to be introduced without changes on the LDRA.

6.1.2. Trusted and Untrusted Interfaces

In [RFC3046], DHCPv4 Relay Agents had their client-facing interfaces set to "trusted" and "untrusted". An LDRA MUST implement a configuration setting for all client-facing interfaces, marking them either as trusted or as untrusted. This setting SHOULD be configurable per interface. When a client-facing interface is deemed untrusted, the LDRA MUST discard any message of type RELAY-FORW (12) received from the client-facing interface.

6.2. Relaying a Relay-Reply Message from the Network

The LDRA MUST intercept and process all IP traffic received on the network-facing interface that has:

- a link-local scoped source address;
- a link-local scoped destination address;
- protocol type UDP; and
- destination port 547

An LDRA MUST inspect the DHCP message type and only forward Relay-Reply messages. Other DHCP message types MUST be silently discarded.

The Relay-Reply message is considered valid by the LDRA if it passes the validity checks to be performed by a relay agent per [RFC3315] and

- the Interface-ID option is present, and the value corresponds to a valid interface in the access node;

- the Relay-Reply peer-address and the destination IP address are identical, and it is a link-local scoped address when no IP address is configured on the LDRA; and

- the link-address is the Unspecified Address when no IP address is configured on the LDRA.

If the Relay-Reply message is valid, the LDRA copies the peer-address into the destination IP address field. The LDRA SHOULD forward the packet to the correct client-facing interface using the destination link-layer (Media Access Control (MAC)) address or the Interface-ID in the Relay-Reply. The LDRA SHOULD NOT retransmit the packet on any other interface. The contents of the Relay Message option are put into an IP/UDP packet and then forwarded to the client.

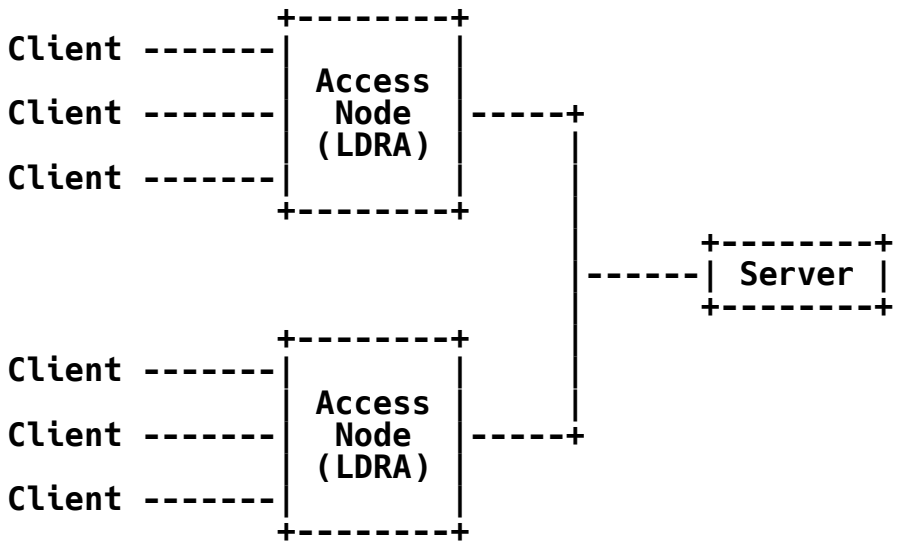
The LDRA MUST copy the link-layer and IP source address from the Relay-Reply message into the IP/UDP packet that is forwarded to the client.

7. Network Topology

The LDRA intercepts any DHCPv6 message received on client-facing interfaces with the traffic pattern specified in Section 6.1. The LDRA MUST NOT forward the original client message to a network-facing interface; it MUST process the message and add the appropriate Relay-Forward options as described in previous sections.

7.1. Client and Server on Same Link

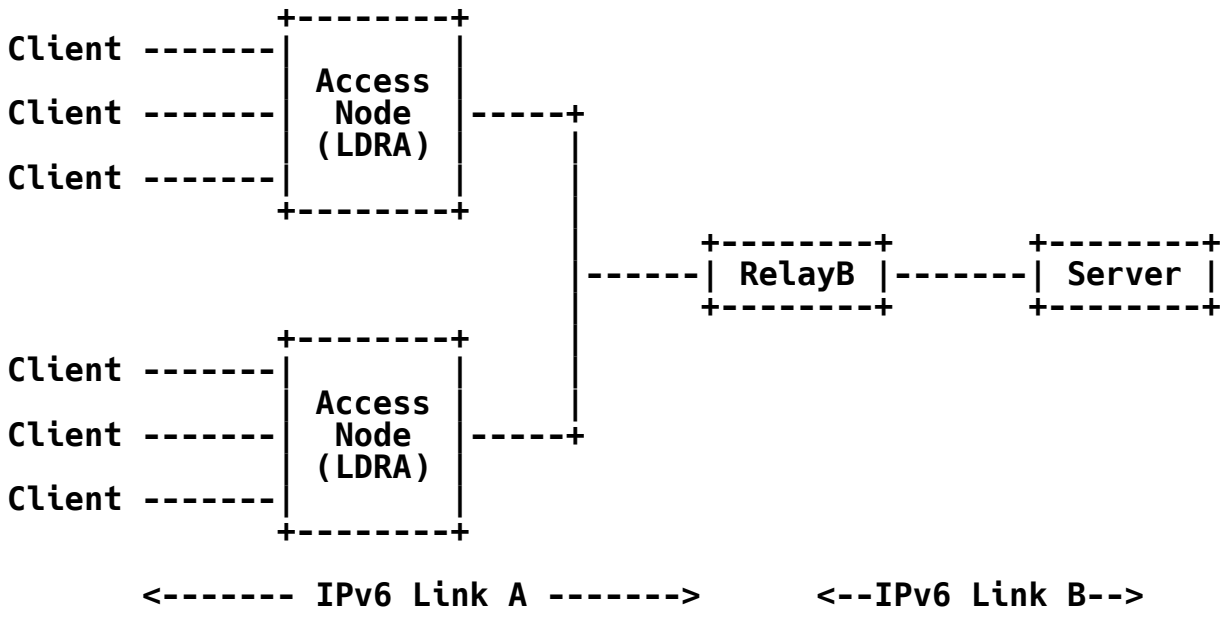
The access node acts as a bridge; it has no information about any IP prefixes that are valid on the link. Thus, a server should consider address and parameter assignment as if the client DHCP message were not relayed.



For example, if a client sent a DHCP Solicit message that was relayed by the LDRA to the server, the server would receive the following Relay-Forward message from the LDRA:

7.2. Client and Server behind Relay Agent

The client and server are on different IPv6 links, separated by one or more relay agents that will typically act as a router. The LDRA will send Relay-Forward messages upstream towards the second relay agent, which in turn will process the messages.

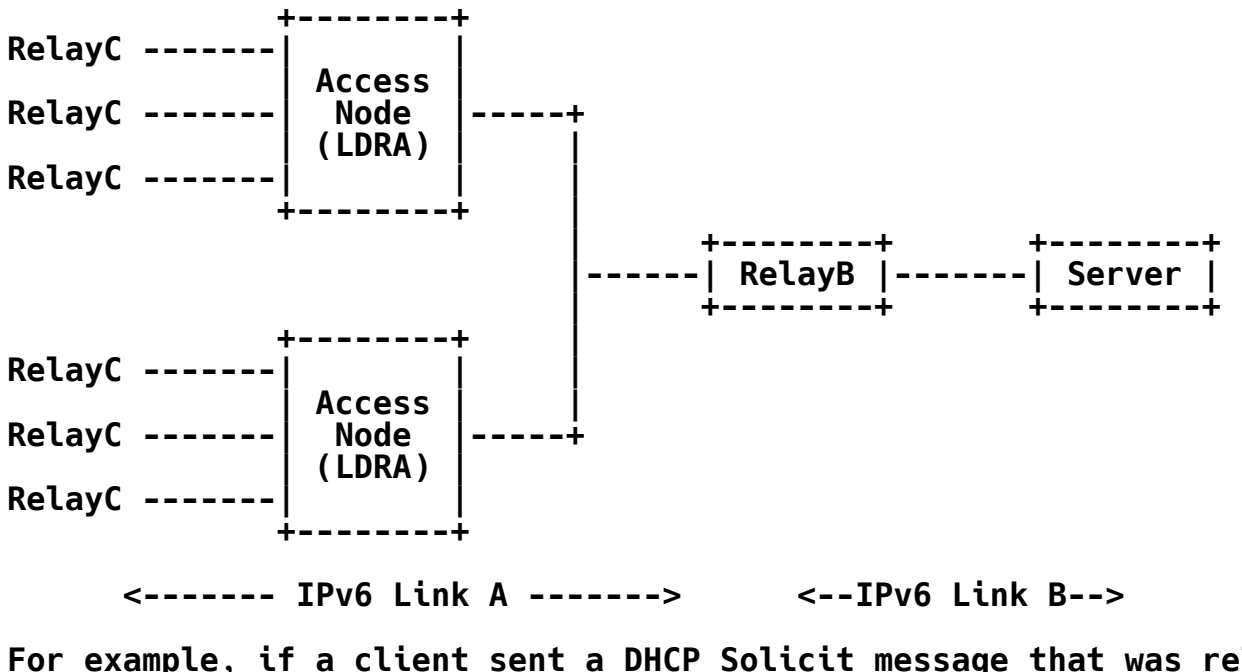


For example, if a client sent a DHCP Solicit message that was relayed by the LDRA to another relay agent and then to the server, the server would receive the following Relay-Forward message from the LDRA:

```
   src-ip:              relayB
   dst-ip:              server
     msg-type:          RELAY-FORW
     hop-count:         1
     link-address:      relayB address from link A
     peer-address:      client link-local address
     Relay-Message Option, which contains:
       msg-type:        RELAY-FORW
       hop-count:       0
       link-address:    Unspecified_Address
       peer-address:    client link-local address
       Interface-ID Option:
         interface-id:  LDRA-inserted interface-id
       Relay-Message Option, which contains:
         msg-type:      SOLICIT
         Solicit Message Options: <from client>
```

7.3. Relay Agent in Front of LDRA

The client and server are on different IPv6 links, separated by one or more relay agents that will typically act as a router, and there is an [RFC3315] Relay Agent on the client-facing interface of the LDRA. The LDRA will send Relay-Forward messages upstream towards the second relay agent, which in turn will process the messages.



For example, if a client sent a DHCP Solicit message that was relayed by RelayC and the LDRA to another relay agent, RelayB, and then to the server, the server would receive the following Relay-Forward message:

```
   src-ip:               relayB
   dst-ip:               server
     msg-type:           RELAY-FORW
     hop-count:          2
     link-address:       relayB address from link A
     peer-address:       relayC
     Relay-Message Option, which contains:
       msg-type:         RELAY-FORW
       hop-count:        1
       link-address:     Unspecified_Address
       peer-address:     relayC
       Interface-ID Option:
         interface-id:   LDRA-inserted interface-id
       Relay-Message Option, which contains:
         msg-type:       RELAY-FORW
         hop-count:      0
         link-address:   global or Unspecified_Address
         peer-address:   end client address
         Interface-ID Option: (if required)
           interface-id: relayC-inserted Interface-ID
         Relay-Message Option, which contains:
           msg-type:      SOLICIT
           Solicit Message Options: <from end client>
```

8. Contributors

The authors would like to thank the following for their support: Lieven Levrau, Alastair Johnson, Robert Haylock, Mickey Vucic, Ludwig Pauwels, Fernando Cuervo, John Kaippallimalil, Fredrik Garneij, Alfred Hoenes, Ted Lemon, Tatuya Jinmei, David Hankins, and Ralph Droms.

Comments are solicited and should be addressed to the DHC WG mailing list (dhcwg@ietf.org) and/or the authors.

9. Security Considerations

The security issues pertaining to DHCPv6 Relay Agents as specified in Section 23 of [RFC3315] are also applicable to LDRAs. The LDRA SHOULD implement some form of rate-limiting on client-originated traffic in order to prevent excessive process utilisation. The traffic to be rate-limited can be easily identified since the LDRA listens only to client-originated IPv6 traffic sent to the All_DHCPv6_Servers_and_Relay_Agents address on UDP port 547 and does not process any other client-originated traffic. As DHCP is session-oriented, messages in excess of the rate-limit may be silently discarded.

The hop-count-based determination of the trustworthiness of the LDRA can be easily defeated by a rogue relay agent on the network-facing interface of the LDRA.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

10.2. Informative References

[L2RA] Joshi, B. and P. Kurapati, "Layer 2 Relay Agent Information", Work in Progress, April 2011.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[TR-101] The Broadband Forum, "Migration to Ethernet-Based DSL Aggregation", Technical Report TR-101, April 2006.

Authors' Addresses

David Miles (editor)
Alcatel-Lucent
L3 / 215 Spring St.
Melbourne, Victoria 3000
Australia

Phone: +61 3 9664 3308
EMail: david.miles@alcatel-lucent.com

Sven Ooghe
Alcatel-Lucent
Copernicuslaan 50
2018 Antwerp,
Belgium

EMail: sven.ooghe@alcatel-lucent.com

Wojciech Dec
Cisco Systems
Haarlerberdweg 13-19
1101 CH Amsterdam,
The Netherlands

EMail: wdec@cisco.com

Suresh Krishnan
Ericsson
8400 Blvd. Decarie
Town of Mount Royal, Quebec
Canada

EMail: suresh.krishnan@ericsson.com

Alan Kavanagh
Ericsson
8400 Blvd. Decarie
Town of Mount Royal, Quebec
Canada

EMail: alan.kavanagh@ericsson.com