                Client Link-Layer Address Option in DHCPv6

Abstract

   This document specifies the format and mechanism that is to be used
   for encoding the client link-layer address in DHCPv6 Relay-Forward
   messages by defining a new DHCPv6 Client Link-Layer Address option.

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/rfc6939.

Table of Contents

1. Introduction

   This specification defines an optional mechanism and the related
   DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents
   that are connected to the same link as the client) to provide the
   client's link-layer address in the DHCPv6 messages being sent towards
   the server.

2. 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].

3. Problem Background and Scenario

   The DHCPv4 specification [RFC2131] provides a way to specify the
   client link-layer address in the DHCPv4 message header. A DHCPv4
   message header has 'htype' and 'chaddr' fields to specify the client
   link-layer address type and the link-layer address, respectively.
   The client link-layer address thus learned can be used by the DHCPv4
   server and the relay agent in different ways. In some of the
   deployments, DHCPv4 servers use 'chaddr' as a customer identifier and
   a key for lookup in the client lease database.

   With the incremental deployment of IPv6 to existing IPv4 networks,
   which results in a dual-stack network environment, there will be
   devices that act as both DHCPv4 and DHCPv6 clients. In service
   provider deployments, a typical DHCPv4 implementation will use the
   client link-layer address as one of the keys to build the DHCP client
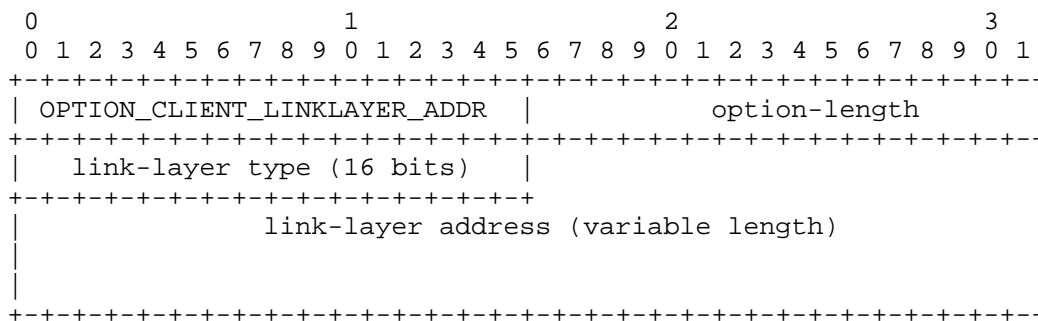   lease database. In dual-stack scenarios, operators need to be able

to associate DHCPv4 and DHCPv6 messages with the same client
interface, based on an identifier that is common to the interface.
The client link-layer address is such an identifier.

Currently, the DHCPv6 specification [RFC3315] does not define a way
to communicate the client link-layer address to the DHCP server in
cases where the DHCP server is not connected to the same network link
as the DHCP client. The DHCPv6 specification mandates that all
clients prepare and send a DHCP Unique Identifier (DUID) as the
client identifier option in all the DHCPv6 message exchanges.
However, none of these methods provide a simple way to extract a
client's link-layer address. This presents a problem to an operator
who is using an existing DHCPv4 system with the client link-layer
address as the customer identifier and who desires to correlate
DHCPv6 assignments using the same identifier. [RFC4361] describes a
mechanism for using the same DUID in both DHCPv4 and DHCPv6.
Unfortunately, this specification requires modification of existing
DHCPv4 clients, and has not seen broad adoption in the industry
(indeed, we are not aware of any commercial implementations).

Providing an option in DHCPv6 Relay-Forward messages to carry the
client link-layer address explicitly will help the above mentioned
scenarios. For example, it can be used along with other identifiers
to associate DHCPv4 and DHCPv6 messages from a dual-stack client.
Further, having the client link-layer address in DHCPv6 will help by
providing additional information for event debugging and logging
related to the client at the relay agent and the server. The
proposed option may be used in a wide range of networks; two notable
deployment models are service provider and enterprise network
environments.

4. DHCPv6 Client Link-Layer Address Option

   The format of the DHCPv6 Client Link-Layer Address option is shown
   below.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | OPTION_CLIENT_LINKLAYER_ADDR  |          option-length        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    link-layer type (16 bits)  |                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
    |                  link-layer address (variable length)        |
    |                                                               |
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
      option-code:       OPTION_CLIENT_LINKLAYER_ADDR (79)
      option-length:     2 + length of link-layer address
      link-layer type:   Client link-layer address type.  The link-layer
                         type MUST be a valid hardware type assigned
                         by the IANA, as described in [RFC0826]
      link-layer address: Client link-layer address
```

5. DHCPv6 Relay Agent Behavior

   DHCPv6 relay agents that receive messages originating from clients
   (for example, Solicit and Request, but not, for example,
   Relay-Forward or Advertise) MAY include the link-layer source address
   of the received DHCPv6 message in the Client Link-Layer Address
   option, in relayed DHCPv6 Relay-Forward messages. The DHCPv6 relay
   agent behavior can depend on configuration that decides whether the
   Client Link-Layer Address option needs to be included.

6. DHCPv6 Server Behavior

   If the DHCPv6 server is configured to store or use a client link-
   layer address, it SHOULD look for the Client Link-Layer Address
   option in the Relay-Forward DHCP message of the DHCPv6 relay agent
   closest to the client. The mechanism described in this document is
   not necessary in the case where the DHCPv6 server is connected to the
   same network link as the client, because the server can obtain the
   link-layer address from the link-layer header of the DHCPv6 message.
   If the DHCP server receives a Client Link-Layer Address option
   anywhere in any encapsulated message that is not a Relay-Forward DHCP
   message, the server MUST silently ignore that option.

There is no requirement that a server return this option and its data
in a downstream DHCP message.

7. DHCPv6 Client Behavior

The Client Link-Layer Address option is only exchanged between the
relay agents and the servers. DHCPv6 clients are not aware of the
usage of the Client Link-Layer Address option. The DHCPv6 client
MUST NOT send the Client Link-Layer Address option, and MUST ignore
the Client Link-Layer Address option if received.

8. IANA Considerations

IANA has assigned an option code (79) to OPTION_CLIENT_LINKLAYER_ADDR
from the "DHCP Option Codes" registry
(http://www.iana.org/assignments/dhcpv6-parameters/).

9. Security Considerations

It is possible for a rogue DHCPv6 relay agent to insert an incorrect
Client Link-Layer Address option for malicious purposes. A DHCPv6
client can also pose as a rogue DHCP relay agent by sending a
Relay-Forward message containing an incorrect Client Link-Layer
Address option. In either case, it would be possible for a DHCPv6
client to masquerade as the same device as a DHCPv4 client, when in
fact the two are distinct.

One possible attack that could be accomplished using this masquerade
would be in the case where a DHCPv4 client is using DHCPv4 to do a
Dynamic DNS update to install an A record so that it can be reached
by other nodes [RFC4702]. A masquerading DHCPv6 client could use
DHCPv6 to install a AAAA record with the same name [RFC4704]. Dual-
stack nodes attempting to connect to the DHCPv4 client might then be
tricked into connecting to the masquerading DHCPv6 client instead.

It is possible that there are other attacks that could be
accomplished using this masquerading technique, although the authors
are not aware of any. To prevent masquerades of this sort, DHCP
server administrators are strongly advised to configure DHCP servers
that use this option to communicate with their relay agents using
IPsec, as described in Section 21.1 of [RFC3315].

In some networks, it may be the case that the operator of the
physical network and the provider of connectivity over that network
are administratively separate, such that the Client Link-Layer
Address option would reveal information to one or the other party
that they do not need and could not otherwise obtain. It is also
possible, in some cases, that a relay agent might communicate with a

DHCP server over an open network where eavesdropping would be possible. In these cases, it is strongly recommended, in order to protect end-user privacy, that network operators use IPsec to provide confidentiality for messages between the relay agent and the DHCP server.

10. Acknowledgements

   Many thanks to Ted Lemon, Bernie Volz, Hemant Singh, Simon Hobson, Tina TSOU, Andre Kostur, Chuck Anderson, Steinar Haug, Niall O'Reilly, Jarrod Johnson, Tomek Mrugalski, and Vincent Zimmer for their input and review.

11. References

11.1. Normative References

   [RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

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

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

   [RFC4361] Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", RFC 4361, February 2006.

11.2. Informative References

   [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

   [RFC4702] Stapp, M., Volz, B., and Y. Rekhter, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option", RFC 4702, October 2006.

   [RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", RFC 4704, October 2006.

Authors' Addresses

   Gaurav Halwasia
   Cisco Systems
   Cessna Business Park, Sarjapura Marathalli Outer Ring Road
   Bangalore, KARNATAKA 560 087
   India

   Phone: +91 80 4429 2703
   EMail: ghalwasi@cisco.com

   Shwetha Bhandari
   Cisco Systems
   Cessna Business Park, Sarjapura Marathalli Outer Ring Road
   Bangalore, KARNATAKA 560 087
   India

   Phone: +91 80 4429 2627
   EMail: shwethab@cisco.com

   Wojciech Dec
   Cisco Systems
   Haarlerbergweg 13-19
   1101 CH Amsterdam, Amsterdam 560 087
   The Netherlands

   EMail: wdec@cisco.com