Client Hardware Address Option in DHCPv6
draft-halwasia-dhc-dhcpv6-hardware-addr-opt-00

Abstract

This document specifies the format and mechanism that is to be used for encoding client hardware address in DHCPv6 messages by defining a new DHCPv6 Client Hardware Address option.

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]*.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This specification defines an optional mechanism and the related DHCPv6
option to allow DHCPv6 client or first hop DHCPv6 relay agent directly
connected to the client to populate client hardware address in the
DHCPv6 messages being sent towards the server.

2. Problem Background and Scenario

DHCPv4 protocol specification [RFC2131] provides a way to specify the
client hardware address in the DHCPv4 message header. DHCPv4 message
header has 'htype' and 'chaddr' fields to specify client hardware
address type and hardware address respectively. The client hardware
address thus learnt can be used by DHCPv4 server and relay 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,
effectievly an enablement of dual-stack, there will be devices that act
as both DHCPv4 and DHCPv6 clients. In service provider deployments, a
typical DHCPv4 implemention will use the client hardware address as one
of the keys to build DHCP client lease database. In dual stack
scenarios it is desirable for the operator to associate DHCPv4 and
DHCPv6 messages as belonging to the same client interface based on an
identifier that is already used by that operator such as the client
hardware address.

Currently, the DHCPv6 protocol specification [RFC3315] does not define a way for DHCP clients to specify client hardware address in the DHCPv6 message sent towards DHCPv6 Server. Similarly DHCPv6 Relay or Server cannot glean client hardware address from the contents of DHCPv6 message received. DHCPv6 protocol specification mandates all clients to prepare and send DUID as the client identifier option in all the DHCPv6 message exchange. However none of these methods provide a simple way to extract client's hardware address.This presents a problem to an operator who is using an existing DHCPv4 system with the client hardware address as the customer identifier, and desires to correlate DHCPv6 assignments using the same identifier. Modifying the system to use DUID based correlation across DHCPv4 and DHCPv6 is possible, but it requires a modification of the DHCPv4 system and associated back-ends. Providing an option in DHCPv6 messages to carry client hardware address explicitly will help above mentioned scenarios. For e.g. it can be used along with other identifiers to associate DHCPv4 and DHCPv6 messages from a dual stack client. Further, having client hardware address in DHCPv6 will help in proving additional information in event debugging and logging related to the client at relay and server.

3. DHCPv6 Client Hardware Address Option

The format of the DHCPv6 Client Hardware Address option is shown below.
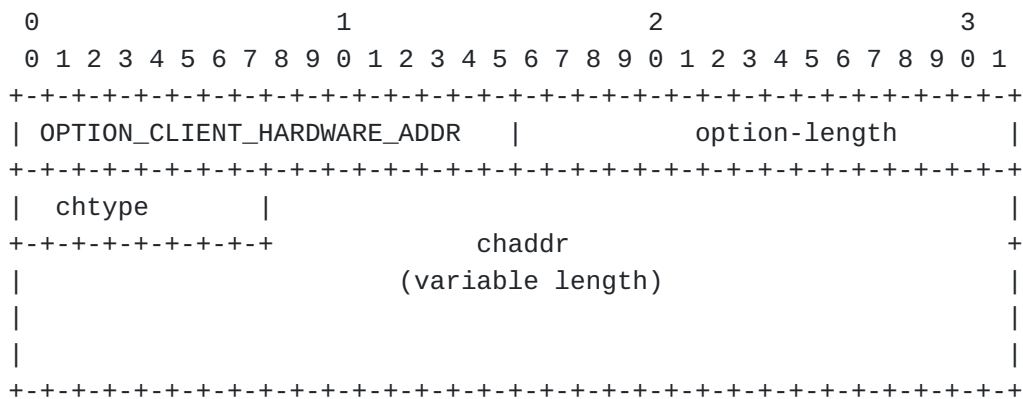
```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | OPTION_CLIENT_HARDWARE_ADDR   |          option-length        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   chtype      |                                               |
    +-+-+-+-+-+-+-+-+-+             chaddr                          +
    |                        (variable length)                     |
    |                                                              |
    |                                                              |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


    option-code:   OPTION_CLIENT_HARDWARE_ADDR (TBD)
    option-length: 1 + length of chaddr
    chtype:        Client Hardware address type, see ARP section in "Assigned
                    Numbers" RFC; e.g., '1' = 10mb ethernet.
    chaddr:        Client hardware address.
```

4. DHCPv6 Client Behavior

All hosts or clients MAY include DHCPv6 Client hardware address option in all the upstream DHCPv6 messages like SOCILIT, REQUEST, RENEW, REBIND, CONFIRM, RELEASE and DELCINE.

[5.](#) DHCPv6 Relay Agent Behavior

DHCPv6 Relay agents which are directly connected to clients/hosts MAY look for Client Hardware Address option in the incoming DHCPv6 client message. In absence of client hardware option, DHCPv6 Relay agents MAY include client hardware address option in relayed DHCPv6 (RELAY-FORW) message. The DHCPv6 Relay agent behaviour can depend on configuration that decides whether Client Hardware Address option needs to be processed and included.
In Relay chaining scenarios, any other relay agent other than first hop DHCPv6 Relay agent or DHCPv6 LDRA [RFC6221] MUST not add this option.

[6.](#) DHCPv6 Server Behavior

If DHCPv6 Server is configured to store or use client hardware address, it MUST first look for the client hardware address option in the client DHCP message. In case it is not found, Server SHOULD look for client hardware option in the RELAY-FORW message of the DHCPv6 Relay agent closest to the client.
There is no requirement that a server return this option and its data in a downstream DHCP message.

[7.](#) [IANA Considerations](#)

IANA is requested to assign an option code to OPTION_CLIENT_HARDWARE_ADDR from the "DHCPv6 and DHCPv6 options" registry (http://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xml).

[8.](#) [Security Considerations](#)

Security issues related DHCPv6 are described in section 23 of [RFC3315].

[9.](#) [Acknowledgements](#)

[10.](#) References

[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.
[RFC2131]	Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
[RFC4580]	Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option", RFC 4580, June 2006.
[RFC4361]	

	Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", RFC 4361, February 2006.
[RFC6221]	Miles, D., Ooghe, S., Dec, W., Krishnan, S. and A. Kavanagh, "Lightweight DHCPv6 Relay Agent", RFC 6221, May 2011.

Authors' Addresses

Gaurav Halwasia Halwasia Cisco Systems Cessna Business Park, Sarjapura Marathalli Outer Ring Road Bangalore, KARNATAKA 560 087 India Phone: +91 80 4426 1321 EMail: ghalwasi@cisco.com

Shwetha Bhandari Bhandari Cisco Systems Cessna Business Park, Sarjapura Marathalli Outer Ring Road Bangalore, KARNATAKA 560 087 India Phone: +91 80 4426 0474 EMail: shwethab@cisco.com

Wojciech Dec Dec Cisco Systems Haarlerbergweg 13-19 1101 CH Amsterdam, Amsterdam 560 087 The Netherlands EMail: wdec@cisco.com