DHC Working Group   Q. Sun
Internet-Draft   Y. Cui
Intended status: Standards Track   Tsinghua University
Expires: July 20, 2014   M. Siodelski
                                                                 ISC
                                                         S. Krishnan
                                                            Ericsson
                                                           I. Farrer
                                                 Deutsche Telekom AG
                                                    January 16, 2014

                      DHCPv4 over DHCPv6 Transport
                   draft-ietf-dhc-dhcpv4-over-dhcpv6-04

Abstract

   IPv4 connectivity is still needed as networks migrate towards IPv6.
   Users require IPv4 configuration even if the uplink to their service
   provider supports IPv6 only. This document describes a mechanism for
   obtaining IPv4 configuration information dynamically in IPv6 networks
   by carrying DHCPv4 messages over DHCPv6 transport. Two new DHCPv6
   messages and two new DHCPv6 options are defined for this purpose.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   As the migration towards IPv6 continues, IPv6-only networks will
   become more prevalent. In such networks, IPv4 connectivity will
   continue to be provided as a service over IPv6-only networks. In
   addition to provisioning IPv4 addresses for clients of this service,
   other IPv4 configuration parameters may also be needed (e.g.
   addresses of IPv4-only services).

   This document describes a transport mechanism to carry DHCPv4
   messages using the DHCPv6 protocol for the dynamic provisioning of
   IPv4 addresses and other DHCPv4 specific configuration parameters
   across IPv6-only networks. It leverages the existing DHCPv4
   infrastructure, e.g. failover, DNS updates, DHCP leasequery, etc.

When IPv6 multicast is used to transport 4o6 messages, another
benefit is that the operator can gain information about the
underlying IPv6 network the 4o6 client is connected to from the the
DHCPv6 relay agents the request has passed through.

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 [RFC2119].

3. Terminology

This document makes use of the following terms:

DHCP 4o6 Client: A DHCP client supporting both the DHCPv6 protocol
                    [RFC3315] as well as the DHCPv4 over DHCPv6
                    protocol described in this document. Such a
                    client is capable of requesting IPv6
                    configuration using DHCPv6 and IPv4 configuration
                    using DHCPv4 over DHCPv6.

DHCP 4o6 Server: A DHCP server that is capable of processing
                    DHCPv4 packets encapsulated in the DHCPv4 Message
                    option (defined below).

CPE: Customer Premises Equipment (also known as
                    Customer Provided Equipment), which provides
                    access for devices connected to a Local Area
                    Network (typically at the customer's site/home)
                    to the Internet Service Provider's network.

DHCPv4 over DHCPv6: A protocol described in this document, used to
                    carry DHCPv4 messages in the payload of DHCPv6
                    messages.

4. Architecture Overview

The architecture described here addresses a typical use case, where a
DHCP client's uplink supports IPv6 only and the Service Provider's
network supports IPv6 and limited IPv4 services. In this scenario,
the client can only use the IPv6 network to access IPv4 services, so
IPv4 services must be configured using IPv6 as the underlying network
protocol.

Although the purpose of this document is to address the problem of
communication between the DHCPv4 client and the DHCPv4 server, the
mechanism that it describes does not restrict the transported

messages types to DHCPv4 only. As the DHCPv4 message is a special
type of BOOTP message, BOOTP messages can also be transported using
the same mechanism.

DHCP clients may be running on CPE devices, end hosts or any other
device that supports the DHCP client function. At the time of
writing, DHCP clients on CPE devices are comparatively easier to
modify than those implemented on end hosts. As a result, this
document uses the CPE as an example for describing the mechanism.
This does not preclude any end-host, or other device requiring IPv4
configuration, from implementing DHCPv4 over DHCPv6 in the future.

This mechanism works by carrying DHCPv4 messages encapsulated within
DHCPv6 messages. Figure 1, below, illustrates one possible
deployment architecture.

The DHCP 4o6 client implements a new DHCPv6 message called
DHCPv4-query, which contains a new option called the DHCPv4 Message
option encapsulating a DHCPv4 message sent by the client. The format
of this option is described in Section 6.1.

The DHCPv6 message can be transmitted either via DHCPv6 Relay Agents
or directly to the DHCP 4o6 Server. The server replies with a
DHCPv4-response message, which is a new DHCPv6 message carrying the
DHCPv4 response encapsulated in the DHCPv4 Message option.

```
              _____          _____
            /              \        /              \
            |              |        |              |
    +--------+-+  IPv6   +-+------------+-+  IPv6   +-+--------+
    | DHCP 4o6 | network |    DHCPv6      | network | DHCP 4o6 |
    |  Client  +---------+  Relay Agent  +---------+  Server  |
    | (on CPE) |         |               |         |          |
    +--------+-+         +-+------------+-+         +-+--------+
            |              |        |              |
            _____/        _____/
```
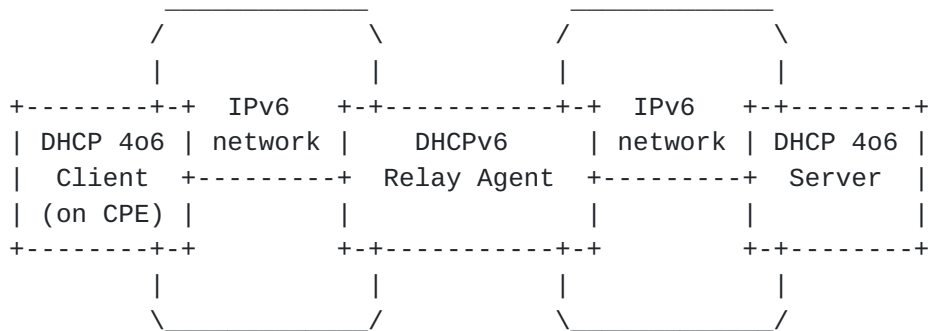
                   Figure 1: Architecture Overview

By default, the DHCPv4-over-DHCPv6 function MUST be disabled on the
client. Before the client can use DHCPv4 over DHCPv6, it MUST obtain
the necessary IPv6 configuration. The client requests the 4o6 Server
Address option from the DHCPv6 server by sending the option code in
Option Request option as described in [RFC3315]. If the DHCPv6
server responds with the 4o6 Server Address option, it is an
indication to the client to attempt using DHCPv4 over DHCPv6 to
obtain IPv4 configuration.

   The DHCP 4o6 client obtains the address(es) of the DHCP 4o6 server(s)
   from the 4o6 Server Address option and uses them to communicate with
   the DHCP 4o6 servers as described in Section 8. If the 4o6 Server
   Address option contains no addresses (is empty), the DHCP 4o6 client
   uses the well-known All_DHCP_Relay_Agents_and_Servers multicast
   address to communicate with the DHCP 4o6 server(s).

   Before applying for an IPv4 address via a DHCPv4-query message, the
   DHCP 4o6 client must identify a suitable network interface for the
   address. Once the request is acknowledged by the DHCP 4o6 server,
   the client can configure the address and other relevant parameters on
   this interface. The mechanism for determining a suitable interface
   is out of the scope of the document.

5. New DHCPv6 Messages

   Two new DHCPv6 messages carry DHCPv4 messages between the client and
   the server using the DHCPv6 protocol: DHCPv4-query and
   DHCPv4-response. This section describes the structures of these
   messages.

5.1. Message Types

   DHCPV4-QUERY (TBD):   The DHCP 4o6 client sends a DHCPv4-query
                           message to a DHCP 4o6 server. The DHCPv4
                           Message option carried by this message
                           contains a DHCPv4 message that the DHCP 4o6
                           client uses to request IPv4 configuration
                           parameters from the server.

   DHCPv4-RESPONSE (TBD): A DHCP 4o6 server sends a DHCPv4-response
                           message to a DHCP 4o6 client. It contains a
                           DHCPv4 Message option carrying a DHCPv4
                           message in response to a DHCPv4 message
                           received by the server in the DHCPv4 Message
                           option of the DHCPv4-query message.

5.2. Message Formats

   Both DHCPv6 messages defined in this document share the following
   format:

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    msg-type   |                   flags                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   .                           options                             .
   .                          (variable)                           .
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
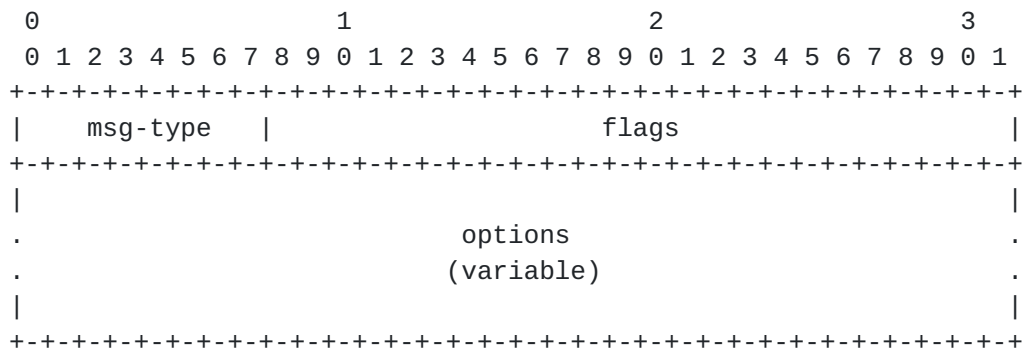
   Figure 2: The format of DHCPv4-query and DHCPv4-response messages

   msg-type   Identifies the message type. It can be either
                   DHCPV4-QUERY (TBD) or DHCPV4-RESPONSE (TBD)
                   corresponding to the contained DHCPv4-query or
                   DHCPv4-response, respectively.

   flags   Specifies flags providing additional information
                   required by the server to process the DHCPv4 message
                   encapsulated in the DHCPv4-query message, or required
                   by the client to process a DHCPv4 message
                   encapsulated in the DHCPv4-response message.

   options   Options carried by the message. The DHCPv4 Message
                   Option (described in Section 6.1) MUST be carried by
                   the message. Only DHCPv6 options for IPv4
                   configuration may be included in this field. It MUST
                   NOT contain DHCPv6 options related solely to IPv6, or
                   IPv6-only service configuration.

5.3. DHCPv4-query Message Flags

   The "flags" field of the DHCPv4-query is used to carry additional
   information that may be used by the server to process the
   encapsulated DHCPv4 message. Currently only one bit of this field is
   used. Remaining bits are reserved for the future use. The "flags"
   field has the following format:

```
       0                   1                   2
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |U|                 Reserved                     |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
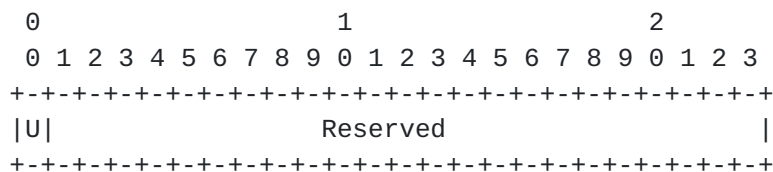
                  Figure 3: DHCPv4-query flags format

   U   Unicast Flag. If set to 1, it indicates that the

                      DHCPv4 message encapsulated within the DHCPv4-query
                      message would be sent to a unicast address if it was
                      sent using IPv4. If this flag is set to 0, it
                      indicates that the DHCPv4 message would be sent to
                      the broadcast address if it was sent using IPv4.

   Reserved   Bits MUST be set to zero when sending and MUST be
                      ignored when receiving.

5.4. DHCPv4-response Message Flags

   This document introduces no flags to be carried in the "flags" field
   of the DHCPv4-response message. They are all reserved for the future
   use. The 4o6 Server MUST set all bits of this field to 0 and the 4o6
   client MUST ignore the content in this field.

6. New DHCPv6 Options

6.1. DHCPv4 Message Option Format

   The DHCPv4 Message option carries a DHCPv4 message that is sent by
   the client or the server. Such messages exclude any IP or UDP
   headers.

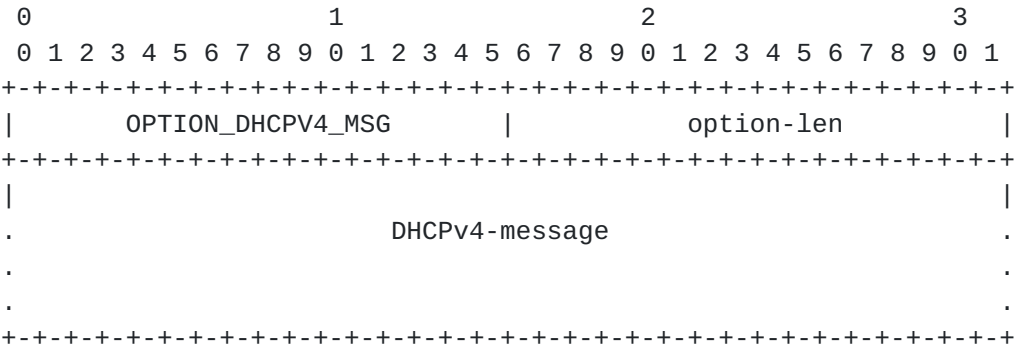   The format of the DHCPv4 Message option is:

```
    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_DHCPV4_MSG       |          option-len           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   .                         DHCPv4-message                        .
   .                                                               .
   .                                                               .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                  Figure 4: DHCPv4 Message option Format

   option-code   OPTION_DHCPV4_MSG (TBD).

   option-len   Length of the DHCPv4 message.

   DHCPv4-message The DHCPv4 message sent by the client or the server.
                   In a DHCPv4-query message it contains a DHCPv4
                   message sent by a client. In a DHCPv4-response
                   message it contains a DHCPv4 message sent by a server
                   in response to a client.

6.2. 4o6 Server Address Option Format

   The 4o6 Server Address option is sent by the DHCPv6 server to a
   client requesting IPv6 configuration. It carries a list of DHCP 4o6
   server's IPv6 addresses that the DHCP 4o6 client should contact to
   obtain IPv4 configuration. This list may include either multicast or
   unicast addresses. The DHCP 4o6 client sends its requests to all
   unique addresses carried in this option.

   This option may also carry no IPv6 addresses, which instructs the
   client to use the All_DHCP_Relay_Agents_and_Servers multicast address
   as the destination address.

   The presence of this option in the DHCPv6 server's response indicates
   to the client that it should use DHCPv4 over DHCPv6 to obtain IPv4
   configuration. If the option is absent, the client MUST NOT enable
   DHCPv4 over DHCPv6 function.

   The format of the 4o6 Server Address option is:

```
    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_DHCP4_O_DHCP6_SERVER   |           option-len          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   .                        IPv6 Address(es)                       .
   .                                                               .
   .                                                               .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
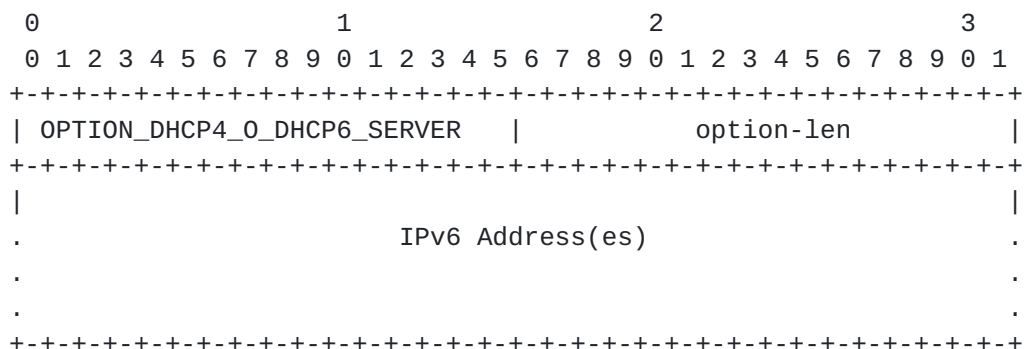
               Figure 5: 4o6 Servers Address Option Format

   option-code   OPTION_DHCP4_O_DHCP6_SERVER (TBD).

   option-len   Length of the IPv6 address(es) carried by the option,
                   i.e. multiple of 16 octets. Minimal length of this
                   option is 0.

   IPv6 Address   Zero or more IPv6 addresses of the DHCP 4o6
                   Server(s).

7. Use of the DHCPv4-query Unicast Flag

   A DHCPv4 client conforming to [RFC2131] may send its DHCPREQUEST
   message to either a broadcast or unicast address depending on its
   state. For example, a client in the RENEWING state uses a unicast
   address to contact the DHCPv4 server to renew its lease. A client in

the REBINDING state uses a broadcast address. If there is a DHCPv4
relay agent in the middle, a client in the RENEWING state may send a
DHCPREQUEST message to the unicast address of the relay agent. In
such a case, the server is unable to determine whether the client
sent the message to a unicast or broadcast address and thus the
server may be unable to correctly determine the client's state.
[RFC5010] introduced the "Flags Suboption" that relay agents add to
relayed messages to indicate whether broadcast or unicast was used by
the client.

In DHCPv4 over DHCPv6, IPv6 is used to deliver DHCPv4 messages to the
4o6 DHCP Server. There is no relation between the outer IPv6 address
and the inner DHCPv4 message. As a result, the server is unable to
determine whether the received DHCPv4 messages should have been sent
using broadcast or unicast in IPv4 by checking the IPv6 address.
This is similar to the case addressed by [RFC5010].

In order to allow the server to determine the client's state, the
"Unicast" flag is carried in the DHCPv4-query message. The client
MUST set this flag to 1 when the DHCPv4 message would have been sent
to the unicast address if using DHCPv4 over IPv4. This flag MUST be
set to 0 if the DHCPv4 client would have sent the message to the
broadcast address in IPv4. The choice whether a given message should
be sent to a broadcast or unicast address is made based on the
[RFC2131] and its extensions.

Note: The "Unicast" flag reflects how the DHCPv4 packet would have
been sent; not how the DHCPv6 packet itself is sent.

8. DHCP 4o6 Client Behavior

The DHCPv4-over-DHCPv6 function MUST be disabled by default. The
client MUST obtain the necessary IPv6 configuration before using
DHCPv4 over DHCPv6. A client intending to use DHCPv4 over DHCPv6
MUST request the 4o6 Server Address option using Option Request
option (ORO) in every Solicit, Request, Renew and Information-request
message.

The DHCPv6 server MAY include the 4o6 Server Address option in its
response to the client. If the client receives this option, it MUST
enable the DHCPv4-over-DHCPv6 function. The client MUST NOT enable
the DHCPv4-over-DHCPv6 function if the DHCPv6 server does not include
the 4o6 Server Address option in its response. If the client does
not receive this option and DHCPv4 over DHCPv6 is already enabled,
the client MUST disable the DHCPv4-over-DHCPv6 function.

If the DHCP 4o6 client receives the 4o6 Server Address option and
there is a DHCPv4 client active on the interface over which that

DHCPv6 option was received, it MUST stop the DHCPv4 client from
sending messages using [RFC2131].

If the 4o6 client receives a 4o6 Server Address option that contains
no IP addresses, i.e. the option is empty, the DHCP 4o6 client MUST
send its requests to the All_DHCP_Relay_Agents_and_Servers multicast
address. If there is a list of IP addresses in the option, the DHCP
4o6 client SHOULD send requests to each unique address carried by the
option.

The DHCP 4o6 client MUST employ an IPv6 address of an appropriate
scope to source the DHCPv4-query message from. When the client sends
a DHCPv4-query message to the multicast address, it MUST use a link-
local address as the source address as described in [RFC3315]. When
the client sends a DHCPv4-query message using unicast, the source
address MUST be the global IPv6 address, acquired in advance.

A client supporting DHCPv4 over DHCPv6 SHOULD use Information Refresh
Time Option [RFC4242] to refresh the status of DHCPv4-over-DHCPv6
function as well as other DHCPv6 configuration data.

The client generates a DHCPv4 message and stores it verbatim in the
DHCPv4 Message option carried by the DHCPv4-query message. The
client MUST put exactly one DHCPv4 Message option into a single
DHCPv4-query message. The client MUST NOT request the 4o6 Server
Address option in the DHCPv4-query message.

The client MUST follow rules defined in Section 7 when setting the
Unicast flag based on the DHCPv4 destination.

On receiving a DHCPv4-response message, the client MUST look for the
DHCPv4 Message option within this message. If this option is not
found, the DHCPv4-response message is discarded. If the DHCPv4
Message option is present, the client extracts the DHCPv4 message it
contains and processes it as described in section 4.4 of [RFC2131].

When dealing with IPv4 configuration, the DHCP 4o6 client MUST follow
the normal DHCPv4 retransmission requirements and strategy as
specified in section 4.1 of [RFC2131]. There are no explicit
transmission parameters associated with a DHCPv4-query message, as
this is governed by the DHCPv4 [RFC2131] "state machine".

The DHCP 4o6 client MUST implement [RFC4361] to ensure that the
device correctly identifies itself.

9. Relay Agent Behavior

   When a DHCPv6 relay agent receives a DHCPv4-query message, it may not
   recognize this message. The unknown message can be forwarded as
   described in [I-D.ietf-dhc-dhcpv6-unknown-msg].

   Additionally, the DHCPv6 relay agent MAY allow the configuration of a
   dedicated DHCPv4 over DHCPv6 specific destination address(es),
   differing from the address(es) of the DHCPv6-only server(s). To
   implement this function, the relay checks the received DHCPv6 message
   type and forwards according to the following logic:

   1. If the message type is DHCPV4-QUERY, the packet is relayed to the
       configured DHCP 4o6 Server's address(es) in the form of normal
       DHCPv6 packet (i.e. DHCPv6/UDP/IPv6).

   2. For any other DHCPv6 message type, forward according to section
       20 of [RFC3315].

   The above logic only allows for separate relay destinations
   configured on the relay agent closest to the client (single relay
   hop). Multiple relaying hops are not considered in the case of
   separate relay destinations.

10. DHCP 4o6 Server Behavior

   When the server receives a DHCPv4-query message from a client, it
   searches for the DHCPv4 Message option. The server discards the
   packet without this option. The server MAY notify an administrator
   about the receipt of a malformed packet. The mechanism for this
   notification is out of scope for this document.

   If the server finds a valid DHCPv4 Message option, it extracts the
   original DHCPv4 message and the contents of the "flags" field carried
   in the DHCPv4-query message and uses them to generate the appropriate
   DHCPv4 response (server to client message). The response is
   generated as described in [RFC2131] with the exception that the
   server SHOULD use the information carried in the "flags" field of the
   DHCPv4-query message to find out whether the client's message would
   have been sent to the broadcast or unicast address if IPv4 has been
   used. This is useful for the server to determine the state of the
   client. The use of the "flags" field is described in detail in
   Section 7. Since the client MUST use a client identifier to identify
   itself (as per [RFC4361]), the server MUST implement [RFC6842] and
   use the client identifier in all DHCPv4 message exchanges with the
   client.

   When an appropriate DHCPv4 response is generated, the 4o6 Server

places it in the payload of a DHCPv4 Message option, which it puts
into the DHCPv4-response message.

If the DHCPv4-query message was received directly by the server, the
DHCPv4-response message MUST be unicast from the interface on which
the original message was received.

If the DHCPv4-query message was received in a Relay-forward message,
the server creates a Relay-reply message with the DHCPv4-response
message in the payload of a Relay Message option, and responds as
described in section 20.3 of [RFC3315].

11. Security Considerations

In this specification, DHCPv4 messages are encapsulated in the newly
defined option and messages. This is similar to the handling of the
current relay agent messages. In order to bypass firewalls or
network authentication gateways, a malicious attacker may leverage
this feature to convey other messages using DHCPv6, i.e. use DHCPv6
as a form of encapsulation. However, the potential risk from this is
no more severe than that with the current DHCPv4 and DHCPv6 practice.

It is possible for a rogue DHCPv6 server to reply with a 4o6 Server
Address Option containing duplicated IPv6 addresses, which could
cause an amplification attack. To avoid this, the client MUST check
if there are duplicate IPv6 addresses in a 4o6 Server Address Option
when receiving one. The client MUST ignore those duplicated IPv6
addresses.

12. IANA Considerations

IANA is requested to allocate two DHCPv6 option codes for use by
OPTION_DHCPV4_MSG and OPTION_DHCP4_O_DHCP6_SERVER from the "DHCP
Option Codes" table, and two DHCPv6 message type codes for the
DHCPV4-QUERY and DHCPV4-RESPONSE from the "DHCP Message Codes" table
of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
Registry. Both tables can be found at http://www.iana.org/
assignments/dhcpv6-parameters/dhcpv6-parameters.xml.

13. Contributors List

Many thanks to Ted Lemon, Bernie Volz, Tomek Mrugalski, Yuchi Chen
and Cong Liu, for their great contributions to the draft.

14. References

14.1. Normative References

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

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

   [RFC4242] Venaas, S., Chown, T., and B. Volz, "Information Refresh
              Time Option for Dynamic Host Configuration Protocol for
              IPv6 (DHCPv6)", RFC 4242, November 2005.

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

   [RFC6842] Swamy, N., Halwasia, G., and P. Jhingran, "Client
              Identifier Option in DHCP Server Replies", RFC 6842,
              January 2013.

14.2. Informative References

   [I-D.ietf-dhc-dhcpv6-unknown-msg]
              Cui, Y., Sun, Q., and T. Lemon, "Handling Unknown DHCPv6
              Messages", draft-ietf-dhc-dhcpv6-unknown-msg-04 (work in
              progress), December 2013.

   [RFC5010] Kinnear, K., Normoyle, M., and M. Stapp, "The Dynamic Host
              Configuration Protocol Version 4 (DHCPv4) Relay Agent
              Flags Suboption", RFC 5010, September 2007.

Authors' Addresses

   Qi Sun
   Tsinghua University
   Beijing 100084
   P.R.China

   Phone: +86-10-6278-5822
   Email: sunqi@csnet1.cs.tsinghua.edu.cn

   Yong Cui
   Tsinghua University
   Beijing 100084
   P.R.China

   Phone: +86-10-6260-3059
   Email: yong@csnet1.cs.tsinghua.edu.cn

   Marcin Siodelski
   950 Charter Street
   Redwood City, CA 94063
   USA

   Phone: +1 650 423 1431
   Email: msiodelski@gmail.com

   Suresh Krishnan
   Ericsson

   Email: suresh.krishnan@ericsson.com

   Ian Farrer
   Deutsche Telekom AG
   GTN-FM4,Landgrabenweg 151
   Bonn, NRW 53227
   Germany

   Email: ian.farrer@telekom.de