Authors: W. Kumari   S. Krishnan
         Google, LLC   Cisco Systems, Inc.
         R. Asati   L. Colitti   J. Linkova
         Cisco Systems, Inc.   Google, LLC   Google, LLC

Registering Self-generated IPv6 Addresses using DHCPv6

Abstract

This document defines a method to inform a DHCPv6 server that a
device has a self-generated or statically configured address.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://
wkumari.github.io/draft-wkumari-dhc-addr-notification/draft-wkumari-
dhc-addr-notification.html. Status information for this document may
be found at https://datatracker.ietf.org/doc/draft-wkumari-dhc-addr-
notification/.

Discussion of this document takes place on the Dynamic Host
Configuration Working Group mailing list (mailto:dhcwg@ietf.org),
which is archived at https://mailarchive.ietf.org/arch/browse/
dhcwg/. Subscribe at https://www.ietf.org/mailman/listinfo/dhcwg/.

Source for this draft and an issue tracker can be found at https://
github.com/wkumari/draft-wkumari-dhc-addr-notification.

Status of This Memo

This Internet-Draft is submitted in full conformance with the
provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF). Note that other groups may also distribute
working documents as Internet-Drafts. The list of current Internet-
Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six
months and may be updated, replaced, or obsoleted by other documents
at any time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

This Internet-Draft will expire on 1 October 2023.

Copyright Notice

Table of Contents

1. **Introduction**

It is very common operational practice, especially in enterprise networks, to use IPv4 DHCP logs for troubleshooting or security purposes. Examples of this include a helpdesk dealing with a ticket such as "The CEO's laptop cannot connect to the printer"; if the MAC address of the printer is known (for example from an inventory system), the IPv4 address can be retrieved from the DHCP logs and the printer pinged to determine if it is reachable. Another common example is a Security Operations team discovering suspicious events in outbound firewall logs and then consulting DHCP logs to determine

which employee's laptop had that IPv4 address at that time so that
they can quarantine it and remove the malware.

This operational practice relies on the DHCP server knowing the IP
address assignments. Therefore, the practice does not work if static
IP addresses are manually configured on devices or self-assigned
addresses (such as when self-configuring an IPv6 address using SLAAC
[RFC4862]) are used.

The lack of this parity with IPv4 is one of the reasons that some
enterprise networks are unwilling to deploy IPv6.

This document provides a mechanism for a device to inform the DHCPv6
server that it has a self-configured IPv6 address (or has a
statically configured address), and thus provides parity with IPv4
in this aspect.

2. Conventions and Definitions

The key words **"MUST"**, **"MUST NOT"**, **"REQUIRED"**, **"SHALL"**, **"SHALL NOT"**,
"SHOULD", **"SHOULD NOT"**, **"RECOMMENDED"**, **"NOT RECOMMENDED"**, **"MAY"**, and
"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

3. Description of Mechanism

After successfully assigning a self-generated IPv6 address on one of
its interfaces, an end-host implementing this specification **SHOULD**
multicast an ADDR-REG-INFORM message in order to inform the DHCPv6
server that this address is in use.

```
+----+   +----------------+                 +---------------+
|Host|   |First-hop router|                 |Addr-Reg Server|
+----+   +----------------+                 +---------------+
|   SLAAC   |                                    |
|<--------->|                                    |
|           |                                    |
|           |        ADDR-REG-INFORM             |
|--------------------------------------------------->|
|           |                                    |Register / log
|           |        ADDR-REG-REPLY              |address
|<---------------------------------------------------
```
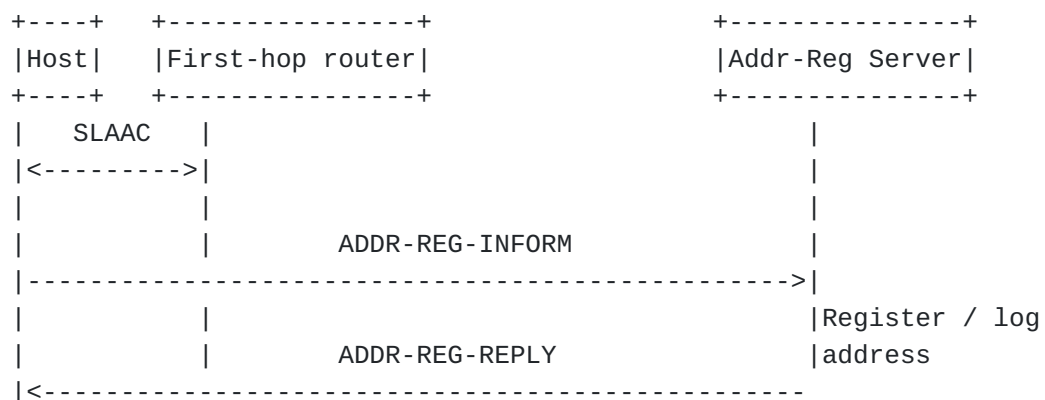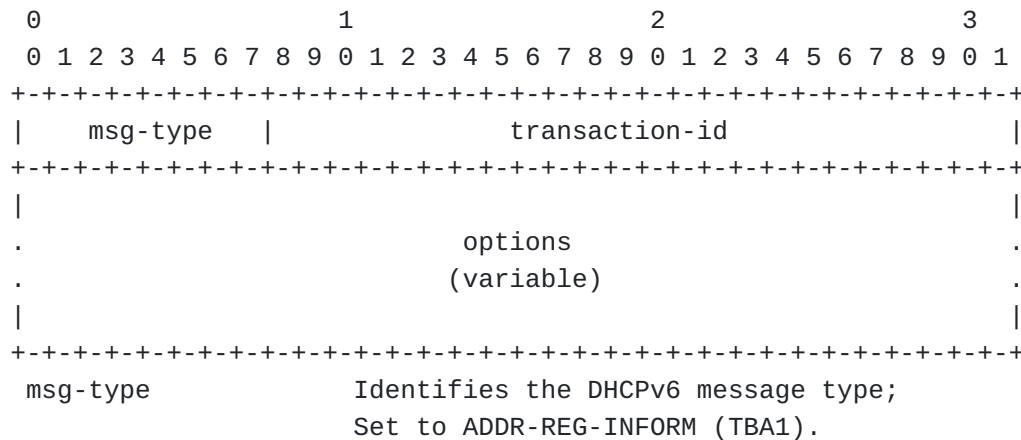
Figure 1: Address Registration Procedure

4. DHCPv6 ADDR-REG-INFORM Message

   The DHCPv6 client sends an ADDR-REG-INFORM message to inform that an
   IPv6 address is in use. The format of the ADDR-REG-INFORM message is
   described as follows:


```
 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   |               transaction-id                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                            options                            .
.                           (variable)                          .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 msg-type              Identifies the DHCPv6 message type;
                       Set to ADDR-REG-INFORM (TBA1).

 transaction-id        The transaction ID for this message exchange.

 options               Options carried in this message.
```

                  Figure 2: DHCPv6 ADDR-REG-INFORM message

   The ADDR-REG-INFORM message **MUST NOT** contain server-identifier
   option and **MUST** contain the IA Address option. The ADDR-REG-INFORM
   message is dedicated for clients to initiate an address registration
   request toward an address registration server. Consequently, clients
   MUST NOT put any Option Request Option(s) in the ADDR-REG-INFORM
   message. Clients **MAY** include other options, such as the Client FQDN
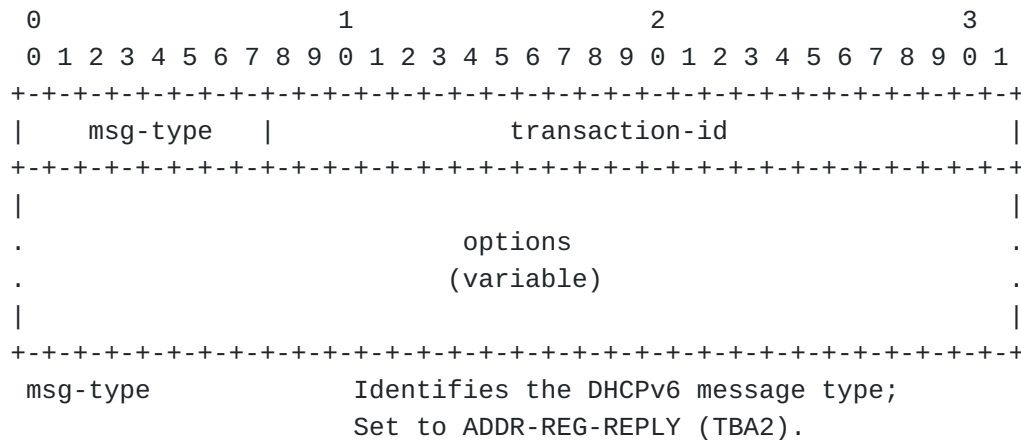   Option [RFC4704].

   Clients **MUST** discard any received ADDR-REG-INFORM messages.

   Servers **MUST** discard any ADDR-REG-INFORM messages that meet any of
   the following conditions:

     *the address is not appropriate for the link;

     *the message does not include a Client Identifier option;

     *the message includes a Server Identifier option;

     *the message does not include the IA Address option;

     *the message includes an Option Request Option.

5. DHCPv6 ADDR-REG-REPLY Message

The DHCPv6 server sends an ADDR-REG-REPLY message in response to a
valid ADDR-REG-INFORM message. The format of the ADDR-REG-REPLY
message is described as follows:

```
 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   |               transaction-id                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                            options                            .
.                           (variable)                          .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 msg-type              Identifies the DHCPv6 message type;
                       Set to ADDR-REG-REPLY (TBA2).

 transaction-id        The transaction ID for this message exchange.

 options               Options carried in this message.
```

Figure 3: DHCPv6 ADDR-REG-REPLY message

The ADDR-REG-INFORM message **MUST** contain an IA Address option for
the address being registered.

Servers **MUST** ignore any received ADDR-REG-REPLY messages.

The IPv6 destination address of the packet is the address being
registered.

6. DHCPv6 Address Registration Procedure

The DHCPv6 protocol is used as the address registration protocol
when a DHCPv6 server performs the role of an address registration
server. The DHCPv6 IA Address option [RFC8415] is adopted in order
to fulfill the address registration interactions.

6.1. DHCPv6 Address Registration Request

The end-host sends a DHCPv6 ADDR-REG-INFORM message to the address
registration server to the All_DHCP_Relay_Agents_and_Servers
multicast address (ff02::1:2). The host **MUST** only send the packet on
the network interface that has the address being registered (i.e. if
the host has multiple interfaces with different addresses, it should
only send the packet on the interface with the address being
registered). The host **MUST** send the packet from the address being

registered. This is primarily for "fate sharing" purposes - for
example, if the network implements some form of L2 security to
prevent a client from spoofing other clients' addresses this
prevents an attacker from spoofing ADDR-REG-INFORM messages. The
host **MUST** send separate messages for each address being registered.

The end-host **MUST** include a Client Identifier option in the ADDR-
REG-INFORM message.

The host **MUST** only send the ADDR-REG-INFORM message for valid
([RFC4862]) addresses of global scope ([RFC4007]). The host **MUST NOT**
send the ADDR-REG-INFORM message for addresses configured by DHCPv6.

The host **MUST NOT** send the ADDR-REG-INFORM message if it has not
received any Router Advertisement message with either M or O flags
set to 1.

After receiving this ADDR-REG-INFORM message, the address
registration server **SHOULD** verify that the address being registered
is "appropriate to the link" as defined by [RFC8415]. If the server
believes that address being registered is not appropriate to the
link [RFC8415], it **MUST** drop the message, and **SHOULD** log this fact.
If the address is appropriate, the server:

  ***SHOULD** register or update a binding between the provided Client
   Identifier and IPv6 address in its database;

  ***SHOULD** log the address registration information (as is done
   normally for clients which have requested an address), unless
   configured not to do so;

  ***SHOULD** mark the address as unavailable for use and not include it
   in future ADVERTISE messages.

  ***SHOULD** send back an ADDR-REG-REPLY message.

If the DHCPv6 server does not support the address registration
function, it **MUST** drop the message, and **SHOULD** log this fact.

DHCPv6 relay agents and switches that relay address registration
messages directly from clients **SHOULD** include the client's link-
layer address in the relayed message using the Client Link-Layer
Address option ([RFC6939])

6.2. DHCPv6 Address Registration Acknowledgement

The server **SHOULD** acknowledge receipt of an ADDR-REG-INFORM message
by sending a ADDR-REG-REPLY message back. The ADDR-REG-REPLY message
only indicates that the ADDR-REG-INFORM message has been received.
It **MUST NOT** be considered as any indication of the address validity

and **MUST NOT** be required for the address to be usable. DHCPv6
relays, or other devices that snoop ADDR-REG-REPLY messages, **MUST
NOT** add or alter any forwarding or security state based on the ADDR-
REG-REPLY message.

6.3. Registration Expiry and Refresh

The client **MUST** refresh the registration every AddrRegRefresh
seconds, where AddrRegRefresh is min(1/3 of the Valid Lifetime filed
in the very first PIO received to form the address; 4 hours).
Registration refresh packets **SHOULD** be retransmitted using the same
logic as described in the 'Retransmission' section below. In
particular, retransmissions **SHOULD** be jittered to avoid
synchronization causing a large number of registrations to expire at
the same time.

If the address registration server does not receive such a refresh
after the preferred lifetime has passed, it **SHOULD** remove the record
of the Client-Identifier-to-IPv6-address binding.

The client **MAY** choose to notify the server when an address is no
longer being used (the client is disconnecting from the network, the
address lifetime expired or the address is being removed from the
interface). To indicate that the address is not being used anymore
the client **MUST** set the preferred-lifetime and valid-lifetime fields
of the IA Address option to zero.

6.4. Retransmission

To reduce the effects of packet loss on registration, the client
SHOULD retransmit the registration message. Retransmissions **SHOULD**
follow the standard retransmission logic specified by section 15 of
[RFC8415] with the following default parameters:

  *IRT 1 sec

  *MRC 3

The client **SHOULD** allow these parameters to be configured by the
administrator.

If an ADDR-REG-REPLY message is received for the address being
registered, the client **MUST** stop retransmission. However, the client
can not rely on the server acknowledging receipt of the registration
message, because the server might not support address registration.

7. Host configuration

DHCP clients **SHOULD** allow the administrator to disable sending ADDR-
REG-INFORM messages. This could be used, for example, to reduce

network traffic on networks where the servers are known not to support the message type. Sending the messages **SHOULD** be enabled by default.

8. Security Considerations

An attacker may attempt to register a large number of addresses in quick succession in order to overwhelm the address registration server and / or fill up log files. These attacks may be mitigated by using generic DHCPv6 protection such as the AUTH option [RFC8415]. The similar attack vector exist today, e.g. an attacker can DoS the server with messages contained spoofed DUIDs.

If a network is using FCFS SAVI [RFC6620], then the DHCPv6 server can trust that the ADDR-REG-INFORM message was sent by the legitimate owner of the address. This prevents a host from registering an address owned by another host.

One of the use-cases for the mechanism described in this document is to identify sources of malicious traffic after the fact. Note, however, that as the device itself is responsible for informing the DHCPv6 server that it is using an address, a malicious or compromised device can simply not send the ADDR-REG-INFORM message. This is an informational, optional mechanism, and is designed to aid in troubleshooting and forensics. On its own, it is not intended to be a strong security access mechanism.

9. IANA Considerations

This document defines a new DHCPv6 message, the ADDR-REG-INFORM message (TBA1) described in Section 4, that requires an allocation out of the registry of Message Types defined at http://www.iana.org/assignments/dhcpv6-parameters/

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, DOI 10.17487/RFC4007, March 2005, <https://www.rfc-editor.org/rfc/rfc4007>.

[RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", RFC 4704, DOI 10.17487/RFC4704, October 2006, <https://www.rfc-editor.org/rfc/rfc4704>.

[RFC4862]
Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/rfc/rfc4862>.

[RFC6939] Halwasia, G., Bhandari, S., and W. Dec, "Client Link-Layer Address Option in DHCPv6", RFC 6939, DOI 10.17487/RFC6939, May 2013, <https://www.rfc-editor.org/rfc/rfc6939>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8415]
Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/rfc/rfc8415>.

Acknowledgments

Contributors

Gang Chen
China Mobile
53A, Xibianmennei Ave.
Xuanwu District
Beijing
P.R. China

Email: phdgang@gmail.com

Authors' Addresses

Warren Kumari
Google, LLC

   Email: warren@kumari.net

   Suresh Krishnan
   Cisco Systems, Inc.

   Email: suresh.krishnan@gmail.com

   Rajiv Asati
   Cisco Systems, Inc.
   7025 Kit Creek road
   Research Triangle Park, 27709-4987
   United States of America

   Email: rajiva@cisco.com

   Lorenzo Colitti
   Google, LLC
   Shibuya 3-21-3,
   Japan

   Email: lorenzo@google.com

   Jen Linkova
   Google, LLC
   1 Darling Island Rd
   Pyrmont 2009
   Australia

   Email: furry@google.com