DHC Working Group   S. Jiang
Internet-Draft   Huawei Technologies Co., Ltd
Intended status: Standards Track   G. Chen
Expires: August 18, 2014   China Mobile
                                                       S. Krishnan
                                                          Ericsson
                                                          R. Asati
                                                     Cisco Systems
                                                 February 14, 2014

            Registering self-generated IPv6 Addresses in DNS using DHCPv6
                   draft-ietf-dhc-addr-registration-04

Abstract

   In networks that are centrally managed, self-generated addresses
   cause some traceability issues due to their decentralized nature.
   One of the most important issues in this regard is the inability to
   register such addresses in DNS. This document defines a mechanism to
   register self-generated and statically configured addresses in DNS
   through a DHCPv6 server.

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 http://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 August 18, 2014.

Table of Contents

1. Introduction

In several common network scenarios, IPv6 addresses are self-
generated by the end-hosts by appending a self-generated interface
identifier to a network-specified prefix. Examples of self-generated
addresses include those created using IPv6 Stateless Address
Configuration [RFC4862] , temporary addresses [RFC4941] and
Cryptographically Generated Addresses (CGA) [RFC3972] etc. In
several tighly controlled networks, hosts with self-generated
addresses may face some limitations. One such limitation is related
to the inability of nodes with self-generated addresses to register
their IPv6-address-to-FQDN bindings in DNS. This is related to the
fact that, in such networks, only certain nodes (e.g. The DHCPv6
server) are allowed to update these bindings in order to prevent end-
hosts from registering arbitrary addresses for their FQDNs or
associating their addresses with arbitary domain names.

For nodes that obtain their addresses through DHCPv6, a solution has
been specified in [RFC4704]. The solution works by including a
Client FQDN option in the SOLICIT, REQUEST, RENEW or REBIND messages
during the process of acquiring an address through DHCPv6. This
document provides an analogous mechanism to register self-generated
addresses in DNS.

A new ADDR-REGISTRATION-REQUEST DHCPv6 message type is defined to
initiate the address registration request, and two new Status codes
is defined to indicate registration errors on the server side.

2. Terminology

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. Solution Overview

   After successfully assigning a self-generated IPv6 address on one of
   its interfaces, an end-host implementing this specification SHOULD
   send an ADDR-REGISTRATION-REQUEST message to a DHCPv6 address
   registration server. After receiving the address registration
   request, the DHCPv6 server registers the IPv6 address to FQDN binding
   towards a configured DNS server. An acknowledgement MAY be sent back
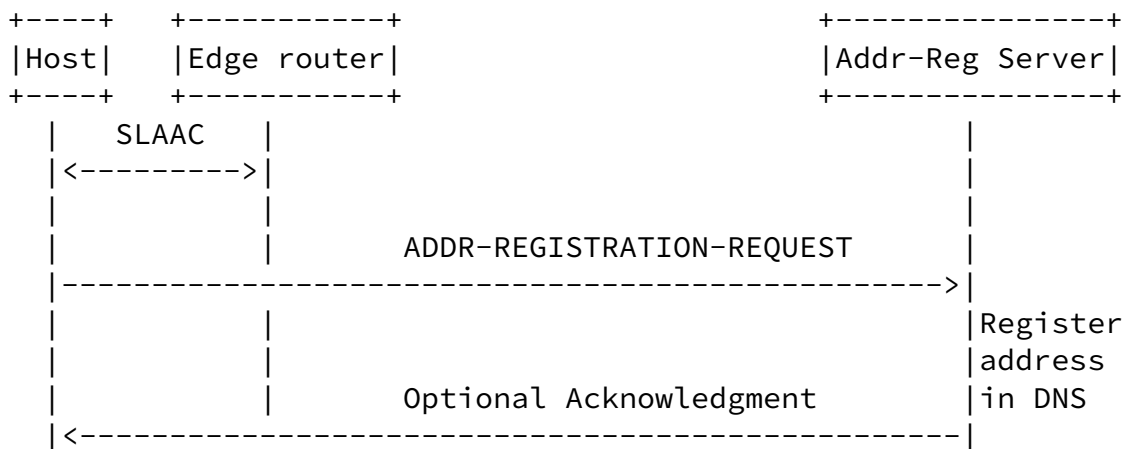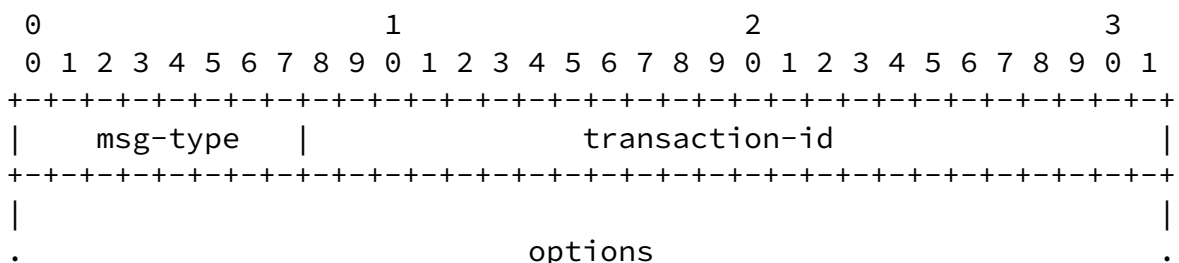   to the end host to indicate whether or not the registration operation
   succeeded..

```
        +----+    +-----------+                  +---------------+
        |Host|    |Edge router|                  |Addr-Reg Server|
        +----+    +-----------+                  +---------------+
          |   SLAAC   |                            |
          |<--------->|                            |
          |           |                            |
          |           |     ADDR-REGISTRATION-REQUEST     |
          |------------------------------------------------>|
          |           |                            |Register
          |           |                            |address
          |           |     Optional Acknowledgment     |in DNS
          |<------------------------------------------------|
```

                  Figure 1: Address Registration Procedure

4. DHCPv6 ADDR-REGISTRATION-REQUEST Message

   The DHCPv6 client sends an ADDR-REGISTRATION-REQUEST message to a
   server to request an address to be registered in the DNS. The format
   of the ADDR-REGISTRATION-REQUEST 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-REGISTRATION-REQUEST (TBA1).

         transaction-id   The transaction ID for this message exchange.

         options   Options carried in this message.

                  DHCPv6 ADDR-REGISTRATION-REQUEST message

   The ADDR-REGISTRATION-REQUEST message MUST NOT contain server-
   identifier option and MUST contain the IA_NA option and the DHCPv6
   FQDN option [RFC4704].

   Clients MUST discard any received ADDR-REGISTRATION-REQUEST messages.
   Servers MUST discard any ADDR-REGISTRATION-REQUEST messages that do
   not include a Client Identifier option or that do include a Server

   Identifier option.

5. 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_NA option [RFC3315] and the DHCPv6 FQDN option
   [RFC4704] are reused in order to fulfill the address registration
   interactions.

5.1. DHCPv6 Address Registration Request

   The end-host sends a DHCPv6 ADDR-REGISTRATION-REQUEST message to the
   address registration server to the All_DHCP_Relay_Agents_and_Servers
   multicast address (ff02::1:2).

   The end-host MUST include a Client Identifier option in the ADDR-
   REGISTRATION-REQUEST message to identify itself to the server. The
   DHCPv6 ADDR-REGISTRATION-REQUEST message MUST contain exactly one
   IA_NA option and exactly one FQDN option. The IA_NA option MUST
   contain at least one IA Address option. The valid-lifetime field of

the IA Address option MUST be set to the period for which the client
would like to register the binding in DNS.

After receiving this ADDR-REGISTRATION-REQUEST message, the address
registration server MUST register the binding between the provided
FQDN and address(es) in DNS. If the DHCPv6 server does not support
address registration function, a Reply message with includes a Status
Code option with the value the RegistrationNotSupported (TBA2) MAY be
sent back to the initiated client.

5.2. Registration expiry and refresh

The address registration client MUST refresh the registration before
it expires (i.e. before the valid-lifetime of the IA address elapses)
by sending a new ADDR-REGISTRATION-REQUEST to the address
registration server. If the address registration server does not
receive such a refresh after the valid-lifetime has passed, it SHOULD
remove the IPv6-address-to-FQDN bindings in DNS.

5.3. Acknowledging successful registration

After all the addresses have been successfully registered in DNS, the
address registration server MAY send a Reply message as the response
to registration requests. The server generates a Reply message and
includes a Status Code option with value Success, a Server Identifier
option with the server's DUID, and a Client Identifier option with

Jiang, et al.   Expires August 18, 2014   [Page 5]

---

the client's DUID. For each IA in the ADDR-REGISTRATION-REQUEST
message for which the server does not succeed in registering, the
server adds an IA option using the IAID from the ADDR-REGISTRATION-
REQUEST message, and includes a Status Code option with the value
RegistrationDenied (TBA3) in the IA option. No other options are
included in the IA option.

6. Security Considerations

An attacker may attempt to register large number of addresses in
quick succession in order to overwhelm the address registration
server. These attacks may be prevented generic DHCPv6 protection by
using the AUTH option [RFC3315] or Secure DHCPv6
[I-D.ietf-dhc-secure-dhcpv6].

7. IANA Considerations

This document defines a new DHCPv6 message, the ADDR-REGISTRATION-REQUEST message (TBA1) described in Section 5, that requires an allocation out of the registry defined at

http://www.iana.org/assignments/dhcpv6-parameters/

This document defines two new DHCPv6 Status code, the RegistrationNotSupported (TBA2) and RegistrationDenied (TBA3) described in Section 6, that requires an allocation out of the registry defined at

http://www.iana.org/assignments/dhcpv6-parameters/

8. Acknowledgements

The authors would like to thank Ralph Droms, Ted Lemon, Bernie Volz, Sten Carlsen, Erik Kline, Lorenzo Colitti, Joel Jaeggli, Sten Carlsen, Mark Smith, Marcin Siodelski and other members of dhc and v6ops working groups for their valuable comments.

9. References

9.1. Normative References

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

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

[RFC3633]   Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic
            Host Configuration Protocol (DHCP) version 6", RFC 3633,
            December 2003.

   [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure
              Neighbor Discovery (SEND)", RFC 3971, March 2005.

   [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)",
              RFC 3972, March 2005.

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

   [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
              Address Autoconfiguration", RFC 4862, September 2007.

   [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy
              Extensions for Stateless Address Autoconfiguration in
              IPv6", RFC 4941, September 2007.

9.2. Informative References

   [I-D.ietf-dhc-secure-dhcpv6]
              Jiang, S. and S. Shen, "Secure DHCPv6 Using CGAs",
              draft-ietf-dhc-secure-dhcpv6-07 (work in progress),
              September 2012.

Authors' Addresses

   Sheng Jiang
   Huawei Technologies Co., Ltd
   Q14, Huawei Campus
   No.156 Beiqing Road
   Hai-Dian District, Beijing 100095
   P.R. China

   Email: jiangsheng@huawei.com

   Gang Chen

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

Phone: 86-13910710674
Email: phdgang@gmail.com

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

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

Rajiv Asati
Cisco Systems

Email: rajiva@cisco.com