Network Working Group   S. Jiang
Internet Draft   Huawei Technologies Co., Ltd
Intended status: Standards Track   G. Chen
Expires: November 8, 2012   China Mobile
                                                      May 8, 2012

            A Generic IPv6 Addresses Registration Solution
                            Using DHCPv6
               draft-ietf-dhc-addr-registration-00.txt

Status of this Memo

Copyright Notice

Abstract

   In the IPv6 address allocation scenarios, host self-generated
   addresses are notionally conflicted with the network managed address
   architecture. These addresses need to be registered in the networking
   management plate for the purposes of central address administration.
   This document introduces a generic address registration solution
   using DHCPv6, and defines one new ND option and one new DHCPv6 option
   in order to propagate the solicitations of registering self-generated
   addresses. The registration procedure reuses the existing IA_NA in
   the DHCPv6 protocol.

Table of Contents

[1](1). Introduction & Requirements

In the IPv6 address allocation scenarios, there are many host self-generated addresses, such as addresses in IPv6 Stateless Address Configuration [RFC4862, [RFC4941](RFC4941)] scenario and Cryptographically Generated Addresses (CGA, [[RFC3972](RFC3972)]), and etc. These addresses are notionally conflicted with the network managed address architecture, such as Dynamic Host Configuration Protocol for IPv6 (DHCPv6, [[RFC3315](RFC3315)]) managed network or network with Access Control List.

Many operators of enterprise networks and similarly tightly administered networks have expressed the desire to be at least aware the hosts' addresses when moving to IPv6. Furthermore, they may want to stop the usage of some hosts' addresses for various reasons.

A useful way to give network administrators most of what they want, while at the same time retaining compatibility with normal stateless configuration would be: if the self-generated IPv6 addresses are used, they may need to be registered in the networking management plate. The host may be required to perform this registration since only registered IPv6 addresses may access the network resources in some scenarios.

In order to fulfill the abovementioned practice, this document introduces a new Neighbor Discovery (ND) option and a new DHCPv6 option to propagate the address registration solicitation from network management to hosts. DHCPv6 protocol is suitable to perform the address registration procedure while the address registration server may play by a DHCPv6 server or a stand-alone server. The existing IA_NA in the DHCPv6 protocol is reused for the registration procedure.

[2](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](RFC2119) [[RFC2119](RFC2119)].

3. Overview of Generic Address Registration Solution

   By current default, the hosts with self-generated addresses do not
   register their addresses to any network devices. However, this may
   result that the network may reject the access request from these
   devices if the address registration is requested.

   As showed in below Figure 1, in the generic address registration
   solution, proposed by this document, the network management plate
   firstly propagates the solicitations of registering self-generated
   addresses, by messages from either local router (step 1a in Figure 1)
   or DHCPv6 server (step 1b in Figure 1).

   By received such solicitations, a host using the self-generated
   address SHOULD send an address registration request message to the
   address registration server (step 2 in Figure 1). The address
   registration server may be acted by a DHCPv6 server. By received the
   address registration request, the address registration server records
   the requested address in the address database, which MAY be used by
   other network functions, such as DNS or ACL, etc. The address
   registration server should also assign lifetimes for the requested
   address. An acknowledgement is sent back to the host with the
   assigned lifetimes (step 3 in Figure 1).

```
   +--------+                    +-----------+   +---------------+
   |  Host  |                    |Local Router|   |Addr-Reg Server|
   +--------+                    +-----------+   +---------------+
       |                             |                  |
       |Addr Register Solicitation(1a)|                  |
       |<----------------------------|                  |
       |                             |                  |
       |            Addr Register Solicitation(1b)       |
       |<------------------------------------------------|
       |                             |                  |
       |Send self-generation addr registration request(2)|
       |------------------------------------------------->|
       |                                                  |Register
       | Reply acknowledgment with assigned lifetimes(3) |the addr
       |<-------------------------------------------------|
```
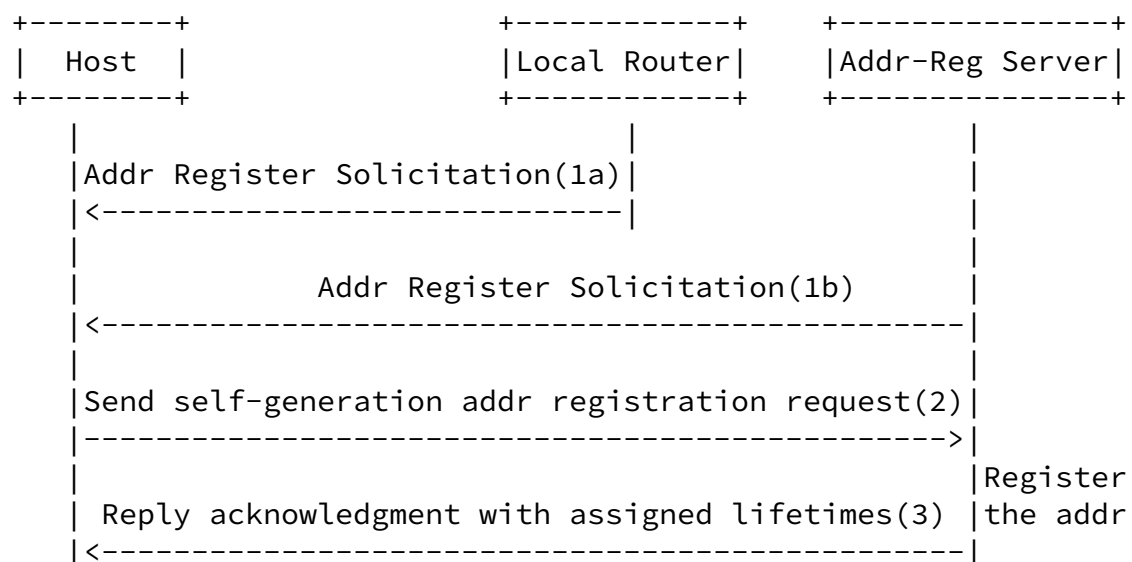
Figure 1: address registration procedure

   By received the acknowledgement, the host can use the registered
   address. It SHOULD use the assigned preferred and valid lifetime for
   the corresponded address.

4. Propagating the Address Registration Solicitation

   In order to indicate or force the hosts with self-generated addresses
   to register their addresses and the appointed address registration
   server, new solicitation options need to be defined.

   There are more than one mechanism in which configuration parameters
   could be pushed to the end hosts. The address registration

   solicitation option can be carried in Router Advertisement (RA)
   message, which is broadcasted by local routers. In the DHCPv6 managed
   network, it can also be carried in DHCPv6 messages.

   More precisely it defines one new ND option and one new DHCPv6 option
   that convey a Fully Qualified Domain Name (FQDN, as per Section 3.1
   of [RFC1035]) of address registration(s). In order to make use of
   these options, this document assumes appropriate name resolution
   means (see Section 6.1.1 of [RFC1123]) are available on the host
   client. The use of the FQDN may benefit for load-balancing purposes.

   By receiving the address registration solicitation option(s), a host
   SHOULD register its self-generated addresses, if there are any, to
   the appointed registration server. The solicitation options may
   include the IPv6 address(es) of address registration server.

   In principle, hosts must receive a prefix from either RA message
   [RFC4861] or DHCPv6 message [I-D.ietf-dhc-host-gen-id] so that they
   can generate an IPv6 address by themselves. The Address Registration
   Solicitation options could be propagated together with prefix
   assignment information.

4.1. ND Address Registration Solicitation Option

   The ND Address Registration Solicitation Option allows routers to
   propagate the solicitation for hosts to register their self-generated
   address. This option also carries a domain name of the appointed
   address registration server. This option SHOULD be propagated

together with ND Prefix Information Option, Section 4.6.2, [RFC4861].
That is also applied to the case of Neighbor Discovery Proxies
[RFC4389]. The format of the ND Address Registration Solicitation
Option 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
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |     Type      |     Length    |  Pad Length   |   Reserved    |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     .                         Domain Name                           .
     .                (Address Registration Server)                  .
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     .                          Padding                              .
     .                                                               .
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
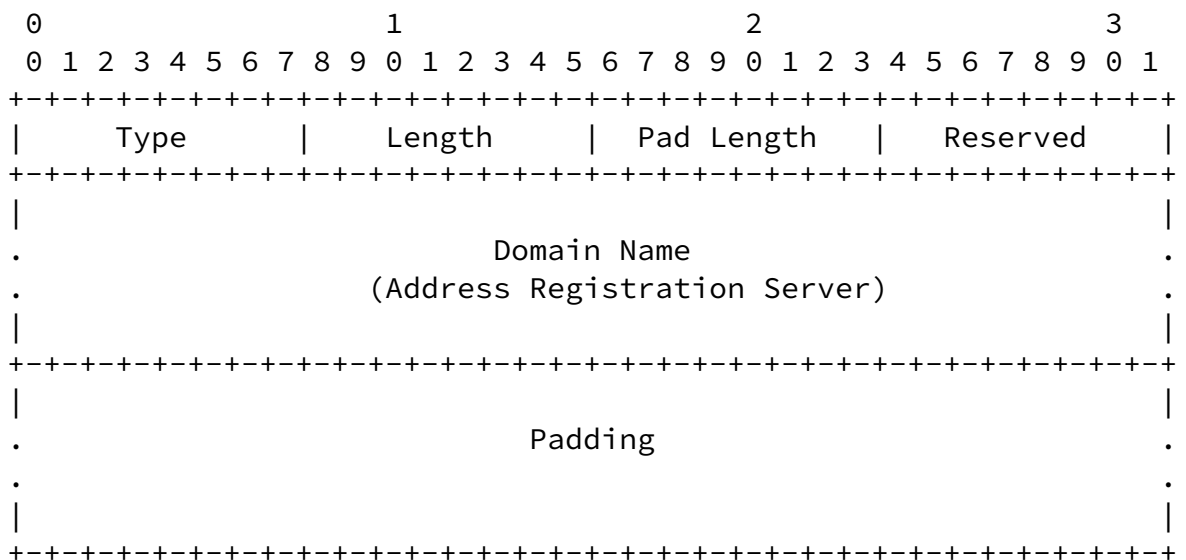
   Fields:

     Type   (TBA1)

     Length   The length of the option in units of 8 octets,
                including the Type and Length fields. The value 0
                is invalid. The receiver MUST discard a message
                that contains this value.

> Pad Length The number of padding octets beyond the end of the
>   Domain Name field but within the length specified
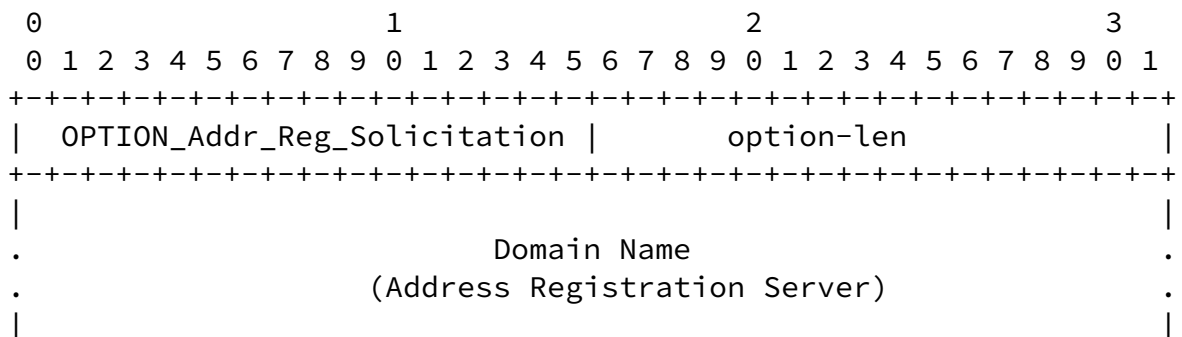>   by the Length field.
>
> Reserved Padding bits. It is for future use also. The value
>   MUST be initialized to zero by the sender, and MUST
>   be ignored by the receiver.
>
> Domain Name A fully qualified domain name of the appointed
>   address registration server. The domain name is
>   encoded as specified in Section 8 of [RFC3315]. Any
>   possible future updates to Section 8 of the Section
>   8 of [RFC3315] also apply to this option.
>
> Padding: A variable-length field making the option length a
>   multiple of 8, containing as many octets as
>   specified in the Pad Length field. Padding octets
>   MUST be set to zero by senders and ignored by
>   receivers.

4.2. DHCPv6 Address Registration Solicitation Option

The DHCPv6 Address Registration Solicitation Option allows DHCPv6
server to propagate the solicitation for hosts to register their
self-generated address. This option also carries a domain name of the
appointed address registration server. This option SHOULD be
propagated together with DHCPv6 Prefix Information Option, Section 5,
[I-D.ietf-dhc-host-gen-id]. The format of the DHCPv6 Address
Registration Solicitation Option 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  OPTION_Addr_Reg_Solicitation |          option-len           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                        Domain Name                            .
.                 (Address Registration Server)                 .
|                                                               |
```

```
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        option-code   OPTION_Addr_Reg_Solicitation (TBA2).

        option-len   Length of this option in octets (option-code and
                       option-len are not included).

        Domain Name   A fully qualified domain name of the appointed
                       address registration server. The domain name is
                       encoded as specified in Section 8 of [RFC3315]. Any
                       possible future updates to Section 8 of the Section
                       8 of [RFC3315] also apply to this option.

5. DHCPv6 Address Registration Procedure

   The current DHCPv6 protocol is reused as the address registration
   protocol while a DHCPv6 serve plays as address registration server.
   Identity Association for Non-temporary Addresses (IA_NA) [RFC3315] is
   reused in order to fulfill the address registration interactions.

5.1. DHCPv6 Address Registration Request

   The host with self-generated address(es) sends a DHCPv6 Request
   message to the appointed address registration server, which may be a
   DHCPv6 server.

   The DHCPv6 Request message SHOULD contain at least one IA_NA option.
   The IA_NA option SHOULD contain at least one IA Address option. The

   host SHOULD set the T1 and T2 fields in any IA_NA options, and the
   preferred-lifetime and valid-lifetime fields in the IA Address
   options to 0.

   By received, the address registration server MUST register the
   requested address in its address database, which MAY be used by other
   network functions, such as DNS or ACL, etc. The address registration
   server SHOULD also assign the lifetimes for these registered
   addresses.

   The address database contains both the self-generated addresses and
   the DHCPv6 assigned addresses. They MAY be marked different in the
   database.

5.2. DHCPv6 Address Registration Acknowledge

   The address registration server sends a Reply message as the response
   to registration requests.

   The DHCPv6 Reply message SHOULD contain at least one IA_NA option.
   The IA_NA option SHOULD contain at least one IA Address option. The
   server SHOULD set the T1 and T2 fields in any IA_NA options, and the
   preferred-lifetime and valid-lifetime fields in the IA Address
   options following the rules defined in Section 22 in [RFC3315].

   By received the acknowledgement from the server, the host can use the
   registered address to access the network. It SHOULD use the values in
   the preferred and valid lifetime fields for the preferred and valid
   lifetimes of the address.

   Note: the host MAY continue to use expired address, such as Locators
   as Upper-Layer Identifiers (ULID) in Shim6 protocol [RFC5533], etc.;
   but the network MAY refuse the network access from such addresses.

6. Security Considerations

   An attacker may use a faked address registration request option to
   indicate hosts reports their address to a malicious server and
   collect the user information. Or, an attacker may register a faked
   address to spoof the networking management plate. In either cases,
   these attacks may be prevented by using Secure Neighbor Discovery
   (SEND, [RFC3971]) if RA Address Registration Request Option is used,
   or AUTH option [RFC3315] or Secure DHCPv6
   [I-D.ietf-dhc-secure-dhcpv6] if DHCPv6 Address Registration Request
   Option is used.

7. IANA Considerations

   This document defines a new Neighbor Discovery [RFC4861] option,
   which MUST be assigned Option Type values within the option numbering
   space for Neighbor Discovery Option Type:

      The Address Registration Solicitation Option (TBA1), described in
      Section 4.1.

This document defines one new DHCPv6 [RFC3315] option, which MUST be assigned Option Type values within the option numbering space for DHCPv6 options:

    The OPTION_Addr_Reg_Solicitation (TBA2), described in
    Section 4.2;

8. Acknowledgments

The authors would like to thank Ralph Dorm, Ted Lemon, Bernie Volz and other member of DHC WG for valuable comments.

9. References

9.1. Normative References

   [RFC1035] Mockapetris, P., "Domain names - implementation and
            specification", STD 13, RFC 1035, November 1987.

   [RFC1123] Braden, R., "Requirements for Internet Hosts - Application
            and Support", STD 3, RFC 1123, October 1989.

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

   [RFC3315] R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins and
            M. Carne, "Dynamic Host Configure Protocol for IPv6",
            RFC3315, July 2003.

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

   [RFC3972] T. Aura, "Cryptographically Generated Address", RFC3972,
            March 2005.

   [RFC4861] T. Narten, E. Nordmark, W. Simpson, and H. Soliman,
            "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
            September 2007.

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

   [RFC4941] T. Narten, R. Draves and S. Krishnan, "Privacy Extensions

for Stateless Address Autoconfiguration in IPv6", RFC 4941,
                September 2007.

   [RFC5533] E. Nordmark, and M. Bagnulo, "Shim6: Level 3 Multihoming
                Shim Protocol for IPv6", RFC 5533, June 2009.

9.2. Informative References

   [RFC4389] D. Thaler, M. Talwar, and C. Patel, "Neighbor Discovery
                Proxies (ND Proxy)", RFC4389, April 2006.

   [I-D.ietf-dhc-secure-dhcpv6]
                S. Jiang and S. Shen, "Secure DHCPv6 Using CGAs", draft-
                ietf-dhc-secure-dhcpv6 (work in progress), December, 2011.

   [I-D.ietf-dhc-host-gen-id]
                S. Jiang, F. Xia, and B. Sarikaya, "Prefix Assignment in
                DHCPv6", draft-ietf-dhc-host-gen-id (work in progress),
                November, 2011.

Author's Addresses

   Sheng Jiang
   Huawei Technologies Co., Ltd
   Q14, Huawei Campus
   No.156 Beiqing Road
   Hai-Dian District, Beijing 100095
   Email: jiangsheng@huawei.com

   Gang Chen
   China Mobile
   53A, Xibianmennei Ave., Xuanwu District, Beijing
   P.R. China
   Phone: 86-13910710674
   Email: phdgang@gmail.com