6man Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 25, 2013

S. Jiang
Huawei Technologies Co., Ltd
G. Chen
China Mobile
S. Krishnan
Ericsson
October 22, 2012

A Generic IPv6 Addresses Registration Solution Using DHCPv6 draft-ietf-dhc-addr-registration-01

Abstract

In networks that are centrally managed, self-generated addresses cause traceability issues due to their decentralized nature. To minimize the issues due to lack of traceability, these self-generated addresses can be registered with the network for allowing centralized address administration. This document defines a generic address registration solution using DHCPv6, using a new ND option and a new DHCPv6 option in order to communicate the use of self-generated addresses.

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 April 25, 2013.

Copyright Notice

Table of Contents

1. Introduction

In several common network scenarios, IPv6 addresses are self-generated by the end-hosts using some information propogated to them by the network (i.e. the network 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. These addresses are potentially incompatible with networks with a centrally managed address architecture such as DHCPv6 [RFC3315] as they lack traceability and stability.

Many operators of enterprise networks and similarly tightly administered networks have expressed the desire to be at least aware of the hosts' self-generated addresses when migrating to IPv6.

One potential way to provide network administrators with most of their needs while retaining compatibility with normal stateless configuration would be to register the self-generated addresses with the systems in place to centrally administer the addresses. The host may be required to perform this registration in some scenarios since only registered IPv6 addresses may be granted access to the network resources .

This document introduces a new IPv6 Neighbor Discovery option and a new DHCPv6 option to propagate the address registration information from the hosts to the network. The DHCPv6 protocol is used to perform the address registration procedure while the address registration server role may be performed by a DHCPv6 server or a stand-alone server.

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. Overview of Generic Address Registration Solution

In the generic address registration solution, the network management system solicits hosts to register their self-generated addresses, by sending solicitation messages from either local router (step 1a in Figure 1) or DHCPv6 server (step 1b in Figure 1).

After receiving such solicitations, a host implementing this specification and using a 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).

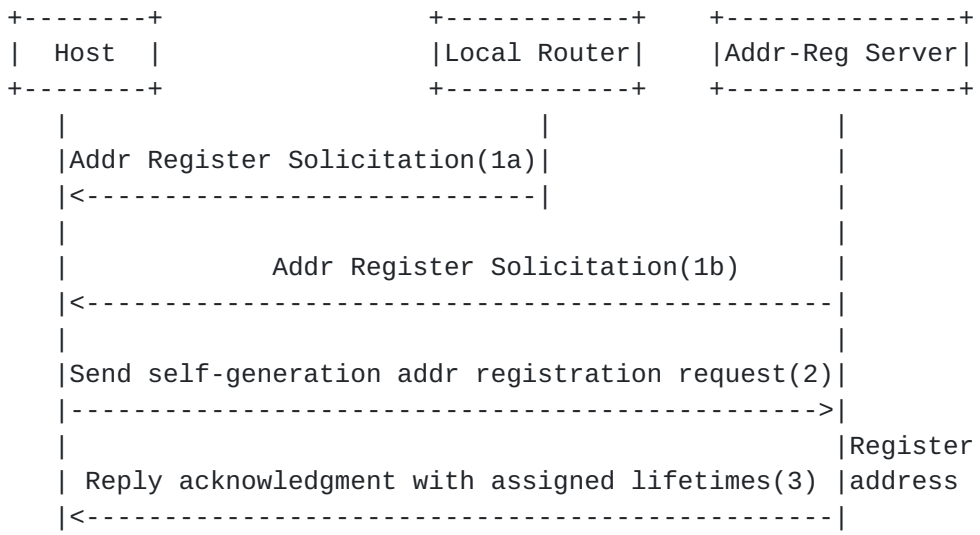


Figure 1: Address Registration Procedure

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

4. Propagating the Address Registration Solicitation

In order to request the hosts with self-generated addresses to register their addresses and the appointed address registration server, new solicitation options are defined.

There is more than one mechanism by 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.

This document defines a new ND option and one new DHCPv6 option that convey a Fully Qualified Domain Name (FQDN, as per Section 3.1 of [RFC1035] to be used as the destination of the address registration

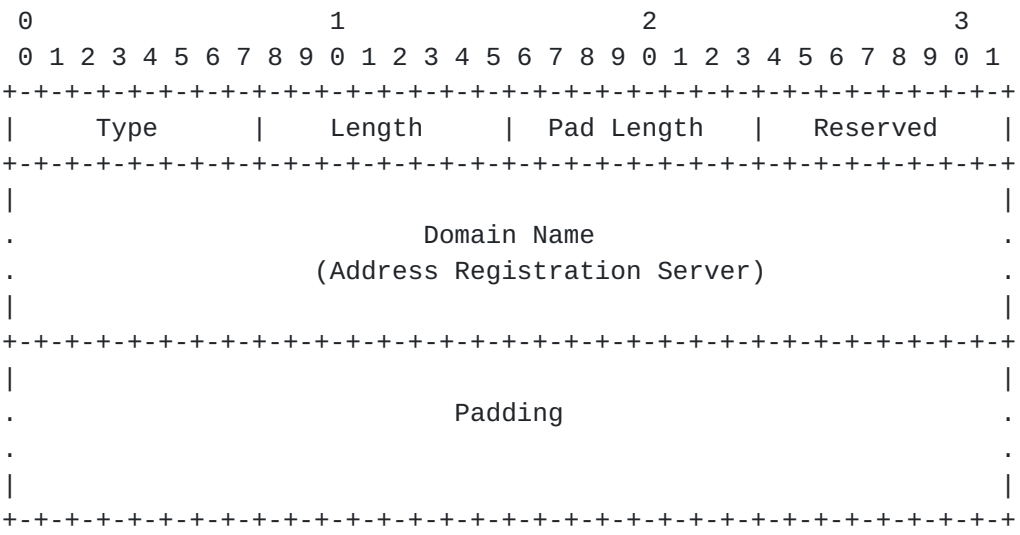
messages. In order to make use of these options, this document assumes that appropriate name resolution mechanisms (see Section 6.1.1 of [RFC1123] are available on the host.

After receving a message containing an address registration solicitation option, a host implementing this specification SHOULD register its self-generated addresses, if any, to the announced address registration server. The solicitation options MAY include the IPv6 address(es) of address registration server.

In principle, hosts need to 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 are expected to be propagated along 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 the fully qualified domain name of the address registration server. This option SHOULD be propagated together with the Prefix Information Option, Section 4.6.2, [RFC4861]. The format of the ND Address Registration Solicitation Option is described as follows:



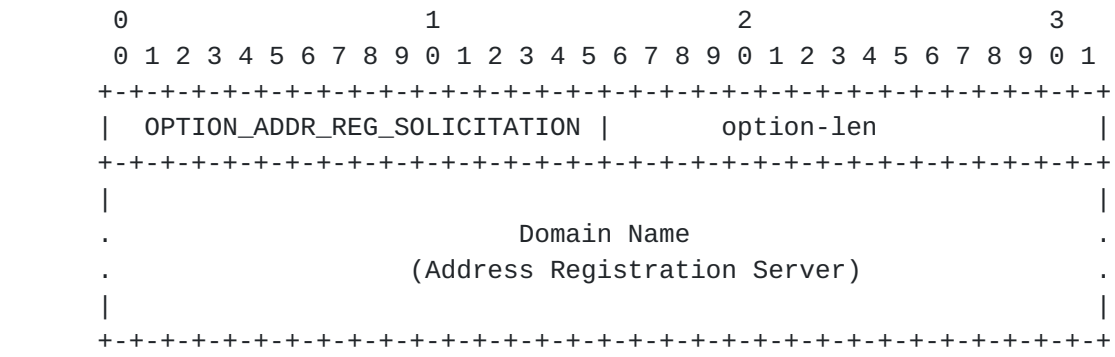
Fields:

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	Fully qualified domain name of the announced address registration server. The domain name is encoded as specified in Section 8 of [RFC3315].
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:



option-code OPTION_ADDR_REG_SOLICITATION (TBA2).

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

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].

5. DHCPv6 Address Registration Procedure

The DHCPv6 protocol is reused as the address registration protocol while a DHCPv6 server can play the role of an address registration server. The IA_NA DHCPv6 option [RFC3315] is reused in order to fulfill the address registration interactions.

5.1. DHCPv6 Address Registration Request

The host with one or more self-generated addresses sends a DHCPv6 Request message to the address registration server received in the address registration solicitation option.

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.

After receiving this address registration request, the address registration server MUST register the requested address in its

address database, which may further be used by other network functions, such as DNS, network access control lists, etc. The address registration server SHOULD also assign the lifetimes for these registered addresses.

The centrally managed address database contains both self-generated addresses and the DHCPv6 assigned addresses. They MAY be marked and treated differently in the database.

5.2. DHCPv6 Address Registration Acknowledge

The address registration server then 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 of [RFC3315].

After receiving 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 of the received message to determine the preferred and valid lifetimes of the address.

Please note that the host MAY continue to use expired address, such as Upper-Layer Identifiers (ULID) in Shim6 protocol [RFC5533], etc. but the network could potentially 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. An attacker may also register large number of fake addresses with the network in order to overwhelm the address registration server. In either case, these attacks may be prevented by using Secure Neighbor Discovery [RFC3971] if the RA Address Registration Request Option is used, and the AUTH option [RFC3315] or Secure DHCPv6 [I-D.ietf-dhc-secure-dhcpv6] if the DHCPv6 Address Registration Request Option is used.

7. IANA Considerations

This document defines a new IPv6 Neighbor Discovery option, the Address Registration Solicitation Option (TBA1) described in Section

4.1, that requires an allocation out of the registry defined at

http://www.iana.org/assignments/icmpv6-parameters

This document defines a new DHCPv6 option, the OPTION_ADDR_REG_SOLICITATION (TBA2) described in Section 4.2, 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 and other members of dhc working group for their 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] 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.

[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.

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

[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.

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

9.2. Informative References

[I-D.ietf-dhc-host-gen-id]
Jiang, S., Xia, F., and B. Sarikaya, "Prefix Assignment in DHCPv6", draft-ietf-dhc-host-gen-id-04 (work in progress), August 2012.

[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