

Network Working Group
Internet Draft
Intended status: Standards Track
Expires: September 7, 2011

S. Jiang
Huawei Technologies Co., Ltd
G. Chen
China Mobile
March 4, 2011

Requirements for Addresses Registration
draft-jiang-6man-addr-registration-req-02.txt

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 September 7, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Abstract

In the IPv6 address allocation scenarios, node self-generated addresses are notionally conflicted with the network managed address architecture. These addresses need to be registered in the networking management plane for the purposes of central address administration. This document discusses the requirements of address registration and analyzes the possible solutions.

Table of Contents

1. Introduction & Requirements.....	3
2. Terminology.....	3
3. Potential Solutions.....	4
3.1. Generic Address Registration Procedure.....	4
3.2. Propagating the Registration Request.....	4
3.3. Address Registration Server and Protocol.....	5
3.3.1. Using DHCPv6 and DHCPv6 server.....	5
3.3.2. Defining a new address Registration Protocol.....	5
4. Security Considerations.....	6
5. IANA Considerations.....	6
6. Change Log [RFC Editor please remove].....	6
7. Acknowledgments.....	6
8. References.....	7
8.1. Normative References.....	7
8.2. Informative References.....	7
Author's Addresses.....	8

1. Introduction & Requirements

In the IPv6 address allocation scenarios, node self-generated addresses, such as addresses in IPv6 Stateless Address Configuration [RFC4862, RFC4941] scenario and Cryptographically Generated Addresses (CGA, [RFC3972]), is notionally conflicted with the network managed address architecture, such as DHCPv6-managed network or network with Access Control List, in which addresses are assigned and managed by the network management plate.

The current IPv4 address allocation mode in DHCPv4-managed network is that the DHCPv4 server assigns addresses. Many operators of enterprise networks and similarly tightly administered networks have expressed the desire to hold on to this model when moving to IPv6, because they don't want to have hosts end up with essentially random IPv6 addresses. However, the notion that a server assigns an address is for the most part incompatible with IPv6 stateless configuration.

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 and granted by the networking management plate. The node may be required to perform this registration since only granted IPv6 addresses are allowed to be used to access the network.

This document discusses the requirements of address registration and analyzes the possible solutions. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) and Router Advertisement may be extended to propagate the address registration request from network management to nodes. A DHCPv6 server may play the address registration server with newly defined DHCPv6 options. However, this may conflict with the original DHCP notion. A new set of protocol may have to be defined for the address registration purpose.

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].

3. Potential Solutions

3.1. Generic Address Registration Procedure

By current default, the nodes 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.

As showed in below Figure 1, in the generic address registration procedure, the network management plate should firstly propagate the request of registering self-generated addresses. By received such requests, a node using the self-generated address should send an address registration message to the network management. The network management should check whether the requested address is accepted, for example, performing a Duplicated Address Detect or checking the address does not use the Reserved IPv6 Interface Identifiers [RFC5453]. If the requested address is accepted by the network management, it is registered in the address manage database, which may be used by other network functions, such as DNS or ACL. An acknowledgement is sent to the node, granting the usage of this address. If the requested address is not accepted by the network management, a rejected acknowledgement is sent to the node to indicate that it must generate a new address.

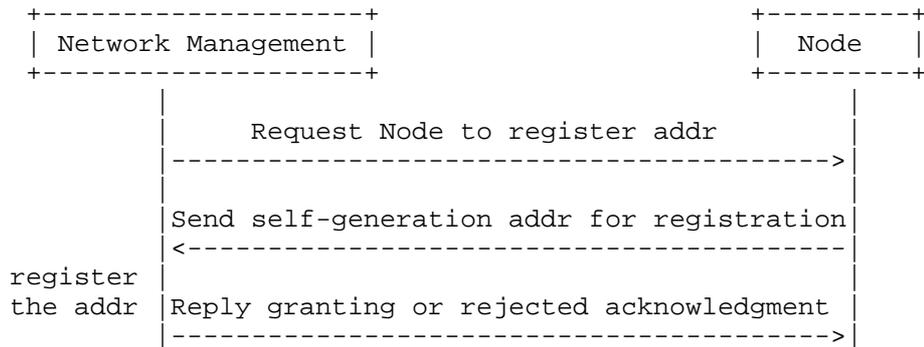


Figure 1: address registration procedure

3.2. Propagating the Registration Request

In order to indicate or force the nodes with self-generated addresses to register their addresses and the appointed address registration server, a new request option needs to be defined.

There are more than one mechanisms in which configuration parameters could be pushed to the end hosts. The address registration request option can be carried in Router Advertisement. In the DHCPv6 managed network, it can also be carried in DHCPv6 messages.

By receiving attendant of the address registration request option, a node MUST register its self-generated addresses, if there are any, to the appointed registration server. The option may be defined to include the default/enforced address registration server.

3.3. Address Registration Server and Protocol

In order to manage the address, an address registration server is needed with the support a set of address registration protocol.

The server should hold all registered addresses. It also needs to check whether the addresses meet the network address management policy, also performing a Duplicated Address Detect or checking the address does not use the Reserved IPv6 Interface Identifiers [RFC5453], etc. Its address data may be used by other network functions, such as DNS or ACL.

A set of address registration protocol need to at least support a basic information exchange: the node sends its address to the server and an acknowledgement is sent to the node.

3.3.1. Using DHCPv6 and DHCPv6 server

The current DHCPv6 protocol can be reused as the address registration protocol while a DHCPv6 server plays as address registration server.

The current DHCPv6 specification allows for a host to communicate a set of "preferred" addresses to the server by listing these addresses in IA options [RFC3315]. In order to response to registration requests, an acknowledgement DHCPv6 option should be defined. It is used to indicate whether the registration of an IPv6 address is accepted.

3.3.2. Defining a new address Registration Protocol

However, the address registration procedure using DHC protocol may conflict with the initial notional of DHC protocol. The DHC protocol was originally designed to push configuration information from the network management side to the hosts while the address registration procedure is collecting information from hosts to the network management side.

A new set of address registration protocol may be defined.

[Author notes for IETF discussion:] Any other existing protocol may be used for address registration purposes?

4. 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. These attacks may be prevented by using secure protocols, in Neighbor Discovery protocol case, Secure Neighbor Discovery (SEND, [RFC3971]); in DHCP case, Secure DHCP [I-D.ietf-dhc-secure-dhcpv6]; or other additional security mechanisms.

An attacker could generate IPv6 address registration requests in order to exhaust the server resources (or to impact on any other operation that depend on the registration of the address).

In the use case of DHCPv6, the address registration procedure is as vulnerable as all other mechanisms based on DHCPv6 to DOS attacks to the server. Proper use of DHCPv6 autoconfiguration facilities [RFC3315], such as AUTH option or Secure DHCP [I-D.jiang-dhc-secure-dhcpv6] can prevent these threats.

5. IANA Considerations

There is no IANA considerations.

6. Change Log [RFC Editor please remove]

draft-jiang-6man-addr-registration-req-00, original version, 2010-03-01

draft-jiang-6man-addr-registration-req-01, minor update, 2010-08-27

draft-jiang-6man-addr-registration-req-02, minor update, 2010-03-04

7. Acknowledgments

The authors would like to thank Cao Wei, Huawei for been involved in the early requirement identification and early discussion.

8. References

8.1. Normative References

- [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, P. Nikander, "SEcure Neighbor Discovery (SEND) ", RFC 3971, March 2005.
- [RFC3972] T. Aura, "Cryptographically Generated Address", RFC3972, March 2005.
- [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.
- [RFC5453] S. Krishnan, "Reserved IPv6 Interface Identifiers", RFC 4543, February 2009.

8.2. Informative References

- [I-D.ietf-dhc-secure-dhcpv6]
S. Jiang and S. Shen "Secure DHCPv6 Using CGAs", draft-ietf-dhc-secure-dhcpv6-02 (work in progress), December, 2010.

Author's Addresses

Sheng Jiang
Huawei Technologies Co., Ltd
Huawei Building, No.3 Xixi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Email: jiangsheng@huawei.com

Gang Chen
China Mobile
53A, Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China
Email: phdgang@gmail.com