Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 17, 2007

J. Jeong, Ed.
ETRI/University of Minnesota
S. Park
SAMSUNG Electronics
L. Beloeil
France Telecom R&D
S. Madanapalli
SAMSUNG ISO
May 16, 2007

IPv6 Router Advertisement Option for DNS Configuration
draft-jeong-dnsop-ipv6-dns-discovery-12.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies a new IPv6 Router Advertisement option to allow IPv6 routers to advertise DNS recursive server addresses to IPv6 hosts.

Table of Contents

1. Introduction

Neighbor Discovery (ND) for IP Version 6 and IPv6 Stateless Address Autoconfiguration provide ways to configure either fixed or mobile nodes with one or more IPv6 addresses, default routes and some other parameters [2][3]. To support the access to additional services in the Internet that are identified by a DNS name, such as a web server, the configuration of at least one recursive DNS server is also needed for DNS name resolution.

It is infeasible for nomadic hosts, such as laptops, to have to enter a DNS resolver each time they connect to a different wireless LAN (WLAN) such as IEEE 802.11 a/b/g [12]-[15]. Normally, DHCP [6]-[8] is used to locate such resolvers. This document provides an alternate, experimental mechanism which uses a new IPv6 Router Advertisement (RA) option to allow IPv6 routers to advertise DNS recursive server addresses to IPv6 hosts.

1.1. Applicability Statements

The only standards-track DNS configuration mechanism in the IETF is DHCP, and its support in hosts and routers is necessary for reasons of interoperability.

RA-based DNS configuration is a useful, optional alternative in networks where an IPv6 host's address is autoconfigured through IPv6 stateless address autoconfiguration, and where the delays in acquiring server addresses and communicating with the servers are critical. RA-based DNS configuration allows the host to acquire the nearest server addresses on every link. Furthermore, it learns these addresses from the same RA message that provides configuration information for the link, thereby avoiding an additional protocol run. This can be beneficial in some mobile environments, such as with Mobile IPv6 [10].

The advantages and disadvantages of the RA-based approach are discussed in [9] along with other approaches, such as the DHCP and Well-known anycast addresses approaches.

1.2. Coexistence of RDNSS Option and DHCP Option

The RDNSS option and DHCP option can be used together [9]. To order the RA and DHCP approaches, the O (Other stateful configuration) flag can be used in the RA message [2]. If no RDNSS option is included, an IPv6 host may perform DNS configuration through DHCPv6 [6]-[8] regardless of whether the O flag is set or not.

2. Definitions

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 [1].

3. Terminology

This document uses the terminology described in [2] and [3]. In addition, four new terms are defined below:

- Recursive DNS Server (RDNSS): Server which provides a recursive DNS resolution service for translating domain names into IP addresses as defined in [4] and [5].

- RDNSS Option: IPv6 RA Option to deliver the RDNSS information to the IPv6 hosts [2].

- DNS Server List: Data structure for managing DNS Server Information existing in IPv6 protocol stack in addition to Neighbor Cache and Destination Cache for Neighbor Discovery [2].

- Resolver Repository: Configuration repository with RDNSS addresses which a DNS resolver on the host uses for DNS name resolution, such as Unix resolver file (i.e., /etc/resolv.conf) and Windows registry.

4. Overview

This document defines a new ND option called RDNSS option that contains the addresses of recursive DNS servers. Existing ND transport mechanisms (i.e., advertisements and solicitations) are used. This works in the same way that hosts learn about routers and prefixes. An IPv6 host can configure the IPv6 addresses of one or more RDNSSes via RA message periodically sent by router or solicited by a Router Solicitation (RS).

Through the RDNSS option along with the prefix information option based on the ND protocol ([2] and [3]), an IPv6 host can perform its network configuration of its IPv6 address and RDNSS simultaneously without needing a separate message exchange for the RDNSS information. The RA option for RDNSS can be used on any network that supports the use of ND.

This approach requires RDNSS information to be configured in the routers sending the advertisements. The configuration of RDNSS

addresses in the routers can be done by manual configuration. The automatic configuration or redistribution of RDNSS information is possible by running a DHCPv6 client running on the router [6]-[8]. The automatic configuration of RDNSS addresses in the routers is out of scope in this document.

5. Neighbor Discovery Extension

The IPv6 DNS configuration mechanism in this document needs a new ND option in Neighbor Discovery, Recursive DNS Server (RDNSS) option.

5.1. Recursive DNS Server Option

RDNSS option contains one or more IPv6 addresses of recursive DNS servers. All of the addresses share the same lifetime value. If it is desirable to have different lifetime values, multiple RDNSS options can be used. Figure 1 shows the format of RDNSS option.

```
  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    |           Reserved            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                           Lifetime                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 :            Addresses of IPv6 Recursive DNS Servers            :
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Recursive DNS Server (RDNSS) Option Format

Fields:

Type   8-bit identifier of the option type (TBD: IANA)

Option Name	Type
RDNSS option	(TBD)

Length   8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The minimum value is 0x03 if one IPv6 address is contained in the option. Every additional RDNSS address increases the length by 0x02. The length field is used by the receiver to determine the number of IPv6 addresses in the option.

Lifetime 32-bit unsigned integer. The maximum time, in seconds (relative to the time the packet is sent), over which this RDNSS MAY be used for name resolution. Hosts MAY send a Router Solicitation to ensure the RDNSS information is fresh before the interval expires. In order to provide fixed hosts with the stable DNS service and allow mobile hosts to prefer local RDNSSes to remote RDNSSes, the value of lifetime should be at least as long as the Maximum RA Interval (MaxRtrAdvInterval) in RFC 2461, and be at most as long as two times MaxRtrAdvInterval; Lifetime SHOULD be bounded as follows:
MaxRtrAdvInterval<=Lifetime<=2*MaxRtrAdvInterval.
A value of all one bits (0xffffffff) represents infinity. A value of zero means that the RDNSS MUST no longer be used.

Addresses of IPv6 Recursive DNS Servers
One or more 128-bit IPv6 addresses of the recursive DNS servers. The number of addresses is determined by the Length field. That is, the number of addresses is equal to (Length - 1) / 2.

5.2. Procedure of DNS Configuration

The procedure of DNS configuration through RDNSS option is the same as any other ND option [2].

5.2.1. Procedure in IPv6 Host

When an IPv6 host receives RDNSS option through RA, it checks whether the option is valid;

- o If the RDNSS option is present, the host SHOULD copy the option's value into the DNS Server List and the Resolver Repository as long as the value of Length field is greater than or equal to the minimum value (0x03). The host MAY ignore additional RDNSS addresses within an RDNSS option and/or additional RDNSS options within an RA when it has gathered a sufficient number of RDNSSes.

- o If the RDNSS option is present but invalid (e.g., it has the length less than 0x03), the host SHOULD discard the option.

6. Implementation Considerations

Note

This non-normative section gives some hints for implementing the processing of RDNSS option in IPv6 host.

For the configuration and management of RDNSS information, the advertised RDNSS addresses can be stored and managed in both the DNS Server List and the Resolver Repository.

In environments where the RDNSS information is stored in user space and ND runs in the kernel, it is necessary to synchronize the DNS Server List for RDNSSes in kernel space and the Resolver Repository in user space. For the synchronization, the implementation where ND works in the kernel should provide the write operation for updating RDNSS information from the kernel to the Resolver Repository. One simple approach to perform this is to have a daemon around (or a program that is called at the defined intervals) that keeps monitoring the lifetime of RDNSSes all the time. Whenever there is an expired entry in the DNS Server List, the daemon can delete the corresponding entry from the Resolver Repository.

6.1. DNS Server List Management

The kernel or user-space process (depending on where RAs are processed) should maintain a data structure called DNS Server List which keeps the list of RDNSSes. Each entry of DNS Server List consists of RDNSS address and Expiration-time as follows:

- o RDNSS address: IPv6 address of Recursive DNS Server which is available for recursive DNS resolution service in the network advertising the RDNSS option; such a network is called site in this document.

- o Expiration-time: Expiration time field giving the time when this entry becomes invalid. Expiration-time is set to the value of Lifetime field of RDNSS option plus the current system time. Whenever a new RDNSS option with the same address is received, this field is updated to have a new expiration time. When Expiration-time becomes less than the current system time, this entry is regared as expired.

Note

An RDNSS MUST be used only as long as both the RA router lifetime and

the RDNSS option lifetime have not expired. The reason is that the RDNSS may not be currently reachable or may not provide service to the host's current address (e.g., due to the network ingress filtering [16][17]).

6.2. Synchronization between DNS Server List and Resolver Repository

When an IPv6 host receives the information of multiple RDNSSes within a site through an RA message with RDNSS option(s), it stores the RDNSS addresses in order into both the DNS Server List and the Resolver Repository. The processing of the RDNSS option included in RA message is as follows:

Step (a): Receive and parse RDNSS option(s). For the RDNSS addresses in each RDNSS option, perform Step (b) through Step (d). Note that Step (e) is performed whenever an entry expires in the DNS Server List.

Step (b): For each RDNSS address, check the following: If the RDNSS address already exists in the DNS Server List and the RDNSS option's "Lifetime" field is set to zero, delete the corresponding RDNSS entry from both the DNS Server List and the Resolver Repository in order to let the RDNSS be not used any more for certain reasons in network management, e.g., the breakdown of the RDNSS or a renumbering situation. The processing of this RDNSS address is finished here. Otherwise, go to Step (c).

Step (c): For each RDNSS address, if it already exists in the DNS Server List, then just update the value of "Expiration-time" field to have a new expiration time with the RDNSS option's "Lifetime" field and the current system time. Otherwise, go to Step (d).

Step (d): For each RDNSS address, if it does not exist in the DNS Server List, register the RDNSS address and lifetime with the DNS Server List and then insert the RDNSS address in front of the Resolver Repository. In the case where the data structure for the DNS Server List is full of RDNSS entries, delete from the DNS Server List the entry with the smallest expiration time that will expire first. The corresponding RDNSS address is also deleted from the Resolver Repository. In the order in the RDNSS option, position the newly added RDNSS addresses in the front of the Resolver Repository so that the RDNSS addresses may be preferred according to their order in the RDNSS option for the DNS name resolution. The processing of these RDNSS addresses is finished here. Note that, in the case where there are several routers advertising RDNSS option(s) in a subnet, the RDNSSes announced lately are more preferred.

Step (e): Delete each expired entry from DNS Server List and the RDNSS address corresponding to the entry from the Resolver Repository.

7. Security Considerations

The security of RA option for RDNSS might be worse than ND protocol security [2]. However, any new vulnerability is not known yet in this RA option. In this context, it can be claimed that the vulnerability of ND is not worse and is a subset of the attacks that any node attached to a LAN can do independently of ND. A malicious node on a LAN can promiscuously receive packets for any router's MAC address and send packets with the router's MAC address as the source MAC address in the L2 header. As a result, the L2 switches send packets addressed to the router to the malicious node. Also, this attack can send redirects that tell the hosts to send their traffic somewhere else. The malicious node can send unsolicited RA or NA replies, answer RS or NS requests, etc. Also, an attacker could configure a host to send out RA with a fraudulent RDNSS address, which is presumably an easier avenue of attack than becoming a rogue router and having to process all traffic for the subnet. It is necessary to disable the RA RDNSS option in both routers and clients administratively to avoid this problem. All of this can be done independently of implementing ND. Therefore, it can be claimed that the RA option for RDNSS has vulnerabilities similar to those existing in current mechanisms.

If Secure Neighbor Discovery (SEND) protocol is used as the security mechanism for ND, all the ND options including RDNSS option are also automatically included in the signatures [11], so the RDNSS transport is integrity-protected. However, since any valid SEND node can still insert RDNSS options, SEND cannot verify who is or is not authorized to send the options.

8. IANA Considerations

The IANA is requested to assign a new IPv6 Neighbor Discovery Option type for the RDNSS option defined in this document.

Option Name	Type
RDNSS option	(TBD)

The IANA registry for these options is:

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

9. Acknowledgements

This draft has greatly benefited from inputs by Robert Hinden, Pekka Savola, Iljitsch van Beijnum, Brian Haberman and Tim Chown. The authors appreciate their contribution.

10. References

10.1. Normative References

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

[2] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[3] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

10.2. Informative References

[4] Mockapetris, P., "Domain Names - Concepts and Facilities", RFC 1034, November 1987.

[5] Mockapetris, P., "Domain Names - Implementation and Specification", RFC 1035, November 1987.

[6] Droms, R., Ed., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[7] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[8] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[9] Jeong, J., Ed., "IPv6 Host Configuration of DNS Server Information Approaches", RFC 4339, February 2006.

[10] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[11] Arkko, J., Ed., "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[12] ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access

Control (MAC) and Physical Layer (PHY) Specifications", March 1999.

[13] IEEE Std 802.11a, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHZ Band", September 1999.

[14] IEEE Std 802.11b, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band", September 1999.

[15] IEEE P802.11g/D8.2, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher Data Rate Extension in the 2.4 GHz Band", April 2003.

[16] Damas, J. and F. Neves, "Preventing Use of Nameservers in Reflector Attacks", draft-ietf-dnsop-reflectors-are-evil-03.txt (Work in Progress), February 2007.

[17] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

Authors' Addresses

Jaehoon Paul Jeong (editor)
ETRI/Department of Computer Science and Engineering
University of Minnesota
117 Pleasant Street SE
Minneapolis, MN 55455
USA

Phone: +1 651 587 7774
Fax: +1 612 625 0572
Email: jjeong@cs.umn.edu
URI: http://www.cs.umn.edu/~jjeong/

Soohong Daniel Park
Mobile Platform Laboratory
SAMSUNG Electronics
416 Maetan-3dong, Yeongtong-Gu
Suwon, Gyeonggi-Do 443-742
Korea

Phone: +82 31 200 4508
Email: soohong.park@samsung.com

Luc Beloeil
France Telecom R&D
42, rue des coutures
BP 6243
14066 CAEN Cedex 4
France

Phone: +33 02 3175 9391
Email: luc.beloeil@francetelecom.com

Syam Madanapalli
SAMSUNG India Software Operations
J. P. Techno Park, 3/1
Millers Road
Bangalore 560052
India

Phone: +91 80 51197777
Email: smadanapalli@gmail.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).