Network Working Group
Internet-Draft
Obsoletes: 5006 (if approved)
Intended status: Standards Track
Expires: March 12, 2011

J. Jeong
Brocade/ETRI
S. Park
SAMSUNG Electronics
L. Beloeil
France Telecom R&D
S. Madanapalli
Ordyn Technologies

September 8, 2010

IPv6 Router Advertisement Options for DNS Configuration
draft-ietf-6man-dns-options-bis-08

Abstract

This document specifies IPv6 Router Advertisement options to allow IPv6 routers to advertise a list of DNS recursive server addresses and a DNS search list to IPv6 hosts.

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on March 12, 2011.

Copyright Notice

Table of Contents

1. Introduction

The purpose of this document is to standardize an IPv6 Router Advertisement (RA) option for DNS Recursive Server Addresses used for the DNS name resolution in IPv6 hosts. This RA option was specified in an earlier experimental specification [RFC5006]. This document is also to define a new RA option for Domain Name Search Lists for an enhanced DNS configuration. Thus, this document obsoleted [RFC5006] defining only the RA option for DNS Recursive Server Addresses.

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 routers and some other parameters [RFC4861][RFC4862]. Most Internet services are identified by using a DNS name. The two RA options defined in this document provide the DNS information needed for an IPv6 host to reach Internet services.

It is infeasible to manually configure nomadic hosts each time they connect to a different network. While a one-time static configuration is possible, it is generally not desirable on general-purpose hosts such as laptops. For instance, locally defined name spaces would not be available to the host if it were to run its own name server software directly connected to the global DNS.

The DNS information can also be provided through DHCP [RFC3315][RFC3736][RFC3646]. However, the access to DNS is a fundamental requirement for almost all hosts, so IPv6 stateless autoconfiguration cannot stand on its own as an alternative deployment model in any practical network without any support for DNS configuration.

These issues are not pressing in dual stack networks as long as a DNS server is available on the IPv4 side, but become more critical with the deployment of IPv6-only networks. As a result, this document defines a mechanism based on IPv6 RA options to allow IPv6 hosts to perform the automatic DNS configuration.

1.1. Applicability Statements

RA-based DNS configuration is a useful alternative in networks where an IPv6 host's address is autoconfigured through IPv6 stateless address autoconfiguration, and where there is either no DHCPv6 infrastructure at all or some hosts do not have a DHCPv6 client. The intention is to enable the full configuration of basic networking information for hosts without requiring DHCPv6. However, when in many networks some additional information needs to be distributed, those networks are likely to employ DHCPv6. In these networks RA-

based DNS configuration may not be needed.

RA-based DNS configuration allows an IPv6 host to acquire the DNS configuration (i.e., DNS recursive server addresses and DNS search list) for the link(s) to which the host is connected. Furthermore, the host learns this DNS configuration from the same RA message that provides configuration information for the link, thereby avoiding also running DHCPv6.

The advantages and disadvantages of the RA-based approach are discussed in [RFC4339] along with other approaches, such as the DHCP and well-known anycast addresses approaches.

1.2. Coexistence of RA Options and DHCP Options for DNS Configuration

Two protocols exist to configure the DNS information on a host, the Router Advertisement options described in this document and the DHCPv6 options described in [RFC3646]. They can be used together. The rules governing the decision to use stateful configuration mechanisms are specified in [RFC4861]. Hosts conforming to this specification MUST extract DNS information from Router Advertisement messages, unless static DNS configuration has been specified by the user. If there is DNS information available from multiple Router Advertisements and/or from DHCP, the host MUST maintain an ordered list of this information as specified in Section 5.3.1.

2. Requirements Language

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. Terminology

This document uses the terminology described in [RFC4861] and [RFC4862]. 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 [RFC1034] and [RFC1035].

- RDNSS Option: IPv6 RA option to deliver the RDNSS information to IPv6 hosts [RFC4861].

- DNS Search List (DNSSL): The list of DNS suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names.

- DNSSL Option: IPv6 RA option to deliver the DNSSL information to IPv6 hosts.

- DNS Repository: Two data structures for managing DNS Configuration Information in the IPv6 protocol stack in addition to Neighbor Cache and Destination Cache for Neighbor Discovery [RFC4861]. The first data structure is the DNS Server List for RDNSS addresses and the second is the DNS Search List for DNS search domain names.

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

4. Overview

This document standardizes the ND option called the RDNSS option defined in [RFC5006] that contains the addresses of recursive DNS servers. This document also defines a new ND option called the DNSSL option for Domain Search List. This is to maintain parity with the DHCPv6 options and to ensure that there is necessary functionality to determine the search domains.

The existing ND message (i.e., Router Advertisement) is used to carry this information. An IPv6 host can configure the IPv6 addresses of one or more RDNSSes via RA messages. Through the RDNSS and DNSSL options, along with the prefix information option based on the ND protocol ([RFC4861] and [RFC4862]), an IPv6 host can perform the network configuration of its IPv6 address and the DNS information simultaneously without needing DHCPv6 for the DNS configuration. The RA options for RDNSS and DNSSL can be used on any network that supports the use of ND.

This approach requires the manual configuration or other automatic mechanisms (e.g., DHCPv6 or vendor proprietary configuration mechanisms) to configure the DNS information in routers sending the advertisements. The automatic configuration of RDNSS addresses and a DNS search list in routers is out of scope for this document.

5. Neighbor Discovery Extension

The IPv6 DNS configuration mechanism in this document needs two new ND options in Neighbor Discovery: (i) the Recursive DNS Server (RDNSS) option and (ii) the DNS Search List (DNSSL) option.

5.1. Recursive DNS Server Option

The 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 the RDNSS option.

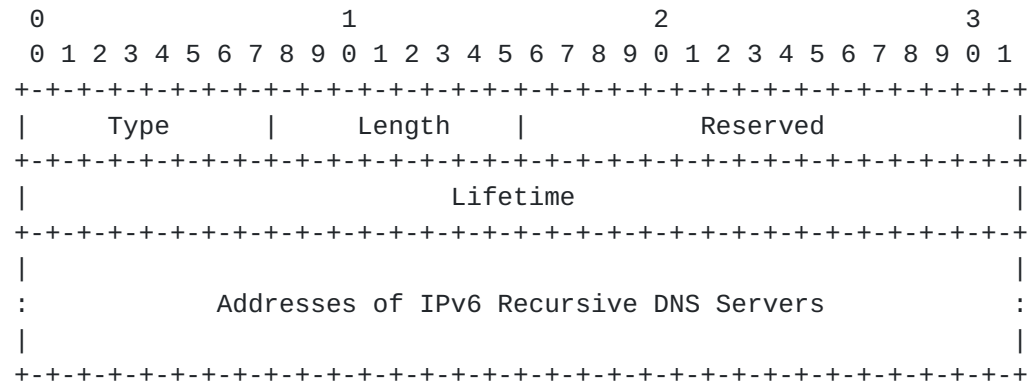

Figure 1: Recursive DNS Server (RDNSS) Option Format

Fields:

Type — 8-bit identifier of the RDNSS option type as assigned by the IANA: 25

Length — 8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The minimum value is 3 if one IPv6 address is contained in the option. Every additional RDNSS address increases the length by 2. 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 address 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 stable DNS service and allow mobile hosts to prefer local RDNSSes to remote RDNSSes, the value of Lifetime SHOULD be bounded as MaxRtrAdvInterval <= Lifetime <= 2*MaxRtrAdvInterval where MaxRtrAdvInterval is the Maximum RA Interval defined in [RFC4861]. A value of all one bits (0xffffffff) represents infinity. A value of zero means that the RDNSS address 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. DNS Search List Option

The DNSSL option contains one or more domain names of DNS suffixes. All of the domain names share the same lifetime value. If it is desirable to have different lifetime values, multiple DNSSL options can be used. Figure 2 shows the format of the DNSSL option.

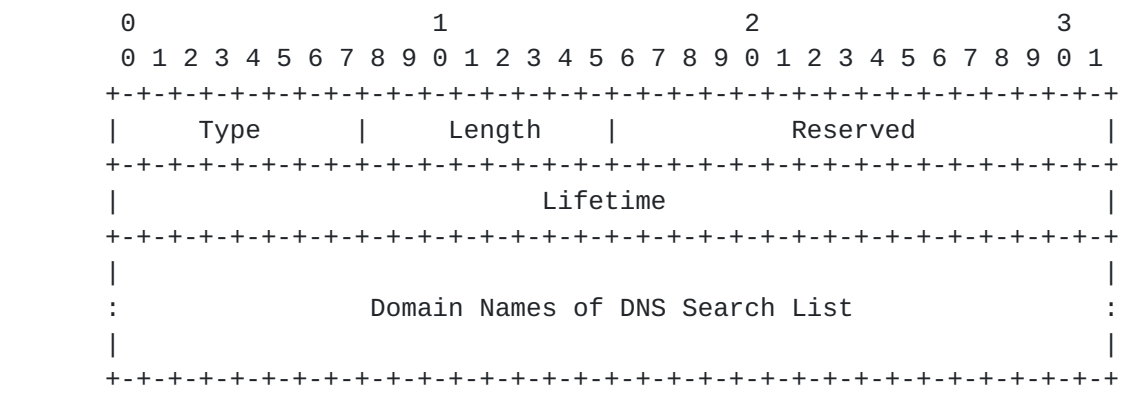

Figure 2: DNS Search List (DNSSL) Option Format

Fields:

Type — 8-bit identifier of the DNSSL option type as assigned by the IANA: (TBD)

Length — 8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The minimum value is 2 if at least one domain name is contained in the option. The Length field is set to a multiple of 8 octets to accommodate all the domain names in the field of Domain Names of DNS Search List.

Lifetime — 32-bit unsigned integer. The maximum time, in seconds (relative to the time the packet is sent), over which this DNSSL domain name MAY be used for name resolution. The Lifetime value has the same semantics as with RDNSS option. That is, 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 DNSSL domain name MUST no longer be used.

Domain Names of DNS Search List
One or more domain names of DNS search list that MUST be encoded using the technique described in Section 3.1 of [RFC1035]. By this technique, each domain name is represented as a sequence of labels ending in a zero octet, defined as domain name representation. For more than one domain name, the corresponding domain name representations are concatenated as they are. Note that for the simple decoding, the domain names MUST NOT be encoded in a compressed form, as described in Section 4.1.4 of [RFC1035]. Because the size of this field MUST be a multiple of 8 octets, for the minimum multiple including the domain name representations, the remaining octets other than the encoding parts of the domain name representations MUST be padded with zeros.

Note: An RDNSS address or a DNSSL domain name MUST be used only as long as both the RA router lifetime (advertised by a Router Advertisement message [RFC4861]) and the corresponding option lifetime have not expired. The reason is that in the current network to which an IPv6 host is connected, the RDNSS may not be currently reachable, that the DNSSL domain name is not valid any more, or that these options do not provide service to the host's current address (e.g., due to network ingress filtering [RFC2827][RFC5358]).

5.3. Procedure of DNS Configuration

The procedure of DNS configuration through the RDNSS and DNSSL options is the same as with any other ND option [RFC4861].

5.3.1. Procedure in IPv6 Host

When an IPv6 host receives DNS options (i.e., RDNSS option and DNSSL option) through RA messages, it processes the options as follows:

- The validity of DNS options is checked with the Length field; that is, the value of the Length field in the RDNSS option is greater than or equal to the minimum value (3) and also the value of the Length field in the DNSSL option is greater than or equal to the minimum value (2).

- If the DNS options are valid, the host SHOULD copy the values of the options into the DNS Repository and the Resolver Repository in order. Otherwise, the host MUST discard the options. Refer to Section 6 for the detailed procedure.

When the IPv6 host has gathered a sufficient number (e.g., three) of RDNSS addresses (or DNS search domain names), it SHOULD maintain RDNSS addresses (or DNS search domain names) by the sufficient number such that the latest received RDNSS or DNSSL is more preferred to the old ones; that is, when the number of RDNSS addresses (or DNS search domain names) is already the sufficient number, the new one replaces the old one that will expire first in terms of Lifetime. As an exceptional case, if the received RDNSS addresses (or DNS search domain names) already exist in the IPv6 host, their Lifetime fields update their expiration time, that is, when the corresponding DNS information expires in the IPv6 host; note that when the Lifetime field has zero, the corresponding RDNSS (or DNS search domain name) is deleted from the IPv6 host. Except for this update, the IPv6 host SHOULD ignore other RDNSS addresses (or DNS search domain names) within an RDNSS (or a DNSSL) option and/or additional RDNSS (or DNSSL) options within an RA. Refer to Section 6 for the detailed procedure. Note that the sufficient number is a system parameter, so it can be determined by a local policy. Also, separate parameters can be specified for the sufficient number of RDNSS addresses and that of DNS search domain names, respectively. In this document, three is RECOMMENDED as a sufficient number considering both the robust DNS query and the reasonably time-bounded recognition of the unreachability of DNS servers.

In the case where the DNS options of RDNSS and DNSSL can be obtained from multiple sources, such as RA and DHCP, the IPv6 host SHOULD keep some DNS options from all sources. Unless explicitly specified for the discovery mechanism, the exact number of addresses and domain names to keep is a matter of local policy and implementation choice. However, it is RECOMMENDED that at least three RDNSS addresses (or DNSSL domain names) can be stored from at least two different sources. The DNS options from Router Advertisements and DHCP SHOULD be stored into DNS Repository and Resolver Repository so that information from DHCP appears there first and therefore takes precedence. Thus, the DNS information from DHCP takes precedence over that from RA for DNS queries. On the other hand, for DNS options announced by RA, if some RAs use the Secure Neighbor Discovery (SEND) protocol [RFC3971] for RA security, they MUST be preferred over those which do not use SEND. Refer to Section 7 for the detailed discussion on SEND for RA DNS options.

5.3.2. Warnings for DNS Options Configuration

There are two warnings for DNS options configuration: (i) warning for multiple sources of DNS options and (ii) warning for multiple network interfaces. First, in the case of multiple sources for DNS options (e.g., RA and DHCP), an IPv6 host can configure its IP addresses from these sources. In this case, it is not possible to control how the host uses DNS information and what source addresses it uses to send DNS queries. As a result, configurations where different information is provided by different sources may lead to problems. Therefore, the network administrator needs to configure DNS options in multiple sources in order to prevent such problems from happening.

Second, if different DNS information is provided on different network interfaces, this can lead to inconsistent behavior. The IETF is working on solving this problem for both DNS and other information obtained by multiple interfaces [ID-mif-problem][ID-mif-practice].

6. Implementation Considerations

Note: This non-normative section gives some hints for implementing the processing of the RDNSS and DNSSL options in an IPv6 host.

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

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

6.1. DNS Repository Management

For DNS repository management, the kernel or user-space process (depending on where RAs are processed) should maintain two data structures: (i) DNS Server List that keeps the list of RDNSS addresses and (ii) DNS Search List that keeps the list of DNS search domain names. Each entry in these two lists consists of a pair of an RDNSS address (or DNSSL domain name) and Expiration-time as follows:

- RDNSS address for DNS Server List: IPv6 address of the Recursive DNS Server, which is available for recursive DNS resolution service in the network advertising the RDNSS option.

- DNSSL domain name for DNS Search List: DNS suffix domain names, which is used to perform DNS query searches for short, unqualified domain names in the network advertising the DNSSL option.

- Expiration-time for DNS Server List or DNS Search List: The time when this entry becomes invalid. Expiration-time is set to the value of the Lifetime field of the RDNSS option or DNSSL option plus the current system time. Whenever a new RDNSS option with the same address (or DNSSL option with the same domain name) is received on the same interface as a previous RDNSS option (or DNSSL option), this field is updated to have a new expiration time. When Expiration-time becomes less than the current system time, this entry is regarded as expired.

6.2. Synchronization between DNS Server List and Resolver Repository

When an IPv6 host receives the information of multiple RDNSS addresses within a network (e.g., campus network and company network) 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 consists of (i) the processing of RDNSS option(s) included in an RA message and (ii) the handling of expired RDNSSes. The processing of RDNSS option(s) is as follows:

Step (a): Receive and parse the RDNSS option(s). For the RDNSS addresses in each RDNSS option, perform Step (b) through Step (d).

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 prevent the RDNSS address from being used any more for certain reasons in network management, e.g., the termination of the RDNSS or a renumbering situation. That is, the RDNSS can resign from its DNS service because the machine running the RDNSS is out of service intentionally or unintentionally. Also, under the renumbering situation, the RDNSS's IPv6 address will be changed, so the previous RDNSS address should not be used any more. 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 the Expiration-time

field according to the procedure specified in the third bullet of Section 6.1. 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 (that is, has more RDNSSes than the sufficient number discussed in Section 5.3.1), delete from the DNS Server List the entry with the shortest expiration time (i.e., the entry that will expire first). The corresponding RDNSS address is also deleted from the Resolver Repository. For the ordering of RDNSS addresses in an RDNSS option, position the first RDNSS address in the RDNSS option as the first one in the Resolver Repository, the second RDNSS address in the option as the second one in the repository, and so on. This ordering allows the RDNSS addresses in the RDNSS option to be preferred according to their order in the RDNSS option for the DNS name resolution. The processing of these RDNSS addresses is finished here.

The handling of expired RDNSSes is as follows: Whenever an entry expires in the DNS Server List, the expired entry is deleted from the DNS Server List, and also the RDNSS address corresponding to the entry is deleted from the Resolver Repository.

6.3. Synchronization between DNS Search List and Resolver Repository

When an IPv6 host receives the information of multiple DNSSL domain names within a network (e.g., campus network and company network) through an RA message with DNSSL option(s), it stores the DNSSL domain names (in order) into both the DNS Search List and the Resolver Repository. The processing of the DNSSL consists of (i) the processing of DNSSL option(s) included in an RA message and (ii) the handling of expired DNSSLs. The processing of DNSSL option(s) is as follows:

Step (a): Receive and parse the DNSSL option(s). For the DNSSL domain names in each DNSSL option, perform Step (b) through Step (d).

Step (b): For each DNSSL domain name, check the following: If the DNSSL domain name already exists in the DNS Search List and the DNSSL option's Lifetime field is set to zero, delete the corresponding DNSSL entry from both the DNS Search List and the Resolver Repository in order to prevent the DNSSL domain name from being used any more for certain reasons in network management, e.g., the termination of the RDNSS or a renaming situation. That

is, the RDNSS can resign from its DNS service because the machine running the RDNSS is out of service intentionally or unintentionally. Also, under the renaming situation, the DNSSL domain names will be changed, so the previous domain names should not be used any more. The processing of this DNSSL domain name is finished here. Otherwise, go to Step (c).

Step (c): For each DNSSL domain name, if it already exists in the DNS Server List, then just update the value of the Expiration-time field according to the procedure specified in the third bullet of Section 6.1. Otherwise, go to Step (d).

Step (d): For each DNSSL domain name, if it does not exist in the DNS Search List, register the DNSSL domain name and lifetime with the DNS Search List and then insert the DNSSL domain name in front of the Resolver Repository. In the case where the data structure for the DNS Search List is full of DNSSL domain name entries (that is, has more DNSSL domain names than the sufficient number discussed in Section 5.3.1), delete from the DNS Server List the entry with the shortest expiration time (i.e., the entry that will expire first). The corresponding DNSSL domain name is also deleted from the Resolver Repository. For the ordering of DNSSL domain names in a DNSSL option, position the first DNSSL domain name in the DNSSL option as the first one in the Resolver Repository, the second DNSSL domain name in the option as the second one in the repository, and so on. This ordering allows the DNSSL domain names in the DNSSL option to be preferred according to their order in the DNSSL option for the DNS domain name used by the DNS query. The processing of these DNSSL domain name is finished here.

The handling of expired DNSSLs is as follows: Whenever an entry expires in the DNS Search List, the expired entry is deleted from the DNS Search List, and also the DNSSL domain name corresponding to the entry is deleted from the Resolver Repository.

7. Security Considerations

In this section, we analyze security threats related to DNS options and then suggest recommendations to cope with such security threats.

7.1. Security Threats

For RDNSS option, an attacker could send an RA with a fraudulent RDNSS address, misleading IPv6 hosts into contacting an unintended DNS server for DNS name resolution. Also, for DNSSL option, an attacker can let IPv6 hosts resolve a host name without DNS suffix into an unintended host's IP address with a fraudulent DNS search

list.

These attacks are similar to Neighbor Discovery attacks that use Redirect or Neighbor Advertisement messages to redirect traffic to individual addresses of malicious parties. That is, as a rogue router, 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, 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 Neighbor Advertisement (NA) replies, answer RS or Neighbor Solicitation (NS) requests, etc. Thus, the attacks related to RDNSS and DNSSL are similar to both Neighbor Discovery attacks and attacks against unauthenticated DHCP, as both can be used for both "wholesale" traffic redirection and more specific attacks.

However, the security of these RA options for DNS configuration does not affect ND protocol security [RFC4861]. This is because learning DNS information via the RA options cannot be worse than learning bad router information via the RA options. Therefore, 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.

7.2. Recommendations

The Secure Neighbor Discovery (SEND) protocol [RFC3971] is used as a security mechanism for ND. It is RECOMMENDED that ND use SEND to allow all the ND options including the RDNSS and DNSSL options to be automatically included in the signatures. Through SEND, the transport for the RA options is integrity-protected; that is, SEND can prevent the spoofing of these DNS options with signatures. Also, SEND enables an IPv6 host to verify that the sender of an RA is actually a router authorized to act as a router. However, since any valid SEND router can still insert RDNSS and DNSSL options, the current SEND cannot verify which one is or is not authorized to send the options. Thus, this verification of the authorized routers for ND options will be required. [ID-csi-send-cert] specifies the usage of extended key for the certificate deployed in SEND. This document defines the roles of routers (i.e., routers acting as proxy and address owner) and explains the authorization of the roles. The mechanism in this document can be extended to verify which routers are authorized to insert RDNSS and DNSSL options.

It is common for network devices such as switches to include mechanisms to block unauthorized ports from running a DHCPv6 server to provide protection from rogue DHCP servers. That means that an attacker on other ports cannot insert bogus DNS servers using DHCPv6.

The corresponding technique for network devices is RECOMMENDED to block rogue Router Advertisement messages including the RDNSS and DNSSL options from unauthorized nodes.

An attacker may provide a bogus DNS Search List option in order to cause the victim to send DNS queries to a specific DNS server when the victim queries non-fully qualified domain names. For this attack, the DNS resolver in IPv6 hosts can mitigate the vulnerability with the recommendations mentioned in [RFC1535], [RFC1536], and [RFC3646].

8. IANA Considerations

The RDNSS option defined in this document is using the IPv6 Neighbor Discovery Option type in RFC 5006 [RFC5006] assigned by the IANA as follows:

Option Name	Type
RDNSS option	25

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

Option Name	Type
DNSSL option	(TBD)

The IANA registry for these options is:

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

9. Acknowledgements

This document has greatly benefited from inputs by Robert Hinden, Pekka Savola, Iljitsch van Beijnum, Brian Haberman, Tim Chown, Erik Nordmark, Dan Wing, Jari Arkko, Ben Campbell, Vincent Roca, and Tony Cheneau. The authors sincerely appreciate their contributions.

10. References

10.1. Normative References

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

[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.

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", RFC 1035, November 1987.

10.2. Informative References

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", RFC 1034, November 1987.

[RFC3315] Droms, R., Ed., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC5006] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Option for DNS Configuration", RFC 5006, September 2007.

[RFC4339] Jeong, J., Ed., "IPv6 Host Configuration of DNS Server Information Approaches", RFC 4339, February 2006.

[RFC3971] Arkko, J., Ed., "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC5358] Damas, J. and F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks", BCP 140, RFC 5358, October 2008.

[RFC2827] 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.

[RFC1535] Gavron, E., "A Security Problem and Proposed Correction With Widely Deployed DNS Software", RFC 1535, October 1993.

[RFC1536] Kumar, A., Postel, J., Neuman, C., Danzig, P.,

and S. Miller, "Common DNS Implementation Errors and Suggested Fixes", RFC 1536, October 1993.

[ID-mif-problem] Blanchet, M. and P. Seite, "Multiple Interfaces Problem Statement", Work in Progress, August 2010.

[ID-mif-practice] Wasserman, M. and P. Seite, "Current Practices for Multiple Interface Hosts", Work in Progress, August 2010.

[ID-csi-send-cert] Gagliano, R., Krishnan, S., and A. Kukec, "Certificate profile and certificate management for SEND", Work in Progress, June 2010.

Appendix A. Changes from RFC 5006

The following changes were made from RFC 5006 "IPv6 Router Advertisement Option for DNS Configuration":

- Added DNS Search List (DNSSL) Option to support the advertisement of DNS suffixes used in the DNS search along with RDNSS Option in RFC 5006.
- Clarified the coexistence of RA options and DHCP options for DNS configuration.
- Modified the procedure in IPv6 host:
  - Clarified the procedure for DNS options in an IPv6 host.
  - Specified a sufficient number of RDNSS addresses or DNS search domain names as three.
  - Specified a way to deal with DNS options from multiple sources, such as RA and DHCP.
- Modified implementation considerations for DNSSL Option handling.
- Modified security considerations to consider more attack scenarios and the corresponding possible solutions.
- Modified IANA considerations to require another IPv6 Neighbor Discovery Option type for DNSSL option.

Authors' Addresses

Jaehoon Paul Jeong
Brocade Communications Systems/ETRI
6000 Nathan Ln N
Plymouth, MN 55442
USA

Phone: +1 763 268 7173
Fax: +1 763 268 6800
EMail: pjeong@brocade.com
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 2 40 44 97 40
EMail: luc.beloeil@orange-ftgroup.com

Syam Madanapalli
Ordyn Technologies
1st Floor, Creator Building, ITPL
Bangalore - 560066
India

Phone: +91-80-40383000
EMail: smadanapalli@gmail.com