Individual Submission
Internet Draft
Jaehoon Paul Jeong
ETRI
Soohong Daniel Park
SAMSUNG Electronics
Luc Beloeil
France Telecom R&D
Syam Madanapalli
SAMSUNG ISO
draft-jeong-dnsop-ipv6-dns-discovery-00.txt
Expires: January 2004
21 July 2003

IPv6 DNS Discovery based on Router Advertisement

Status of this Memo

Abstract

This document specifies the steps a node takes in deciding how to autoconfigure DNS information, such as the address of recursive DNS server and DNS zone suffix.

Conventions used in this document

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 RFC 2119 [2].

Table of Contents

1. Terminology

This memo uses the terminology described in [3][4]. In addition, a new term is defined below:

Recursive DNS Server (RDNSS) — A Recursive DNS Server is a name server that offers the recursive service of DNS name resolution.

2. Introduction

IPv6 stateless address autoconfiguration provides a way to autoconfigure either fixed or mobile nodes with one or more IPv6 addresses, default routes and some other parameters [3][4].

For the support of the various services in the Internet, such as web service, not only the configuration of IP address for network interface, but also that of at least one recursive DNS server for DNS name resolution is necessary.

This document defines the process of DNS discovery based on IPv6 Router Advertisement (RA) to find out DNS information, such as the address of recursive DNS server and DNS zone suffix within the local network.

3. Overview

An IPv6 host can autoconfigure DNS information via RA message sent periodically by router [5]-[7]. Namely, an IPv6 host can autoconfigure the IPv6 address of RDNSS for DNS name resolution through DNS Server option included in RA message. Also, through DNS Zone Suffix option in RA message, the IPv6 host can acquire the DNS zone suffix within the local network.

4. Neighbor Discovery Extension

The DNS discovery mechanism in this document needs two new RA options in Neighbor Discovery; (1) DNS Server option and (2) DNS Zone Suffix option that will introduce 4.1 and 4.2 sections.

4.1 DNS Server Option

DNS Server option contains the IPv6 address of the recursive DNS server. When advertising more than one DNS Server option, as many DNS Server options as DNS servers are included in an RA message. Figure 1 shows the format of DNS Server 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     | Pref |         Reserved        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                  IPv6 Address of DNS Server                   +
|                                                               |
+                                                               +
|                                                               |
```

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

    Figure 1. DNS Server Option Format
```

Fields:

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

                           Option Name              Type

                           DNS Server               (TBD)
```



```
  Length          8-bit unsigned integer.  The length of the
                  option (including the type and length fields)
                  in units of 8 octets.  The value 0 is invalid.
                  Nodes MUST silently discard an ND packet that
                  contains an option with length zero.

  Pref            The preference of a DNS server.  A 4 bit unsigned
                  integer.  A decimal value of 15 indicates the
                  highest preference.  A decimal value of 0
                  indicates that the DNS server can not be used.
                  The field can be used for load balancing of DNS
                  queries with multiple RDNSSes according to local
                  policy.

  Valid Lifetime  32-bit unsigned integer.  The maximum time, in
                  seconds, over which this DNS server is used for
                  name resolution.  Hosts should contact the source
                  of this information, router, before expiry of
                  this time interval.  A value of all one bits
                  (0xffffffff) represents infinity.

  IPv6 Address of DNS Server
                  Recursive DNS Server's address for DNS name
                  resolution.
```

"Pref"=0 SHOULD require a "Valid Lifetime"=0 because the corresponding DNS server SHOULD not be used any more.

4.2 DNS Zone Suffix Option

DNS Zone Suffix option contains the suffix of the DNS zone where the subnet is placed. When advertising more than one DNS Zone Suffix option, as many DNS Zone Suffix options as DNS zones are included in an RA message. Figure 2 shows the format of DNS Zone Suffix 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     | Pref |        Reserved         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                         DNS Zone Suffix                       ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2. DNS Zone Suffix Option Format

Fields:

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

Option Name	Type
DNS Zone Suffix	(TBD)

Length — 8-bit unsigned integer. The length of the option in units of 8 octets.

Pref — The preference of a DNS zone suffix. A 4 bit unsigned integer. A decimal value of 15 indicates the highest preference. A decimal value of 0 indicates that the DNS zone suffix can not be used. The field can be used for arranging DNS zone suffix according to local policy.

Valid Lifetime — 32-bit unsigned integer. The maximum time, in seconds, over which this DNS zone suffix is valid. Hosts should contact the source of this information, router, before expiry of this time interval. A value of all one bits (0xffffffff)

represents infinity.

DNS Zone Suffix
The DNS zone suffix of the domain where the subnet is placed. This field is comprised of a sequence of labels, where each label consists of a length octet followed by that number of octets. The suffix terminates with the zero length octet for the null label of the root. This field SHOULD be padded with zeroes to be the multiple of 8 octets.

5. Procedure of DNS Discovery

```
 IPv6 Host                         Router
      |            global              |
   (a)|(-------------RS-------------->)|
   (b)|<------RA w/ DNS options--------|
   (c)|       Processing of RA         |
   (d)|    Address Autoconfiguration   |
   (e)|(Stateful DNS Autoconfiguration)|
      |                                |
```

Figure 3. Procedure of DNS Discovery

Figure 3 shows the procedure of DNS Discovery on the basis of IPv6 RA message. The procedure consists of the following steps.

Step (a) : IPv6 Host sends RS (Router Solicitation) message to get RA message. It is optional.

Step (b) : For the RS message received from IPv6 Host, Router sends RA message, which contains prefix information option for the stateless address autoconfiguration and MAY contain DNS options for DNS information, namely the address of DNS server and DNS zone suffix. For DNS Zone Suffix option to be contained, DNS Server option SHOULD be contained ahead.

Step (c) : If there are DNS options, IPv6 Host processes the options and stores them in its DNS configuration file or database.

Step (d) : Through stateless or stateful address autoconfiguration, a

unique global IPv6 address is autoconfigured in the network interface of the IPv6 Host.

Step (e) : Unless DNS information is configured through RA message, the IPv6 Host MAY try to get DNS information through stateful mechanism, such as DHCPv6. In order to allow stateful protocol used for DNS discovery, O-bit (Other stateful configuration flag) within RA message SHOULD be set. When DNS information has been delivered through RA message, the DNS discovery by stateful protocol is skipped.

6. Autoconfiguration of DNS Information

The addresses of DNS servers are announced by DNS options in RA message. These addresses can be used for recursive DNS service providing DNS name resolution. The newly discovered DNS information, the RDNSS's address and DNS zone suffix, are stored in the configuration file for DNS resolver; i.e., /etc/resolv.conf in UNIX.

6.1 RDNSS Configuration and Selection

When an IPv6 host perceives multiple RDNSSes through RA message, it stores the RDNSS addresses in order into the configuration file which the resolver on the host uses for DNS name resolution on the basis of the value of "Pref" field in the DNS Server option. The following algorithm is simply based on the rule of selecting an RDNSS in the order from the most preferred RDNSS, provided that its preference value is not zero. The processing of the DNS Server option received in RA message by an IPv6 host is as follows:

The IPv6 host's operation is like below for each DNS Server option:

Step (a) : Receive and parse all DNS Server options.

Step (b) : Arrange the addresses of RDNSSes in a descending order, starting with the biggest value of "Pref" field of the DNS Server option and store them in the configuration file used by resolver for DNS name Resolution (DNS configuration).

Step (c) : For each DNS Server option, check the following: If the Value of "Pref" or "Valid Lifetime" field is set to zero,

exclude the corresponding RDNSS entry from the list of RDNSSes of DNS configuration in order to let the RDNSS not used any more.

Whenever the resolver on the host performs the name resolution, it refers to the address of RDNSS in order from the first RDNSS stored in DNS configuration.

In case that there are several routers advertising DNS information in a subnet, "Pref" field is used to arrange the information.

6.2 DNS Zone Suffix Configuration

DNS zone suffix is delivered as DNS Zone Suffix option via RA message from router. The processing of the DNS Zone Suffix option received in RA message by an IPv6 host is as follows:

Step (a) : Receive and parse all DNS Zone Suffix options.

Step (b) : Arrange the DNS zone suffix in a descending order, starting with the biggest value of "Pref" field of the DNS Zone Suffix option and store them in DNS configuration.

Step (c) : For each DNS Zone Suffix option, check the following: If the value of "Pref" or "Valid Lifetime" field is set to zero, exclude the corresponding DNS zone suffix from the list of DNS zone suffixes of DNS configuration in order to let the DNS zone suffix not used any more.

This DNS zone suffix MAY be used for forming IPv6 host's DNS name.

7. Applicability Statements

RA-based DNS discovery is efficient in many kinds of wireless networks where IPv6 address is autoconfigured by IPv6 stateless address autoconfiguration, such as SOHO, home network, HMIPv6 [8],

NEMO and MANET connected to the Internet. Especially, in the environments where DHCPv6 is difficult to adapt, RA-based DNS discovery is recommended.

8. Open Issues

There might be some issues regarding RA-based DNS discovery as follows:

- o How to optimize bandwidth on the link?
- o How to implement RA-based DNS discovery?
- o What about the use of "Pref" or "Valid Lifetime" field?
- o How to interact with stateful mechanism?
- o What about several routers on the same link that could advertise distinct parameters? (Multihoming considerations)

9. Security Considerations

This security is essentially related to Neighbor Discovery protocol security [3].

If someone wants to hijack correct RS message, they could send an RA message with incorrect DNS Server options and DNS Zone Suffix options to the originated host and they would take incorrect RA message through the above mechanism, which is unsafe processing. As described in [3], an IPv6 host can check the validity of NDP messages. If the NDP message includes an IP Authentication Header, the message can be authenticated. Security issues regarding the Neighbor Discovery protocol are being discussed in IETF SEND (Securing Neighbor Discovery) working group [9].

10. Copyright

11. Normative References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

[3] T. Narten, E. Nordmark and W. Simpson, "Neighbour Discovery for IP version 6", RFC 2461, December 1998.

[4] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC2462, December 1998.

12. Informative References

[5] Jaehoon Paul Jeong, Byungyeob Kim, Jungsoo Park and Hyoungjun Kim, "IPv6 Router Advertisement based DNS Autoconfiguration", draft-jeong-ipv6-ra-dns-autoconf-00.txt, April 2003.

[6] Luc Beloeil, "IPv6 Router Advertisement DNS resolver Option", draft-beloeil-ipv6-dns-resolver-option-01.txt, January 2003.

[7] Soohong Daniel Park and Syam Madanapalli, "IPv6 Extensions for DNS Plug and Play", draft-park-ipv6-extensions-dns-pnp-00.txt, April 2003.

[8] Jaehoon Paul Jeong, Jungsoo Park, Kyeongjin Lee and Hyoungjun Kim, "The Autoconfiguration of Recursive DNS Server and the Optimization of DNS Name Resolution in Hierarchical Mobile IPv6", draft-jeong-hmipv6-dns-optimization-01.txt, June 2003.

[9] J. Arkko, J. Kempf, B. Sommerfeld, B. Zill and P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ipsec-01.txt, June 2003.

13. Authors' Addresses

Jaehoon Paul Jeong
ETRI / PEC
161 Gajong-Dong, Yusong-Gu
Daejon 305-350
Korea

Phone: +82-42-860-1664
EMail: paul@etri.re.kr

Soohong Daniel Park
Mobile Platform Laboratory,
SAMSUNG Electronics
Korea

Phone: +82-31-200-3728
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
Network Systems Division,
SAMSUNG India Software Operations
India

Phone: +91-80-555-0555
EMail: syam@samsung.com