IPv6 Router Advertisement based DNS Autoconfiguration

Abstract
This document specifies the steps a node takes in deciding how to autoconfigure its domain name per interface in IP version 6 and the address of recursive DNS server. The autoconfiguration process includes a node’s creating a domain name for its global address, verifying the uniqueness of the name in the domain where it is placed and registering both the regular domain name and inverse domain name information of the node with DNS server automatically. Also, it autoconfigures the address of recursive DNS server for DNS name resolution.

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.

Table of Contents

1. Terminology ............................ 2
2. Introduction ............................. 2
3. Overview .................................. 3
4. Neighbor Discovery Extension - DNS Option Message Format .... 3
5. Autoconfiguration of Domain Name ........................... 5
   5.1 Generation of Domain Name ............... 7
   5.2 Verification of the Uniqueness of Domain Name .... 7
   5.3 Registration of Domain Name ............. 7
6. Autoconfiguration of Recursive DNS Server ....................... 7
   6.1 RDNSS Selection by IPv6 Node ............. 8
   6.2 Detection of RDNSS Failure ............... 8
7. Security Considerations ................................ 9
8. References .................................. 9
9. Authors’ Addresses .......................... 10

1. Terminology

This memo uses the terminology described in [3][4]. In addition, two new terms are defined below:

Duplicate Name Detection (DND)  A mechanism to verify the uniqueness of a domain name through DNS dynamic update.

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 [5] provides a way to autoconfigure either fixed or mobile nodes with one or more IPv6 addresses and default routes.

For the support of the various services in the Internet, such as web service, not only the configuration of IP address in network interface, but also that of the recursive DNS server for DNS name resolution are necessary [6][7][8]. Also, via the IPv6 autoconfiguration facility, the domain name for the autoconfigured IPv6 address needs to be autoconfigured in the node and registered with DNS server managing the domain where the node is placed.
This document defines the process for generating a domain name, verifying the uniqueness of the name through DND [3][9] and registering the domain name information with DNS server managing the zone of the domain through DNS dynamic update [3]. Also, it specifies the autoconfiguration of the IPv6 address(es) of recursive DNS server for DNS name resolution.

3. Overview

An IPv6 node can autoconfigure its domain name via IPv6 Router Advertisement (RA) based domain name autoconfiguration [4]. This automatic mechanism allows a node to generate its own domain name using a combination of locally available information and information advertised by routers. A router sends RA message advertising DNS zone suffix that includes the subnet(s) associated with a link and the address of DNS server managing the DNS zone. When a node receives RA message, it selects one of user identifiers configured within itself and then makes its domain name by combining its selected user identifier and the DNS zone suffix within RA message. The node SHOULD verify the uniqueness of the name through DND. If there is no duplication, the node registers the domain name information consisting of regular domain name and inverse domain name information with DNS server managing the zone of the domain through DNS dynamic update. Otherwise, it tries to make a new name with one of the other candidates of configured user identifiers and DNS zone suffix and then configure the name through the procedure of verifying the uniqueness of the name through DND again. In the absence of routers, a node can generate only local domain name with local zone "local" [10] and verifies the uniqueness of the name through DND [3][9]. If the name is unique, the node configures the name as its domain name. Otherwise, it tries to make a new name and configure the name through the procedure of verifying the uniqueness of the name again.

Also, a node can autoconfigure the IPv6 address of RDNSS for DNS name resolution through DNS option included in RA message.

4. Neighbor Discovery Extension - DNS Option Message Format

The DNS autoconfiguration mechanism in this document needs a new RA option in Neighbor Discovery like Figure 1 [4].
### DNS Option Message Format

![Figure 1. DNS Option Message Format](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>8-bit identifier of the type of option.</td>
</tr>
<tr>
<td><strong>Option Name</strong></td>
<td></td>
</tr>
<tr>
<td>Source Link-Layer Address</td>
<td>1</td>
</tr>
<tr>
<td>Link-Layer Address</td>
<td>2</td>
</tr>
<tr>
<td>Prefix Information</td>
<td>3</td>
</tr>
<tr>
<td>Redirected Header</td>
<td>4</td>
</tr>
<tr>
<td>MTU</td>
<td>5</td>
</tr>
<tr>
<td>DNS Information</td>
<td>(TBD)</td>
</tr>
</tbody>
</table>

**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 cannot be used.
A 1-bit autonomous DNS configuration flag. When set indicates that this DNS zone suffix can be used for stateless domain name autoconfiguration.

IPv6 Address of DNS Server
The IPv6 address of DNS server managing the domain which the DNS zone suffix indicates. The scope of the address SHOULD be global. The prefix of the address is /64. This address can be used as recursive DNS server’s address for DNS name resolution.

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.

When advertising more than one DNS option, as many DNS options as DNS servers are included in an RA message.

5. Autoconfiguration of Domain Name

IPv6 Node            Router               DNS Server
|    global    |            |               |
| (a)         | (----RS---->) |            |
| (b)         | <-----RA-----> |            |
| (c)         | ---DAD NS---> |            |
| (d)         | no NA       |            |
| (e)         | ------------------------> |
| (f)         | <------------------------> |
| (g)         | ------------------------> |
| (h)         | <------------------------> |
| (i)         | <------------------------> |
| (j)         | <------------------------> |

_Figure 2. Procedure of IPv6 Address and Domain Name Autoconfiguration_
Figure 2 shows the procedure of autoconfiguring a domain name as well as an IPv6 address in an IPv6 node [11][12]. The procedure consists of two phases. The first phase is the address autoconfiguration (step (a) through step (d)) and the second is the domain name autoconfiguration (step (e) through step (j)) as follows:

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

Step (b): For the RS message received from IPv6 Node, router sends RA message, which contains prefix option for the stateless address autoconfiguration and DNS option informing IPv6 nodes of the address of DNS server and DNS zone suffix.

Step (c): After making an IPv6 address, the IPv6 Node sends NS (Neighbor Solicitation) message for duplicate address detection (DAD).

Step (d): If there is no NA (Neighbor Advertisement) message for the NS message, the tentative address is unique in the subnet and it can be used as the IPv6 node's address.

Step (e): After autoconfiguring an IPv6 address, IPv6 Node makes a unique domain name with one of the candidates of user id and the DNS zone suffix announced by DNS option message. It sends DNS Server a dynamic update request message for verifying the uniqueness of the domain name through DNS dynamic update [3][9].

Step (f): DNS Server sends the IPv6 Node a dynamic update response message. If the response indicates the verified domain name is unique, the IPv6 Node performs the following step (g). Otherwise, It performs the previous step (e) again.

Step (g): IPv6 Node sends DNS Server a dynamic update request message for registering regular domain name information.

Step (h): DNS Server sends IPv6 Node a dynamic update response message indicating the successful registration of regular domain name information.

Step (i): IPv6 Node sends DNS Server a dynamic update request message for registering inverse domain name information.

Step (j): DNS Server sends IPv6 Node a dynamic update response message indicating the successful registration of inverse domain name information.
Some parts of the above steps MIGHT be tied together. Step (g) and step (i) can be merged in a single step. Also, step (h) and step (j) can be performed together.

5.1 Generation of Domain Name

The generation of domain name depends on the local policy. This document suggests an example of the naming schemes for the domain name generation.

The following procedure is based on user preferred identifiers, such as foo, foo1, foo2, etc. These user identifiers are stored in the configuration file for domain name autoconfiguration.

Step (a) : Node selects one unused user identifier in order from the list of user identifiers.

Step (b) : Node combines the user identifier with the advertised DNS zone suffix. When multiple DNS zone suffixes and DNS servers are known, node selects one unused DNS zone suffix in the descending order of "Pref" field from the list of DNS zone suffixes. When verifying and registering the domain name, node uses the DNS server corresponding to the DNS zone suffix.

As another example of generating a unique domain name, a domain name can be made with user identifier and a part of uniqueness-verified IP address [13].

5.2 Verification of the Uniqueness of Domain Name

Node verifies the uniqueness of a generated domain name through DND with the advertised DNS server. If there is a name conflict, the node generates a new domain name with unused user identifier and DNS zone suffix and then verifies the uniqueness of the name again. Otherwise, it registers the domain name information.

5.3 Registration of Domain Name

For the unique domain name, the node registers both the regular domain name and inverse domain name information of the node with DNS server sequentially as described in Figure 2.

6. Autoconfiguration of Recursive DNS Server

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. For the autoconfiguration of the domain name and recursive DNS server, the DNS zone suffix and RDNSS’s
address are stored in the configuration file for DNS resolver; i.e.,
/etc/resolv.conf in UNIX.

6.1 RDNSS Selection by IPv6 Node

When an IPv6 node perceives multiple RDNSSes through RA message, it
stores the RDNSS addresses in order into the configuration which the
resolver on the node uses for DNS name resolution on the basis of the
value of "Pref" field and the prefix of "IPv6 Address of DNS Server"
field in the DNS option. The following algorithm is simply based on
the rule of selecting the nearest possible RDNSS from the node by hop
count between the node and RDNSS, provided that its preference value
did not reach the maximum value of 15. When the distances are the
same, this algorithm uses the preference value to arrange the RDNSSes.
The IPv6 node operation is shown below:

Step (a) : Receive and parse all DNS options

Step (b) : Arrange the addresses of RDNSSes in an ascending order,
starting with the nearest RDNSS and store them in the configuration
for DNS name resolution used by resolver. (i.e., the longest prefix
matching between the "IPv6 Address of DNS Server" field and the
node’s IPv6 address MAY be used to decide the distance between the
node and RDNSS, how far away the node is from the RDNSS.)

Step (c) : For each RDNSS entry, check the following; If the value of
"Pref" field is set to zero, exclude the RDNSS entry from the list of
RDNSSes of the configuration for DNS name resolution.

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

6.2 Detection of RDNSS Failure

Router advertising DNS option message checks periodically if the
RDNSSes registered with the router are alive. The dynamic detection
of RDNSS failure in a router can be done by simply pinging the RDNSS
periodically (e.g., every ten seconds). If no response is received,
the router MAY try to aggressively ping the RDNSS for a short period
of time (e.g., once every 5 seconds for 15 seconds). Whenever the
router detects a failure of any RDNSS, it advertises the failure with
a new RA message including a DNS option of which "Pref" field has
zero for the RDNSS. When an IPv6 node receives the RA message, it
perceives that the RDNSS is out of work or the path to the RDNSS is
broken and excludes the RDNSS from the configuration for name
resolution. Also, If the node has its domain name associated with
the DNS zone suffix managed by the failed RDNSS, it MAY generate a
new domain name with DNS zone suffix managed by another live RDNSS and register the domain name information with the RDNSS.

7. Security Considerations

Ordinary DNS servers accept DNS dynamic update messages only from trusted nodes. In the current DNS, which lacks public-key infrastructure (PKI), the user of a host cannot be identified. In order to support the autoconfiguration of an unidentifiable host’s domain name, DNS dynamic update SHOULD allow the registration of not only the DNS resource record of "AAAA" type, but also that of "PTR" type for any host [14]. The former is for the regular domain name information and the latter for inverse domain name information.

Basically, since there is no mechanism to prevent denial-of-service (DoS) attack in DNS, the number of issued dynamic update messages from IPv6 nodes cannot be controlled by DNS server [14][15]. In order to minimize the effects of malicious or misconfigured registration requests, it is necessary for DNS server to control them. In Mobile IPv6, a correspondent node may silently discard some or all binding update messages when it is flooded with the messages [16]. Like this, DNS server MAY discard some or all DNS messages when being filled with the messages.

8. References


9. Authors’ Addresses

Jae-Hoon Jeong
ETRI / PEC
161 Gajong-Dong, Yusong-Gu
Daejon 305-350
Korea
Phone: +82 42 860 1664
EMail: paul@etri.re.kr

Byung-Yeob Kim
ETRI / PEC
161 Gajong-Dong, Yusong-Gu
Daejon 305-350
Korea

Jeong, Kim, Park, Kim Expires - October 2003 [Page 10]
Phone: +82 42 860 6627
EMail: skylane@etri.re.kr

Jung-Soo Park
ETRI / PEC
161 Gajong-Dong, Yusong-Gu
Daejon 305-350
Korea

Phone: +82 42 860 6514
EMail: pjs@etri.re.kr

Hyoung-Jun Kim
ETRI / PEC
161 Gajong-Dong, Yusong-Gu
Daejon 305-350
Korea

Phone: +82 42 860 6576
EMail: khj@etri.re.kr