Internet Engineering Task Force
Internet Draft
Expiration: December 2005
File: draft-yan-ipv6-ra-dns-01.txt

R. Yan
Alcatel Shanghai Bell
X. Duan
China Mobile

DNS update in IPv6 stateless configuration
<draft-yan-ipv6-ra-dns-01.txt>

June 25, 2005

Status of this Memo

Copyright Notice

Abstract

This document specifies a method to update domain name for IPv6 node whose address is configured using IPv6 stateless address configuration. It is implemented by defining a new option in Router Advertisement (RA) / Router Solicitation (RS) messages.

Table of Contents

1. Introduction

The Domain Name System [2], [3] provides a mechanism to associate addresses and other Internet infrastructure elements with hierarchically built domain names. For an IPv6 host, the general resource records maintained in DNS server are AAAA and PTR. The DNS update specification [6] describes a mechanism that enables DNS information to be updated over a network.

IPv6 stateless address autoconfiguration [7] allows a host to generate an unique IPv6 address by combining the prefix, advertised by the router, and the local interface identifier without the help of DHCPv6 server or DHCPv6 client.

To perform DNS update for the IPv6 host whose addresses are configured using IPv6 stateless address autoconfiguration, this document defined a new RS/RA option to transfer domain name information and negotiate who will perform DNS update between the host and the router.

2. Terminology

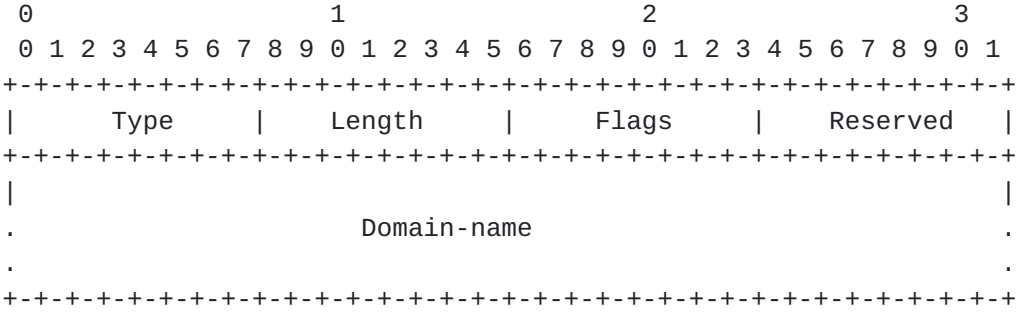
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

Familiarity with the DNS Update protocol [6], IPv6 Neighbour Discovery [8] , and Stateless Address Autoconfiguration [7] is assumed.

3. The Domain Name option

This section defines a new option in RS/RA message, called "Domain Name Option". The option contains a Domain-name, which is used to transfer domain information between IPv6 host and router, and a Flags, which IPv6 host and router use to negotiate who does DNS updates.

The Format of the Domain Name option is shown below:



Type:	8-bit identifier of the type of option(TBD)
Length:	The length of the option in units of 8 octets. The minimum length of the option is 1
Flags:	Flag bits used between host and router to negotiate who performs DNS updates
Domain-name:	The partial or fully qualified domain name

The Domain Name option MUST only appear in options field in Router Advertisement and Router Solicitation message.

When appear in RA message, it MUST be used together with Prefix options, to mean that it will be bound with the address(es) configured using those prefix(es).

When RS message includes Domain Name option, its source address MUST be generated using the prefix advertised by the previous RA message.

3.1 The Flags Field

The Format of the Flags field:

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|H|R|     RSV   |
+-+-+-+-+-+-+-+-+
```

If the router wants to take responsibility for the DNS updates for the host, it will set the "R" bit and clear the "H" bit when sending Domain Name option.

If the router wants host to take responsibility for the DNS updates on its own, it will set the "H" bit and clear "R" bit when sending Domain Name option.

Host MUST only send the Domain Name option in an RS message.

When a host sends the Domain Name option in RS message, it clears the "H" bit to indicate that it will not perform any DNS updates, and that it expects the router to perform DNS updates on its behalf.

If "R" bit is cleared, and "H" bit is set in RA message, but host have no ability to update DNS on its own, it can still request the router to perform DNS updates by setting both "R" and "H" bit in RS message.

The remaining bits in the Flags field are reserved for future assignment. IPv6 hosts and routers which send the Host FQDN option MUST set the RSV bits to 0, and they MUST ignore these bits.

3.2 The Domain Name Field

The Domain Name field of the option carries all or part of the FQDN of an IPv6 host. The data in the Domain Name field MUST appear in uncompressed DNS encoding as specified in [3].

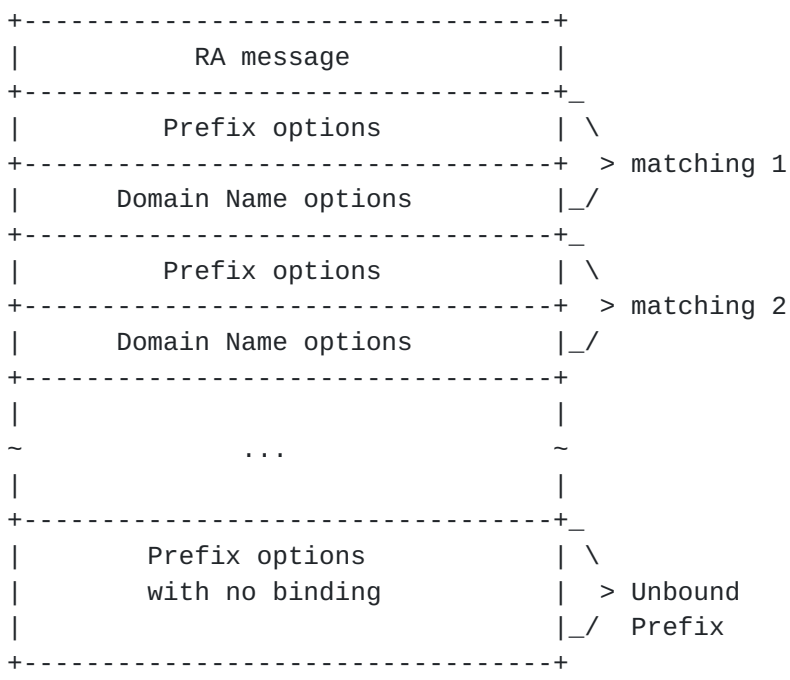
Domain Name field MUST be padded with 0 to 4-bytes alignment.

The router MUST send the zone suffix or NULL in Domain Name Field in Domain Name options. The host MUST send either FQDN or host name in Domain Name Field in Domain Name options.

4. Binding rule

As we know, the mapping between IPv6 address and FQDN is multiple-to-multiple. A host can register one FQDN with multiple IPv6 addresses, and also can register one IPv6 address with multiple FQDN. This document specifies a mechanism allowing the router to decide which prefix(es) is bound to which domain name. It is implemented by defining the sequence of the Domain Name option and Prefix option.

The Domain Name option MUST be used in combine with Prefix option as defined below:

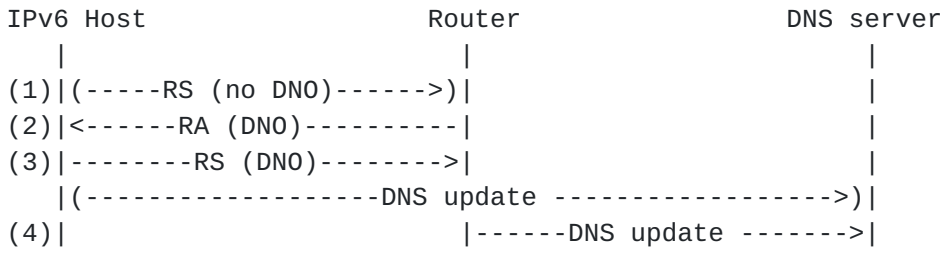


Domain Name options MUST be placed after one or more Prefix options, to mean that they are in a "matching". Hosts can choose to update the binding, whose IPv6 address and domain name are generated from the prefix and domain information in this matching. A typical case is that multiple Prefix options are bound with one Domain Name option.

Prefix option can be conveyed in RA message without binding with any Domain Name option. These "unbound" Prefix MUST be placed after the last Domain Name option.

5. Procedure of DNS update

The processing of Domain Name option is handled like any other ND options and would happen when an RA is received. The following figure shows an illustration of the procedure.



(DNO is abbreviation of Domain Name Option in the figure)

The procedure consists of the following steps:

Step (1) : IPv6 Host sends RS (Router Solicitation) message without the Domain Name option to get a RA message. It is optional.

Step (2) : For the RS message sent by IPv6 Host, router sends a RA message, which contains Prefix Information option(s) for stateless address autoconfiguration and Domain Name option(s) for DNS update.

Step (3) : IPv6 Host processes the RA message, if the result of the negotiation is router performs DNS update, IPv6 host will sends RS message to the router. The RS message contains a Domain Name option, with the source address set to the address generated using that prefix. Then, the process moves to Step (4). If the result of the negotiation is host performs DNS update, it will update its domain name directly with DNS server and finish the whole process.

Step (4) : The router sends DNS update message to the DNS server.

6. Requirements

The following describes the requirements of host and router that implements the Domain Name option.

6.1 Router requirements

Router MUST only include Domain Name options for the bindings in RA messages.

Router MAY include one or more Domain Name options in a single RA message.

Router MUST include Domain Name options as the rules defined in Section 5.

Router sends the Domain Name options with the "R" flags bit set and "H" flags bit clear, or, "R" flags bit clear and "H" flags bit set.

Router MAY be configured to update RR for the host, or simply request host to update on its own if there are no security requirement in local network. In both cases, router MUST be able to update RRs because some hosts may not have the ability to update DNS by itself.

There is no requirement that router stores the result of the DNS update when it update RR for the host. Host is required to check the DNS result by sending DNS query to the DNS server.

6.2 Host requirements

Host MUST only include Domain Name option in the Options field of Router Solicitation message.

Host MUST send RS message with Domain Name option after receiving prefix from a previous RA message.

Host MUST only send RS message including Domain Name option to the router if it wants router to take responsibility for the DNS updates. The destination address of this RS message is the unicast address of the router, and the source address MUST be set to the unicast address generated using prefix in a "matching".

Host sends the Domain Name option with the "H" flags bit set, the "R" flags bit clear, and with the desired partial domain name.

There is no requirement that the host send identical Domain Name option data several times. In particular, if a host has sent Domain Name options to the router, and the configuration of the host changes so that its notion of its domain name changes, it MAY update the

records in the DNS server by itself, or send the new name data in a Domain Name option to the router, requesting the router to update the records in DNS server.

Host MAY not send RS message with Domain Name option for DNS update if it do not need a domain name, e.g. a mobile user may not need a new domain name in foreign network. How to prevent host to update which DNS is the implementation issue.

7. DNS Update Conflicts

This document does not address how an IPv6 host or router prevents name conflicts.

Implementers of this work will need to consider how name conflicts will be prevented. One possible method may be that the router maintain a mapping table for all hosts in local network, and different router are configured with different domain name suffix.

8. Interaction with DHCPv6 and MIPv6

There may exist cases in which a host can get different global IPv6 address using both RA and DHCP, and the host may want to use a single domain name for all address. In such case, the administrator SHOULD have site local policy to make sure that the zone suffix in the router and in the DHCPv6 server are the same. This can be done by using the Zone Suffix option in DHCPv6 [12]. Host can register each address using FQDN option [13] via DHCPv6 and using Domain Name option via RA/RS separately.

If a mobile host in foreign network want to access other PC, it can simply use the care-of-address, if other PC want to communicate the a mobile host in foreign network, it can still use the old domain name of that host and get its home address, them the MIPv6 mechanism will be used. So, for a mobile host in foreign network, it is unnecessary to re-update DNS using new Domain Name option broadcasted by local router. If a mobile host detects it has been located in a foreign network, it can just ignore the Domain Name option included in RA message sent by the foreign router.

However, it will be interesting if the mobile host update a new DNS using its original domain name in foreign network, i.e. it updates AAAA record in its home DNS server, and updates PTR record in local foreign DNS server. Such kind of method can replace some functions of MIPv6. Hosts which want to connect to this mobile host will directly get its foreign address by DNS resolution. This issue will be studied in a separate document.

9. Security Considerations

Unauthenticated updates to the DNS can lead to tremendous confusion, through malicious attack or through inadvertent misconfiguration. Administrators should be wary of permitting unsecured DNS updates to zones which are exposed to the global Internet. Both host and router SHOULD use some form of update request origin authentication procedure (e.g., Secure DNS Dynamic Update [9]) when performing DNS updates.

Malicious host may be able to mount a denial of service attack to router by repeated RS messages with "Domain Name" option. Some kind of security mechanism (e.g., Secure Neighbour Discovery [11]) may be used to setup a trust model between router and hosts.

Whether the router may be responsible for DNS update or whether it left this responsibility to host itself is a site-local matter. The choice between the two alternatives may be based on the security model that is used with the DNS update protocol.

10. Acknowledgements

I would like to thank Chris Liljenstolpe, Stefaan De Cnodder, Yinglan Jiang, and Emmanuel Desmet for their valuable comments and kindly help.

11. References

11.1 Normative References

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

[2] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[3] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[4] Deering, S. and R. Hiden, "Internet Protocol, Version 6 (IPv6) Specification", RFC2460, December 1998.

[5] Thomson, S., Huitema, C., Ksinant, V. and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[6] P. Vixie, S. Thomson, Y. Rekhter and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC2136, April 1997.

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

[8] T. Narten, E. Nordmark, W. Simpson , "Neighbor Discovery for IP Version 6", RFC2461, December 1998.

11.2 Informative References

[9] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[10] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[11] J. Arkko, J. Kempf, B. Sommerfeld, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ndopt-06.txt, July 17, 2004.

[12] R. Yan, L. Gui, Y. Jiang, "Zone suffix option for DHCPv6", draft-yan-dhc-dhcpv6-opt-dnszone-02.txt, December 24, 2004.

[13] B. Volz, "The DHCPv6 Client FQDN Option", draft-ietf-dhc-dhcpv6-fqdn-00.txt, September, 2004.

Author Information:

Renxiang Yan
Research & Innovation Center
Alcatel Shanghai Bell Co., Ltd.
388#, NingQiao Road, Pudong Jinqiao
Shanghai 201206 P.R. China

Phone: +86 (21) 5854-1240, ext:7169
Email: renxiang.yan@alcatel-sbell.com.cn

Xiaodong Duan
Research & Development Center
China Mobile Communications Corporation
53A, Xibianmennei Ave., Xuanwu District,
Beijing, 100053 P.R. China
Phone: +86 (10) 6600-6688, ext. 3062

Email: duanxiaodong@chinamobile.com