IPv6 Host Configuration of DNS Server Information Approaches
draft-ietf-dnsop-ipv6-dns-configuration-04.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which we become aware will be disclosed, in accordance with RFC3668.

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 27, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document describes three approaches for IPv6 recursive DNS server address configuration. It details the operational attributes of three solutions: RA option, DHCPv6 option, and Well-known anycast addresses for recursive DNS servers. Additionally, it suggests four deployment scenarios considering multi-solution resolution. Therefore, this document will give the audience a
guideline for IPv6 DNS configuration to select approaches suitable for their host DNS configuration.

Table of Contents

1. Introduction............................................................3
2. Terminology.....................................................................3
3. IPv6 DNS Configuration Approaches...................................3
   3.1. RA Option............................................................3
       3.1.1. Advantages..................................................4
       3.1.2. Disadvantages.............................................5
       3.1.3. Observations.............................................6
   3.2. DHCPv6 Option....................................................6
       3.2.1. Advantages................................................7
       3.2.2. Disadvantages.............................................8
       3.2.3. Observations.............................................9
   3.3. Well-known Anycast Addresses...................................9
       3.3.1. Advantages................................................10
       3.3.2. Disadvantages.............................................10
       3.3.3. Observations.............................................10
4. Interworking among IPv6 DNS Configuration Approaches.............11
5. Deployment Scenarios...................................................12
   5.1. ISP Network.......................................................12
       5.1.1. RA Option Approach......................................12
       5.1.2. DHCPv6 Option Approach................................13
       5.1.3. Well-known Addresses Approach........................13
   5.2. Enterprise Network...............................................14
   5.3. 3GPP Network......................................................14
       5.3.1. Currently Available Mechanisms and Recommendations.15
       5.3.2. RA Extension..............................................16
       5.3.3. Stateless DHCPv6..........................................16
       5.3.4. Well-known Addresses...................................17
       5.3.5. Recommendations..........................................17
   5.4. Unmanaged Network.................................................18
       5.4.1. Case A: Gateway does not provide IPv6 at all...........18
       5.4.2. Case B: A dual-stack gateway connected to a dual-stack ISP....18
       5.4.3. Case C: A dual-stack gateway connected to an IPv4-only ISP.....19
       5.4.4. Case D: A gateway connected to an IPv6-only ISP...........19
6. Security Considerations.................................................19
7. Acknowledgements..........................................................19
8. Normative References.....................................................20
9. Informative References..................................................20
10. Appendix A - Link-layer Multicast Acknowledgements with RA Option..........................................................21
11. Authors’ Addresses....................................................22
12. Intellectual Property Statement........................................23
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 [3][4]. To support 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.

This document describes three approaches of recursive DNS server address configuration for IPv6 host: (a) RA option [8], (b) DHCPv6 option [5]-[7], and (c) Well-known anycast addresses for recursive DNS servers [9]. Also, it suggests applicable scenarios for four kinds of networks: (a) ISP network, (b) Enterprise network, (c) 3GPP network, and (d) Unmanaged network.

This document is just an analysis of each possible approach, and does not make any recommendation on particular one or on a combination of particular ones. Some approaches may even not be adopted at all as a result of further discussion.

Therefore, the objective of this document is to help the audience select approaches suitable for IPv6 host configuration of recursive DNS server.

2. Terminology

This document uses the terminology described in [3]-[9]. 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.

3. IPv6 DNS Configuration Approaches

In this section, the operational attributes of three solutions are described in detail.

3.1. RA Option

RA approach is to define a new ND option called RDNSS option that contains a recursive DNS server address. Existing ND transport mechanisms (i.e., advertisements and solicitations) are used. This
works in the same way that nodes 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) [8].

This approach needs RDNSS information to be configured in the routers doing the advertisements. The configuration of RDNSS address can be performed manually by operator or other ways, such as automatic configuration through DHCPv6 client running on the router. When advertising more than one RDNSS options, an RA message includes as many RDNSS options as RDNSSes.

Through ND protocol and RDNSS option along with prefix information option, an IPv6 host can perform its network configuration of its IPv6 address and RDNSS simultaneously [3][4]. The RA option for RDNSS can be used on any network that supports the use of ND.

However, it is worth noting that some link layers (e.g., WLAN) need to acknowledge multicast packets, which may increase the amount of link-layer traffic. This is discussed in Appendix A.

The RA approach is useful in some mobile environments where the addresses of the RDNSSes are changing because the RA option includes a lifetime field that allows client to use RDNSSes nearer to the client. This can be configured to a value that will require the client to time out the entry and switch over to another RDNSS address [8]. However, from the viewpoint of implementation, lifetime would seem to make matters a bit more complex. Instead of just writing DNS configuration file, such as resolv.conf for the list of RDNSS addresses, we have 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.

The preference value of RDNSS, included in RDNSS option, allows IPv6 hosts to select primary RDNSS among several RDNSSes; this can be used for load balancing of RDNSSes [8].

3.1.1. Advantages

The RA option for RDNSS has a number of advantages. These include:

1) The RA option is an extension of existing ND/Autoconfig mechanisms [3][4], and does not require a change in the base ND protocol.

2) This approach, like ND, works well on a variety of link types including point-to-point links, point-to-multipoint, and multipoint (i.e., Ethernet LANs), etc. RFC2461 [3] states, however,
that there may be some link type on which ND is not possible; on such a link, some other mechanism will be needed for DNS configuration.

3) All of the information a host needs to run basic Internet applications such as email, the web, ftp, etc., can be obtained with the addition of this option to ND and address auto-configuration. The use of a single mechanism is more reliable and easier to provide than when the RDNSS information is learned via another protocol mechanism. Debugging problems when multiple protocol mechanisms are being used is harder and much more complex.

4) This mechanism works over a broad range of scenarios and leverages IPv6 ND. This works well on links that support broadcast reliably (e.g., Ethernet LANs) but not necessarily on other links (e.g., Wireless LANs). Also, this works well on links that are high performance (e.g., Ethernet LANs) and low performance (e.g., Cellular networks). In the latter case, combining the RDNSS information with the other information in the RA, the host can learn all of the information needed to use most Internet applications such as the web in a single packet. This not only saves bandwidth where this is an issue, but also minimizes the delay to learn the RDNSS information.

5) The RA approach could be used as a model for other similar types of configuration information. New RA options for other server addresses that are common to all clients on a subnet would be easy to define. This includes things like NTP servers, SIP servers, etc.

3.1.2. Disadvantages

1) ND is mostly implemented in kernel part of operating system. Therefore, if ND supports the configuration of some additional services, such as DNS, NTP and SIP servers, ND should be extended in kernel part, and complemented by a user-land process. DHCPv6, however, has more flexibility for extension of service discovery because it is an application layer protocol.

2) The current ND framework should be modified due to the synchronization between another ND cache for RDNSSes in kernel space and DNS configuration file in user space. Because it is unacceptable to write and rewrite the DNS configuration file (e.g., resolv.conf) from the kernel, another approach is needed. One simple approach to solve this is to have a daemon listening to what the kernel conveys, and to have the daemon do these steps, but such a daemon is not necessary with the current ND framework.
3) It is necessary to configure RDNSS addresses at least at one router on every link where this information needs to be configured by RA option.

3.1.3. Observations

The proposed RDNSS RA option along with IPv6 ND and Auto-configuration allows a host to obtain all of the information it needs to access basic Internet services like the web, email, ftp, etc. This is preferable in environments where hosts use RAs to autoconfigure their addresses and all hosts on the subnet share the same router and server addresses. If the configuration information can be obtained from a single mechanism, it is preferable because it does not add additional delay, and it uses a minimum of bandwidth. Environments like this include homes, public cellular networks, and enterprise environments where no per host configuration is needed, but exclude public WLAN hot spots.

DHCPv6 is preferable where it is being used for address configuration and if there is a need for host specific configuration [5]-[7]. Environments like this are most likely enterprise environments where the local administration chooses to have per host configuration control.

Note: the observation section is based on what the proponents of each approach think makes a good overall solution.

3.2. DHCPv6 Option

DHCPv6 [5] includes the "DNS Recursive Name Server" option, through which a host can obtain a list of IP addresses of recursive DNS servers [7]. The DNS Recursive Name Server option carries a list of IPv6 addresses of RDNSSes to which the host may send DNS queries. The DNS servers are listed in the order of preference for use by the DNS resolver on the host.

The DNS Recursive Name Server option can be carried in any DHCPv6 Reply message, in response to either a Request or an Information-request message. Thus, the DNS Recursive Name Server option can be used either when DHCPv6 is used for address assignment, or when DHCPv6 is used only for other configuration information as stateless DHCPv6 [6].

Stateless DHCPv6 can be deployed either using DHCPv6 servers running on general-purpose computers, or on router hardware. Several router vendors currently implement stateless DHCPv6 servers. Deploying stateless DHCPv6 in routers has the advantage that no special hardware is required, and should work well for networks
However, routers can also act as DHCPv6 relay agents. In this case, the DHCPv6 server need not be on the router - it can be on a general purpose computer. This has the potential to give the operator of the DHCPv6 server more flexibility in how the DHCPv6 server responds to individual clients - clients can easily be given different configuration information based on their identity, or for any other reason. Nothing precludes adding this flexibility to a router, but generally in current practice, DHCP servers running on general-purpose hosts tend to have more configuration options than those that are embedded in routers.

DHCPv6 currently provides a mechanism for reconfiguring DHCPv6 clients that use stateful configuration assignment. To do this, the DHCPv6 server sends a Reconfigure message to the client. The client validates the Reconfigure message, and then contacts the DHCPv6 server to obtain updated configuration information. Using this mechanism, it is currently possible to propagate new configuration information to DHCPv6 clients as this information changes.

The DHCP Working Group is currently studying an additional mechanism through which configuration information, including the list of RDNSSes, can be updated. The lifetime option for DHCPv6 [10] assigns a lifetime to configuration information obtained through DHCPv6. At the expiration of the lifetime, the host contacts the DHCPv6 server to obtain updated configuration information, including the list of RDNSSes. This lifetime gives the network administrator another mechanism to configure hosts with new RDNSSes by controlling the time at which the host refreshes the list.

The DHCP Working Group has also discussed the possibility of defining an extension to DHCPv6 that would allow the use of multicast to provide configuration information to multiple hosts with a single DHCPv6 message. Because of the lack of deployment experience, the WG has deferred consideration of multicast DHCPv6 configuration at this time. Experience with DHCPv4 has not identified a requirement for multicast message delivery, even in large service provider networks with tens of thousands of hosts that may initiate a DHCPv4 message exchange simultaneously.

3.2.1. Advantages

The DHCPv6 option for RDNSS has a number of advantages. These include:
1) DHCPv6 currently provides a general mechanism for conveying network configuration information to clients. So configuring DHCPv6 servers allows the network administrator to configure RDNSSes along with the addresses of other network services, as well as location-specific information like time zones.

2) As a consequence, when the network administrator goes to configure DHCPv6, all the configuration information can be managed through a single service, typically with a single user interface and a single configuration database.

3) DHCPv6 allows for the configuration of a host with information specific to that host, so that hosts on the same link can be configured with different RDNSSes as well as other configuration information. This capability is important in some network deployments such as service provider networks or WiFi hot spots.

4) A mechanism exists for extending DHCPv6 to support the transmission of additional configuration that has not yet been anticipated.

5) Hosts that require other configuration information such as the addresses of SIP servers and NTP servers are likely to need DHCPv6 for other configuration information.

6) The specification for configuration of RDNSSes through DHCPv6 is available as an RFC. No new protocol extensions such as new options are necessary.

7) Interoperability among independent implementations has been demonstrated.

3.2.2. Disadvantages

The DHCPv6 option for RDNSS has a few disadvantages. These include:

1) Update currently requires message from server (however, see [10]).

2) Because DNS information is not contained in RA message, the host must receive two messages from the router, and must transmit at least one message to the router. On networks where bandwidth is at a premium, this is a disadvantage, although on most networks it is not a practical concern.

3) Increased latency for initial configuration - in addition to waiting for an RA message, the client must now exchange packets
with a DHCPv6 server; even if it is locally installed on a router, this will slightly extend the time required to configure the client. For clients that are moving rapidly from one network to another, this will be a disadvantage.

### 3.2.3. Observations

In the general case, on general-purpose networks, stateless DHCPv6 provides significant advantages and no significant disadvantages. Even in the case where bandwidth is at a premium and low latency is desired, if hosts require other configuration information in addition to a list of RDNSSes or if hosts must be configured selectively, those hosts will use DHCPv6 and the use of the DHCPv6 DNS recursive name server option will be advantageous.

However, we are aware of some applications where it would be preferable to put the RDNSS information into an RA packet; for example, on a cell phone network, where bandwidth is at a premium and extremely low latency is desired. The final DNS configuration draft should be written so as to allow these special applications to be handled using DNS information in the RA packet.

### 3.3. Well-known Anycast Addresses

First of all, the well-known anycast addresses approach is much different from that discussed at IPv6 Working Group in the past [9]. It should be noted that "anycast" in this memo is simpler than that of RFC1546 [11] and RFC3513 [12] where it is assumed to be prohibited to have multiple servers on a single link sharing an anycast address. That is, on a link, anycast address is assumed to be unique. DNS clients today already have redundancy by having multiple well-known anycast addresses configured as RDNSS addresses. There is no point to have multiple RDNSSes sharing an anycast address on a single link.

The approach with well-known anycast addresses is to set well-known anycast addresses in clients’ resolver configuration files from the beginning, say, as factory default. Thus, there is no transport mechanism and no packet format [9].

An anycast address is an address shared by multiple servers (in this case, the servers are RDNSSes). Request from a client to the anycast address is routed to a server selected by the routing system. However, it is a bad idea to mandate "site" boundary on anycast addresses, because most users just do not have their own servers and want to access their ISPs’ across their site boundaries. Larger sites may also depend on their ISPs or may have their own RDNSSes within "site" boundaries.
3.3.1. Advantages

The basic advantage of the well-known addresses approach is that it uses no transport mechanism. Thus,
1) There is no delay to get response and no further delay by packet losses.

2) The approach can be combined with any other configuration mechanisms including but not limited to factory default configuration, RA-based approach and DHCP based approach.

3) The approach works over any environment where DNS works.

Another advantage is that the approach needs to configure DNS servers as a router, but nothing else. Considering that DNS servers do need configuration, the amount of overall configuration effort is proportional to the number of the DNS servers and scales linearly. It should be noted that, in the simplest case where a subscriber to an ISP does not have any DNS server, the subscriber naturally accesses DNS servers of the ISP even though the subscriber and the ISP do nothing and there is no protocol to exchange DNS server information between the subscriber and the ISP.

3.3.2. Disadvantages

Well-known anycast addresses approach requires that DNS servers (or routers near it as a proxy) act as routers to advertise their anycast addresses to the routing system, which requires some configuration (see the last paragraph of the previous section on the scalability of the effort).

3.3.3. Observations

If other approaches are used in addition, the well-known anycast addresses should also be set in RA or DHCP configuration files to reduce configuration effort of users.

Redundancy by multiple RDNSSes is better provided by multiple servers having different anycast addresses than multiple servers sharing same anycast address because the former approach allows stale servers to still generate routes to their anycast addresses. Thus, in a routing domain (or domains sharing DNS servers), there will be only one server having an anycast address unless the domain is so large that load distribution is necessary.

Small ISPs will operate one RDNSS at each anycast address which is shared by all the subscribers. Large ISPs may operate multiple
RDNSSes at each anycast address to distribute and reduce load, where boundary between RDNSSes may be fixed (redundancy is still provided by multiple addresses) or change dynamically. DNS packets with the well-known anycast addresses are not expected (though not prohibited) to cross ISP boundaries, as ISPs are expected to take care of themselves.

Because "anycast" in this memo is simpler than that of RFC1546 [11] and RFC3513 [12] where it is assumed to be administratively prohibited to have multiple servers on a single link sharing an anycast address, anycast in this memo should be implemented as UNICAST of RFC2461 [3] and RFC3513 [12]. As a result, ND-related instability disappears. Thus, anycast in well-known anycast addresses approach can and should use the anycast address as a source unicast (according to RFC3513 [12]) address of packets of UDP and TCP responses. With TCP, if route flips and packets to an anycast address are routed to a new server, it is expected that the flip is detected by ICMP or sequence number inconsistency and the TCP connection is reset and retried.

4. Interworking among IPv6 DNS Configuration Approaches

Three approaches can work together for IPv6 host configuration of RDNSS. This section shows a consideration on how these approaches can interwork each other.

For ordering between RA and DHCP approaches, O (Other stateful configuration) flag in RA message can be used [8]. If no RDNSS option is included, an IPv6 host may perform DNS configuration through DHCPv6 [5]-[7] regardless of whether the O flag is set or not.

The well-known anycast addresses approach fully interworks with the other approaches. That is, the other approaches can remove configuration effort on servers by using the well-known addresses as the default configuration. Moreover, clients preconfigured with well-known anycast addresses can be further configured to use other approaches to override the well-known addresses, if configuration information from other approaches are available. That is, all the clients should have the well-known anycast addresses preconfigured, in the case where there are no other mechanisms available. In order to fly anycast approach with the other solutions, there are three options.

The first option is that well-known addresses are used as last resort, when an IPv6 host can not get RDNSS information through RA and DHCP. The well-known anycast addresses have to be pre-configured in IPv6 hosts’ resolver configuration files.
The second is that an IPv6 host can configure well-known addresses as the most preferable in its configuration file even though either RA option or DHCP option is available.

The last is that the well-known anycast addresses can be set in RA or DHCP configuration to reduce configuration effort of users. According to either RA or DHCP mechanism, the well-known addresses can be obtained by IPv6 host. Because this approach is the most convenient for users, the last option is recommended.

Note: this section does not necessarily mean this document suggests adopting all these three approaches and making them interwork in the way described here. In fact, some approaches may even not be adopted at all as a result of further discussion.

5. Deployment Scenarios

Regarding DNS configuration on the IPv6 host, several mechanisms are being considered at the DNSOP Working Group such as RA option, DHCPv6 option and well-known preconfigured anycast addresses as of today, and this document is a final result from the long thread. In this section, we suggest four applicable scenarios of three approaches for IPv6 DNS configuration.

Note: in the applicable scenarios, authors do not implicitly push any specific approaches into the restricted environments. No enforcement is in each scenario and all mentioned scenarios are probable. The main objective of this work is to provide a useful guideline for IPv6 DNS configuration.

5.1. ISP Network

A characteristic of ISP network is that multiple Customer Premises Equipment (CPE) devices are connected to IPv6 PE (Provider Edge) routers and each PE connects multiple CPE devices to the backbone network infrastructure [13]. The CPEs may be hosts or routers.

In the case where the CPE is a router, there is a customer network that is connected to the ISP backbone through the CPE. Typically, each customer network gets a different IPv6 prefix from an IPv6 PE router, but the same RDNSS configuration will be distributed.

This section discusses how the different approaches to distributing DNS information are compared in an ISP network.

5.1.1. RA Option Approach
When the CPE is a host, the RA option for RDNSS can be used to allow the CPE to get RDNSS information as well as /64 prefix information for stateless address autoconfiguration at the same time when the host is attached to a new subnet [8]. Because an IPv6 host must receive at least one RA message for stateless address autoconfiguration and router configuration, the host could receive RDNSS configuration information in that RA without the overhead of an additional message exchange.

When the CPE is a router, the CPE may accept the RDNSS information from the RA on the interface connected to the ISP, and copy that information into the RAs advertised in the customer network.

This approach is more valuable in the mobile host scenario, in which the host must receive at least an RA message for detecting a new network, than in other scenarios generally although administrator should configure RDNSS information on the routers. Secure ND [14] can provide extended security when using RA message.

5.1.2. DHCPv6 Option Approach

DHCPv6 can be used for RDNSS configuration through the use of the DNS option, and can provide other configuration information in the same message with RDNSS configuration [5]-[7]. DHCPv6 DNS option is already in place for DHCPv6 as RFC 3646 [7] and moreover DHCPv6-lite or stateless DHCP [6] is nowhere as complex as a full DHCPv6 implementation. DHCP is a client-server model protocol, so ISP can handle user identification on its network intentionally, and also authenticated DHCP [15] can be used for secure message exchange.

The expected model for deployment of IPv6 service by ISPs is to assign a prefix to each customer, which will be used by the customer gateway to assign a /64 prefix to each network in the customer’s network. Prefix delegation with DHCP (DHCPv6 PD) has already been adopted by ISPs for automating the assignment of the customer prefix to the customer gateway [17]. DNS configuration can be carried in the same DHCPv6 message exchange used for DHCPv6 to efficiently provide that information, along with any other configuration information needed by the customer gateway or customer network. This service model can be useful to Home or SOHO subscribers. The Home or SOHO gateway, which is a customer gateway for ISP, can then pass that RDNSS configuration information to the hosts in the customer network through DHCP.

5.1.3. Well-known Addresses Approach

Well-known anycast addresses approach is also a feasible and simple mechanism for ISP [9]. The use of well-known anycast addresses
avoids some of the security risks in rogue messages sent through an external protocol like RA or DHCPv6. The configuration of hosts for the use of well-known anycast addresses requires no protocol or manual configuration, but the configuration of routing for the anycast addresses requires intervention on the part of the network administrator. Also, the number of special addresses would be equal to the number of RDNSSes that could be made available to subscribers.

5.2. Enterprise Network

Enterprise network is defined as a network that has multiple internal links, one or more router connections, to one or more Providers and is actively managed by a network operations entity [16]. An enterprise network can get network prefixes from ISP by either manual configuration or prefix delegation [17]. In most cases, because an enterprise network manages its own DNS domains, it operates its own DNS servers for the domains. These DNS servers within enterprise network process recursive DNS name resolution requests of IPv6 hosts as RDNSS. RDNSS configuration in enterprise network can be performed like in Section 4, in which three approaches can be used together.

IPv6 host can decide which approach is or may be used in its subnet with O flag in RA message [8]. As the first option in Section 4, well-known anycast addresses can be used as a last resort when RDNSS information can not be obtained through either RA option or DHCP option. This case needs IPv6 hosts to preconfigure the well-known anycast addresses in their DNS configuration files.

When the enterprise prefers well-known anycast approach to the others, IPv6 hosts should preconfigure the well-known anycast addresses like in the first option.

The last option, a more convenient and transparent way, does not need IPv6 hosts to preconfigure the well-known anycast addresses because the addresses are delivered to IPv6 hosts through either RA option or DHCPv6 option as if they were unicast addresses. This way is most recommended for the sake of user’s convenience.

5.3. 3GPP Network

IPv6 DNS configuration is a missing part of IPv6 autoconfiguration and an important part of the basic IPv6 functionality in the 3GPP User Equipment (UE). Higher level description of the 3GPP architecture can be found in [18], and transition to IPv6 in 3GPP networks is analyzed in [19] and [20].
In 3GPP architecture, there is a dedicated link between the UE and the GGSN called the Packet Data Protocol (PDP) Context. This link is created through the PDP Context activation procedure. There is a separate PDP context type for IPv4 and IPv6 traffic. If a 3GPP UE user is communicating using IPv6 (having an active IPv6 PDP context), it cannot be assumed that (s)he has simultaneously active IPv4 PDP context, and DNS queries could be done using IPv4. A 3GPP UE can thus be an IPv6 node, and it needs to somehow discover the address of the RDNSS. Before IP-based services (e.g., web browsing or e-mail) can be used, the IPv6 (and IPv4) RDNSS addresses need to be discovered in the 3GPP UE.

Section 5.3.1 briefly summarizes currently available mechanisms in 3GPP networks and recommendations. 5.3.2 analyzes the Router Advertisement based solution, 5.3.3 analyzes the Stateless DHCPv6 mechanism, and 5.3.4 analyzes the Well-known addresses approach. Section 5.3.5 finally summarizes the recommendations.

5.3.1. Currently Available Mechanisms and Recommendations

3GPP has defined a mechanism, in which RDNSS addresses can be received in the PDP context activation (a control plane mechanism). That is called the Protocol Configuration Options Information Element (PCO-IE) mechanism. The RDNSS addresses can also be received over the air (using text messages), or typed in manually in the UE. Note that the two last mechanisms are not very well scalable. The UE user most probably does not want to type IPv6 RDNSS addresses manually in his/her UE. The use of well-known addresses is briefly discussed in section 5.3.4.

It is seen that the mechanisms above most probably are not sufficient for the 3GPP environment. IPv6 is intended to operate in a zero-configuration manner, no matter what the underlying network infrastructure is. Typically, the RDNSS address is needed to make an IPv6 node operational – and the DNS configuration should be as simple as the address autoconfiguration mechanism. It must also be noted that there will be additional IP interfaces in some near future 3GPP UEs, e.g., WLAN, and 3GPP-specific DNS configuration mechanisms (such as PCO-IE) do not work for those IP interfaces. In other words, a good IPv6 DNS configuration mechanism should also work in a multi-access network environment.

From 3GPP point of view, the best IPv6 DNS configuration solution is feasible for a very large number of IPv6-capable UEs (can be even hundreds of millions in one operator’s network), is automatic and thus requires no user action. It is suggested to standardize a lightweight, stateless mechanism that works in all network environments. The solution could then be used for 3GPP, 3GPP2,
WLAN and other access network technologies. A light, stateless IPv6 DNS configuration mechanism is thus not only needed in 3GPP networks, but also 3GPP networks and UEs would certainly benefit from the new mechanism.

5.3.2. RA Extension

Router Advertisement extension [8] is a lightweight IPv6 DNS configuration mechanism that requires minor changes in 3GPP UE IPv6 stack and Gateway GPRS Support Node (GGSN, the default router in the 3GPP architecture) IPv6 stack. This solution can be specified in the IETF (no action needed in the 3GPP) and taken in use in 3GPP UEs and GGSNs.

In this solution, an IPv6-capable UE configures DNS information via RA message sent by its default router (GGSN), i.e., RDNSS option for recursive DNS server is included in the RA message. This solution is easily scalable for a very large number of UEs. The operator can configure the RDNSS addresses in the GGSN as a part of normal GGSN configuration. The IPv6 RDNSS address is received in the Router Advertisement, and an extra Round Trip Time (RTT) for asking RDNSS addresses can be avoided.

If thinking about cons, this mechanism still requires standardization effort in the IETF, and the end nodes and routers need to support this mechanism. The equipment software update should, however, be pretty straightforward, and new IPv6 equipment could support RA extension already from the beginning.

5.3.3. Stateless DHCPv6

DHCPv6-based solution needs the implementation of Stateless DHCP [6] and DHCPv6 DNS options [7] in the UE, and a DHCPv6 server in the operator’s network. A possible configuration is such that the GGSN works as a DHCP relay.

Pros for Stateless DHCPv6-based solution are

1) Stateless DHCPv6 is a standardized mechanism.

2) DHCPv6 can be used for receiving other configuration information than RDNSS addresses, e.g., SIP server addresses.

3) DHCPv6 works in different network environments.

4) When DHCPv6 service is deployed through a single, centralized server, the RDNSS configuration information can be updated by the network administrator at a single source.
Some issues with DHCPv6 in 3GPP networks are listed below:

1) DHCPv6 requires an additional server in the network unless the (Stateless) DHCPv6 functionality is integrated into an existing router already, and it is one box more to be maintained.

2) DHCPv6 is not necessarily needed for 3GPP UE IPv6 addressing (3GPP Stateless Address Autoconfiguration is typically used), and not automatically implemented in 3GPP IPv6 UEs.

3) Scalability and reliability of DHCPv6 in very large 3GPP networks (with tens or hundreds of millions of UEs) may be an issue, at least the redundancy needs to be taken care of. However, if the DHCPv6 service is integrated into the network elements, such as router operating system, scalability and reliability is comparable with other DNS configuration approaches.

4) It is sub-optimal to utilize the radio resources in 3GPP networks for DHCPv6 messages if there is a simpler alternative available.
   
   a) Use of Stateless DHCPv6 adds one round trip delay to the case in which the UE can start transmitting data right after the Router Advertisement.

5) If the DNS information (suddenly) changes, Stateless DHCPv6 can not automatically update the UE, see [23].

5.3.4. Well-known Addresses

Using well-known addresses is also a feasible and a light mechanism for 3GPP UEs. Those well-known addresses can be preconfigured in the UE software and the operator makes the corresponding configuration on the network side. So this is a very easy mechanism for the UE, but requires some configuration work in the network. When using well-known addresses, UE forwards queries to any of the preconfigured addresses. In the current proposal [9], IPv6 anycast addresses are suggested.

Note: IPv6 DNS configuration proposal based on the use of well-known site-local addresses developed at the IPv6 Working Group was seen as a feasible mechanism for 3GPP UEs, but opposition by some people in the IETF and finally deprecating IPv6 site-local addresses made it impossible to standardize it. Note that this mechanism is implemented in some existing operating systems today (also in some 3GPP UEs) as a last resort of IPv6 DNS configuration.

5.3.5. Recommendations
It is suggested that a lightweight, stateless DNS configuration mechanism is specified as soon as possible. From 3GPP UE’s and networks’ point of view, Router Advertisement based mechanism looks most promising. The sooner a light, stateless mechanism is specified, the sooner we can get rid of using well-known site-local addresses for IPv6 DNS configuration.

5.4. Unmanaged Network

There are 4 deployment scenarios of interest in unmanaged networks [24]:

1) A gateway which does not provide IPv6 at all;
2) A dual-stack gateway connected to a dual-stack ISP;
3) A dual-stack gateway connected to an IPv4-only ISP; and
4) A gateway connected to an IPv6-only ISP.

5.4.1. Case A: Gateway does not provide IPv6 at all

In this case, the gateway does not provide IPv6; the ISP may or may not provide IPv6. Automatic or Configured tunnels are the recommended transition mechanisms for this scenario.

The case where dual-stack hosts behind an NAT, that need access to an IPv6 RDNSS, can not be entirely ruled out. The DNS configuration mechanism has to work over the tunnel, and the underlying tunneling mechanism could be implementing NAT traversal. The tunnel server assumes the role of a relay (both for DHCP and Well-known anycast addresses approaches).

RA-based mechanism is relatively straightforward in its operation, assuming the tunnel server is also the IPv6 router emitting RAs. Well-known anycast addresses approach seems also simple in operation across the tunnel, but the deployment model using Well-known anycast addresses in a tunneled environment is unclear or not well understood.

5.4.2. Case B: A dual-stack gateway connected to a dual-stack ISP

This is similar to a typical IPv4 home user scenario, where DNS configuration parameters are obtained using DHCP. Except that Stateless DHCPv6 is used, as opposed to the IPv4 scenario where the DHCP server is stateful (maintains the state for clients).
5.4.3. Case C: A dual-stack gateway connected to an IPv4-only ISP

This is similar to Case B. If a gateway provides IPv6 connectivity by managing tunnels, then it is also supposed to provide access to an RDNSS. Like this, the tunnel for IPv6 connectivity originates from the dual-stack gateway instead of the host.

5.4.4. Case D: A gateway connected to an IPv6-only ISP

This is similar to Case B.

6. Security Considerations

As security requirements depend solely on applications and are different application by application, there can be no generic requirement defined at higher IP or lower application layer of DNS.

However, it should be noted that cryptographic security requires configured secret information that full autoconfiguration and cryptographic security are mutually exclusive. People insisting on secure full autoconfiguration will get false security, false autoconfiguration or both.

In some deployment scenario [19], where cryptographic security is required for applications, secret information for the cryptographic security is preconfigured through which application specific configuration data, including those for DNS, can be securely configured. It should be noted that if applications requiring cryptographic security depend on DNS, the applications also require cryptographic security to DNS. Therefore, the full autoconfiguration of DNS is not acceptable.

However, with full autoconfiguration, weaker but still reasonable security is being widely accepted and will continue to be acceptable. That is, with full autoconfiguration, which means there is no cryptographic security for the autoconfiguration, it is already assumed that local environment is secure enough that information from local autoconfiguration server has acceptable security even without cryptographic security. Thus, communication between a local DNS client and a local DNS server has the acceptable security.

For security considerations of each approach, refer to the corresponding drafts [5]-[9].

7. Acknowledgements
8. Normative References


9. Informative References


[21] 3GPP TS 23.060 V5.4.0, "General Packet Radio Service (GPRS); Service description; Stage 2 (Release 5)", December 2002.

[22] 3GPP TS 24.008 V5.8.0, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 5)", June 2003.


10. Appendix A - Link-layer Multicast Acknowledgements with RA Option

One benefit of RA option is to be able to multicast the advertisements, reducing the need for duplicated unicast communications.
However, some link-layers may not support this as well as others. Consider, for example, WLAN networks where multicast is unreliable. The unreliability problem is caused by lack of ACK for multicast, especially on the path from the Access Point (AP) to the Station (STA), which is specific to CSMA/CA of WLAN. Namely, multicast packet is unacknowledged on the path from the AP to the STA, but acknowledged in the reverse direction from the STA to the AP. For example, when a router is placed at wired network connected to an AP, a host may sometimes not receive RA message advertised through the AP.

The fact that this problem has not been addressed in Neighbor Discovery [3] indicates that the extra link-layer acknowledgements have not been considered a serious problem till now.

A possible mitigation technique could be to map all-nodes link-local multicast address to the link-layer broadcast address, and to rely on the ND retransmissions for message delivery.

11. Authors’ Addresses

Jaehoon Paul Jeong, Editor  
ETRI/University of Minnesota at Twin Cities  
117 Pleasant Street SE  
Minneapolis, MN 55455  
USA  
Phone: +1 651 587 7774  
EMail: jjeong@cs.umn.edu

Ralph Droms  
Cisco Systems  
1414 Massachusetts Ave.  
Boxboro, MA 01719  
USA  
Phone: +1 978 936 1674  
EMail: rdroms@cisco.com

Robert M. Hinden  
Nokia  
313 Fairchild Drive  
Mountain View, CA 94043  
USA  
Phone: +1 650 625 2004  
EMail: bob.hinden@nokia.com
12. Intellectual Property Statement

The following intellectual property notice is copied from RFC3668, Section 5.

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright Statement

The following copyright notice is copied from RFC3667, Section 5.4. It describes the applicable copyright for this document.

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.