DNS Configuration in IPv6

Approaches, Analysis, and Deployment Scenarios

IPv6 provides abundant address space and automatic network-parameter configuration. The IETF has proposed three approaches for DNS configuration in IPv6 hosts for recursive DNS server addresses and the DNS search list. The authors analyze these approaches and describe four deployment scenarios in IPv6 wired and wireless networks. They provide guidelines for DNS configuration that IPv6 network administrators and users can apply in their target networks.

Soohong Park
Samsung Electronics

Jaehoon (Paul) Jeong
Sungkyunkwan University

Choong Seon Hong
Kyung Hee University

Neighbor discovery for IPv6[1] and IPv6 stateless address autoconfiguration[2] let IPv6 hosts configure fixed or mobile nodes with one or more IPv6 addresses, default routes, and other network parameters (for example, link maximum transmission unit and hop limit value). With neighbor discovery, IPv6 routers and hosts can perform this network configuration without a dedicated server.

To easily access servers, IPv6 hosts must be configured with DNS server addresses for name resolution. The DNS service converts a server's DNS name into the corresponding IP address. This service is critical for communication between IPv6 hosts because remembering the addresses is difficult, and typing a 128-bit IPv6 address for every networking operation, such as Web browsing, is inconvenient.

The IETF has discussed three approaches for DNS configuration in IPv6 hosts, all applicable to a variety of IPv6 wired and wireless networks[3]:

- the router advertisement approach,[4]
- the DHCPv6 approach,[5] and
- the well-known anycast addresses approach.[6]

The DNS configuration not only provides recursive DNS server addresses with IPv6 hosts, but also lets the IPv6 hosts recognize the DNS search list used to construct fully qualified domain names for DNS queries.

We analyze these three approaches and describe their deployment in four scenarios: an ISP network, an enterprise network, a 3GPP network, and an unmanaged network. This article builds on our early work on IPv6 DNS configuration[3,4] to reflect current trends

1089-7801/13/$31.00 © 2013 IEEE

(for example, smartphones and tablets using both Wi-Fi and 3G/4G networks) and future demands (for example, wireless sensor or vehicular networks).

IPv6 DNS Configuration Approaches

Figure 1 shows the reference model for DNS server configuration in IPv6 networks.

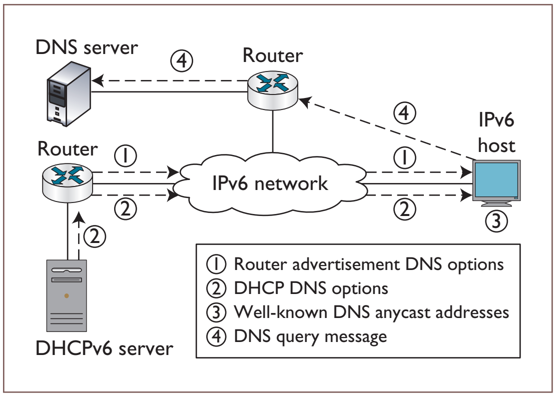

Figure 1. Reference model for DNS configuration in IPv6 networks. In this model, the network administrator must preconfigure the router advertisement and DHCPv6 approaches in the router and DHCPv6 server. Anycast can be configured in the IPv6 host independently.

IPv6 Router Advertisement Approach

An IPv6 host can obtain information about available DNS server addresses and the server search list using the recursive DNS server (RDNSS) option for a list of addresses for DNS name resolution, or the DNS search list (DNSSL) option for a list of domain suffix names for fully qualified domain name construction.[4] Figures 2a and 2b describe the router advertisement RDNSS and DNSSL option formats, respectively. A detailed option field description is available elsewhere.[4] This approach uses existing neighbor discovery transport mechanisms (that is, router advertisement and router solicitation).

The router advertisement approach for DNS options is similar to how IPv6 hosts use neighbor discovery to learn about routers and prefixes on a link. An IPv6 host can configure the IPv6 DNS server address and the DNS search list via a router advertisement message periodically sent by a router or solicited by an IPv6 host's router. In this approach, the routers sending the advertisements must be configured with the DNS server address and DNS search list. The network administrator can manually configure the routers, or the configuration can be automated, such as through a DHCPv6 client running on the router. When advertising more than one RDNSS option, a router advertisement message can deliver as many RDNSS options as it can accommodate in an IPv6 datagram. The same rule applies to the DNSSL option.

Through the Neighbor Discovery Protocol (NDP), when delivering an RDNSS option and DNSSL option as well as a prefix information option with one router advertisement message, an IPv6 host can simultaneously configure its own IPv6 address, DNS server addresses, and DNS search list. By using a one-way router advertisement message, this network configuration minimizes configuration time. Networks that support neighbor discovery will also support the router advertisement options for RDNSS and DNSSL. These options include a lifetime field that the IPv6 host can configure to a value that will let the client time out the entry and switch over to another DNS server address or DNS search name list near its current roaming network. However, from an implementation viewpoint, lifetime might make matters a bit more complex. For example, instead of just writing the DNS configuration file, such as a resolv.conf in Unix (or Linux) for the list of DNS server addresses and DNS search list, the IPv6 host must run a daemon (or a program that's called at the defined intervals) that continuously monitors the DNS server lifetime.

To reduce DNS query resolution time, the IPv6 host uses the most recently received DNS server address and DNS search list, assuming that the most recently received router advertisement reflects the locality of the nearest DNS server and DNS search list. In addition, mobile hosts moving to different domains are usually denied access to DNS servers from outside their access network. Thus, DNS query resolution should use the most recently announced DNS servers rather than the servers announced in the previous access network.

DHCPv6 Approach

DHCPv6 includes the DNS recursive name server option and the domain search list option.[5] Figures 2c and 2d describe these two DHCPv6 DNS option formats. Field descriptions are available elsewhere.[5] The DNS servers and

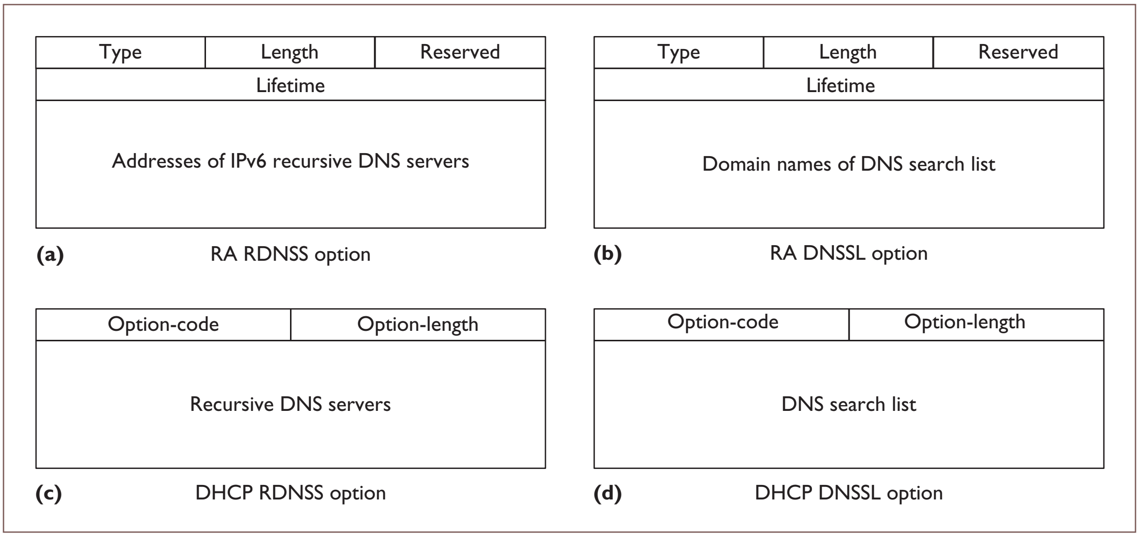

Figure 2. IPv6 host DNS configuration through router advertisement using the (a) recursive DNS server (RDNSS) and (b) DNS search list (DNSSL) options; and through DHCP using the (c) RDNSS and (d) DNSSL options. For both approaches, new options are required in the existing specifications to delegate DNS information. The IETF has standardized these options, which run in the current IPv6 networks.

domain names are listed in these two options in preference order for use by the DNS resolver on the host. DHCPv6 reply messages carry the DHCPv6 DNS options in response to requests or information-request messages. Thus, the IPv6 host can opt for the DNS options when using DHCPv6 for address assignment or when using stateless DHCPv6 to obtain other configuration information.[7]

DHCPv6 provides a mechanism for reconfiguring and propagating new configuration information to DHCPv6 clients when DNS information (such as DNS servers and the DNS search list) is changed or updated.

DHCPv6 and neighbor discovery for DNS configuration can be used on links that don't support multicast – that is, nonbroadcast multiple access (NBMA) network links – as long as those links support the LAN emulation for multicast.[8]

Well-Known Anycast Addresses Approach

In the third approach, DNS servers' well-known anycast addresses are set in the IPv6 host's resolver configuration file (or registry) as factory default.[6] This approach can remove the protocol overhead (that is, delay and control traffic) for DNS configuration in IPv6 hosts. The IPv6 anycast address uses the same format as the IPv6 unicast address.[9] The Internet Assigned Numbers Authority (IANA) doesn't yet assign well-known anycast addresses to DNS services, but because this approach requires no transport mechanism and no packet format for zero-latency DNS configuration, we consider it a candidate for IPv6 DNS configuration.[6]

The IPv6 anycast address assigns an IPv6 anycast address to more than one interface, and a packet sent to an anycast address is routed to the nearest interface with that address, according to the routing protocol's measure of distance, such as hop count.[9] Using the anycast feature, the IPv6 host can send DNS messages to the nearest or a specific DNS server.

Multiple DNS servers share an anycast address. The system routes a DNS request message from a client to the anycast address to exactly one of the DNS servers sharing that address. Anycast routing can be realized such that a DNS query with an anycast destination address is routed to the DNS server with the lowest routing distance, which might be a hop count or some other metric. We don't recommend mandating a site boundary (defined as a marginal region of topology belonging to a single organization and located within a single geographic location as part of an independently administered network such as a campus or company network) for anycast addresses to prevent the DNS queries from crossing this boundary for limited DNS query propagation. For an anycasting site boundary, well-known anycast addresses are registered as host route entries[9] into routers placed at the site boundary, which can physically limit the forwarding of a DNS query within the sites' networks. Anycasting among sites might be supported when sites without their own DNS servers want to access their ISPs' DNS servers across their site boundaries. However, because many sites run their own DNS servers, network administrators will rarely use anycast routing of DNS queries across site boundaries.

For efficient link usage, a network should have only one DNS server for a given anycast address on an IPv6 link, so only one DNS server can respond to DNS queries. The well-known anycast addresses configuration provides better redundancy when multiple DNS servers have different anycast addresses than when they share the same address. When the servers have different addresses, stale servers (retired from the DNS service) can redirect messages to anycast addresses toward the other servers. Thus, one server with an anycast address can cover a small-scale routing domain without requiring DNS traffic load distribution.

The well-known anycast addresses approach can interwork with the router advertisement and DHCP approaches when they're available.[3] As a first option, IPv6 hosts prefer well-known anycast addresses for DNS resolution even when the router advertisement or DHCP options are available. As a second option, both the router advertisement and DHCP options override preconfigured well-known anycast addresses in IPv6 hosts. If both router advertisement and DHCP provide IPv6 hosts with DNS configuration information, the hosts prefer the information from DHCP for DNS queries over that from router advertisement.[4] Thus, the DNS options from router advertisement and DHCP are stored in the DNS configuration file (for example, resolv.conf) such that the DNS information from DHCP appears earlier in the file than that from router advertisement.[4] When neither router advertisement nor DHCP can provide IPv6 DNS options for IPv6 hosts, they use the well-known anycast addresses as a last resort for DNS name resolution. We recommend the second option because both router advertisement and DHCP explicitly provide IPv6 hosts with RDNSS addresses.

Because IANA doesn't yet assign well-known anycast addresses for DNS service, network administrators can use router advertisement or the DHCP approach to configure IPv6 hosts with anycast addresses, as discussed earlier. Administrators can choose any anycast address for DNS service according to their local policy. Once IANA begins to assign well-known anycast addresses, the router advertisement and DHCP approaches will still be useful for automatically configuring these addresses in IPv6 hosts.

Deployment Scenarios

We deployed the three IPv6 DNS configuration approaches in four scenarios: an ISP network, a 3GPP network, an enterprise network, and an unmanaged network.

ISP Network

An ISP network provides Internet connectivity to many public or private networks. Figure 3a shows a typical ISP network providing Internet connectivity to various customer networks — enterprise, campus, downtown, and city. As the figure shows, in an ISP network, multiple customer premises equipment (CPE) devices are connected to IPv6 Provider Edge routers, which connect these devices to the backbone network infrastructure.

CPEs can be hosts or routers. If the CPE is a router, it connects a customer network to the ISP backbone. Typically, an IPv6 Provider Edge router assigns a different IPv6 prefix to each customer network, but the different IPv6 prefix networks have the same DNS configuration. In this case, the CPE might copy the DNS configuration information from the router advertisement on the interface connected to the ISP into the router advertisements in the customer network. When the CPE is a host, it can use the RDNSS and DNSSL options to simultaneously get DNS configuration information and 64-bit prefix information for stateless address autoconfiguration when it's attached to a new subnet. Because an IPv6 host must receive at least one router advertisement message for stateless address autoconfiguration and router configuration, the host could receive RDNSS and DNSSL options in the router advertisement without an additional message exchange. A secure neighbor discovery operation called `SEND` can provide extended security for router advertisement messages.

An IPv6 host can use DHCPv6 for DNS configuration through DNS options, and DHCPv6 can provide other configuration information in

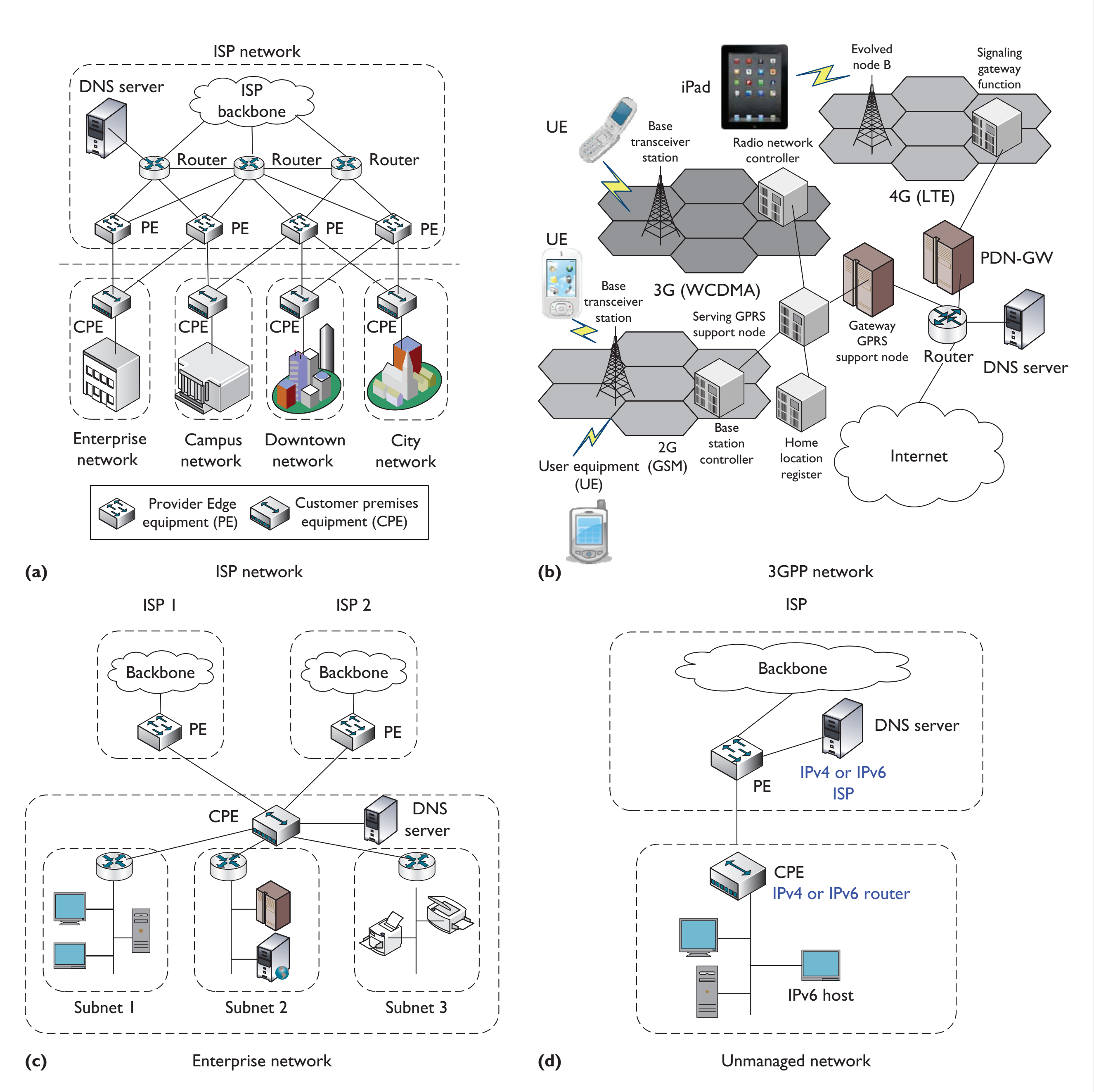

Figure 3. IPv6 deployment scenarios: (a) ISP network, (b) 3GPP network, (c) enterprise network, and (d) unmanaged network (such as a home network).

the same message. DHCP is a client-server protocol, so an ISP can handle user identification on its network intentionally, and can use authenticated DHCP for secure message exchange.

The expected model for IPv6 deployment by ISPs is to assign a prefix to each customer. The customer gateway will use this prefix to assign a 64-bit prefix to each subnetwork, which includes multiple IPv6 hosts. ISPs already use prefix delegation with DHCP to automatically assign the customer prefix to the customer gateway. DNS configuration information can be carried in the same DHCPv6 message exchange to provide this prefix information, along with any other configuration information that the customer gateway or network needs. This service model can be useful to home or small office/home office (SOHO) subscribers. The home or

SOHO gateway, which is a customer gateway for an ISP, can then pass that DNS configuration information to the hosts in the customer network through DHCP.

The well-known anycast addresses approach is also a feasible, simple mechanism for ISPs. The approach avoids security risks in rogue messages sent through external protocols, such as router advertisement or DHCPv6. Rogue router advertisements are an orthogonal problem. For example, even when a host is using DNS anycast, a rogue router advertisement can effectively perform a denial-of-service attack on it. Configuring hosts for well-known anycast addresses requires no protocol or manual configuration; however, configuring routers for these addresses requires the network administrator's intervention. In addition, subscribers must have an equal number of special anycast addresses and DNS servers available to them.

3GPP Network

IPv6 DNS configuration is an important part of the basic IPv6 functionality in 3GPP networks, such as 2G, 3G, and 4G networks. Here, we focus on the DNS configuration of 3G networks, the most popular 3GPP networks, even though 4G networks (such as long-term evolution, or LTE) are now being deployed. The 3GPP network architecture depicted in Figure 3b includes a dedicated link between the user equipment and the gateway General Packet Radio Service (GPRS) support node (GGSN), which serves as a default router. In 3G networks, this dedicated link is called the Packet Data Protocol (PDP) context,[10] where GPRS supports packet-switched functionality for Internet data delivery. In the 4G LTE network in Figure 3b, Packet Data Network Gateway (PDN-GW)[11] provides functions similar to GGSN, such as IP address allocation to user equipment. This dedicated link is created through the PDP context activation procedure in 3G networks.[12]

A separate PDP context type exists for IPv4 and IPv6 traffic. If a 3GPP device is communicating using IPv6 (having an active IPv6 PDP context), the user doesn't necessarily have a simultaneously active IPv4 PDP context, so the user can't send DNS queries using IPv4. If a 3GPP device becomes an IPv6 node, it must discover the DNS server addresses and the DNS search list for DNS name resolution of IP-based services (for example, Web browsing or email).

3GPP defines the Protocol Configuration Options Information Element (PCO-IE) mechanism as a control plane mechanism in which a device can receive DNS server addresses and the DNS search list in the PDP context activation. Note that this PCO-IE exists as an additional mechanism for protocol configuration according to specific 3GPP network versions (such as the Global System for Mobile Communications, Wideband Code Division Multiple Access, and LTE). However, the DNS configuration in the network layer (for example, IPv6) can provide a common interface for DNS configuration for all 3GPP network versions including 4G, leading to low protocol development costs. The DNS server addresses and the DNS search list can also be received over the air using text messages, or manually typed into the user's device. However, users don't want to type such extremely long IPv6 DNS server addresses or the DNS search list into their devices. Thus, mechanisms such as PCO-IE and manual configuration for DNS aren't sufficient for the 3GPP environment.

Because IPv6 was originally intended to operate in a zero-configuration manner, no matter the underlying network infrastructure, DNS configuration was required in IPv6, and the DNS options were standardized in RFC 6106 for integration with IPv6 stateless address autoconfiguration.[4] From a 3GPP viewpoint, the best IPv6 DNS configuration solution should be feasible for a large number of IPv6-capable devices with low control traffic for DNS configuration and shouldn't require any user action.

The router advertisement approach is a lightweight IPv6 DNS configuration mechanism that requires minor changes in the 3GPP device and GGSN IPv6 stacks. In this solution, an IPv6-capable device configures its IPv6 address and DNS information through router advertisement messages sent by its default router (GGSN). This lightweight solution is scalable for many devices. The operator can configure the RDNSS addresses and DNS search list in the GGSN as a part of normal GGSN configuration. Moreover, the equipment software update must be fairly straightforward, and new IPv6 equipment should support the router advertisement extension from the beginning.

For the DHCPv6 solution, the network administrator must implement stateless DHCPv6 and DHCPv6 DNS options in the user device, and a DHCPv6 server in the operator's network. One possible configuration is for the GGSN to act as a DHCP relay. Clearly, DHCPv6 creates additional software implementation overhead and requires additional runtime resources (for example, processor time and memory space) to run the DHCPv6 client. Actually, the router advertisement approach also creates less traffic overhead. Nevertheless, to support a network configuration (for example, intersystem mobility policies and access-network-specific information) other than a DNS configuration, DHCPv6 must be implemented in user devices with more runtime resource consumption.[13]

The well-known anycast addresses approach is also a feasible, light-weight mechanism for 3GPP devices. Users can configure well-known anycast addresses in the device software, with the operator making the corresponding configuration on the network side for anycast routing. Thus, this is an easy mechanism for the device, but requires some configuration work in the network. When using well-known anycast addresses, devices forward queries to any of the preconfigured addresses.

Enterprise Network

An enterprise network has multiple internal links, one or more router connections to one or more providers, and is actively managed by a network operation entity. Figure 3c shows a typical enterprise network consisting of multiple subnets. This enterprise network is connected to the Provider Edge routers of two ISPs (ISP 1 and ISP 2) through its CPE, which is a border gateway router. An enterprise network can obtain network prefixes from an ISP by either manual configuration or prefix delegation.[14] In most cases, because an enterprise network manages its own DNS domains, it operates its own DNS servers for its domains, as Figure 3c shows. These DNS servers process DNS name resolution requests from IPv6 hosts as RDNSSs.

All three approaches, or some combination of them, can be used together for DNS configuration in an IPv6 enterprise network according to its local policy. The well-known anycast addresses approach can be combined with the router advertisement or DHCP approaches, as discussed earlier. When the enterprise provides either router advertisement or DHCPv6 for DNS configuration, IPv6 hosts can decide which approach it will use in its subnet with an O flag in the router advertisement message.[1,4] In this case, IPv6 hosts prefer the RDNSS addresses delivered through router advertisement or DHCP to the well-known anycast addresses approach. If the enterprise network provides IPv6 hosts with both router advertisement and DHCP options for DNS configuration, the latter are preferable for DNS name resolution.[4]

Unmanaged Network

The deployment cases of interest in unmanaged networks, such as home or office networks, include

- a gateway that doesn't provide IPv6 at all,
- a dual-stack gateway connected to a dual-stack ISP,
- a dual-stack gateway connected to an IPv4-only ISP, and
- a gateway connected to an IPv6-only ISP.

Figure 3d shows these four scenarios in a home network. In the figure, CPE is the gateway for the home network, and Provider Edge equipment is the access router in the ISP network to provide IPv4 or IPv6 Internet connectivity.

In the first case, the gateway CPE doesn't provide IPv6 for dual-stack IPv6 hosts, and the ISP might or might not provide IPv6. In this scenario, automatic or configured tunnels connect the IPv6 hosts and tunnel servers over an IPv4 network. In addition, dual-stack hosts behind a network address translator (NAT) running in the unmanaged network's CPE might need access to an IPv6 DNS server. In this case, the DNS configuration mechanism must work over the tunnel, and the underlying tunneling mechanism must support NAT traversal. In this case, we assume the tunnel server acts as a relay (for both the DHCPv6 and well-known anycast addresses approaches). We can use the IPv6 router advertisement approach in a relatively straightforward way if the tunnel server is the IPv6 router emitting router advertisements. The well-known anycast addresses approach also seems simple in operation across the tunnel, but its deployment in a tunneled environment isn't yet well studied.

In the second case, a dual-stack gateway (denoted as CPE) is connected to a dual-stack ISP. In this case, DHCPv4 passes the addresses of the DNS servers accessible through IPv4, and

Table 1. Comparison of three approaches for IPv6 DNS configuration.

Approach	Configuration place	No. of messages for configuration	DNS server address option	DNS search list option	Related RFC	Target networks	Implementation
Router advertisement option	Router	1	Yes	Yes	RFC 6106	Mobile networks, unmanaged networks	iOS, Windows, Linux, FreeBSD, Cisco IOS
DHCP option	DHCP server	2	Yes	Yes	RFC 3646	Enterprise networks, ISP networks	iOS, Android, Windows, Linux, FreeBSD, Cisco IOS
Well-known anycast addresses	IPv6 host	0	Yes	No	None	ISP networks	N/A

IPv6 neighbor discovery and DHCPv6 (or stateless DHCPv6) pass the addresses of the DNS servers accessible through IPv6. Thus, dual-stack hosts must combine information about IPv4 and IPv6 DNS services into a single list. The IETF's Multiple Interfaces (MIF) working group is developing a specification for this function. In theory, the responses returned by a DNS server are independent of the IP version used to query the server, and all DNS servers should return the same response to a given query. Therefore, all DNS servers can be considered equivalent. The network administrator can also use the well-known anycast addresses approach in this dual-stack scenario together with the router advertisement and DHCPv6 approaches in the same way as in the enterprise network discussed earlier.

In the third case, a dual-stack gateway (denoted as CPE) is connected to an IPv4-only ISP (similarly to the first case). If a gateway provides IPv6 connectivity for IPv6 hosts by managing tunnels, it must also provide access to a DNS server for the IPv6 hosts through the tunnels. This case is different from the first in that the tunnel for IPv6 connectivity (as IPv6 over IPv4) originates from the dual-stack gateway CPE instead of the unmanaged network's IPv6 host.

In the last case, a gateway (denoted as CPE) is connected to an IPv6-only ISP. This is similar to the second case because the gateway has an IPv6 stack and is connected to an IPv6 ISP network. We can use DHCPv6 and stateless DHCPv6 for IPv6 DNS configuration in the IPv6 hosts. We could also use the router advertisement approach and well-known anycast addresses approach because the unmanaged network and the ISP network are IPv6 networks. The network in this case is a pure IPv6 network consisting of an IPv6 unmanaged network and an IPv6 ISP network — different from the second case, where IPv4 and IPv6 networks coexist.

The gateway CPE doesn't always pass the same DNS configuration information to the hosts in the unmanaged network that the gateway uses for its own DNS resolution. For example, in the third case, the gateway obtains DNS information from the DHCPv4 server and uses it for DNS name resolution. On the other hand, this gateway can provide IPv6 hosts in the unmanaged network with the different DNS information obtained through the tunneled IPv6 network.

IPv6 network administrators and users can use Table 1 to select the appropriate DNS configuration for their networks.

As the table shows, the router advertisement approach is appropriate for mobile networks (such as 3G/4G networks) serving mobile devices because it can configure them for their IPv6 address and DNS configuration (that is, RDNSS and DNSSL) together in a router advertisement message, leading to efficient link usage for DNS configuration. The router advertisement approach also suits unmanaged networks (for example, small home and office networks using a WLAN) that don't need tight network access control.

The DHCP option is appropriate for enterprise and ISP networks requiring tight network administration because it's used for IPv6 address configuration to authenticated network nodes. The DHCP option for DNS search list is also provided to IPv6 hosts in enterprise and ISP networks that use the DNS search list for DNS name resolution.

Centrally configured ISP networks can use the well-known anycast addresses approach for DNS service configuration such that anycast routing can load balance DNS queries from IPv6 hosts in customer networks (such as unmanaged networks) toward DNS servers. Because routers in these networks don't use the DNS search list for DNS name resolution, the well-known anycast addresses approach is sufficient.

Acknowledgments

This research was supported by Korea's Ministry of Science, ICT, and Future Planning under the Information Technology Research Center support program supervised by the National IT Promotion Agency (NIPA-2013-(H0301-13-2001)). This research was also supported in part by the Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (no. 2012033347). Choong Seon Hong is the corresponding author of this article.

References

1. T. Narten, E. Nordmark, and W. Simpson, *Neighbor Discovery for IP Version 6 (IPv6)*, IETF RFC 4861, Sept. 2007; www.ietf.org/rfc/rfc4861.txt.
2. S. Thomson and T. Narten, *IPv6 Stateless Address Autoconfiguration*, IETF RFC 4862, Sept. 2007; www.ietf.org/rfc/rfc4862.txt.
3. J. Jeong et al., *IPv6 Host Configuration of DNS Server Information Approaches*, IETF RFC 4339, Feb. 2006; www.ietf.org/rfc/rfc4339.txt.
4. J. Jeong et al., *IPv6 Router Advertisement Options for DNS Configuration*, IETF RFC 6106, Nov. 2010; www.ietf.org/rfc/rfc6106.txt.
5. R. Droms et al., *DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, IETF RFC 3646, Dec. 2003; www.ietf.org/rfc/rfc3646.txt.
6. M. Ohta, "Preconfigured DNS Server Addresses," IETF Internet draft, work in progress, Feb. 2004.
7. R. Droms, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*, IETF RFC 3736, Apr. 2004; www.ietf.org/rfc/rfc3736.txt.
8. G. Armitage et al., *IPv6 over Non-Broadcast Multiple Access (NBMA) Networks*, IETF RFC 2491, Jan. 1999; www.ietf.org/rfc/rfc2491.txt.
9. R. Hinden and S. Deering, *Internet Protocol Version 6 (IPv6) Addressing Architecture*, IETF RFC 4291, Apr. 2003; www.ietf.org/rfc/rfc4291.txt.
10. M. Wasserman, *Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards*, IETF RFC 3314, Sept. 2002; www.ietf.org/rfc/rfc3314.txt.
11. C. Monfreid, "The LTE Network Architecture — A Comprehensive Tutorial," Alcatel-Lucent white paper, 2012; www.telecomsource.net/showthread.php?2021-The-LTE-Network-Architecture-A-Comprehensive-Tutorial-(white-paper)#.UXkHf7WsiSo.
12. "General Packet Radio Service (GPRS); Service Description; Stage 2 (Release 5)," 3GPP TS 23.060 V5.4.0, Dec. 2002; www.3gpp.org/ftp/Specs/html-info/23060.htm.
13. S. Das and G. Bajko, *DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery*, IETF RFC 6153, Feb. 2011; www.ietf.org/rfc/rfc6153.txt.
14. O. Troan and R. Droms, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6*, IETF RFC 3633, Dec. 2003; www.ietf.org/rfc/rfc3633.txt.

Soohong Park is a senior standards specialist in the Software R&D Center at Samsung Electronics. His research includes wireless and mobile networks, the Internet Protocol, and application and ontology metadata. Park has a PhD from the Department of Computer Engineering at Kyung Hee University. He's a member of IEEE. Contact him at soohongp@gmail.com.

Jaehoon (Paul) Jeong is an assistant professor in the Department of Software at Sungkyunkwan University, Korea. His research includes vehicular networks, wireless sensor networks, and mobile ad hoc networks. Jeong has a PhD from the Department of Computer Science and Engineering at the University of Minnesota, Twin Cities. He's a member of IEEE, the IEEE Computer Society, and ACM. Contact him at pauljeong@skku.edu.

Choong Seon Hong is a professor of computer engineering at Kyung Hee University. His research interests include ad hoc networks, Internet services and management, cognitive radio networks, network security, and the future Internet. Hong has a PhD in information and computer science from Keio University. He's a senior member of IEEE, and a member of ACM, the Institute of Electronics, Information, and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), the Korean Institute of Information Scientists and Engineers (KIISE), the Korean Institute of Communications and Information Sciences (KICS), and the Korea Information Processing Society (KIPS). Contact him at cshong@khu.ac.kr.