INTERNET-DRAFT Y. Shirasaki
Expires: October, 2004 S. Miyakawa
T. Yamasaki
NTT Communications
A. Takenouchi
NTT
April 27, 2004

A Model of IPv6/IPv4 Dual Stack Internet Access Service
draft-shirasaki-dualstack-service-04.txt

Status of this Memo

Abstract

This memo shows an example of how to provide IPv6 / IPv4 dual stack services to home users. In order to simplify user setup, these services should have a mechanism to configure IPv6 specific parameters automatically. We focus on two basic parameters, the prefix assigned to the user and the addresses of IPv6 DNS servers, and specify the way to deliver them to Customer Premises Equipments (CPE) automatically.

This memo is a digest of the user network interface specification of NTT communications' dual stack ADSL access service.

1. Introduction

This memo describes two topics. One is the architecture of IPv6/IPv4 dual stack access service. The other is the automatic configuration function for IPv6 specific parameters.

The architecture is mainly targeted at a leased line ADSL service for home users. It assumes that there is a Point-to-Point Protocol (PPP) logical link between CPE and Provider Edge (PE). In order to exclude factors which are specific to access lines from this architecture, we only specify PPP and its upper layers. To satisfy [RFC3177], the length of prefix which is delegated to CPE is /48, but /64 is also a possible option.

In this architecture, IPv6/IPv4 dual stack service is specified as follows.

o IPv6 and IPv4 connectivities are provided over a single PPP logical link.

o IPv6 connectivity is independent of IPv4 connectivity. IPV6CP and IPCP work independently over a single PPP logical link.

Figure 1 shows the outline of the service architecture. NTT Communications is providing a commercial service based on this architecture since the Summer 2002.

```
       |                                             _____________
[HOST]-+ +-----------+               +----------+   /             \
       | | Customer  |   ADSL line   | Provider |  | ISP core and  |
       +-+ Premises  +---------------+   Edge   |--| The internet  |
       | | Equipment | to subscriber +-----+----+   \_____________/
[HOST]-+ +-----------+                     |         |   |
       |                             +-----+------+  | +-+----------+
                                     | AAA server |  | | DNS server |
                                     +------------+  | +------------+
                                                   +-+--------------+
                                                   | NTP server etc.|
                                                   +----------------+
```

Figure 1: Dual stack access service architecture

The automatic configuration function aims at simplification of user setup. Usually, users have to configure at least two IPv6 specific parameters, prefix(es) assigned to them and IPv6 DNS servers' addresses. The function is composed of two sub-functions as below.

o Delegation of prefix(es) to be used in the user site

o Notification of IPv6 DNS server addresses, and/or other server addresses

Section 2 of this memo details user network interface. Section 3 describes an example of connection sequence.

2. User Network Interface

In this section, details of the user network interface specification are described. Only PPP over Ethernet (PPPoE) and its upper layers are mentioned. The other layers such as Ethernet and lower layers are out of scope. IPv4 related parameter configuration is also out of scope.

2.1. Below the IP Layer

The service uses PPP connection and Challenge Handshake Authentication Protocol (CHAP) authentication to identify each CPE. Both CPE and PE handle both IPCP [RFC1661] and IPV6CP [RFC2472] identically / simultaneously over a single PPP connection. It means either CPE or PE can open/close any Network Control Protocol (NCP) session anytime without any side-effect for each other. It is intended that users can choose between three services, IPv4 only, IPv6 only and IPv4/IPv6 dual stack. A CPE connected to an ADSL line discovers a PE with PPPoE mechanism [RFC2516].

Note that because CPE and PE can negotiate only their interface identifiers with IPV6CP, PE and CPE can use only link-local scope addresses before the prefix delegation mechanism, described below, is run.

2.2. IP Layer

After IPV6CP negotiation, the CPE initiates a prefix delegation request. The PE chooses global-scope prefix for the CPE with information from an Authentication, Authorization, and Accounting (AAA) server or local prefix pools, and delegates the prefix to the CPE. Once the prefix is delegated, the prefix is subnetted and assigned to the local interfaces of the CPE. The CPE begins sending router advertisement of the prefixes on each links. Eventually hosts can acquire global-scope prefixes through conventional IPv6 stateless [RFC2462] or stateful auto-configuration mechanisms [RFC3315] etc, and become to communicate using global-scope addresses.

2.3. Prefix Delegation

PE delegates prefixes to CPE by DHCPv6 [RFC3315] with prefix delegation options [RFC3633]. The model of sequence for prefix delegation is as follows:

- o A CPE requests prefix(es) from a PE by sending a DHCPv6 Solicit message which has a link-local source address negotiated by IPV6CP, mentioned in the previous section, and includes an IA_PD option.

- o An AAA server notifies prefix(es) to the PE, or the PE chooses prefix(es) from its local pool and the PE returns an Advertise message which contains an IA_PD option and IA_PD Prefix options. The prefix-length in the IA_PD Prefix option is 48.

- o The CPE chooses prefix(es) and sends a Request message containing an IA_PD option and IA_PD Prefix options for chosen prefix(es) back to the PE.

- o The PE confirms the prefix(es) in the Request message and returns a Reply message.

If IPV6CP is terminated or restarted by any reason, CPE must initiate a Rebind/Reply message exchange as described in [RFC3633].

2.4. Address Assignment

CPE assigns global-scope /64 prefixes subnetted from the delegated prefix to its downstream interfaces. In the case where the delegated prefix has infinite lifetimes, the preferred and valid lifetimes of assigned /64 prefixes should be their default values in [RFC2461].

Because a link-local address is already assigned to CPE's upstream interface, global-scope address assignment for that interface is optional.

2.5. Routing

CPE and PE use static routing between them, and no routing protocol traffic is necessary.

CPE configures its PPPoE logical interface or the link-local address of PE as IPv6 default gateway automatically after the prefix delegation exchange.

When CPE receives packets which are destined for the addresses in the delegated /48 prefix, CPE must not forward the packets to a PE. CPE should return ICMPv6 Destination Unreachable message to a source

address or silently discard the packets, when the original packet is destined for the unassigned prefix in the delegated prefix. (e.g. CPE should install a reject route or null interface as next hop for the delegated prefix.)

2.6. Obtaining Addresses of DNS Servers

The service provides IPv6 recursive DNS servers in the ISP site. PE notifies the global unicast addresses of these servers with Domain Name Server option, which is described in [RFC3646], in Advertise/Reply messages on the prefix delegation message exchange.

Devices connected to user network may know recursive DNS server address with the mechanism described in [RFC3736].

The CPE may serve as a local DNS proxy server and include its address into the DNS server address list. This is easy to implement, because it is an analogy of IPv4 SOHO router (192.168.0.1 is a DNS proxy server and a default router in most sites).

2.7. Miscellaneous Information

PE may notify other IPv6 enabled server addresses such as Network Time Protocol servers [OPT-NTP], SIP servers [RFC3319], etc. in an Advertise/Reply messages on the prefix delegation message exchange if those are available.

2.8. Connectivity Monitoring

ICMPv6 Echo Request will be sent to user network for connectivity monitoring in the service. CPE must return single IPv6 Echo Reply packet when it receives ICMPv6 Echo Request packet. The health check packets are destined for subnet-router anycast address for the delegated prefix.

The old document of APNIC IPv6 address assignment policy required that APNIC could ping the subnet anycast address to check an address usage.

To achieve this requirement, for example, once the prefix 3ffe:ffff:ffff::/48 is delegated, the CPE must reply to the ICMPv6 Echo Request destined for 3ffe:ffff:ffff:: anytime while IPV6CP and DHCPv6-PD for upstream is up. Because some implementations couldn't reply when 3ffe:ffff:ffff::/64 was assigned to its downstream physical interface and the interface is down, such implementation should assign 3ffe:ffff:ffff::/64 for loopback interface, which is always up, and 3ffe:ffff:ffff:1::/64, 3ffe:ffff:ffff:2::/64, etc. for physical interfaces.

3. An Example of Connection Sequence

Following figure is an example of normal link-up sequence from start of PPPoE to start of IPv6/IPv4 communications. IPv4 communication becomes available after IPCP negotiation. IPv6 communication with link-local scope addresses becomes possible after IPV6CP negotiation. IPv6 communication with global-scope addresses becomes possible after prefix delegation and conventional IPv6 address configuration mechanism. IPCP is independent of IPV6CP and prefix delegation.

```
CPE                      PE
 |                        |
 |----------PADI-------->| \
 |<---------PADO---------|  | PPPoE
 |----------PADR-------->|  | Discovery Stage
 |<---------PADS---------| /
 |                        |
 |---Configure-Request-->| \
 |<--Configure-Request---|  | PPP Link Establishment Phase
 |<----Configure-Ack-----|  | (LCP)
 |-----Configure-Ack---->| /
 |                        |
 |<------Challenge-------| \
 |-------Response------->|  | PPP Authentication Phase (CHAP)
 |<-------Success--------| /
 |                        |
 |---Configure-Request-->| \
 |<--Configure-Request---|  |
 |<----Configure-Nak-----|  | PPP Network Layer Protocol Phase
 |<----Configure-Ack-----|  | (IPCP)
 |---Configure-Request-->|  |
 |<----Configure-Ack-----| /
 |                        |
 |---Configure-Request-->| \
 |<--Configure-Request---|  | PPP Network Layer Protocol Phase
 |<----Configure-Ack-----|  | (IPV6CP)
 |-----Configure-Ack---->| /
 |                        |
 |--------Solicit------->| \
 |<------Advertise-------|  | DHCPv6
 |--------Request------->|  |
 |<--------Reply---------| /
 |                        |
```

Figure 2: An example of connection sequence

4. Security Considerations

In this architecture, PE and CPE trusts the point-to-point link between them, where one trusts that there is no man-in-the-middle, and trusts PPPoE authentication. Because of this, the DHCP authentication is not considered necessary and is not used.

The service provides always-on global-scope prefix for users. Each device connected to user network has global-scope addresses. Without any packet filters, devices might be accessible from outside of the user network in that case. CPE and each device involved in the service should have functionality against unauthorized accesses such as stateful inspection packet filter. Relationship between CPE and devices connected to user network for this problem should be considered in the future.

5. Acknowledgments

Thanks for the input and review by Tatsuya Sato, Hideki Mouri, Koichiro Fujimoto, Hiroki Ishibashi, Ralph Droms, Ole Troan, Pekka Savola, and IPv6-ops-IAJapan members.

Normative References

[RFC3177]
IAB and IESG, "IAB/IESG Recommendations on IPv6 Address Allocations to Sites", RFC 3177, September 2001.

[RFC1661]
Simpson, W., "The Point-to-Point Protocol (PPP)", RFC 1661, July 1994

[RFC2472]
Haskin, D. and Allen, E., "IP Version 6 over PPP", RFC 2472, December 1998.

[RFC2516]
Mamakos, L., "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[RFC2462]
Thomson, S. and Narten, T., "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC3315]
Droms, R., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3633]
Troan, O. and Droms, R., "IPv6 Prefix Options for Dynamic Host

Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC2461]
Narten, T., Nordmark, E. and Simpson, W., "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC3646]
Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC3736]
Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[OPT-NTP]
Vijayabhaskar, A.K., "Simple Network Time Protocol Configuration Option for DHCPv6", draft-ietf-dhc-dhcpv6-opt-sntp-00 (work in progress), November 2003.

[RFC3319]
Schulzrinne, H. and Volz, B., "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers", RFC 3319, July 2003.

Informative References

[PD-Req]
Miyakawa, S. and Droms, R., "Requirements for IPv6 prefix delegation", draft-ietf-ipv6-prefix-delegation-requirement-04 (work in progress), February 2004.

Authors' Addresses

Yasuhiro Shirasaki
NTT Communications Corporation
Tokyo Opera City Tower 21F
3-20-2 Nishi-Shinjuku, Shinjuku-ku
Tokyo 163-1421, Japan
E-mail: yasuhiro@nttv6.jp

Shin Miyakawa, Ph. D
NTT Communications Corporation
Tokyo Opera City Tower 21F
3-20-2 Nishi-Shinjuku, Shinjuku-ku
Tokyo 163-1421, Japan
E-mail: miyakawa@nttv6.jp

Toshiyuki Yamasaki
NTT Communications Corporation
1-1-6 Uchisaiwaicho, Chiyoda-ku
Tokyo 100-8019, Japan
E-mail: t.yamasaki@ntt.com

Ayako Takenouchi
NTT Cyber Solutions Laboratories, NTT Corporation
3-9-11 Midori-Cho, Musashino-Shi
Tokyo 180-8585, Japan
E-mail: takenouchi.ayako@lab.ntt.co.jp

Acknowledgment

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