              A Model of IPv6/IPv4 Dual Stack Internet Access Service

Status of This Memo

Copyright Notice

IESG Note

Abstract

   This memo is a digest of the user network interface specification of
   NTT Communications' dual stack ADSL access service, which provide a
   IPv6/IPv4 dual stack services to home users. In order to simplify
   user setup, these services have a mechanism to configure IPv6
   specific parameters automatically. The memo focuses on two basic
   parameters: the prefix assigned to the user and the addresses of
   IPv6 DNS servers, and it specifies a way to deliver these parameters
   to Customer Premises Equipment (CPE) automatically.

1. Introduction

   This memo is a digest of the user network interface specification of
   NTT Communications' dual stack ADSL access service, which provide
   IPv6/IPv4 dual stack services to home users. In order to simplify
   user setup, these services have a mechanism to configure IPv6
   specific parameters automatically. The memo focuses on two basic
   parameters: the prefix assigned to the user and the addresses of
   IPv6 DNS servers, and it specifies a way to deliver these parameters
   to Customer Premises Equipment (CPE) automatically.

   This memo covers two topics: an architecture for IPv6/IPv4 dual stack
   access service and an 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 Customer Premises Equipment (CPE) and Provider
   Edge (PE) equipment. In order to exclude factors that are specific
   to access lines, this architecture only specifies PPP and its upper
   layers. To satisfy [RFC3177], the prefix length that is delegated to
   the 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 an outline of the service architecture. NTT
   Communications has been providing a commercial service based on this
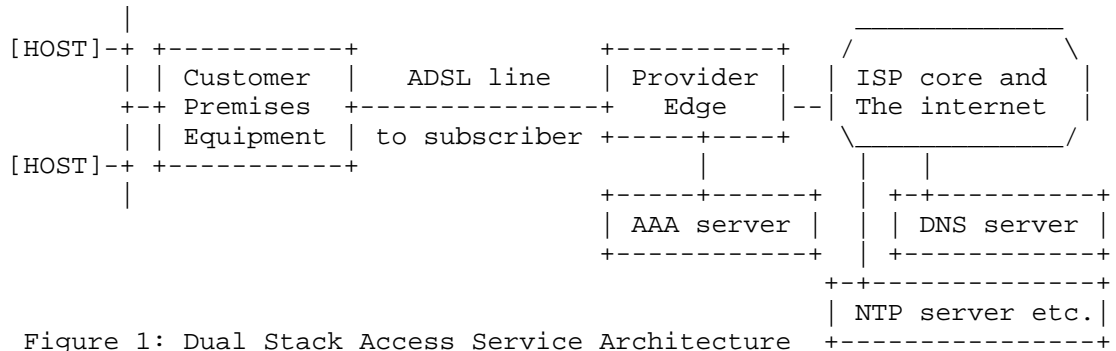   architecture since the Summer 2002.

```
           |                                              _____
[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 [RFC3769] and IPv6 DNS
   servers' addresses. The function is composed of two sub-functions:

      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 the user/network interface. Section 3
   describes an example connection sequence.

2. User/Network Interface

   This section describes details of the user/network interface
   specification. 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.
   The CPE and PE handle both the PPP Internet Protocol Control Protocol
   (IPCP) [RFC1332] and the Internet Protocol V6 Control Protocol
   (IPV6CP) [RFC2472] identically and simultaneously over a single PPP
   connection. This means either the CPE or the PE can open/close any
   Network Control Protocol (NCP) session at any time without any side-
   effect for the other. It is intended that users can choose among
   three services: IPv4 only, IPv6 only, and IPv4/IPv6 dual stack. A
   CPE connected to an ADSL line discovers a PE with the 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 a global-scope prefix for the CPE with
   information from an Authentication, Authorization, and Accounting
   (AAA) server or local prefix pools, and it 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 advertisements for the prefixes on each link. Eventually,
   hosts can acquire global-scope prefixes through conventional IPv6
   stateless [RFC2462] or stateful auto-configuration mechanisms
   ([RFC3315], etc.) and begin to communicate using global-scope
   addresses.

2.3. Prefix Delegation

   The PE delegates prefixes to CPE using Dynamic Host Configuration
   Protocol for IPv6 (DHCPv6) [RFC3315] with the prefix delegation
   options [RFC3633]. The sequence for prefix delegation is as follows:

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

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

       IA_PD option and IA_PD Prefix options for the chosen prefix(es)
       back to the PE.

     o The PE confirms the prefix(es) in the Request message in 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

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

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

2.5. Routing

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

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

   When the CPE receives packets that are destined for the addresses in
   the delegated /48 prefix, the CPE must not forward the packets to a
   PE. The 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.
   (For example, the 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. The
   PE notifies the global unicast addresses of these servers with the
   Domain Name Server option that is described in [RFC3646], in
   Advertise/Reply messages on the prefix delegation message exchange.

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

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

2.7. Miscellaneous Information

   The PE may notify other IPv6-enabled server addresses, such as
   Network Time Protocol servers [RFC4075], SIP servers [RFC3319], etc.,
   in an Advertise/Reply message on the prefix delegation message
   exchange, if those are available.

2.8. Connectivity Monitoring

   ICMPv6 Echo Request will be sent to the user network for connectivity
   monitoring in the service. The CPE must return a single IPv6 Echo
   Reply packet when it receives an ICMPv6 Echo Request packet. The
   health-check packets are addressed to a 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 address
   usage.

To achieve this requirement, for example, once the prefix
2001:db8:ffff::/48 is delegated, the CPE must reply to the ICMPv6
Echo Request destined for 2001:db8:ffff:: any time that IPV6CP and
DHCPv6-PD are up for the upstream direction. Because some
implementations couldn't reply when 2001:db8:ffff::/64 was assigned
to its downstream physical interface and the interface was down, such
an implementation should assign 2001:db8:ffff::/64 for the loopback
interface, which is always up, and 2001:db8:ffff:1::/64,
2001:db8:ffff:2::/64, etc., to physical interfaces.

3. An Example of Connection Sequence

```
          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----------|  /
           |                         |
```
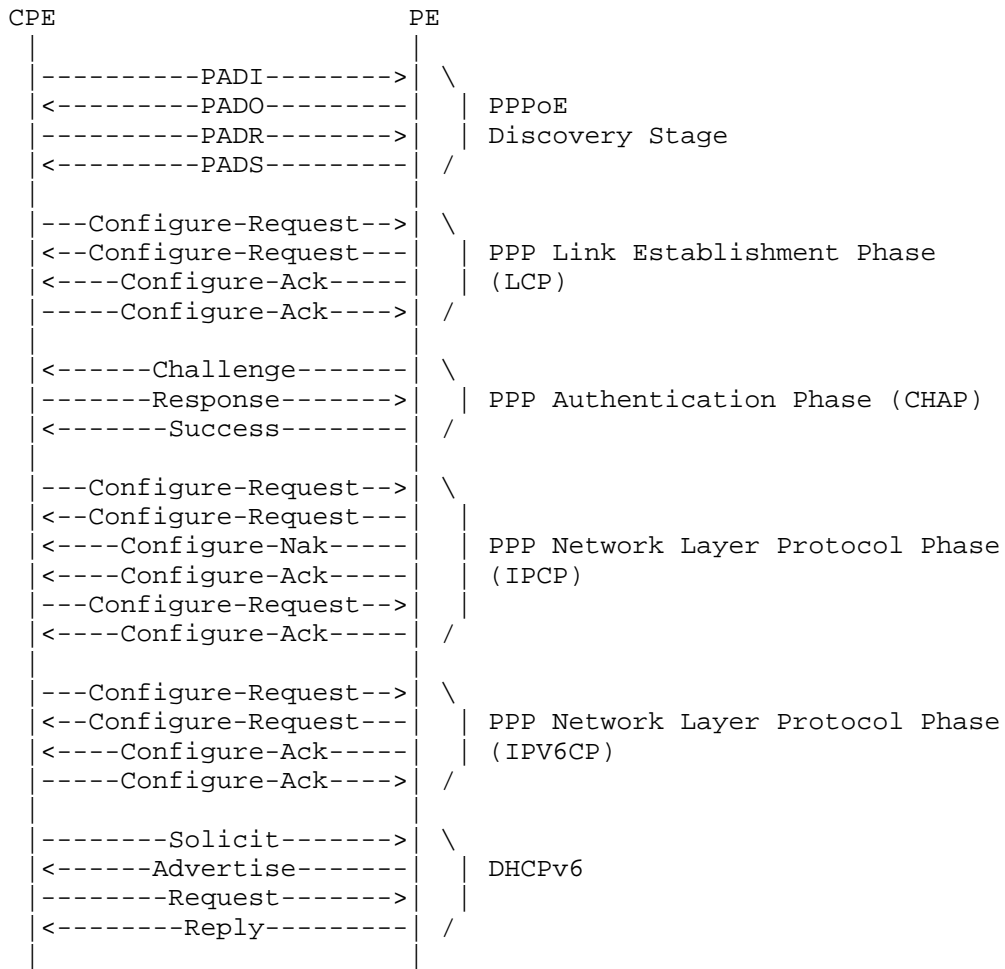
                 Figure 2: Example of Connection Sequence

Figure 2 is an example of a 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.

4. Security Considerations

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

   The service provides an 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
   the user network in that case. The CPE and each device involved in
   the service should have functionality to protect against unauthorized
   accesses, such as a stateful inspection packet filter. The
   relationship between CPE and devices connected to the user network
   for this problem should be considered in the future.

5. Acknowledgements

   Thanks are given 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.

6. References

6.1. Normative References

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

   [RFC1332] McGregor, G., "The PPP Internet Protocol Control Protocol
             (IPCP)", RFC 1332, May 1992.

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

   [RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D.,
             and R. Wheeler, "A Method for Transmitting PPP Over
             Ethernet (PPPoE)", RFC 2516, February 1999.

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

   [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and
             M. Carney, "Dynamic Host Configuration Protocol for IPv6
             (DHCPv6)", RFC 3315, July 2003.

   [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic
             Host Configuration Protocol (DHCP) version 6", RFC 3633,
             December 2003. RFC 3633, December 2003.

   [RFC2461] Narten, T., Nordmark, E. and W. Simpson, "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.

   [RFC4075] Kalusivalingam, V., "Simple Network Time Protocol (SNTP)
             Configuration Option for DHCPv6", RFC 4075, May 2005.

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

6.2. Informative References

   [RFC3769] Miyakawa, S. and R. Droms, "Requirements for IPv6 Prefix
             Delegation", RFC 3769, June 2004.

Authors' Addresses

    Yasuhiro Shirasaki
    NTT Communications Corporation
    Tokyo Opera City Tower 21F
    3-20-2 Nishi-Shinjuku, Shinjuku-ku
    Tokyo 163-1421, Japan

    EMail: 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

    EMail: miyakawa@nttv6.jp

    Toshiyuki Yamasaki
    NTT Communications Corporation
    1-1-6 Uchisaiwaicho, Chiyoda-ku
    Tokyo 100-8019, Japan

    EMail: t.yamasaki@ntt.com

    Ayako Takenouchi
    NTT Cyber Solutions Laboratories, NTT Corporation
    3-9-11 Midori-Cho, Musashino-Shi
    Tokyo 180-8585, Japan

    EMail: takenouchi.ayako@lab.ntt.co.jp

Full Copyright Statement

Intellectual Property

Acknowledgement