Basic Requirements for IPv6 Customer Edge Routers
draft-palet-v6ops-rfc7084-bis-00

Abstract

   This document specifies requirements for an IPv6 Customer Edge (CE)
   router. Specifically, the current version of this document focuses
   on the basic provisioning of an IPv6 CE router and the provisioning
   of IPv6 hosts attached to it. The document also covers several
   transition technologies, as required in a world where IPv4 addresses
   are no longer available, so hosts in the customer LANs with IPv4-only
   or IPv6-only applications or devices, requiring to communicate with
   IPv4-only services at the Internet, are able to do so. The document
   obsoletes RFC 7084.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   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."

   This Internet-Draft will expire on August 24, 2017.

Copyright Notice

Table of Contents

1. Introduction

This document defines basic IPv6 features for a residential or small-
office router, referred to as an "IPv6 CE router", in order to
establish an industry baseline for features to be implemented on such
a router.

These routers typically also support IPv4, at least in the LAN side.

This document specifies how an IPv6 CE router automatically
provisions its WAN interface, acquires address space for provisioning
of its LAN interfaces, and fetches other configuration information
from the service provider network. Automatic provisioning of more

complex topology than a single router with multiple LAN interfaces is
out of scope for this document. In some cases manual provisioning
may be acceptable, when intended for a small number of customers.

See [RFC4779] for a discussion of options available for deploying
IPv6 in service provider access networks.

This document also covers the IP transition technologies required in
a world where IPv4 addresses are no longer available, so the service
providers need to provision IPv6-only WAN access, while at the same
time ensuring that IPv4-only or IPv6-only devices or applications in
the customer LANs can still reach IPv4-only devices or applications
in Internet, which still don't have IPv6 support.

1.1. Requirements Language

Take careful note: Unlike other IETF documents, the key words "MUST",
"MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",
"RECOMMENDED", "MAY", and "OPTIONAL" in this document are not used as
described in RFC 2119 [RFC2119]. This document uses these keywords
not strictly for the purpose of interoperability, but rather for the
purpose of establishing industry-common baseline functionality. As
such, the document points to several other specifications (preferable
in RFC or stable form) to provide additional guidance to implementers
regarding any protocol implementation required to produce a
successful CE router that interoperates successfully with a
particular subset of currently deploying and planned common IPv6
access networks.

2. Terminology

End-User Network   one or more links attached to the IPv6 CE
                            router that connect IPv6 hosts.

IPv6 Customer Edge Router   a node intended for home or small-office
                            use that forwards IPv6 packets not
                            explicitly addressed to itself. The IPv6
                            CE router connects the end-user network to
                            a service provider network.

IPv6 Host   any device implementing an IPv6 stack
                            receiving IPv6 connectivity through the
                            IPv6 CE router.

LAN Interface   an IPv6 CE router's attachment to a link in
                            the end-user network. Examples are
                            Ethernet (simple or bridged), 802.11
                            wireless, or other LAN technologies. An

IPv6 CE router may have one or more
network-layer LAN interfaces.

Service Provider   an entity that provides access to the
                          Internet. In this document, a service
                          provider specifically offers Internet
                          access using IPv6, and it may also offer
                          IPv4 Internet access. The service provider
                          can provide such access over a variety of
                          different transport methods such as DSL,
                          cable, wireless, and others.

WAN Interface   an IPv6 CE router's attachment to a link
                          used to provide connectivity to the service
                          provider network; example link technologies
                          include Ethernet (simple or bridged), PPP
                          links, Frame Relay, or ATM networks, as
                          well as Internet-layer (or higher-layer)
                          "tunnels", such as tunnels over IPv4 or
                          IPv6 itself.

3. Architecture

3.1. Current IPv4 End-User Network Architecture

An end-user network will likely support both IPv4 and IPv6. It is
not expected that an end user will change their existing network
topology with the introduction of IPv6. There are some differences
in how IPv6 works and is provisioned; these differences have
implications for the network architecture. A typical IPv4 end-user
network consists of a "plug and play" router with NAT functionality
and a single link behind it, connected to the service provider
network.

A typical IPv4 NAT deployment by default blocks all incoming
connections. Opening of ports is typically allowed using a Universal
Plug and Play Internet Gateway Device (UPnP IGD) [UPnP-IGD] or some
other firewall control protocol.

Another consequence of using private address space in the end-user
network is that it provides stable addressing; that is, it never
changes even when you change service providers, and the addresses are
always there even when the WAN interface is down or the customer edge
router has not yet been provisioned.

Many existing routers support dynamic routing (which learns routes
from other routers), and advanced end-users can build arbitrary,

complex networks using manual configuration of address prefixes
combined with a dynamic routing protocol.

3.2. IPv6 End-User Network Architecture

The end-user network architecture for IPv6 should provide equivalent
or better capabilities and functionality than the current IPv4
architecture.

The end-user network is a stub network. Figure 1 illustrates the
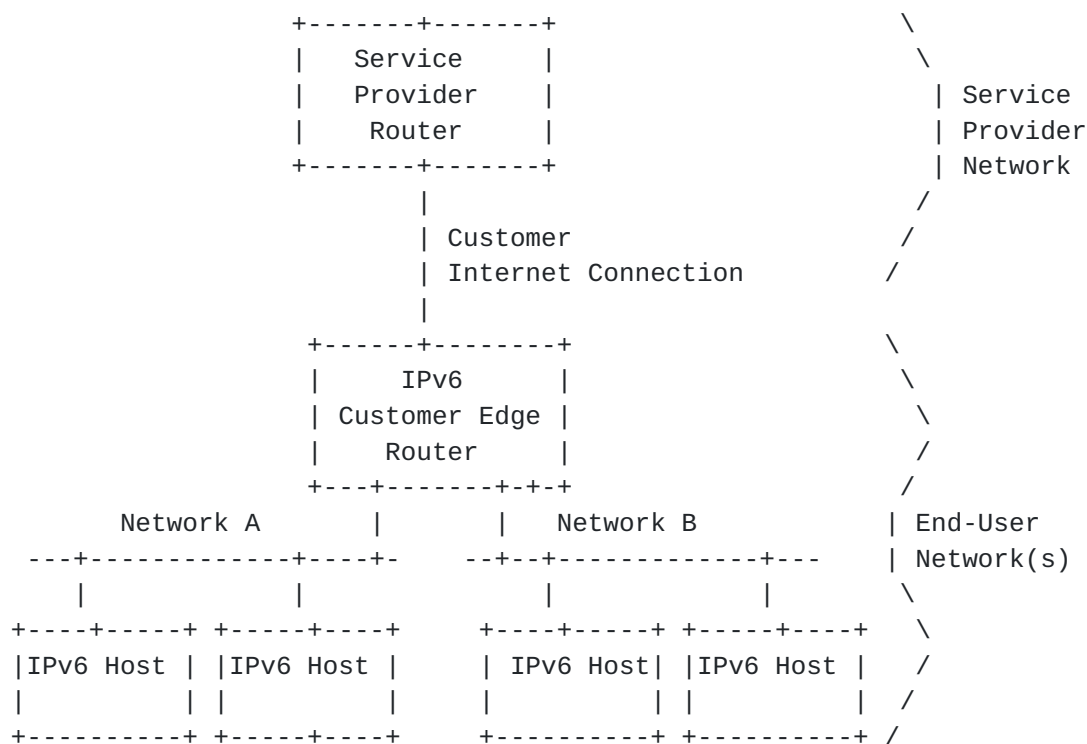model topology for the end-user network.

```
                    +-------+-------+                      \
                    |    Service    |                       \
                    |    Provider   |                        | Service
                    |     Router    |                        | Provider
                    +-------+-------+                        | Network
                            |                               /
                            | Customer                     /
                            | Internet Connection         /
                            |
                  +------+--------+                      \
                  |      IPv6     |                       \
                  | Customer Edge |                        \
                  |     Router    |                        /
                  +---+-------+-+-+                       /
          Network A   |       |    Network B           | End-User
      ---+------------+----+-    --+--+-------------+---   | Network(s)
         |            |           |            |        \
  +----+-----+ +-----+----+    +----+-----+ +-----+----+   \
  |IPv6 Host | |IPv6 Host |    | IPv6 Host| |IPv6 Host |   /
  |          | |          |    |          | |          |  /
  +----------+ +-----+----+    +----------+ +----------+ /
```

          Figure 1: An Example of a Typical End-User Network

This architecture describes the:

o Basic capabilities of an IPv6 CE router

o Provisioning of the WAN interface connecting to the service
   provider

o Provisioning of the LAN interfaces

For IPv6 multicast traffic, the IPv6 CE router may act as a Multicast
Listener Discovery (MLD) proxy [RFC4605] and may support a dynamic
multicast routing protocol.

The IPv6 CE router may be manually configured in an arbitrary
topology with a dynamic routing protocol. Automatic provisioning and
configuration are described for a single IPv6 CE router only.

3.2.1. Local Communication

Link-local IPv6 addresses are used by hosts communicating on a single
link. Unique Local IPv6 Unicast Addresses (ULAs) [RFC4193] are used
by hosts communicating within the end-user network across multiple
links, but without requiring the application to use a globally
routable address. The IPv6 CE router defaults to acting as the
demarcation point between two networks by providing a ULA boundary, a
multicast zone boundary, and ingress and egress traffic filters.

At the time of this writing, several host implementations do not
handle the case where they have an IPv6 address configured and no
IPv6 connectivity, either because the address itself has a limited
topological reachability (e.g., ULA) or because the IPv6 CE router is
not connected to the IPv6 network on its WAN interface. To support
host implementations that do not handle multihoming in a multi-prefix
environment [MULTIHOMING-WITHOUT-NAT], the IPv6 CE router should not,
as detailed in the requirements below, advertise itself as a default
router on the LAN interface(s) when it does not have IPv6
connectivity on the WAN interface or when it is not provisioned with
IPv6 addresses. For local IPv6 communication, the mechanisms
specified in [RFC4191] are used.

ULA addressing is useful where the IPv6 CE router has multiple LAN
interfaces with hosts that need to communicate with each other. If
the IPv6 CE router has only a single LAN interface (IPv6 link), then
link-local addressing can be used instead.

Coexistence with IPv4 requires any IPv6 CE router(s) on the LAN to
conform to these recommendations, especially requirements ULA-5 and
L-4 below.

4. Requirements

4.1. General Requirements

The IPv6 CE router is responsible for implementing IPv6 routing; that
is, the IPv6 CE router must look up the IPv6 destination address in
its routing table to decide to which interface it should send the
packet.

In this role, the IPv6 CE router is responsible for ensuring that
traffic using its ULA addressing does not go out the WAN interface
and does not originate from the WAN interface.

G-1: An IPv6 CE router is an IPv6 node according to the IPv6 Node
      Requirements specification [RFC6434].

G-2: The IPv6 CE router MUST implement ICMPv6 according to
      [RFC4443]. In particular, point-to-point links MUST be handled
      as described in Section 3.1 of [RFC4443].

G-3: The IPv6 CE router MUST NOT forward any IPv6 traffic between
      its LAN interface(s) and its WAN interface until the router has
      successfully completed the IPv6 address and the delegated
      prefix acquisition process.

G-4: By default, an IPv6 CE router that has no default router(s) on
      its WAN interface MUST NOT advertise itself as an IPv6 default
      router on its LAN interfaces. That is, the "Router Lifetime"
      field is set to zero in all Router Advertisement messages it
      originates [RFC4861].

G-5: By default, if the IPv6 CE router is an advertising router and
      loses its IPv6 default router(s) and/or detects loss of
      connectivity on the WAN interface, it MUST explicitly
      invalidate itself as an IPv6 default router on each of its
      advertising interfaces by immediately transmitting one or more
      Router Advertisement messages with the "Router Lifetime" field
      set to zero [RFC4861].

4.2. WAN-Side Configuration

The IPv6 CE router will need to support connectivity to one or more
access network architectures. This document describes an IPv6 CE
router that is not specific to any particular architecture or service
provider and that supports all commonly used architectures.

IPv6 Neighbor Discovery and DHCPv6 protocols operate over any type of
IPv6-supported link layer, and there is no need for a link-layer-
specific configuration protocol for IPv6 network-layer configuration
options as in, e.g., PPP IP Control Protocol (IPCP) for IPv4. This
section makes the assumption that the same mechanism will work for
any link layer, be it Ethernet, the Data Over Cable Service Interface
Specification (DOCSIS), PPP, or others.

WAN-side requirements:

W-1: When the router is attached to the WAN interface link, it MUST
      act as an IPv6 host for the purposes of stateless [RFC4862] or
      stateful [RFC3315] interface address assignment.

W-2:   The IPv6 CE router MUST generate a link-local address and
       finish Duplicate Address Detection according to [RFC4862] prior
       to sending any Router Solicitations on the interface. The
       source address used in the subsequent Router Solicitation MUST
       be the link-local address on the WAN interface.

W-3:   Absent other routing information, the IPv6 CE router MUST use
       Router Discovery as specified in [RFC4861] to discover a
       default router(s) and install a default route(s) in its routing
       table with the discovered router's address as the next hop.

W-4:   The router MUST act as a requesting router for the purposes of
       DHCPv6 prefix delegation ([RFC3633]).

W-5:   The IPv6 CE router MUST use a persistent DHCP Unique Identifier
       (DUID) for DHCPv6 messages. The DUID MUST NOT change between
       network-interface resets or IPv6 CE router reboots.

W-6:   The WAN interface of the CE router SHOULD support a Port
       Control Protocol (PCP) client as specified in [RFC6887] for use
       by applications on the CE router. The PCP client SHOULD follow
       the procedure specified in Section 8.1 of [RFC6887] to discover
       its PCP server. This document takes no position on whether
       such functionality is enabled by default or mechanisms by which
       users would configure the functionality. Handling PCP requests
       from PCP clients in the LAN side of the CE router is out of
       scope.

   Link-layer requirements:

   WLL-1: If the WAN interface supports Ethernet encapsulation, then
           the IPv6 CE router MUST support IPv6 over Ethernet [RFC2464].

   WLL-2: If the WAN interface supports PPP encapsulation, the IPv6 CE
           router MUST support IPv6 over PPP [RFC5072].

   WLL-3: If the WAN interface supports PPP encapsulation, in a dual-
           stack environment with IPCP and IPV6CP running over one PPP
           logical channel, the Network Control Protocols (NCPs) MUST be
           treated as independent of each other and start and terminate
           independently.

   Address assignment requirements:

   WAA-1:   The IPv6 CE router MUST support Stateless Address
            Autoconfiguration (SLAAC) [RFC4862].

WAA-2:   The IPv6 CE router MUST follow the recommendations in
           Section 4 of [RFC5942], and in particular the handling of
           the L flag in the Router Advertisement Prefix Information
           option.

WAA-3:   The IPv6 CE router MUST support DHCPv6 [RFC3315] client
           behavior.

WAA-4:   The IPv6 CE router MUST be able to support the following
           DHCPv6 options: Identity Association for Non-temporary
           Address (IA_NA), Reconfigure Accept [RFC3315], and
           DNS_SERVERS [RFC3646]. The IPv6 CE router SHOULD be able to
           support the DNS Search List (DNSSL) option as specified in
           [RFC3646].

WAA-5:   The IPv6 CE router SHOULD implement the Network Time
           Protocol (NTP) as specified in [RFC5905] to provide a time
           reference common to the service provider for other
           protocols, such as DHCPv6, to use. If the CE router
           implements NTP, it requests the NTP Server DHCPv6 option
           [RFC5908] and uses the received list of servers as primary
           time reference, unless explicitly configured otherwise. LAN
           side support of NTP is out of scope for this document.

WAA-6:   If the IPv6 CE router receives a Router Advertisement
           message (described in [RFC4861]) with the M flag set to 1,
           the IPv6 CE router MUST do DHCPv6 address assignment
           (request an IA_NA option).

WAA-7:   If the IPv6 CE router does not acquire a global IPv6
           address(es) from either SLAAC or DHCPv6, then it MUST create
           a global IPv6 address(es) from its delegated prefix(es) and
           configure those on one of its internal virtual network
           interfaces, unless configured to require a global IPv6
           address on the WAN interface.

WAA-8:   The CE router MUST support the SOL_MAX_RT option [RFC7083]
           and request the SOL_MAX_RT option in an Option Request
           Option (ORO).

WAA-9:   As a router, the IPv6 CE router MUST follow the weak host
           (Weak End System) model [RFC1122]. When originating packets
           from an interface, it will use a source address from another
           one of its interfaces if the outgoing interface does not
           have an address of suitable scope.

WAA-10:   The IPv6 CE router SHOULD implement the Information Refresh
          Time option and associated client behavior as specified in
          [RFC4242].

Prefix delegation requirements:

WPD-1:   The IPv6 CE router MUST support DHCPv6 prefix delegation
          requesting router behavior as specified in [RFC3633]
          (Identity Association for Prefix Delegation (IA_PD) option).

WPD-2:   The IPv6 CE router MAY indicate as a hint to the delegating
          router the size of the prefix it requires. If so, it MUST
          ask for a prefix large enough to assign one /64 for each of
          its interfaces, rounded up to the nearest nibble, and SHOULD
          be configurable to ask for more.

WPD-3:   The IPv6 CE router MUST be prepared to accept a delegated
          prefix size different from what is given in the hint. If the
          delegated prefix is too small to address all of its
          interfaces, the IPv6 CE router SHOULD log a system management
          error. [RFC6177] covers the recommendations for service
          providers for prefix allocation sizes.

WPD-4:   By default, the IPv6 CE router MUST initiate DHCPv6 prefix
          delegation when either the M or O flags are set to 1 in a
          received Router Advertisement (RA) message. Behavior of the
          CE router to use DHCPv6 prefix delegation when the CE router
          has not received any RA or received an RA with the M and the
          O bits set to zero is out of scope for this document.

WPD-5:   Any packet received by the CE router with a destination
          address in the prefix(es) delegated to the CE router but not
          in the set of prefixes assigned by the CE router to the LAN
          must be dropped. In other words, the next hop for the
          prefix(es) delegated to the CE router should be the null
          destination. This is necessary to prevent forwarding loops
          when some addresses covered by the aggregate are not
          reachable [RFC4632].

          (a) The IPv6 CE router SHOULD send an ICMPv6 Destination
               Unreachable message in accordance with Section 3.1 of
               [RFC4443] back to the source of the packet, if the
               packet is to be dropped due to this rule.

WPD-6:   If the IPv6 CE router requests both an IA_NA and an IA_PD
          option in DHCPv6, it MUST accept an IA_PD option in DHCPv6
          Advertise/Reply messages, even if the message does not

            contain any addresses, unless configured to only obtain its
            WAN IPv6 address via DHCPv6; see [DHCPv6-STATEFUL-ISSUES].

   WPD-7:   By default, an IPv6 CE router MUST NOT initiate any dynamic
            routing protocol on its WAN interface.

   WPD-8:   The IPv6 CE router SHOULD support the [RFC6603] Prefix
            Exclude option.

4.3. LAN-Side Configuration

   The IPv6 CE router distributes configuration information obtained
   during WAN interface provisioning to IPv6 hosts and assists IPv6
   hosts in obtaining IPv6 addresses. It also supports connectivity of
   these devices in the absence of any working WAN interface.

   An IPv6 CE router is expected to support an IPv6 end-user network and
   IPv6 hosts that exhibit the following characteristics:

   1. Link-local addresses may be insufficient for allowing IPv6
       applications to communicate with each other in the end-user
       network. The IPv6 CE router will need to enable this
       communication by providing globally scoped unicast addresses or
       ULAs [RFC4193], whether or not WAN connectivity exists.

   2. IPv6 hosts should be capable of using SLAAC and may be capable of
       using DHCPv6 for acquiring their addresses.

   3. IPv6 hosts may use DHCPv6 for other configuration information,
       such as the DNS_SERVERS option for acquiring DNS information.

   Unless otherwise specified, the following requirements apply to the
   IPv6 CE router's LAN interfaces only.

   ULA requirements:

   ULA-1:   The IPv6 CE router SHOULD be capable of generating a ULA
            prefix [RFC4193].

   ULA-2:   An IPv6 CE router with a ULA prefix MUST maintain this prefix
            consistently across reboots.

   ULA-3:   The value of the ULA prefix SHOULD be configurable.

   ULA-4:   By default, the IPv6 CE router MUST act as a site border
            router according to Section 4.3 of [RFC4193] and filter
            packets with local IPv6 source or destination addresses
            accordingly.

ULA-5: An IPv6 CE router MUST NOT advertise itself as a default
         router with a Router Lifetime greater than zero whenever all
         of its configured and delegated prefixes are ULA prefixes.

LAN requirements:

L-1:   The IPv6 CE router MUST support router behavior according to
         Neighbor Discovery for IPv6 [RFC4861].

L-2:   The IPv6 CE router MUST assign a separate /64 from its
         delegated prefix(es) (and ULA prefix if configured to provide
         ULA addressing) for each of its LAN interfaces.

L-3:   An IPv6 CE router MUST advertise itself as a router for the
         delegated prefix(es) (and ULA prefix if configured to provide
         ULA addressing) using the "Route Information Option" specified
         in Section 2.3 of [RFC4191]. This advertisement is
         independent of having or not having IPv6 connectivity on the
         WAN interface.

L-4:   An IPv6 CE router MUST NOT advertise itself as a default
         router with a Router Lifetime [RFC4861] greater than zero if
         it has no prefixes configured or delegated to it.

L-5:   The IPv6 CE router MUST make each LAN interface an advertising
         interface according to [RFC4861].

L-6:   In Router Advertisement messages ([RFC4861]), the Prefix
         Information option's A and L flags MUST be set to 1 by
         default.

L-7:   The A and L flags' ([RFC4861]) settings SHOULD be user
         configurable.

L-8:   The IPv6 CE router MUST support a DHCPv6 server capable of
         IPv6 address assignment according to [RFC3315] OR a stateless
         DHCPv6 server according to [RFC3736] on its LAN interfaces.

L-9:   Unless the IPv6 CE router is configured to support the DHCPv6
         IA_NA option, it SHOULD set the M flag to zero and the O flag
         to 1 in its Router Advertisement messages [RFC4861].

L-10:   The IPv6 CE router MUST support providing DNS information in
         the DHCPv6 DNS_SERVERS and DOMAIN_LIST options [RFC3646].

L-11:   The IPv6 CE router MUST support providing DNS information in
         the Router Advertisement Recursive DNS Server (RDNSS) and DNS
         Search List options. Both options are specified in [RFC6106].

L-12: The IPv6 CE router SHOULD make available a subset of DHCPv6
       options (as listed in Section 5.3 of [RFC3736]) received from
       the DHCPv6 client on its WAN interface to its LAN-side DHCPv6
       server.

L-13: If the delegated prefix changes, i.e., the current prefix is
       replaced with a new prefix without any overlapping time
       period, then the IPv6 CE router MUST immediately advertise the
       old prefix with a Preferred Lifetime of zero and a Valid
       Lifetime of either a) zero or b) the lower of the current
       Valid Lifetime and two hours (which must be decremented in
       real time) in a Router Advertisement message as described in
       Section 5.5.3, (e) of [RFC4862].

L-14: The IPv6 CE router MUST send an ICMPv6 Destination Unreachable
       message, code 5 (Source address failed ingress/egress policy)
       for packets forwarded to it that use an address from a prefix
       that has been invalidated.

4.4. Transition Technologies Support

4.4.1. 464XLAT

464XLAT [RFC6877] is a simple and scalable technique to quickly
deploy limited IPv4 access service to IPv6-only edge networks without
encapsulation ...

The CE router SHOULD support 464XLAT functionality. If 464XLAT is
supported, it MUST be implemented according to .... The following CE
Requirements also apply:

464XLAT requirements:

464XLAT-1: Place holder ... .

4.4.2. MAP-E

MAP-E [RFC7597] is a mechanism for transporting IPv4 packets across
an IPv6 network using IP encapsulation, including a generic mechanism
for mapping between IPv6 addresses and IPv4 addresses as well as
transport-layer ports ...

The CE router SHOULD support MAP-E functionality. If MAP-E is
supported, it MUST be implemented according to .... The following CE
Requirements also apply:

MAP-E requirements:

   MAP-E-1: Place holder ... .

4.4.3. MAP-T

   MAP-T [RFC7599] is a mechanism similar to MAP-E, differing from it in
   that MAP-T uses IPv4-IPv6 translation, rather than encapsulation, as
   the form of IPv6 domain transport ...

   The CE router SHOULD support MAP-T functionality. If MAP-T is
   supported, it MUST be implemented according to .... The following CE
   Requirements also apply:

   MAP-T requirements:

   MAP-T-1: Place holder ... .

4.4.4. 6in4

   6in4 [RFC4213] specifies an tunneling mechanism tailored to advance
   deployment of IPv6 to end users via a service provider's IPv4 network
   infrastructure. ...

   The CE router SHOULD support 6in4 functionality. If 6in4 is
   supported, it MUST be implemented according to .... The following CE
   Requirements also apply:

   6in4 requirements:

   6in4-1: Place holder ... .

4.4.5. 6rd

   6rd [RFC5969] specifies an automatic tunneling mechanism tailored to
   advance deployment of IPv6 to end users via a service provider's IPv4
   network infrastructure. Key aspects include automatic IPv6 prefix
   delegation to sites, stateless operation, simple provisioning, and
   service that is equivalent to native IPv6 at the sites that are
   served by the mechanism. It is expected that such traffic is
   forwarded over the CE router's native IPv4 WAN interface and not
   encapsulated in another tunnel.

   The CE router MAY support 6rd functionality. If 6rd is supported, it
   MUST be implemented according to [RFC5969]. The following CE
   Requirements also apply:

   6rd requirements:

6RD-1:   The IPv6 CE router MUST support 6rd configuration via the 6rd
         DHCPv4 Option 212. If the CE router has obtained an IPv4
         network address through some other means such as PPP, it
         SHOULD use the DHCPINFORM request message [RFC2131] to
         request the 6rd DHCPv4 Option. The IPv6 CE router MAY use
         other mechanisms to configure 6rd parameters. Such
         mechanisms are outside the scope of this document.

6RD-2:   If the IPv6 CE router is capable of automated configuration
         of IPv4 through IPCP (i.e., over a PPP connection), it MUST
         support user-entered configuration of 6rd.

6RD-3:   If the CE router supports configuration mechanisms other than
         the 6rd DHCPv4 Option 212 (user-entered, TR-069 [TR-069],
         etc.), the CE router MUST support 6rd in "hub and spoke"
         mode. 6rd in "hub and spoke" requires all IPv6 traffic to go
         to the 6rd Border Relay. In effect, this requirement removes
         the "direct connect to 6rd" route defined in Section 7.1.1 of
         [RFC5969].

6RD-4:   A CE router MUST allow 6rd and native IPv6 WAN interfaces to
         be active alone as well as simultaneously in order to support
         coexistence of the two technologies during an incremental
         transition period such as a transition from 6rd to native
         IPv6.

6RD-5:   Each packet sent on a 6rd or native WAN interface MUST be
         directed such that its source IP address is derived from the
         delegated prefix associated with the particular interface
         from which the packet is being sent (Section 4.3 of
         [RFC3704]).

6RD-6:   The CE router MUST allow different as well as identical
         delegated prefixes to be configured via each (6rd or native)
         WAN interface.

6RD-7:   In the event that forwarding rules produce a tie between 6rd
         and native IPv6, by default, the IPv6 CE router MUST prefer
         native IPv6.

4.4.6. Dual-Stack Lite (DS-Lite)

   Dual-Stack Lite [RFC6333] enables both continued support for IPv4
   services and incentives for the deployment of IPv6. It also
   de-couples IPv6 deployment in the service provider network from the
   rest of the Internet, making incremental deployment easier. Dual-
   Stack Lite enables a broadband service provider to share IPv4
   addresses among customers by combining two well-known technologies:

IP in IP (IPv4-in-IPv6) and Network Address Translation (NAT). It is
expected that DS-Lite traffic is forwarded over the CE router's
native IPv6 WAN interface, and not encapsulated in another tunnel.

The IPv6 CE router MAY implement DS-Lite functionality. If DS-Lite
is supported, it MUST be implemented according to [RFC6333]. This
document takes no position on simultaneous operation of Dual-Stack
Lite and native IPv4. The following CE router requirements also
apply:

WAN requirements:

DLW-1:   The CE router MUST support configuration of DS-Lite via the
         DS-Lite DHCPv6 option [RFC6334]. The IPv6 CE router MAY use
         other mechanisms to configure DS-Lite parameters. Such
         mechanisms are outside the scope of this document.

DLW-2:   The IPv6 CE router MUST NOT perform IPv4 Network Address
         Translation (NAT) on IPv4 traffic encapsulated using DS-Lite.

DLW-3:   If the IPv6 CE router is configured with an IPv4 address on
         its WAN interface, then the IPv6 CE router SHOULD disable the
         DS-Lite Basic Bridging BroadBand (B4) element.

4.4.7. Lightweight 4over6 (lw4o6)

Lw4o6 [RFC7596] specifies an extension to DS-Lite, which moves the
NAPT function from the DS-Lite tunnel concentrator to the tunnel
client located in the CE, removing the requirement for a CGN function
in the tunnel concentrator and reducing the amount of centralized
state. ...

The CE router MAY support lw4o6 functionality. If DS-Lite is
implemented, lw4o6 MUST be as well. If lw4o6 is supported, it MUST
be implemented according to .... The following CE Requirements also
apply:

lw6o4 requirements:

lw6o4-1: Place holder ... .

4.5. Security Considerations

It is considered a best practice to filter obviously malicious
traffic (e.g., spoofed packets, "Martian" addresses, etc.). Thus,
the IPv6 CE router ought to support basic stateless egress and
ingress filters. The CE router is also expected to offer mechanisms
to filter traffic entering the customer network; however, the method

   by which vendors implement configurable packet filtering is beyond
   the scope of this document.

   Security requirements:

   S-1: The IPv6 CE router SHOULD support [RFC6092]. In particular,
         the IPv6 CE router SHOULD support functionality sufficient for
         implementing the set of recommendations in [RFC6092],
         Section 4. This document takes no position on whether such
         functionality is enabled by default or mechanisms by which
         users would configure it.

   S-2: The IPv6 CE router SHOULD support ingress filtering in
         accordance with BCP 38 [RFC2827]. Note that this requirement
         was downgraded from a MUST from RFC 6204 due to the difficulty
         of implementation in the CE router and the feature's redundancy
         with upstream router ingress filtering.

   S-3: If the IPv6 CE router firewall is configured to filter incoming
         tunneled data, the firewall SHOULD provide the capability to
         filter decapsulated packets from a tunnel.

5. Acknowledgements

   This document is an update of RFC7084, whose original authors were:
   Hemant Singh, Wes Beebee, Chris Donley and Barbara Stark. The rest
   of the text on this section is the original acknowledgements section
   of the earlier document.

   Thanks to the following people (in alphabetical order) for their
   guidance and feedback:

   Mikael Abrahamsson, Tore Anderson, Merete Asak, Rajiv Asati, Scott
   Beuker, Mohamed Boucadair, Rex Bullinger, Brian Carpenter, Tassos
   Chatzithomaoglou, Lorenzo Colitti, Remi Denis-Courmont, Gert Doering,
   Alain Durand, Katsunori Fukuoka, Brian Haberman, Tony Hain, Thomas
   Herbst, Ray Hunter, Joel Jaeggli, Kevin Johns, Erik Kline, Stephen
   Kramer, Victor Kuarsingh, Francois-Xavier Le Bail, Arifumi Matsumoto,
   David Miles, Shin Miyakawa, Jean-Francois Mule, Michael Newbery,
   Carlos Pignataro, John Pomeroy, Antonio Querubin, Daniel Roesen,
   Hiroki Sato, Teemu Savolainen, Matt Schmitt, David Thaler, Mark
   Townsley, Sean Turner, Bernie Volz, Dan Wing, Timothy Winters, James
   Woodyatt, Carl Wuyts, and Cor Zwart.

   This document is based in part on CableLabs' eRouter specification.
   The authors wish to acknowledge the additional contributors from the
   eRouter team:

Ben Bekele, Amol Bhagwat, Ralph Brown, Eduardo Cardona, Margo Dolas, Toerless Eckert, Doc Evans, Roger Fish, Michelle Kuska, Diego Mazzola, John McQueen, Harsh Parandekar, Michael Patrick, Saifur Rahman, Lakshmi Raman, Ryan Ross, Ron da Silva, Madhu Sudan, Dan Torbet, and Greg White.

6. Contributors

The following people have participated as co-authors or provided substantial contributions to this document: Ralph Droms, Kirk Erichsen, Fred Baker, Jason Weil, Lee Howard, Jean-Francois Tremblay, Yiu Lee, John Jason Brzozowski, and Heather Kirksey. Thanks to Ole Troan for editorship in the original RFC 6204 document.

7. References

7.1. Normative References

[RFC1122]   Braden, R., Ed., "Requirements for Internet Hosts -
            Communication Layers", STD 3, RFC 1122,
            DOI 10.17487/RFC1122, October 1989,
            <http://www.rfc-editor.org/info/rfc1122>.

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119,
            DOI 10.17487/RFC2119, March 1997,
            <http://www.rfc-editor.org/info/rfc2119>.

[RFC2131]   Droms, R., "Dynamic Host Configuration Protocol",
            RFC 2131, DOI 10.17487/RFC2131, March 1997,
            <http://www.rfc-editor.org/info/rfc2131>.

[RFC2464]   Crawford, M., "Transmission of IPv6 Packets over Ethernet
            Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998,
            <http://www.rfc-editor.org/info/rfc2464>.

[RFC2827]   Ferguson, P. and D. Senie, "Network Ingress Filtering:
            Defeating Denial of Service Attacks which employ IP Source
            Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827,
            May 2000, <http://www.rfc-editor.org/info/rfc2827>.

[RFC3315]   Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins,
            C., and M. Carney, "Dynamic Host Configuration Protocol
            for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July
            2003, <http://www.rfc-editor.org/info/rfc3315>.

   [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic
              Host Configuration Protocol (DHCP) version 6", RFC 3633,
              DOI 10.17487/RFC3633, December 2003,
              <http://www.rfc-editor.org/info/rfc3633>.

   [RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic
              Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646,
              DOI 10.17487/RFC3646, December 2003,
              <http://www.rfc-editor.org/info/rfc3646>.

   [RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed
              Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March
              2004, <http://www.rfc-editor.org/info/rfc3704>.

   [RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol
              (DHCP) Service for IPv6", RFC 3736, DOI 10.17487/RFC3736,
              April 2004, <http://www.rfc-editor.org/info/rfc3736>.

   [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and
              More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191,
              November 2005, <http://www.rfc-editor.org/info/rfc4191>.

   [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast
              Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005,
              <http://www.rfc-editor.org/info/rfc4193>.

   [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms
              for IPv6 Hosts and Routers", RFC 4213,
              DOI 10.17487/RFC4213, October 2005,
              <http://www.rfc-editor.org/info/rfc4213>.

   [RFC4242] Venaas, S., Chown, T., and B. Volz, "Information Refresh
              Time Option for Dynamic Host Configuration Protocol for
              IPv6 (DHCPv6)", RFC 4242, DOI 10.17487/RFC4242, November
              2005, <http://www.rfc-editor.org/info/rfc4242>.

   [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet
              Control Message Protocol (ICMPv6) for the Internet
              Protocol Version 6 (IPv6) Specification", RFC 4443,
              DOI 10.17487/RFC4443, March 2006,
              <http://www.rfc-editor.org/info/rfc4443>.

   [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick,
              "Internet Group Management Protocol (IGMP) / Multicast
              Listener Discovery (MLD)-Based Multicast Forwarding
              ("IGMP/MLD Proxying")", RFC 4605, DOI 10.17487/RFC4605,
              August 2006, <http://www.rfc-editor.org/info/rfc4605>.

   [RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing
              (CIDR): The Internet Address Assignment and Aggregation
              Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August
              2006, <http://www.rfc-editor.org/info/rfc4632>.

   [RFC4779] Asadullah, S., Ahmed, A., Popoviciu, C., Savola, P., and
              J. Palet, "ISP IPv6 Deployment Scenarios in Broadband
              Access Networks", RFC 4779, DOI 10.17487/RFC4779, January
              2007, <http://www.rfc-editor.org/info/rfc4779>.

   [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
              "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
              DOI 10.17487/RFC4861, September 2007,
              <http://www.rfc-editor.org/info/rfc4861>.

   [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
              Address Autoconfiguration", RFC 4862,
              DOI 10.17487/RFC4862, September 2007,
              <http://www.rfc-editor.org/info/rfc4862>.

   [RFC5072] Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6
              over PPP", RFC 5072, DOI 10.17487/RFC5072, September 2007,
              <http://www.rfc-editor.org/info/rfc5072>.

   [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch,
              "Network Time Protocol Version 4: Protocol and Algorithms
              Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010,
              <http://www.rfc-editor.org/info/rfc5905>.

   [RFC5908] Gayraud, R. and B. Lourdelet, "Network Time Protocol (NTP)
              Server Option for DHCPv6", RFC 5908, DOI 10.17487/RFC5908,
              June 2010, <http://www.rfc-editor.org/info/rfc5908>.

   [RFC5942] Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet
              Model: The Relationship between Links and Subnet
              Prefixes", RFC 5942, DOI 10.17487/RFC5942, July 2010,
              <http://www.rfc-editor.org/info/rfc5942>.

   [RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4
              Infrastructures (6rd) -- Protocol Specification",
              RFC 5969, DOI 10.17487/RFC5969, August 2010,
              <http://www.rfc-editor.org/info/rfc5969>.

   [RFC6092] Woodyatt, J., Ed., "Recommended Simple Security
              Capabilities in Customer Premises Equipment (CPE) for
              Providing Residential IPv6 Internet Service", RFC 6092,
              DOI 10.17487/RFC6092, January 2011,
              <http://www.rfc-editor.org/info/rfc6092>.

   [RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli,
              "IPv6 Router Advertisement Options for DNS Configuration",
              RFC 6106, DOI 10.17487/RFC6106, November 2010,
              <http://www.rfc-editor.org/info/rfc6106>.

   [RFC6177] Narten, T., Huston, G., and L. Roberts, "IPv6 Address
              Assignment to End Sites", BCP 157, RFC 6177,
              DOI 10.17487/RFC6177, March 2011,
              <http://www.rfc-editor.org/info/rfc6177>.

   [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
              Stack Lite Broadband Deployments Following IPv4
              Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011,
              <http://www.rfc-editor.org/info/rfc6333>.

   [RFC6334] Hankins, D. and T. Mrugalski, "Dynamic Host Configuration
              Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite",
              RFC 6334, DOI 10.17487/RFC6334, August 2011,
              <http://www.rfc-editor.org/info/rfc6334>.

   [RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node
              Requirements", RFC 6434, DOI 10.17487/RFC6434, December
              2011, <http://www.rfc-editor.org/info/rfc6434>.

   [RFC6603] Korhonen, J., Ed., Savolainen, T., Krishnan, S., and O.
              Troan, "Prefix Exclude Option for DHCPv6-based Prefix
              Delegation", RFC 6603, DOI 10.17487/RFC6603, May 2012,
              <http://www.rfc-editor.org/info/rfc6603>.

   [RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT:
              Combination of Stateful and Stateless Translation",
              RFC 6877, DOI 10.17487/RFC6877, April 2013,
              <http://www.rfc-editor.org/info/rfc6877>.

   [RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and
              P. Selkirk, "Port Control Protocol (PCP)", RFC 6887,
              DOI 10.17487/RFC6887, April 2013,
              <http://www.rfc-editor.org/info/rfc6887>.

   [RFC7083] Droms, R., "Modification to Default Value of SOL_MAX_RT",
              RFC 7083, November 2013.

   [RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I.
              Farrer, "Lightweight 4over6: An Extension to the Dual-
              Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596,
              July 2015, <http://www.rfc-editor.org/info/rfc7596>.

   [RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S.,
              Murakami, T., and T. Taylor, Ed., "Mapping of Address and
              Port with Encapsulation (MAP-E)", RFC 7597,
              DOI 10.17487/RFC7597, July 2015,
              <http://www.rfc-editor.org/info/rfc7597>.

   [RFC7599] Li, X., Bao, C., Dec, W., Ed., Troan, O., Matsushima, S.,
              and T. Murakami, "Mapping of Address and Port using
              Translation (MAP-T)", RFC 7599, DOI 10.17487/RFC7599, July
              2015, <http://www.rfc-editor.org/info/rfc7599>.

7.2. Informative References

   [DHCPv6-STATEFUL-ISSUES]
              Troan, O. and B. Volz, "Issues with multiple stateful
              DHCPv6 options", Work in Progress, May 2013.

   [MULTIHOMING-WITHOUT-NAT]
              Troan, O., Ed., Miles, D., Matsushima, S., Okimoto, T.,
              and D. Wing, "IPv6 Multihoming without Network Address
              Translation", Work in Progress, December 2010.

   [RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for
              IPv4/IPv6 Translation", RFC 6144, DOI 10.17487/RFC6144,
              April 2011, <http://www.rfc-editor.org/info/rfc6144>.

   [TR-069]   Broadband Forum, "CPE WAN Management Protocol", TR-069
              Amendment 4, July 2011,
              <http://www.broadband-forum.org/technical/trlist.php>.

   [UPnP-IGD]
              UPnP Forum, , "InternetGatewayDevice:2 Device Template
              Version 1.01", December 2010,
              <http://upnp.org/specs/gw/igd2/>.

Author's Address

   Jordi Palet Martinez
   Consulintel, S.L.
   Molino de la Navata, 75
   La Navata - Galapagar, Madrid 28420
   Spain

   EMail: jordi.palet@consulintel.es
   URI: http://www.consulintel.es/