IPv6 Operations (v6ops)
Internet-Draft
Intended status: Informational
Expires: April 19, 2019
J. Palet Martinez
The IPv6 Company
H. M.-H. Liu
D-Link Systems, Inc.
M. Kawashima
NEC Platforms, Ltd.
October 16, 2018

Requirements for IPv6 Customer Edge Routers to Support IPv4 Connectivity as-a-Service

draft-ietf-v6ops-transition-ipv4aas-10

Abstract

This document specifies the IPv4 service continuity requirements for an IPv6 Customer Edge (CE) router, either provided by the service provider or through the retail market.

Specifically, this document extends the "Basic Requirements for IPv6 Customer Edge Routers" in order to allow the provisioning of IPv6 transition services for the support of "IPv4 as-a-Service" (IPv4aaS) by means of new transition mechanisms. The document only covers transition technologies for delivering IPv4 in IPv6-only access networks, commonly called "IPv4 as-a-Service" (IPv4aaS). This is required in a world where sufficient IPv4 addresses are no longer available for every possible customer/device. However, devices or applications in the customer LANs may be IPv4-only or IPv6-only and still need to communicate with IPv4-only services at the Internet.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document defines IPv4 service continuity features over an IPv6-only network, for a residential or small-office router, referred to as an "IPv6 Transition CE Router", in order to establish an industry baseline for transition features to be implemented on such a router.

These routers rely upon "Basic Requirements for IPv6 Customer Edge Routers" ([RFC7084]), so the scope of this document is to ensure the IPv4 "service continuity" support, in the LAN side and the access to IPv4-only Internet services from an IPv6-only access WAN even from IPv6-only applications or devices in the LAN side.

This document covers a set of IP transition techniques required when ISPs have, or want to have, an IPv6-only access network. This is a common situation in a world where sufficient public IPv4 addresses are no longer available for every possible customer and device, and become prohibitive expense, so the service providers need to provision IPv6-only WAN access. At the same time, they need to ensure that both IPv4-only and IPv6-only devices or applications in the customer networks can still reach IPv4-only devices and applications in the Internet.

This document specifies the IPv4 service continuity mechanisms to be supported by an IPv6 Transition CE Router, and relevant provisioning or configuration information differences from [RFC7084].

This document is not a recommendation for service providers to use any specific transition mechanism.

Automatic provisioning of more complex topology than a single router with multiple LAN interfaces may be handled by means of HNCP ([RFC7788]), which is out of the scope of this document.

Service providers who specify feature sets for IPv6 Transition CE Router may specify a different set of features than those included in this document. Since it is impossible to know prior to sale which transition mechanism a device will need over the lifetime of the device, IPv6 Transition CE Router intended for the retail market MUST support all the IPv4aaS transition mechanism supported by this document.

A complete description of "Usage Scenarios" and "End-User Network Architecture" is provided in Annexes A and B, respectively.

1.1. Requirements Language - Special Note

The keywords "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 to provide additional guidance to implementers regarding any protocol implementation required to produce a successful IPv6 Transition CE Router that interoperates successfully with a particular subset of currently deploying and planned common IPv6-only access networks.

Additionally, the keyword "DEFAULT" is to be interpreted in this document as pertaining to a configuration as applied by a vendor, prior to the administrator changing it for its initial activation.

2. Terminology

This document uses the same terms as in [RFC7084], with minor clarifications.

"IPv4aaS" stands for "IPv4 as-a-Service", meaning transition technologies for delivering IPv4 in IPv6-only connectivity.

The term "IPv6 transition Customer Edge Router with IPv4aaS" (shortened as "IPv6 Transition CE Router") is defined as an "IPv6 Customer Edge Router" that provides features for the delivery of IPv4 services over an IPv6-only WAN network, including IPv6-IPv4 communications.

The "WAN Interface" term used across this document, defines an IPv6 Transition CE Router attachment to an IPv6-only link used to provide connectivity to a service provider network, including link Internet-layer (or higher layers) "tunnels", such as IPv4-in-IPv6 tunnels.

3. Requirements

The IPv6 Transition CE Router MUST comply with [RFC7084] (Basic Requirements for IPv6 Customer Edge Routers) and this document add new requirements, as described in the following sub-sections.

3.1. LAN-Side Configuration

A new LAN requirement is added, which in fact is common in regular IPv6 Transition CE Router, and it is required by most of the transition mechanisms:

L-1: The IPv6 Transition CE Router MUST implement a DNS proxy as described in [RFC5625] (DNS Proxy Implementation Guidelines).

3.2. Transition Technologies Support for IPv4 Service Continuity (IPv4 as-a-Service - IPv4aaS)

The main target of this document is the support of IPv6-only WAN access. To enable legacy IPv4 functionality, this document also includes the support of IPv4-only devices and applications in the customers LANs, as well as IPv4-only services on the Internet. Thus, both IPv4-only and the IPv6-only devices in the customer-side LANs of the IPv6 Transition CE Router are able to reach the IPv4-only services.

This document takes no position on simultaneous operation of one or several transition mechanisms and/or native IPv4.

In order to seamlessly provide the IPv4 Service Continuity in Customer LANs, allowing an automated IPv6 transition mechanism provisioning, general transition requirements are defined.

General transition requirements:

TRANS-1: The IPv6 Transition CE Router MUST support the DHCPv6 S46 priority options described in [RFC8026] (Unified IPv4-in-IPv6 Softwire Customer Premises Equipment (CPE): A DHCPv6-Based Prioritization Mechanism).

TRANS-2: The IPv6 Transition CE Router MUST have a GUI, CLI and/or API option to manually enable/disable each of the supported transition mechanisms.

TRANS-3: If an IPv6 Transition CE Router supports more than one LAN subnet, the IPv6 Transition CE Router MUST allow appropriate subnetting and configuring the address space (which may depend on each transition mechanism) among the several interfaces. In some transition mechanisms, this may require differentiating mappings/translations per interfaces.

In order to allow the service provider to disable all the transition mechanisms and/or choose the most convenient one, the IPv6 Transition

CE Router MUST follow the following configuration steps:

CONFIG-1: Request the relevant configuration options for each supported transition mechanisms, which MUST remain disabled at this step.

CONFIG-2: Following Section 1.4 of [RFC8026], MUST check for a valid match in OPTION_S46_PRIORITY, which allows enabling/disabling a transition mechanism.

CONFIG-3: Keep disabled all the transition mechanisms if no match is found between the priority list and the candidate list.

The following sections describe the requirements for supporting each one of the transition mechanisms. An IPv6 Transition CE Router intended for the retail market MUST support all of them.

3.2.1. 464XLAT

464XLAT [RFC6877] is a technique to provide IPv4 service over an IPv6-only access network without encapsulation. This architecture assumes a NAT64 [RFC6146] (Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers) function deployed at the service provider or a third-party network.

The IPv6 Transition CE Router SHOULD support CLAT functionality. If 464XLAT is supported, it MUST be implemented according to [RFC6877]. The following IPv6 Transition CE Router requirements also apply:

464XLAT requirements:

464XLAT-1: The IPv6 Transition CE Router MUST perform IPv4 Network Address Translation (NAT) on IPv4 traffic translated using the CLAT, unless a dedicated /64 prefix has been acquired, either using DHCPv6-PD [RFC3633] (IPv6 Prefix Options for DHCPv6) or by alternative means.

464XLAT-2: The IPv6 Transition CE Router SHOULD support IGD-PCP IWF [RFC6970] (UPnP Internet Gateway Device - Port Control Protocol Interworking Function).

464XLAT-3: If PCP ([RFC6887]) is implemented, the IPv6 Transition CE Router MUST also implement [RFC7291] (DHCP Options for the PCP). Following ([RFC6887]), if no PCP server is configured, the IPv6 Transition CE Router MAY verify if the default gateway, or the NAT64 is the PCP server. Plain IPv6 mode (i.e., no IPv4-in-IPv6 encapsulation is used) MUST be used to send PCP requests to the server.

464XLAT-4: The IPv6 Transition CE Router MUST implement [RFC7050] (Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis) in order to discover the PLAT-side translation IPv4 and IPv6 prefix(es)/suffix(es).

464XLAT-5: If PCP is implemented, the IPv6 Transition CE Router MUST follow [RFC7225] (Discovering NAT64 IPv6 Prefixes Using the PCP), in order to learn the PLAT-side translation IPv4 and IPv6 prefix(es)/suffix(es) used by an upstream PCP-controlled NAT64 device.

464XLAT-6: [RFC8115] MUST be implemented and a DHCPv6 Option "OPTION_V6_PREFIX64" ([RFC8115]), with zeroed ASM_mPrefix64 and SSM_mPrefix64, MUST also be considered as a valid NAT64 prefix (uPrefix64).

464XLAT-7: The priority for the NAT64 prefix, in case the network provides several choices, MUST be: 1) [RFC7225], 2) [RFC8115], and 3) [RFC7050].

464XLAT-8: If a DHCPv6 Option "OPTION_V6_PREFIX64" ([RFC8115]), with zeroed ASM_mPrefix64 and SSM_mPrefix64 provides a NAT64 prefix, or one or more NAT64 prefixes are learnt by means of either [RFC7050] or [RFC7225], then 464XLAT MUST be included in the candidate list of possible S46 mechanism (Section 1.4.1 of [RFC8026]).

The NAT64 prefix could be discovered by means of [RFC7050] only in the case the service provider uses DNS64 ([RFC6147]). If DNS64 ([RFC6147]) is not used, or not trusted, as the DNS configuration at the CE (or hosts behind the CE) may be modified by the customer, then the service provider may opt to configure the NAT64 prefix either by means of [RFC7225] or [RFC8115], which also can be used if the service provider uses DNS64 ([RFC6147]).

3.2.2. Dual-Stack Lite (DS-Lite)

Dual-Stack Lite [RFC6333] enables continued support for IPv4 services. 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 IPv6 Transition CE Router's native IPv6 WAN interface, and not encapsulated in another tunnel.

The IPv6 Transition CE Router SHOULD implement DS-Lite B4 functionality [RFC6333]. If DS-Lite is supported, it MUST be implemented according to [RFC6333]. The following IPv6 Transition CE

Router requirements also apply:

DS-Lite requirements:

DSLITE-1: The IPv6 Transition CE Router MUST support configuration of DS-Lite via the DS-Lite DHCPv6 option [RFC6334] (DHCPv6 Option for Dual-Stack Lite). The IPv6 Transition CE Router MAY use other mechanisms to configure DS-Lite parameters. Such mechanisms are outside the scope of this document.

DSLITE-2: The IPv6 Transition CE Router SHOULD support IGD-PCP IWF [RFC6970] (UPnP Internet Gateway Device - Port Control Protocol Interworking Function).

DSLITE-3: If PCP ([RFC6887]) is implemented, the IPv6 Transition CE Router SHOULD implement [RFC7291] (DHCP Options for the PCP). If PCP ([RFC6887]) is implemented and a PCP server is not configured, the IPv6 Transition CE Router MUST assume, by DEFAULT, that the AFTR is the PCP server. Plain IPv6 mode (i.e., no IPv4-in-IPv6 encapsulation is used) MUST be used to send PCP requests to the server.

DSLITE-4: The IPv6 Transition CE Router MUST NOT perform IPv4 Network Address Translation (NAT) on IPv4 traffic encapsulated using DS-Lite ([RFC6333]).

3.2.3. 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 IPv6 Transition CE Router, removing the requirement for a CGN function in the tunnel concentrator and reducing the amount of centralized state.

The IPv6 Transition CE Router SHOULD implement lwB4 functionality [RFC7596]. If DS-Lite is implemented, lw4o6 SHOULD be implemented as well. If lw4o6 is supported, it MUST be implemented according to [RFC7596]. The following IPv6 Transition CE Router requirements also apply:

lw4o6 requirements:

LW4O6-1: The IPv6 Transition CE Router MUST support configuration of lw4o6 via the lw4o6 DHCPv6 options [RFC7598] (DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients). The IPv6 Transition CE Router MAY use other mechanisms to configure lw4o6 parameters. Such

mechanisms are outside the scope of this document.

LW4O6-2: The IPv6 Transition CE Router MUST support the DHCPv4-over-DHCPv6 (DHCP 4o6) transport described in [RFC7341] (DHCPv4-over-DHCPv6 Transport).

LW4O6-3: The IPv6 Transition CE Router MAY support Dynamic Allocation of Shared IPv4 Addresses as described in [RFC7618] (Dynamic Allocation of Shared IPv4 Addresses).

3.2.4. MAP-E

MAP-E [RFC7597] is a mechanism for transporting IPv4 packets across an IPv6 network using IP encapsulation, including an algorithmic mechanism for mapping between IPv6 and IPv4 addresses.

The IPv6 Transition CE Router SHOULD support MAP-E CE functionality [RFC7597]. If MAP-E is supported, it MUST be implemented according to [RFC7597]. The following IPv6 Transition CE Router requirements also apply:

MAP-E requirements:

MAPE-1: The IPv6 Transition CE Router MUST support configuration of MAP-E via the MAP-E DHCPv6 options [RFC7598] (DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients). The IPv6 Transition CE Router MAY use other mechanisms to configure MAP-E parameters. Such mechanisms are outside the scope of this document.

MAPE-2: The IPv6 Transition CE Router MAY support Dynamic Allocation of Shared IPv4 Addresses as described in [RFC7618] (Dynamic Allocation of Shared IPv4 Addresses).

3.2.5. MAP-T

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

The IPv6 Transition CE Router SHOULD support MAP-T CE functionality [RFC7599]. If MAP-T is supported, it MUST be implemented according to [RFC7599]. The following IPv6 Transition CE Router requirements also apply:

MAP-T requirements:

MAPT-1: The IPv6 Transition CE Router MUST support configuration of

MAP-T via the MAP-T DHCPv6 options [RFC7598] (DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients). The IPv6 Transition CE Router MAY use other mechanisms to configure MAP-T parameters. Such mechanisms are outside the scope of this document.

MAPT-2: The IPv6 Transition CE Router MAY support Dynamic Allocation of Shared IPv4 Addresses as described in [RFC7618] (Dynamic Allocation of Shared IPv4 Addresses).

4. IPv4 Multicast Support

Existing IPv4 deployments support IPv4 multicast for services such as IPTV. In the transition phase, it is expected that multicast services will still be provided using IPv4 to the customer LANs.

If the IPv6 Transition CE Router supports delivery of IPv4 multicast services, then it MUST support [RFC8114] (Delivery of IPv4 Multicast Services to IPv4 Clients over an IPv6 Multicast Network) and [RFC8115] (DHCPv6 Option for IPv4-Embedded Multicast and Unicast IPv6 Prefixes).

5. UPnP Support

If the UPnP WANIPConnection:2 service [UPnP-WANIPC] is enabled on a CE router, but cannot be associated with an IPv4 interface established by an IPv4aaS mechanism or cannot determine which ports are available, an AddPortMapping() or AddAnyPortMapping() action MUST be rejected with error code 729 "ConflictWithOtherMechanisms". Port availability could be determined through PCP or access to a configured port set (if the IPv4aaS mechanism limits the available ports).

An AddPortMapping() request for a port that is not available MUST result in "ConflictInMappingEntry".

An AddAnyPortMapping() request for a port that is not available SHOULD result in a successful mapping with an alternative "NewReservedPort" value from within the configured port set range, or as assigned by PCP as per [RFC6970], Section 5.6.1.

Note that IGD:1 and its WANIPConnection:1 service have been deprecated by OCF.

6. Comparison to RFC7084

This document doesn't include support for 6rd ([RFC5969]), because as in an IPv6-in-IPv4 tunneling.

Regarding DS-LITE [RFC6333], this document includes slightly different requirements, because the PCP ([RFC6887]) support and the prioritization of the transition mechanisms, including dual-stack.

7. Code Considerations

One of the apparent main issues for vendors to include new functionalities, such as support for new transition mechanisms, is the lack of space in the flash (or equivalent) memory. However, it has been confirmed from existing open source implementations (OpenWRT/LEDE, Linux, others), that adding the support for the new transitions mechanisms, requires around 10-12 Kbytes (because most of the code base is shared among several transition mechanisms already supported by [RFC7084]), as a single data plane is common to all them, which typically means about 0,15% of the existing code size in popular CEs already in the market [OpenWRT].

In general, the new requirements don't have extra cost in terms of RAM memory, neither other hardware requirements such as more powerful CPUs, if compared to the cost of NAT44 code so, existing hardware supports them with minimal impact.

The other issue seems to be the cost of developing the code for those new functionalities. However, at the time of writing this document, it has been confirmed that there are several open source versions of the required code for supporting all the new transition mechanisms, and even several vendors already have implementations and provide it to ISPs, so the development cost is negligible, and only integration and testing cost may become a minor issue.

8. Security Considerations

The IPv6 Transition CE Router must comply with the Security Considerations as stated in [RFC7084], as well as those stated by each transition mechanism implemented by the IPv6 Transition CE Router.

9. IANA Considerations

IANA is requested, by means of this document, to update the "Option Codes permitted in the S46 Priority Option" registry available at https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#option-codes-s46-priority-option, with the following

entry.

Option Code	S46 Mechanism	Reference
113	464XLAT	[thisdoc]

Table 1: DHCPv6 Option Code for 464XLAT

10. Acknowledgements

Thanks to Mikael Abrahamsson, Fred Baker, Mohamed Boucadair, Brian Carpenter, Ian Farrer, Lee Howard, Richard Patterson, Barbara Stark, Ole Troan, James Woodyatt, Lorenzo Colitti and Alejandro D'Egidio, for their review and comments in this and/or previous versions of this document.

11. Annex A: Usage Scenarios

The situation previously described, where there is ongoing IPv6 deployment and lack of IPv4 addresses, is not happening at the same pace in every country, and even within every country, every ISP. For different technical, financial, commercial/marketing and socio-economic reasons, each network is transitioning at their own pace, and nobody has a magic crystal ball to make a guess of the global transition timings.

Different studies (for example [IPv6Survey]) also show that the IPv6 deployment is a changing situation. In a single country, it may happen that not all operators provide IPv6 support, and consumers may switch ISPs and use the same IPv6 Transition CE Router with an ISP that provides IPv4-only and an ISP that provides IPv6 with IPv4aaS.

So, it is clear that, to cover all those evolving situations, an IPv6 Transition CE Router is required, at least from the perspective of the transition support, which can accommodate those changes.

Moreover, because some services will remain IPv4-only for an undetermined time, and some service providers will remain IPv4-only for an undetermined period of time, IPv4 will be needed for an undetermined period of time. There will be a need for CEs with support "IPv4 as-a-Service" for an undetermined period of time.

This document, based on those premises, ensures that the IPv6 Transition CE Router allows the continued transition from networks that today may provide access with dual-stack or IPv6-in-IPv4, as described in [RFC7084], and as an "extension" to it, evolve to an

IPv6-only access with IPv4-as-a-Service.

Considering that situation and different possible usage cases, the IPv6 Transition CE Router described in this document is expected to be used typically, in residential/household, Small Office/Home Office (SOHO) and Small/Medium Enterprise (SME). Common usage is any kind of Internet access (web, email, streaming, online gaming, etc.) and even more advanced requirements including inbound connections (IP cameras, web, DNS, email, VPN, etc.).

The above is not intended to be comprehensive list of all the possible usage cases, just an overall view. In fact, combinations of the above usages are also possible, as well as situations where the same CE is used at different times in different scenarios or even different services providers that may use a different transition mechanism.

The mechanisms for allowing inbound connections are "naturally" available in any IPv6 router, when using GUA (IPv6 Global Unicast Addresses), unless they are blocked by firewall rules, which may require some manual configuration by means of a GUI, CLI and/or API.

However, in the case of IPv4aaS, because the usage of private addresses and NAT and even depending on the specific transition mechanism, inbound connections typically require some degree of more complex manual configuration such as setting up a DMZ, virtual servers, or port/protocol forwarding. In general, IPv4 CE Routers already provide a GUI and/or a CLI to manually configure them, or the possibility to setup the CE in bridge mode, so another CE behind it, takes care of that. The requirements for that support are out of the scope of this document.

It is not relevant who provides the IPv6 Transition CE Router. In most of the cases is the service provider, and in fact is responsible, typically, of provisioning/managing at least the WAN side. However, commonly the user has access to configure the LAN interfaces, firewall, DMZ, and many other features. However, in fact, in many cases, the user must supply or may replace the IPv6 Transition CE Router. This makes even more relevant that all the IPv6 Transition CE Routers support the same requirements defined in this document.

The IPv6 Transition CE Router described in this document is not intended for usage in other scenarios such as large Enterprises, Data Centers, Content Providers, etc. So even if the documented requirements meet their needs, they may have additional requirements, which are out of the scope of this document.

12. Annex B: End-User Network Architecture

According to the descriptions in the preceding sections, 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 upstream, connected to the service provider network.

From the perspective of an "IPv4 user" behind an IPv6 transition Customer Edge Router with IPv4aaS, this doesn't change.

However, while a typical IPv4 NAT deployment by default blocks all incoming connections and may allow opening of ports using a Universal Plug and Play Internet Gateway Device (UPnP IGD) [UPnP-IGD] or some other firewall control protocol, in the case of an IPv6-only access and IPv4aaS, that may not be feasible depending on specific transition mechanism details. PCP (Port Control Protocol, [RFC6887]) may be an alternative solution.

Another consequence of using IPv4 private address space in the end-user network is that it provides stable addressing; that is, it doesn't change, even when you change service providers, and the addresses are always usable even when the WAN interface is down or the customer edge router has not yet been provisioned. In the case of an IPv6-only access, private IPv4 addresses are also available if the IPv4aaS transition mechanism keeps running the NAT interface towards the LAN side when the WAN interface is down.

More advanced 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. Once again, this is true for both, IPv4 and IPv6.

In general, 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, in the sense that is not providing transit to other external networks. However, HNCP ([RFC7788]) allows support for automatic provisioning of downstream routers. 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            |
    ---+----------------+-+-    --+---+-------------+--    |
       |                |             |             |       \
   +---+------+         |        +----+-----+ +-----+----+   \
   |IPv6 Host |         |        | IPv4 Host| |IPv4/IPv6 |   /
   |          |         |        |          | | Host     |  /
   +----------+         |        +----------+ +----------+ /
                        |                                 |
                 +------+--------+                        | End-User
                 |     IPv6       |                        | Network(s)
                 |    Router      |                         \
                 +------+--------+                          \
          Network C     |                                    \
    ---+-------------+--+---                                  |
       |             |                                        |
   +---+------+ +----+-----+                                  |
   |IPv6 Host | |IPv6 Host |                                 /
   |          | |          |                                /
   +----------+ +----------+                               /
```

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

This architecture describes the:

o Basic capabilities of the IPv6 Transition CE Router

o Provisioning of the WAN interface connecting to the service provider

o Provisioning of the LAN interfaces

The IPv6 Transition CE Router may be manually configured in an arbitrary topology with a dynamic routing protocol or using HNCP ([RFC7788]). Automatic provisioning and configuration is described

for a single IPv6 Transition CE Router only.

13. ANNEX C: Changes from -00

Section to be removed for WGLC. Significant updates are:

1. ID-Nits: IANA section.

2. ID-Nits: RFC7084 reference removed from Abstract.

3. This document no longer updates RFC7084.

4. UPnP section reworded.

5. "CE Router" changed to "IPv6 Transition CE Router".

6. Reduced text in Annex A.

14. ANNEX D: Changes from -01

Section to be removed for WGLC. Significant updates are:

1. TRANS requirements reworked in order to increase operator control and allow gradual transitioning from dual-stack to IPv6-only on specific customers.

2. New TRANS requirement so all the supported transition mechanisms are disabled by default, in order to facilitate the operator management.

3. New TRANS requirement in order to allow turning on/off each transition mechanism by the user.

4. Clarification on how to obtain multiple /64 for 464XLAT.

5. S46 priority update to RFC8026 for including 464XLAT and related changes in several sections.

15. ANNEX E: Changes from -02

Section to be removed for WGLC. Significant updates are:

1. RFC8026 update removed, not needed with new approach.

2. TRANS and 464XLAT requirements reworded in order to match new approach to allow operator control on each/all the transition mechanisms.

3. Added text in 464XLAT to clarify the usage.

16. ANNEX F: Changes from -03

Section to be removed for WGLC. Significant updates are:

1. Several editorial changes across the document, specially TRANS requirements.

2. DNS proxy MUST instead of SHOULD.

17. ANNEX G: Changes from -04

Section to be removed for WGLC. Significant updates are:

1. Removed G-1.

2. Added support for draft-pref64folks-6man-ra-pref64.

3. General text clarifications.

18. ANNEX H: Changes from -05

Section to be removed for WGLC. Significant updates are:

1. Reworded and shorter UPnP section and new informative reference.

2. New general transition requirement in case multiple public IPv4 prefixes are provided, so to run multiple instances according to each specific transition mechanism.

3. General text clarifications.

19. ANNEX I: Changes from -06

Section to be removed for WGLC. Significant updates are:

1. Removed reference and text related to pref64folks-6man-ra-pref64.

2. General text clarifications.

20. ANNEX J: Changes from -07

Section to be removed for WGLC. Significant updates are:

1. Added text to UPnP section.

21. ANNEX K: Changes from -08

Section to be removed for WGLC. Significant updates are:

1. Editorial edits.

22. ANNEX K: Changes from -09

Section to be removed for WGLC. Significant updates are:

1. Minor editorial edit.

23. References

23.1. Normative References

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

[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, <https://www.rfc-editor.org/info/rfc3633>.

[RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, DOI 10.17487/RFC5625, August 2009, <https://www.rfc-editor.org/info/rfc5625>.

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

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc6334>.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, <https://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, <https://www.rfc-editor.org/info/rfc6887>.

[RFC6970] Boucadair, M., Penno, R., and D. Wing, "Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF)", RFC 6970, DOI 10.17487/RFC6970, July 2013, <https://www.rfc-editor.org/info/rfc6970>.

[RFC7050] Savolainen, T., Korhonen, J., and D. Wing, "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis", RFC 7050, DOI 10.17487/RFC7050, November 2013, <https://www.rfc-editor.org/info/rfc7050>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <https://www.rfc-editor.org/info/rfc7084>.

[RFC7225] Boucadair, M., "Discovering NAT64 IPv6 Prefixes Using the Port Control Protocol (PCP)", RFC 7225, DOI 10.17487/RFC7225, May 2014, <https://www.rfc-editor.org/info/rfc7225>.

[RFC7291] Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", RFC 7291, DOI 10.17487/RFC7291, July 2014, <https://www.rfc-editor.org/info/rfc7291>.

[RFC7341] Sun, Q., Cui, Y., Siodelski, M., Krishnan, S., and I. Farrer, "DHCPv4-over-DHCPv6 (DHCP 4o6) Transport", RFC 7341, DOI 10.17487/RFC7341, August 2014, <https://www.rfc-editor.org/info/rfc7341>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc7597>.

[RFC7598] Mrugalski, T., Troan, O., Farrer, I., Perreault, S., Dec, W., Bao, C., Yeh, L., and X. Deng, "DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients", RFC 7598, DOI 10.17487/RFC7598, July 2015, <https://www.rfc-editor.org/info/rfc7598>.

[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, <https://www.rfc-editor.org/info/rfc7599>.

[RFC7618] Cui, Y., Sun, Q., Farrer, I., Lee, Y., Sun, Q., and M. Boucadair, "Dynamic Allocation of Shared IPv4 Addresses", RFC 7618, DOI 10.17487/RFC7618, August 2015, <https://www.rfc-editor.org/info/rfc7618>.

[RFC8026] Boucadair, M. and I. Farrer, "Unified IPv4-in-IPv6 Softwire Customer Premises Equipment (CPE): A DHCPv6-Based Prioritization Mechanism", RFC 8026, DOI 10.17487/RFC8026, November 2016, <https://www.rfc-editor.org/info/rfc8026>.

[RFC8114] Boucadair, M., Qin, C., Jacquenet, C., Lee, Y., and Q. Wang, "Delivery of IPv4 Multicast Services to IPv4 Clients over an IPv6 Multicast Network", RFC 8114, DOI 10.17487/RFC8114, March 2017, <https://www.rfc-editor.org/info/rfc8114>.

[RFC8115] Boucadair, M., Qin, J., Tsou, T., and X. Deng, "DHCPv6 Option for IPv4-Embedded Multicast and Unicast IPv6 Prefixes", RFC 8115, DOI 10.17487/RFC8115, March 2017, <https://www.rfc-editor.org/info/rfc8115>.

23.2. Informative References

[IPv6Survey]
Palet Martinez, J., "IPv6 Deployment Survey", January 2018, <https://indico.uknof.org.uk/event/41/contribution/5/material/slides/0.pdf>.

[OpenWRT] OpenWRT, "OpenWRT Packages", January 2018, <https://openwrt.org/packages/start>.

[RFC7788] Stenberg, M., Barth, S., and P. Pfister, "Home Networking Control Protocol", RFC 7788, DOI 10.17487/RFC7788, April 2016, <https://www.rfc-editor.org/info/rfc7788>.

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

[UPnP-WANIPC]
UPnP Forum, "WANIPConnection:2 Service", December 2010, <http://upnp.org/specs/gw/UPnP-gw-WANIPConnection-v2-Service.pdf>.

Authors' Addresses

Jordi Palet Martinez
The IPv6 Company
Molino de la Navata, 75
La Navata - Galapagar, Madrid 28420
Spain

Email: jordi.palet@theipv6company.com
URI: http://www.theipv6company.com/

Hans M.-H. Liu
D-Link Systems, Inc.
17595 Mount Herrmann St.
Fountain Valley, California 92708
US

Email: hans.liu@dlinkcorp.com
URI: http://www.dlink.com/

Masanobu Kawashima
NEC Platforms, Ltd.
800, Shimomata
Kakegawa-shi, Shizuoka 436-8501
Japan

Email: kawashimam@vx.jp.nec.com
URI: https://www.necplatforms.co.jp/en/