Internet Engineering Task Force (IETF)
Request for Comments: 8585
Category: Informational
ISSN: 2070-1721

J. Palet Martinez
The IPv6 Company
H. M.-H. Liu
D-Link Systems, Inc.
M. Kawashima
NEC Platforms, Ltd.

May 2019

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

Abstract

This document specifies the IPv4 service continuity requirements for IPv6 Customer Edge (CE) routers that are provided either by the service provider or by vendors who sell through the retail market.

Specifically, this document extends the basic requirements for IPv6 CE routers as described in RFC 7084 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 IPv4aaS, i.e., transition technologies for delivering IPv4 in IPv6-only access networks. IPv4aaS is necessary because there aren't sufficient IPv4 addresses available for every possible customer/device. However, devices or applications in the customer Local Area Networks (LANs) may be IPv4-only or IPv6-only and still need to communicate with IPv4-only services on the Internet.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8585.

Table of Contents

1. Introduction 3
1.1. Requirements Language 4
2. Terminology 5
3. Requirements 5
3.1. LAN-Side Configuration 5
3.2. Transition Technologies Support for IPv4 Service Continuity (IPv4-as-a-Service) 5
3.2.1. 464XLAT 7
3.2.2. Dual-Stack Lite (DS-Lite) 8
3.2.3. Lightweight 4over6 (lw4o6) 9
3.2.4. MAP-E 10
3.2.5. MAP-T 10
4. IPv4 Multicast Support 11
5. UPnP Support 11
6. Comparison to RFC 7084 12
7. Code Considerations 12
8. Security Considerations 13
9. IANA Considerations 13
10. References 13
10.1. Normative References 13
10.2. Informative References 16
Appendix A. Usage Scenarios 17
Appendix B. End-User Network Architecture 18
Acknowledgements 21
Authors' Addresses 21

1. Introduction

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

These routers rely upon requirements for IPv6 CE routers defined in [RFC7084]. The scope of this document is to ensure IPv4 service continuity support for devices in the LAN side. This ensures that remote IPv4-only services continue to be accessible, for both IPv4-only and IPv6-only applications and devices, located in the LAN side behind an IPv6 Transition CE Router connected to an IPv6-only access network. These ISP access networks are typically referred to as Wide Area Networks (WANs), even if they may be metropolitan or regional in some cases. Figure 1 presents a simplified view of this architecture.

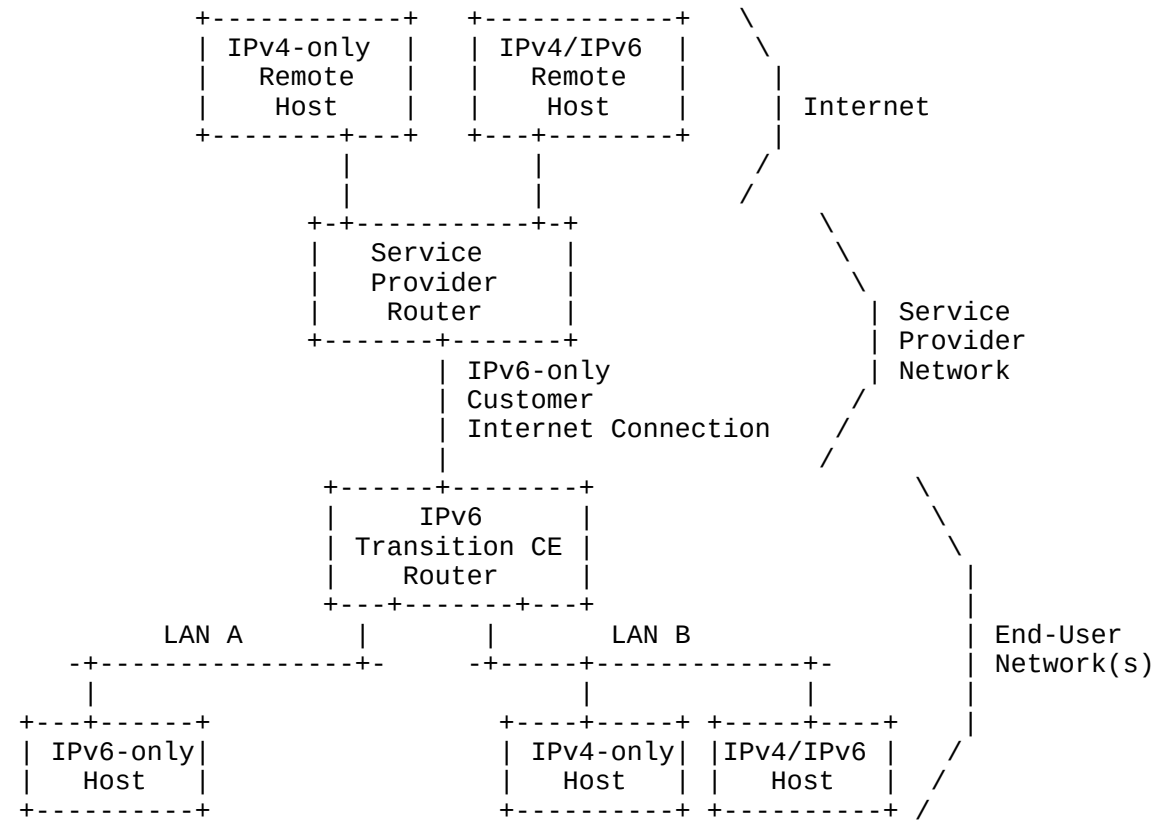

Figure 1: Simplified Typical IPv6-Only Access Network

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 when sufficient IPv4 addresses are no longer available for every possible customer and device, which causes IPv4 addresses to become prohibitively expensive. This, in turn, may result in service providers provisioning IPv6-only WAN access. At the same time, they need to ensure that both IPv4-only and IPv6-only devices and applications in the customer networks can still reach IPv4-only devices and applications on 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 the Home Networking Control Protocol (HNCP) [RFC7788], which is out of the scope of this document.

Since it is impossible to know prior to sale which transition mechanism a device will need over its lifetime, an IPv6 Transition CE Router intended for the retail market MUST support all the IPv4aaS transition mechanisms listed in this document. Service providers that specify feature sets for the IPv6 Transition CE Router may define a different set of features from those included in this document, for example, features that support only some of the transition mechanisms enumerated in this document.

Appendices A and B contain a complete description of the usage scenarios and end-user network architecture, respectively. These appendices, along with [RFC7084], will facilitate a clearer understanding of this document.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 term "WAN Interface" as used in this document is defined as 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"). This document adds new requirements, as described in the following subsections.

3.1. LAN-Side Configuration

A new LAN requirement is added, which is, in fact, common in regular IPv6 Transition CE Routers, and 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)

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 customer LANs, as well as IPv4-only services on the Internet. Thus, both IPv4-only and IPv6-only devices in the customer-side LANs of the IPv6 Transition CE Router are able to reach the IPv4-only services.

Note that this document only configures IPv4aaS in the IPv6 Transition CE Router itself; it does not forward such information to devices attached to the LANs. Thus, the WAN configuration and availability of native IPv4 or IPv4aaS are transparent for the devices attached to the LANs.

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

In order to seamlessly provide IPv4 service continuity in the customer LANs and allow automated IPv6 transition mechanism provisioning, the following 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 and either a CLI or API (or both) 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 configuration of the address space among several interfaces. In some transition mechanisms, this may require differentiating mappings/translations on a per-interface basis.

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 the steps in 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, unless a NAT64 [RFC6146] prefix has been configured, in which case, 464XLAT [RFC6877] MUST be enabled.

Because 464XLAT has no DHCPv6 configuration options, it can't currently be included in the OPTION_S46_PRIORITY. In the future, an update of [RFC8026] or a NAT64 DHCPv6 configuration option may enable it. Meanwhile, if an operator provides 464XLAT, it needs to ensure that OPTION_S46_PRIORITY is not sent for any other transition mechanism to the relevant customers.

The following subsections 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 Stateful NAT64 [RFC6146] function deployed at the service provider or a third-party network.

The IPv6 Transition CE Router MUST support customer-side translator (CLAT) functionality [RFC6877] if intended for the retail market. If 464XLAT is supported, it MUST be implemented according to [RFC6877]. The following IPv6 Transition CE Router requirements also apply.

464XLAT requirements:

464XLAT-1: Unless a dedicated /64 prefix has been acquired, either by using DHCPv6-PD (Dynamic Host Configuration Protocol for IPv6 Prefix Delegation) or by alternative means, the IPv6 Transition CE Router MUST perform IPv4 Network Address Translation (NAT) on IPv4 traffic translated using the CLAT.

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

464XLAT-3: If the Port Control Protocol (PCP) [RFC6887] is implemented, the IPv6 Transition CE Router MUST also implement [RFC7291] ("DHCP Options for the Port Control Protocol (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. The IPv6 Transition CE Router MUST use plain IPv6 mode (i.e., not IPv4-in-IPv6 encapsulation) 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 provider-side translator (PLAT) 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 Port Control Protocol (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: If the network provides several choices for the discovery/learning of the NAT64 prefix, the priority to use one or the other MUST follow this order: 1) [RFC7225] and 2) [RFC7050].

The NAT64 prefix could be discovered by means of the method defined in [RFC7050] only if the service provider uses DNS64 [RFC6147]. It may be the case that the service provider does not use or does not trust DNS64 [RFC6147] because the DNS configuration at the CE (or hosts behind the CE) can be modified by the customer. In that case, the service provider may opt to configure the NAT64 prefix by means of the option defined in [RFC7225]. This can also be used if the service provider uses DNS64 [RFC6147].

3.2.2. Dual-Stack Lite (DS-Lite)

DS-Lite [RFC6333] enables continued support for IPv4 services. DS-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 MUST implement DS-Lite B4 functionality [RFC6333] if intended for the retail market. 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] ("Dynamic Host Configuration Protocol for IPv6 (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].

DSLITE-3: If PCP [RFC6887] is implemented, the IPv6 Transition CE Router SHOULD implement [RFC7291]. If PCP [RFC6887] is implemented and a PCP server is not configured, the IPv6 Transition CE Router MUST assume, by default, that the Address Family Transition Router (AFTR, commonly called "CGN" - Carrier-Grade NAT) is the PCP server. The IPv6

Transition CE Router MUST use plain IPv6 mode (i.e., not IPv4-in-IPv6 encapsulation) to send PCP requests to the server. The term "default" above is to be interpreted as pertaining to a configuration as applied by a vendor prior to the administrator changing it for its initial activation.

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 that 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 an AFTR (CGN) function in the tunnel concentrator and reducing the amount of centralized state.

The IPv6 Transition CE Router MUST implement lwB4 functionality [RFC7596] if intended for the retail market. 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 (DHCP 4o6) 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

Mapping of Address and Port with Encapsulation (MAP-E) [RFC7597] is a mechanism for transporting IPv4 packets across an IPv6 network using IP encapsulation. MAP-E includes an algorithmic mechanism for mapping between IPv6 and IPv4 addresses.

The IPv6 Transition CE Router MUST support MAP-E CE functionality [RFC7597] if intended for the retail market. 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]. 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].

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 MUST support MAP-T CE functionality [RFC7599] if intended for the retail market. 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]. 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].

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][OCF-IGD] 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 Section 5.6.1 of [RFC6970].

Note that IGD:1 and its WANIPConnection:1 service have been deprecated by OCF (Open Connectivity Foundation) [OCF-IGD].

6. Comparison to RFC 7084

This document doesn't include support for 6rd [RFC5969] because it is an IPv6-in-IPv4 tunneling.

Regarding DS-LITE [RFC6333], this document includes slightly different requirements related to the support of PCP [RFC6887], IGD-PCP IWF [RFC6970], and the prioritization of the transition mechanisms, including dual-stack.

7. Code Considerations

At the time of this writing, one of the apparent main issues for vendors with regard to including 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 (e.g., OpenWRT/LEDE, Linux, and VPP) that adding the support for the new transition mechanisms requires around 10-12 KBs because most of the code base is shared among several transition mechanisms, which are already supported by [RFC7084]. A single data plane is common to all of them, which typically means, in popular CEs already in the market [OpenWRT], the new required code is only about 0.15% of the total existing code size.

In general, the new requirements don't have extra cost in terms of RAM memory, nor other hardware requirements such as more powerful CPUs, if compared to the cost of NAT44 code. Thus, existing hardware should be able to support all of 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 several vendors already have implementations and provided them to ISPs. Therefore, the development cost is negligible, and only integration and testing cost may become an issue.

Finally, in some cases, operators supporting several transition mechanisms may need to consider training costs for staff in all the techniques for the operation and management of these mechanisms, even if the costs are not directly caused by supporting this document but because of business decisions.

8. Security Considerations

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

As described in the Security Considerations of [RFC8026] and [RFC8415], there are generic DHCP security issues, which, in the case of this document, mean that malicious nodes may alter the priority of the transition mechanisms.

Access network architecture for securing DHCP within the access network is out of scope for this document. Securing DHCP in the LAN is also not in scope. DHCP packets MUST NOT be forwarded between LAN and WAN interfaces of an IPv6 Transition CE Router.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. 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>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

10.2. Informative References

[IPv6Survey] Palet Martinez, J., "Best Current Operational Practice for operators: IPv6 Prefix Assignment for end-customers -- persistent vs non-persistent and what size to choose", January 2018, <https://indico.uknof.org.uk/event/41/contribution/5/material/slides/0.pdf>.

[OCF-IGD] Open Connectivity Foundation, "Internet Gateway Device (IGD) V 2.0", March 2015, <https://openconnectivity.org/developer/specifications/upnp-resources/upnp/internet-gateway-device-igd-v-2-0>.

[OpenWRT] OpenWRT, "Packages", <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/UPnP-gw-InternetGatewayDevice-v2-Device.pdf>.

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

Appendix A. Usage Scenarios

The situation of ongoing IPv6 deployment and a lack of IPv4 addresses is not happening at the same pace in every country and even within every country for every ISP. For different technical, financial, commercial/marketing, and socio-economic reasons, each network is transitioning at their own pace; the global transition timings cannot be reliably estimated.

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

So, to cover all those evolving situations, an IPv6 Transition CE Router is required, at least from the perspective of transition support.

Moreover, because some services and service providers will remain IPv4-only for an undetermined period of time, IPv4 service continuity is required. Thus, there is a need for CEs to support IPv4aaS indefinitely.

Based on these premises, this document 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]) to networks that provide IPv6-only access with IPv4aaS.

Considering that situation and different possible usage cases, the IPv6 Transition CE Router described in this document is expected to be used 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 more advanced requirements include inbound connections (IP cameras, web, DNS, email, VPN, etc.).

The above is not intended to be a comprehensive list of all the possible usage cases, just an overview. In fact, combinations of the above usages are also possible, along with situations where the same CE is used at different times in different scenarios or even with different IPv4aaSes at different service providers.

The mechanisms for allowing inbound connections are naturally available in any IPv6 router when using IPv6 Global Unicast Addresses (GUAs), unless they are blocked by firewall rules, which may require some manual configuration.

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

Who provides the IPv6 Transition CE Router is not relevant. In most cases, the service provider is responsible for provisioning/managing, at least on the WAN side. Commonly, the user has access to configure the LAN interfaces, firewall, DMZ, and many other features. However, in many cases, the user must supply or may replace the IPv6 Transition CE Router. This underscores the importance of the IPv6 Transition CE Routers fulfilling the 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. Even if the documented requirements meet their needs, they may have additional requirements, which are out of the scope of this document.

Appendix B. End-User Network Architecture

An end-user network will likely support both IPv4 and IPv6 (see Section 1 and Appendix A). It is not expected that end users 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 CE Router, 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][OCF-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 [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 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 2 illustrates the model topology for the end-user network.

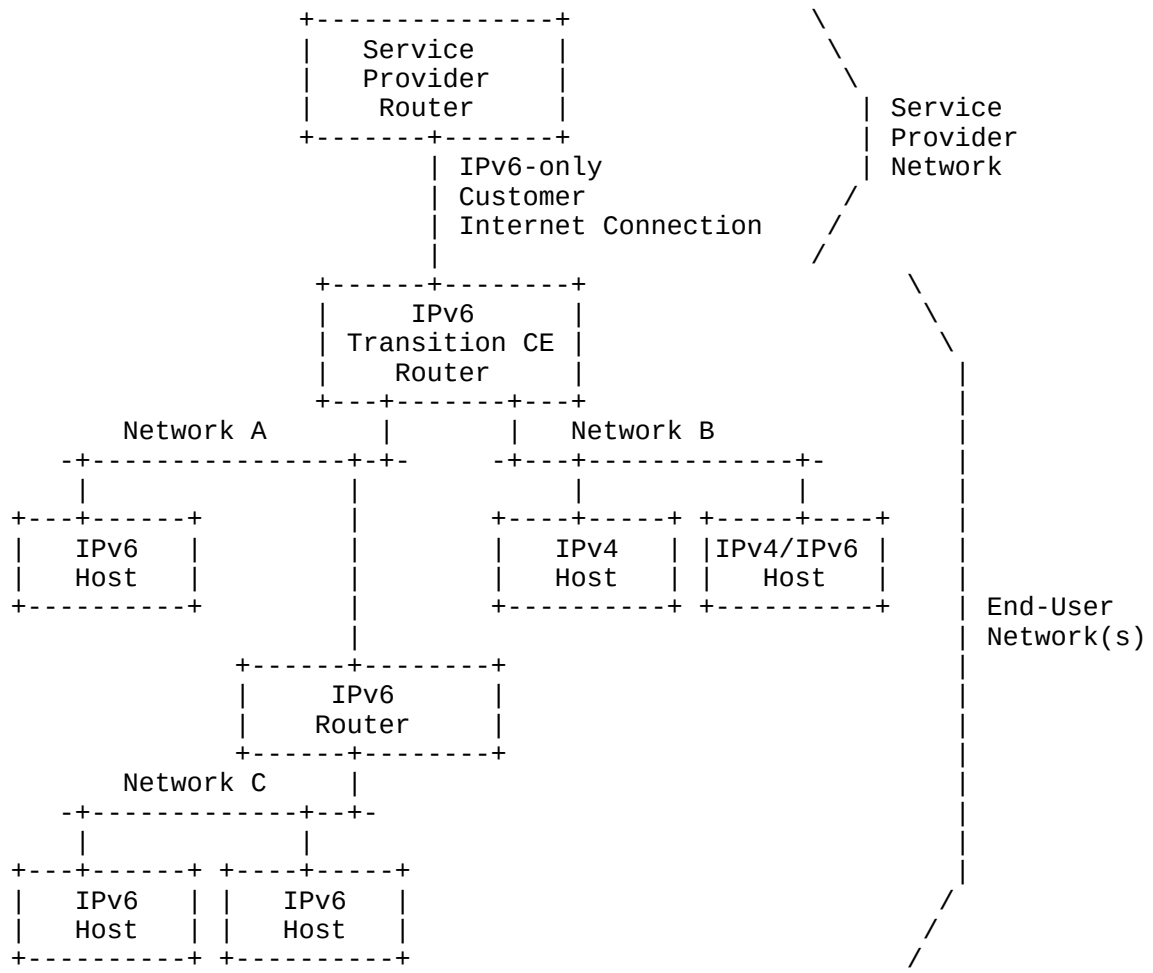

Figure 2: Example of a Typical End-User Network

This architecture describes the:

- Basic capabilities of the IPv6 Transition CE Router
- Provisioning of the WAN interface connecting to the service provider
- Provisioning of the LAN interfaces

The IPv6 Transition CE Router may be manually configured in an arbitrary topology with a dynamic routing protocol or HNCP [RFC7788]. Automatic provisioning and configuration are described for a single IPv6 Transition CE Router only.

Acknowledgements

Thanks to Mikael Abrahamsson, Fred Baker, Mohamed Boucadair, Brian Carpenter, Lorenzo Colitti, Alejandro D'Egidio, Ian Farrer, Lee Howard, Richard Patterson, Barbara Stark, Ole Troan, and James Woodyatt for their review and comments in this and/or previous draft versions of this document. Thanks also for the Last Call reviews by Dan Romascanu (OPS-DIR); Christian Huitema (SEC-DIR); Daniele Ceccarelli (RTG-DIR); Martin Stiemerling (TSV-ART); Matthew Miller (Gen-ART); and Alissa Cooper, Benjamin Kaduk, Suresh Krishnan, Ben Campbell, Spencer Dawkins, Mirja Kuhlewind, and Adam Roach (all IESG).

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
United States of America

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

Masanobu Kawashima
NEC Platforms, Ltd.
2-3, Kanda-Tsukasamachi
Chiyoda-ku, Tokyo 101-8532
Japan

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