IPv6 Operations (v6ops)
Internet-Draft
Intended status: Informational
Expires: April 20, 2018

J. Palet Martinez
Consulintel, S.L.
October 17, 2017

Transition Requirements for IPv6 Customer Edge Routers
draft-palet-v6ops-rfc7084-bis-transition-01

Abstract

This document specifies the transition requirements for an IPv6 Customer Edge (CE) router. Specifically, this document extends the "Basic Requirements for IPv6-only Customer Edge Routers" ([RFC7084]) in order to allow the provisioning of IPv6 transition services for the hosts attached to it. The document covers several transition technologies, either for delivering IPv6 in IPv4-only access networks and specially for delivering IPv4 "as-a-service" 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.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

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

These routers are based on "Basic Requirements for IPv6-only Customer Edge Routers" ([RFC7084]), so the scope of this documents is to include also IPv4 support, at least in the LAN side.

This document covers the IP transition technologies required when ISPs have already and IPv4-only access network that they can't turn to dual-stack or IPv6-only, as well as the situation 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.

This document specifies the transition mechanisms to be supported by an IPv6 transition CE router, relevant provisioning or configuration information differences from [RFC7084]. 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.

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 IPv6 Transition CE router that interoperates successfully with a particular subset of currently deploying and planned common IPv6 access networks.

2. Terminology

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

The term "IPv6 transition Customer Edge Router" is defined as an "IPv6 Customer Edge Router" that provides transition support to allow IPv4-IPv6 coexistence either in the WAN, the LAN or both.

The "WAN Interface" term used across this document, means that can also support link technologies based in Internet-layer (or higher-layers) "tunnels", such as tunnels IPv4-in-IPv6 or IPv6-in-IPv4.

3. Usage Scenarios

The IPv6 Transition CE router described in this document is expected to be used typically, in any of the following scenarios:

1. Residential/household users. Common usage is any kind of Internet access (web, email, streaming, online gaming, etc.).

2. Residential with Small Office/Home Office (SOHO). Same usage as for the first scenario.

3. Small Office/Home Office (SOHO). Same usage as for the first scenario.

4. Small and Medium Enterprise (SME). Same usage as for the first scenario.

5. Residential/household with advanced requirements. Same basic usage as for the first scenario, however there may be requirements for exporting services to the WAN (IP cameras, web, DNS, email, VPN, etc.).

6. Small and Medium Enterprise (SME) with advanced requirements. Same basic usage as for the first scenario, however there may be requirements for exporting services to the WAN (IP cameras, web, DNS, email, VPN, etc.).

The above list is not intended to be comprehensive of all the possible usage scenarios, just the main ones. In fact, combinations of the above usages are also possible, for example a residential with SOHO and advanced requirements.

The mechanisms for exporting IPv6 services are commonly "naturally" available in any IPv6 router, as when using GUA, unless they are blocked by firewall rules, which may require some manual configuration by means of a GUI and/or CLI.

However, in the case of IPv4, because the usage of private addresses and NAT, it typically requires some degree of manual configuration such as setting up a DMZ, virtual servers, or port/protocol forwarding. In general, CE routers already provide GUI and/or CLI to manually configure them, or the possibility to setup the CE in bridge mode, so another CE behind it, takes care of that. It is out of the scope of this document the definition of any requirements for that.

The main difference for an IPv6 Transition CE router to support one or several of the above indicated scenarios, is related to the packet processing capabilities, performance, even other details such as the number of WAN/LAN interfaces, their maximum speed, memory for keeping tables or tracking connections, etc. So, it is out of the scope of this document to classify them.

For example, an SME may have just 10 employees (micro-SME), which commonly will be considered same as a SOHO, but a small SME can have up to 50 employees, or 250 for a medium one. Depending on the IPv6 Transition CE router capabilities or even how it is being configured (for instance, using SLAAC or DHCPv6), it may support even a higher number of employees if the traffic in the LANs is low, or switched by another device(s), or the WAN bandwidth requirements are low, etc. The actual bandwidth capabilities of access with technologies such as FTTH, cable and even 3GPP/LTE, allows the support of such usages, and indeed, is a very common situation that access networks and the IPv6 Transition CE provided by the service provider are the same for SMEs and residential users.

There is also no difference in terms of who actually 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 aspects. In fact, in many cases, the user must supply, or at least can replace the IPv6 Transition CE router, which 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 bigger Enterprises, Data Centers, Content Providers, etc. So, even if the documented requirements meet their needs, may have additional requirements, which are out of the scope of this document.

4. Architecture

4.1. 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.

4.2. 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, 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 an 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.

5. Requirements

5.1. General Requirements

The IPv6 Transition CE router must comply with the general requirements stated in [RFC7084]. Furthermore, a new general requirement is added:

G-6 The IPv6-only CE router MUST comply with [RFC7608].

5.2. LAN-Side Configuration

The IPv6 Transition CE router must comply with LAN-Side Configuration as stated in [RFC7084].

In addition, a new LAN Requirement is:

L-15 The IPv6 CE router SHOULD implement a DNS proxy as described in [RFC5625].

5.3. Transition Technologies Support

Even if the main target of this document is the support of IPv6-only WAN access, for some time, there will be a need to support IPv4-only devices and applications in the customers LANs, in one side of the picture. In the other side, some Service Providers willing to deploy IPv6, may not be able to do so in the first stage, neither as IPv6-only or dual-stack in the WAN. Consequently, transition technologies to resolve both issues should be taken in consideration.

5.3.1. IPv4 Service Continuity in Customer LANs

5.3.1.1. 464XLAT

464XLAT [RFC6877] is a technique to provide IPv4 access service to IPv6-only edge networks without encapsulation.

The IPv6 Transition CE router SHOULD support CLAT functionality. If 464XLAT is supported, it MUST be implemented according to [RFC6877]. The following CE 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 using DHCPv6-PD [RFC3633].

464XLAT-2: The IPv6 Transition CE router MUST implement [RFC7050] in order to discover the PLAT-side translation IPv4 and IPv6 prefix(es)/suffix(es). In environments with PCP support, the IPv6 Transition CE SHOULD follow [RFC7225] to learn the PLAT-side translation IPv4 and IPv6 prefix(es)/suffix(es) used by an upstream PCP-controlled NAT64 device.

5.3.1.2. 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 IPv6 Transition CE router’s native IPv6 WAN interface, and not encapsulated in another tunnel.

The IPv6 Transition CE router SHOULD 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 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]. 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 MUST support the DHCPv6 S46 priority option described in [RFC8026].

DSLITE-3: The IPv6 Transition CE router MUST NOT perform IPv4 Network Address Translation (NAT) on IPv4 traffic encapsulated using DS-Lite.

DSLITE-4: If the IPv6 Transition CE router is configured with an IPv4 address on its WAN interface, then the IPv6 Transition CE router SHOULD disable the DS-Lite Basic Bridging BroadBand (B4) element.

5.3.1.3. 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 lw4o6 functionality. If DS-Lite is implemented, lw4o6 MUST be supported as well. If lw4o6 is supported, it MUST be implemented according to [RFC7596]. This document takes no position on simultaneous operation of lw4o6 and native IPv4. 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]. 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 DHCPv6 S46 priority option described in [RFC8026].

LW4O6-3: The IPv6 Transition CE router MUST support the DHCPv4-over-DHCPv6 (DHCP 4o6) transport described in [RFC7341].

LW4O6-4: The IPv6 Transition CE router MAY support Dynamic Allocation of Shared IPv4 Addresses as described in [RFC7618].

5.3.1.4. 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 IPv6 Transition CE router SHOULD support MAP-E functionality. If MAP-E is supported, it MUST be implemented according to [RFC7597]. The following CE 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 MUST support the DHCPv6 S46 priority option described in [RFC8026].

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

MAP-T requirements:

MAPT-1: The CE router MUST support configuration of MAP-T 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.

MAPT-2: The IPv6 Transition CE router MUST support the DHCPv6 S46 priority option described in [RFC8026].

5.3.2. Support of IPv6 in IPv4-only WAN access

5.3.2.1. 6in4

6in4 [RFC4213] specifies a tunneling mechanism to allow end-users to manually configure IPv6 support via a service provider’s IPv4 network infrastructure.

The IPv6 Transition CE router MAY support 6in4 functionality. 6in4 used for a manually configured tunnel requires a subset of the 6rd parameters (delegated prefix and remote IPv4 end-point). The on-wire and forwarding plane is identical for both mechanisms, however 6in4 doesn’t support mesh traffic and requires manually provisioning. Thus, if the device supports either 6rd or 6in4, it’s commonly a minor UI addition to support both. If 6in4 is supported, it MUST be implemented according to [RFC4213]. The following CE Requirements also apply:

6in4 requirements:

6IN4-1: The IPv6 Transition CE router SHOULD support 6in4 automated configuration by means of the 6rd DHCPv4 Option 212. If the IPv6 Transition 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 Transition CE router MAY use other mechanisms to configure 6in4 parameters. Such mechanisms are outside the scope of this document.

6IN4-2: If the IPv6 Transition CE router is capable of automated configuration of IPv4 through IPCP (i.e., over a PPP connection), it MUST support user-entered configuration of 6in4.

6IN4-3: If the IPv6 Transition CE router supports configuration mechanisms other than the 6rd DHCPv4 Option 212 (user-entered, TR-069 [TR-069], etc.), the IPv6 Transition CE router MUST support 6in4 in "hub and spoke" mode. 6in4 in "hub and spoke" requires all IPv6 traffic to go to the 6rd Border Relay, which in this case is the tunnel-end-point. In effect, this requirement removes the "direct connect to 6rd" route defined in Section 7.1.1 of [RFC5969].

6IN4-4: The IPv6 Transition CE router MUST allow 6in4 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 6in4 to native IPv6.

6IN4-5: Each packet sent on a 6in4 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]).

6IN4-6: The IPv6 Transition CE router MUST allow different as well as identical delegated prefixes to be configured via each (6in4 or native) WAN interface.

6IN4-7: In the event that forwarding rules produce a tie between 6in4 and native IPv6, by default, the IPv6 Transition CE router MUST prefer native IPv6.

5.3.2.2. 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 IPv6 Transition CE router's native IPv4 WAN interface and not encapsulated in another tunnel.

The IPv6 Transition 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 Transition CE router MUST support 6rd configuration via the 6rd DHCPv4 Option 212. If the IPv6 Transition 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 Transition CE router MAY use other mechanisms to configure 6rd parameters. Such mechanisms are outside the scope of this document.

6RD-2: If the IPv6 Transition 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 IPv6 Transition CE router supports configuration mechanisms other than the 6rd DHCPv4 Option 212 (user-entered, TR-069 [TR-069], etc.), the IPv6 Transition 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: The IPv6 Transition 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 IPv6 Transition 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 Transition CE router MUST prefer native IPv6.

5.4. IPv4 Multicast Support

Actual 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.

In order to support the delivery of IPv4 multicast services to IPv4 clients over an IPv6 multicast network, the IPv6 Transition CE router SHOULD support [RFC8114] and [RFC8115].

5.5. Security Considerations

The IPv6 Transition CE router must comply with the Security Considerations as stated in draft-palet-v6ops-rfc7084-bis2.

6. Acknowledgements

Thanks to James Woodyatt, Mohamed Boucadair, Masanobu Kawashima, Mikael Abrahamsson, Barbara Stark, Ole Troan and Brian Carpenter for their review and comments.

7. ANNEX A: 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), that adding the support for the new transitions mechanisms, requires around 10-12 Kbytes (because most of the code is shared among several transition mechanisms), which typically means about 0,15% of the existing code size in popular CEs in the market.

It is also clear that the new requirements don’t have extra cost in terms of RAM memory, neither other hardware requirements such as more powerful CPUs.

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 the new transition mechanisms, so the development cost is negligent, and only integration and testing cost may become a minor issue.

8. References

8.1. 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>.

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

[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>.

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

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

[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>.

[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>.

[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>.

[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>.

[RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "IPv6 Prefix Length Recommendation for Forwarding", BCP 198, RFC 7608, DOI 10.17487/RFC7608, July 2015, <https://www.rfc-editor.org/info/rfc7608>.

[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>.

8.2. Informative References

[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>.

[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/