V6OPS
Internet-Draft
Intended status: Informational
Expires: April 18, 2021

G. Fioccola
P. Volpato
Huawei Technologies

October 15, 2020

IPv6 Transition Deployment Status
draft-vf-v6ops-ipv6-deployment-00

Abstract

Looking globally, IPv6 is growing faster than IPv4 and this means that the collective wisdom of the networking industry has selected IPv6 for the future. This document provides an overview of IPv6 transition deployment status and a view on how the transition to IPv6 is progressing among network operators that are introducing IPv6 or have already adopted an IPv6-only solution. It also aims to analyze the transition challenges and therefore encourage actions and more investigations on some areas that are still under discussion. The overall IPv6 incentives are also examined.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 18, 2021.

Table of Contents

1. Introduction

The focus of this document is to provide a survey of the deployed IPv6 transition technologies and to highlight the difficulties in the transition. This process helps to understand what is missing and how to improve the current IPv6 deployment strategies of the network operators and enterprises. The objective is to give an updated view of the practices and plans already described in [RFC6036]. The scope is to report the current IPv6 status and encourage actions and more investigations on some areas that are still under discussion as well as the main incentives for the IPv6 adoption.

[RFC6180] discussed the IPv6 deployment models and migration tools. [RFC6036] described the Service Provider Scenarios for IPv6 Deployment, [RFC7381] introduced the guidelines of the IPv6 deployment for Enterprise and [RFC6883] provided guidance and suggestions for Internet Content Providers and Application Service Providers. On the other hand, this document focuses on the end-to-end services and in particular on the device - network - content communication chain.

[ETSI-IP6-WhitePaper] reported the IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward. IPv6 is becoming a priority again and a new wave of IPv6 deployment is expected, due the exhaustion of the IPv4 address space since 2010, in addition technologies like 5G, cloud, IoT require its use, governments and standard bodies (including IETF) demand it, and the device - network - content communication chain is calling for its adoption. In this regard it is possible to mention the IAB Statement on IPv6 stating that "IETF will stop requiring IPv4 compatibility in new or extended protocols".

The following sections give the global picture of IPv6 to show how IPv6 is growing faster than IPv4 worldwide in all measures including number of users, percentage of content, and amount of traffic. This testifies that the key Internet industry players have decided strategically to invest and deploy IPv6 in large-scale to sustain the Internet growth.

Then it is presented the survey among network operators about the IPv6 deployment and the considerations that have come out. IPv6 transition solutions for Mobile BroadBand (MBB), Fixed BroadBand (FBB) and enterprise services are ready. Dual-Stack is the most

deployed solution for IPv6 introduction, while 464XLAT and Dual Stack Lite (DS-Lite) seem the most suitable for IPv6-only service delivery.

Finally, The IPv6 incentives are presented but the general IPv6 challenges are also reported in particular in relation to Architecture, Operations, Performance and Security issues. These considerations aim to start a call for action on the areas of improvement, that are often mentioned as reason for not deploying IP6.

2. The global picture of IPv6

The utilization of IPv6 has been monitored by many agencies and institutions worldwide. Different analytics have been made available, ranging from the number of IPv6 users, its relative utilization over the Internet, to the number of carriers able to route IPv6 network prefixes. The scope of this section then is to provide a glance at the status of the IPv6 adoption, so to get an indication of the relevance of IPv6 today. For each analytic listed in the next subsections the trend over the past five years is given, expressed as the Compound Annual Growth Rate (CAGR). In general, this shows how IPv6 has grown in the past few years, and that is growing faster than IPv4.

2.1. IPv6 connectivity

Some OTTs and Internet Registries keep track of the utilization of IPv6 worldwide, collecting the number of end points (IPv6 addresses) that access their servers. The following table show the percentage of IPv6 connections as collected and reported by [APNIC1], [FACEBOOK], and [GOOGLE] in the period January 1, 2015 to January 1, 2020. It has to be noted that [FACEBOOK] started their collection in September, 2017. As such, January, 2018 is the first data point reported in the table. For each data set, the relative CAGR shows how steady the IPv6 growth results.

Source	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Jan 2020	CAGR
APNIC	3.13 %	5.51%	8.05%	16.83 %	20.11%	24.58%	51.01%
Faceboo k	N/A	N/A	N/A	18.35 %	23.66%	26.24%	19.58%
Google	5.84 %	10.41 %	16.51 %	21.84 %	26.32%	30.16%	38.87%

Table 1: IPv6 connectivity percentage

The next table also shows the relative increase of IPv6 connections as measured by [AKAMAI] on their platforms over the last five years. The percentage is expressed as the number of hits generated by IPv6 users over the total hits. For the sake of conciseness, only a few examples are reported.

Source	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Jan 2020	CAGR
Reliance (IN)	6.7%	10.7%	73.2%	84.0%	86.3%	87.0%	67%
ATT (USA)	20.9%	40.0%	49.0%	59.6%	68.4%	67.7%	26%
Softbank (JP)	2.1%	11.2%	20.9%	28.7%	40.8%	45.8%	85%

Table 2: IPv6 connectivity percentage - Operators

2.2. Number of IPv6 users

The analytics provided by [APNIC1] also give an estimation on the number of IPv6 users worldwide, which is constantly increasing. The next table shows the growth for the five economies with the highest numbers of IPv6 users at January 2020 as well as the estimation of the total IPv6 users worldwide.

Country	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Jan 2020	CAGR
India	0.10	4.27	61.99	227.22	250.10	360.74	413.7%
USA	31.91	84.80	95.15	109.86	122.79	137.31	33.9%
China	4.12	4.52	4.87	2.84	8.32	130.10	99.5%
Brazil	0.14	9.77	12.84	26.42	32.87	50.48	226.9%
Japan	10.49	18.43	17.11	27.56	28.98	40.86	31.2%
World	74.24	179.42	290.68	513.68	574.02	989.25	67.9%

Table 3: IPv6 users worldwide (in millions)

2.3. Web sites supporting IPv6

The progression of IPv6 web sites on the global Internet is shown in the next table, as reported by [W3TECHS]

Country	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Jan 2020	CAGR
Servers	5.2%	6.1%	9.6%	11.4%	13.3%	15.0%	24%

Table 4: IPv6 web servers worldwide

As explained by [W3TECHS], the statistic above refers to the whole Internet and includes all sizes of providers, businesses and enterprises. As such, it has to be noted that the biggest OTTs and Content Providers host a large amount of servers which are actually counted as one single website. The relative percentage of IPv6 capable servers would be much higher, as these players alone provide a big portion of the contents accessed every day by the Internet community.

2.4. Regional Internet Registries' Allocations

Regional Internet Registries (RIRs) are responsible for assigning an IPv6 address block to ISPs or enterprises. An ISP will use the assigned block to provide addresses to their end users. For example, a mobile carrier will assign one or several /64 prefixes to the end users. Several analytics are available for the RIRs. The next table

shows the amount of individual allocations, per RIR, in the time period 2015-2019 [APNIC2].

Registry	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Cumulated	CAGR
AFRINIC	86	116	112	110	115	539	58%
APNIC	778	1,681	1,369	1,474	1,484	6,786	72%
ARIN	602	646	684	658	605	3,195	52%
LACNIC	1,061	1,010	1,549	1,450	1,618	6,688	58%
RIPE	2,206	2,141	2,051	2,617	3,105	12,120	53%
Total	4,733	5,594	5,765	6,309	6,927	29,328	58%

Table 5: IPv6 web servers worldwide

[APNIC2] also compares the number of allocations for both address families, and the result is in favor of IPv6. The average yearly growth is 58% for IPv6 in the period 2015-2019 versus 47% for IPv4, a sign that IPv6 is growing bigger than IPv4. This is described in the next table.

Address family	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Cumulated	CAGR
IPv6	4,733	5,594	5,765	6,309	6,927	29,328	58%
IPv4	11,732	9,787	9,440	10,199	14,033	55,191	47%

Table 6: Allocations per address family

2.5. Networks supporting IPv6

The next table is based on [POTAROO] and shows the percentage of ASes supporting IPv6 compared to the total ASes worldwide. The number of IPv6-capable ASes increases from 21.1% in January 2015 to 27.5% in January 2020. This equals to 15.19% CAGR for IPv6 enabled networks. This also shows that the number of networks supporting IPv6 is growing faster than the ones supporting IPv4, since the total (IPv6 and IPv4) networks grow at 9.23% CAGR.

Advertised ASN	Jan 2015	Jan 2016	Jan 2017	Jan 2018	Jan 2019	Jan 2020	CAGR
IPv6-capable	9,182	10,744	12,663	14,506	16,440	18,623	15.19%
Total ASN	43,543	44,549	44,368	60,281	63,782	67,713	9.23%
Ratio	21.1%	24.1%	28.5%	24.1%	25.8%	27.5%	

Table 7: IPv6 web servers worldwide

3. Survey among Network Operators

It was started an IPv6 poll to more than 50 network operators about the status of IPv6 deployment. This poll reveals that more than 30 operators will migrate fixed and mobile users to IPv6 in next 2 years. The IPv6 Poll has been submitted in particular to network operators considering that, as showed by the previous section, both user devices and contents seem more ready for IPv6. The answers to the questionnaire can be found in Appendix.

The main Questions asked are:

* Do you plan to move more fixed or mobile or enterprise users to IPv6 (e.g. Dual-Stack) or IPv6-only in the next 2 years? What are the reasons to do so? Which transition solution will you use, Dual-Stack, DS-Lite, 464XLAT, MAP-T/E?

* Do you need to change network devices for the above goal? Will you migrate your metro or backbone or backhaul network to support IPv6?

The result of this questionnaire highlights that major IPv6 migration will happen in next 2 years. Dual Stack is always the most adopted solution and the transition to IPv6-only is motivated in particular by business reasons like the 5G and IoT requirements. In addition it is worth mentioning that the migration of transport network (metro and backbone) is not considered a priority today for many network operators and the focus is in particular on the end to end IPv6 services.

More details about the answers received can be found in the Appendix.

4. IPv6 deployments worldwide

This section reports the most deployed approaches for the IPv6 migration in MBB, FBB and enterprise.

4.1. IPv6 service design for Mobile, Fixed broadband and enterprises

The consolidated strategy, as also described in [ETSI-IP6-WhitePaper], is based on two stages, namely: (1) IPv6 introduction, and (2) IPv6-only. The first stage aims at delivering the service in a controlled manner, where the traffic volume of IPv6-based services is minimal. When the service conditions change, e.g. when the traffic grows beyond a certain threshold, then the move to the second stage may occur. In this latter case, the service is delivered solely on IPv6.

4.1.1. IPv6 introduction

In order to enable the deployment of an IPv6 service over an underlay IPv4 architecture, there are two possible approaches:

- Enabling Dual-Stack at the CPE
- Tunneling IPv6 traffic over IPv4, e.g. with 6rd.

So, from a technical perspective, the first stage is based on Dual-Stack [RFC4213] or tunnel-based mechanisms such as Generic Routing Encapsulation (GRE), IPv6 Rapid Deployment (6rd), Connection of IPv6 Domains via IPv4 Clouds (6to4), and others.

Dual-Stack [RFC4213] is more robust, and easier to troubleshoot and support. Based on information provided by operators with the answers to the poll (see Appendix A), it can be stated that Dual-Stack is currently the most widely deployed IPv6 solution, for MBB, FBB and enterprises, accounting for about 50% of all IPv6 deployments, see both Appendix A and the statistics reported in [ETSI-IP6-WhitePaper]. Therefore, for operators that are willing to introduce IPv6 the most common approach is to apply the Dual-Stack transition solution.

With Dual-Stack, IPv6 can be introduced together with other network upgrade and many parts of network management and IT systems can still work in IPv4. This avoids major upgrade of such systems to support IPv6, which is possibly the most difficult task in IPv6 transition. In other words, the cost and effort on the network management and IT system upgrade are moderate. The benefits are to start to accommodate future services and save the NAT costs.

The CPE has only an IPv6 address at the WAN side and uses an IPv6 connection to the operator gateway, e.g. Broadband Network Gateway (BNG) or Packet Gateway (PGW) / User Plane Function (UPF). However, the hosts and content servers can still be IPv4 and/or IPv6. For example, NAT64 can enable IPv6 hosts to access IPv4 servers. The backbone network underlay can also be IPv4 or IPv6.

Although the Dual-Stack IPv6 transition is a good solution to be followed in the IPv6 introduction stage, it does have few disadvantages in the long run, like the duplication of the network resources, as well as other limitations for network operation. For this reason, when IPv6 increases to a certain limit, it would be better to switch to the IPv6-only stage.

4.1.2. IPv6-only service delivery

The second stage, named here IPv6-only, can be a complex decision that depends on several factors, such as economic factors, policy and government regulation.

[I-D.lmhp-v6ops-transition-comparison] discusses and compares the technical merits of the most common transition solutions for IPv6-only service delivery, 464XLAT, DS-lite, Lightweight 4over6 (lw4o6), MAP-E, and MAP-T, but without providing an explicit recommendation. As the poll highlights, the most widely deployed IPv6 transition solution for MBB is 464XLAT and for FBB is DS-Lite.

Based on the survey among network operators in Appendix A it is possible to analyze the IPv6 transition technologies that are already deployed or that will be deployed. The different answers to the questionnaire and in particular [ETSI-IP6-WhitePaper] reported detailed statistics on that and it can be stated that, besides Dual-Stack, the most widely deployed IPv6 transition solution for MBB is 464XLAT [RFC6877], and for FBB is DS-Lite [RFC6333], both of which are IPv6-only solutions.

Looking at the different feedback from network operators, in some cases, even when using private addresses, such as 10.0.0.0/8 space [RFC1918], the address pool is not large enough, e.g. for large mobile operators or large Data Centers (DCs), Dual-Stack is not enough, because it still requires IPv4 addresses to be assigned. Also, Dual-Stack will likely lead to duplication of several network operations both in IPv6 and IPv4 and this increases the amount of state information in the network with a waste of resources. For this reason, in some scenarios (e.g. MBB or DCs) IPv6-only stage could be more efficient from the start since the IPv6 introduction phase with Dual-Stack may consume more resources (for example CGNAT costs).

So, in general, it is possible to state that, when the Dual-Stack disadvantages outweigh the IPv6-only complexity, it makes sense to migrate to IPv6-only. Some network operators already started this process, while others are still waiting.

5. Considerations coming out of IPv6 deployments

Global IPv4 address depletion is reported by most network operators as the important driver for IPv6 deployment. Indeed, the main reason for IPv6 deployment given is related to the run out of private 10.0.0.0/8 space [RFC1918]. 5G and IoT service deployment is another incentive not only for business reasons but also for the need of more addresses.

The answers in Appendix shows that the IPv6 deployment strategy is based mainly on Dual Stack architecture and most of the network operators are migrating or plan to migrate in the next few years.

It is interesting to see that most of the network operators have no big plans to migrate transport network (metro and backbone) soon, since they do not see business reasons. It seems that despite the future benefit with IPv6 (e.g. SRv6) which may justify in the long term a migration to native IPv6, there is no pressure to migrate to native IPv6 forwarding in the short term. Most of the network operators said that a software upgrade can be enough to support IPv6 where it is needed for now.

This survey demonstrates that full replacement of IPv4 will take long time. Indeed the transition to IPv6 has different impacts and requirements depending on the network segment:

- It is possible to say that almost all mobile devices are already IPv6 capable while for fixed access most of the CPEs are Dual Stack. Data Centers are also evolving and deploying IPv6 to cope with the increasing demand of cloud services.

- While the access network seems not strongly impacted because it is mainly based on layer 2 traffic, regarding Edge and BNG, most network operators that provide IPv6 connectivity runs BNG devices in Dual Stack in order to distribute both IPv4 and IPv6.

- For Metro and Backbone, the trend is to keep MPLS Data Plane and run IPv6/IPv4 over PE devices at the border. All MPLS services can be guaranteed in IPv6 as well through 6PE/6VPE protocols.

In this scenario it is clear that the complete deployment of a full IPv6 data plane will take more time. If we look at the long term evolution, IPv6 can bring other advantages like introducing advanced

protocols developed only on IPv6 (e.g. SRv6) to implement all the controlled SLA services aimed by the 5G technology and beyond.

6. IPv6 incentives

It is possible to state that IPv6 adoption is no longer optional, indeed there are several incentives for the IPv6 deployment:

Technical incentives: all Internet technical standard bodies and network equipment vendors have endorsed IPv6 and view it as the standards-based solution to the IPv4 address shortage. The IETF, as well as other SDOs, need to ensure that their standards do not assume IPv4. The IAB expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6. It is recommended that all networking standards assume the use of IPv6 and be written so they do not require IPv4 ([RFC6540]). In addition, every Internet registry worldwide strongly recommends immediate IPv6 adoption.

Business incentives: with the emergence of new digital technologies, such as 5G, IOT and Cloud, new use cases have come into being and posed more new requirements for IPv6 deployment. Over time, numerous technical and economic stop-gap measures have been developed in an attempt to extend the lifetime of IPv4, but all of these measures add cost and complexity to network infrastructure and raise significant barriers to innovation. It is widely recognized that full transition to IPv6 is the only viable option to ensure future growth and innovation in Internet technology and services. Several large networks and Data Centers have already evolved their internal infrastructures to be IPv6-only. Forward looking large corporations are also working toward migrating their enterprise networks to IPv6-only environments.

Governments incentives: governments have a huge responsibility in promoting IPv6 deployment within their countries. There are example of governments already adopting policies to encourage IPv6 utilization or enforce increased security on IPv4. So, even without funding the IPv6 transition, governments can recommend to add IPv6 compatibility for every connectivity, service or products bid. This will encourage the network operators and vendors who don't want to miss out on government related bids to evolve their infrastructure to be IPv6 capable. Any public incentives for technical evolution will be bonded to IPv6 capabilities of the technology itself.

7. Call for action

There are some areas of improvement, that are often mentioned in the literature and during the discussions on IPv6 deployment. This section lists these topics and wants to start a call for action to encourage more investigations on these aspects.

7.1. Transition choices

From an architectural perspective, a service provider or an enterprise may perceive quite a complex task the transition to IPv6, due to the many technical alternatives available and the changes required in management and operations. Moreover, the choice of the method to support the transition may depend on factors specific to the operator's or the enterprise's context, such as the IPv6 network design that fits the service requirements, the deployment strategy, and the service and network operations.

This section briefly highlights the basic approaches that service providers and enterprises may take. The scope is to raise the discussion whether actions may be taken that allow to overcome the issues highlighted and further push the adoption of IPv6.

7.1.1. Service providers

For a service provider, the IPv6 transition often refers to the service architecture (also referred to as overlay) and not to the network architecture (underlay). IPv6 is introduced at the service layer when a service requiring IPv6-based connectivity is deployed in an IPv4-based network. In this case, as already mentioned in the previous sections, a strategy is based on two stages: IPv6 introduction and IPv6-only.

7.1.2. Enterprises

As described in [RFC7381], enterprises face different challenges than operators. The overall problem for many enterprises is to handle IPv6-based connectivity to the upstream providers, while supporting a mixed IPv4/IPv6 domain in the internal network. The dual stage approach may be still applicable, even if the priorities to apply either stage are different.

7.2. Network Operations

An important factor is represented by the need for training the network operations workforce. Deploying IPv6 requires it as policies and procedures have to be adjusted in order to successfully plan and complete an IPv6 migration. Staff has to be aware of the best

practices for managing IPv4 and IPv6 assets. In addition to network nodes, network management applications and equipment need to be properly configured and in same cases also replaced. This may introduce more complexity and costs for the migration.

7.3. Performance

Despite their relative differences, people tend to compare the performance of IPv6 versus IPv4. In some cases, IPv6 behaving "worse" than IPv4 tends to re-enforce the justification of not moving towards the full adoption of IPv6. This position is supported when looking at available analytics on two critical parameters: packet loss and latency. These parameters have been constantly monitored over time, but only a few extensive researches and measurement campaigns are currently providing up-to-date information. This paragraph will look briefly at both of them, considering the available measurements. Operators are invited to bring in their experience and enrich the information reported below.

7.3.1. IPv6 latency

[APNIC3] constantly compares the latency of both address families. Currently, the worldwide average is still in favor of IPv4. Zooming at the country or even at the operator level, it is possible to get more detailed information and appreciate that cases exist where IPv6 is faster than IPv4. [APRICOT] highlights how when a difference in performance exists it is often related to asymmetric routing issues. Other possible explanations for a relative latency difference lays on the specificity of the IPv6 header which allows packet fragmentation. In turn, this means that hardware needs to spend cycles to analyze all of the header sections and when it is not capable of handling one of them it drops the packet. Even considering this, a difference in latency stands and sometimes it is perceived as a limiting factor for IPv6. A few measurement campaigns on the behavior of IPv6 in Content Delivery Networks (CDN) are also available [MAPRG-IETF99], [INFOCOM]. The TCP connect time is still higher for IPv6 in both cases, even if the gap has reduced over the analysis time window.

7.3.2. IPv6 packet loss

[APNIC3] also provides the failure rate of IPv6. Two reports, namely [RIPE1] and [APRICOT], discussed the associated trend, showing how the average worldwide failure rate of IPv6 worsened from around 1.5% in 2016 to a value exceeding 2% in 2020. Reasons for this effect may be found in endpoints with an unreachable IPv6 address, routing instability or firewall behaviours. Yet, this worsening effect may appeae as disturbing for a plain transition to IPv6. Operators are

once again invited to share their experience and discuss the performance of IPv6 in their network scenarios.

7.4. IPv6 security

IPv6 presents a number of exciting possibilities for the expanding global Internet, however, there are also noted security challenges associated with the transition to IPv6. [I-D.ietf-opsec-v6] analyzes the operational security issues in several places of a network (enterprises, service providers and residential users).

The security aspects have to be considered to keep the same level of security as it exists nowadays in an IPv4-only network environment. The autoconfiguration features of IPv6 will require some more attention for the things going on at the network level. Router discovery and address autoconfiguration may produce unexpected results and security holes. The IPsec protocol implementation has initially been set as mandatory in every node of the network, but then relaxed to recommendation due to extremely constrained hardware deployed in some devices e.g., sensors, Internet of Things (IoT).

There are some concerns in terms of the security but, on the other hand, IPv6 offers increased efficiency. There are measurable benefits to IPv6 to notice, like more transparency, improved mobility, and also end to end security (if implemented).

As reported in [ISOC], comparing IPv6 and IPv4 at the protocol level, one may probably conclude that the increased complexity of IPv6 results in an increased number of attack vectors, that imply more possible ways to perform different types attacks. However, a more interesting and practical question is how IPv6 deployments compare to IPv4 deployments in terms of security. In that sense, there are a number of aspects to consider.

Most security vulnerabilities related to network protocols are based on implementation flaws. Typically, security researchers find vulnerabilities in protocol implementations, which eventually are "patched" to mitigate such vulnerabilities. Over time, this process of finding and patching vulnerabilities results in more robust implementations. For obvious reasons, the IPv4 protocols have benefited from the work of security researchers for much longer, and thus IPv4 implementations are generally more robust than IPv6.

Besides the intrinsic properties of the protocols, the security level of the resulting deployments is closely related to the level of expertise of network and security engineers. In that sense, there is obviously much more experience and confidence with deploying and

operating IPv4 networks than with deploying and operating IPv6 networks.

Finally, implementation of IPv6 security controls obviously depends on the availability of features in security devices and tools. Whilst there have been improvements in this area, there is a lack of parity in terms of features and/or performance when considering IPv4 and IPv6 support in security devices and tools.

7.4.1. Protocols security issues

It is important to say that IPv6 is not more or less secure than IPv4 and the knowledge of the protocol is the best security measure.

In general there are security concerns related to IPv6 that can be classified as follows:

- Basic IPv6 protocol (Basic header, Extension Headers, Addressing)
- IPv6 associated protocols (ICMPv6, NDP, MLD, DNS, DHCPv6)
- Internet-wide IPv6 security (Filtering, DDoS, Transition Mechanisms)

ICMPv6 is an integral part of IPv6 and performs error reporting and diagnostic functions. Since it is used in many IPv6 related protocols, ICMPv6 packet with multicast address should be filtered carefully to avoid attacks. Neighbor Discovery Protocol (NDP) is a node discovery protocol in IPv6 which replaces and enhances functions of ARP. Multicast Listener Discovery (MLD) is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like Internet Group Management Protocol (IGMP) is used in IPv4.

These IPv6 associated protocols like ICMPv6, NDP and MLD are something new compared to IPv4, so they adds new security threats and the related solutions are still under discussion today. NDP has vulnerabilities [RFC3756] [RFC6583]. The specification says to use IPsec but it is impractical and not used, on the other hand, SEND (SEcure Neighbour Discovery) [RFC3971] is not widely available.

[RIPE2] describes the most important threats and solutions regarding IPv6 security.

8. Security Considerations

This document has no impact on the security properties of specific IPv6 protocols or transition tools. The security considerations

relating to the protocols and transition tools are described in the relevant documents.

9. Contributors

The following people provided relevant contributions to this document:

TBC

10. Acknowledgements

TBC

11. IANA Considerations

This document has no actions for IANA.

12. References

12.1. 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>.

12.2. Informative References

[AKAMAI] AKAMAI, "IPv6 Adoption Visualization", 2020, <https://www.akamai.com/uk/en/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp>.

[APNIC1] APNIC, "IPv6 Capable Rate by country (%)", 2020, <https://stats.labs.apnic.net/ipv6>.

[APNIC2] APNIC2, "Addressing 2019", 2020, <https://labs.apnic.net/?p=1288>.

[APNIC3] APNIC, "Average RTT Difference (ms) (V6 - V4) for World (XA)", 2020, <https://stats.labs.apnic.net/v6perf/XA>.

[APRICOT] Huston, G., "Average RTT Difference (ms) (V6 - V4) for World (XA)", 2020, <https://2020.apricot.net/assets/files/APAE432/ipv6-performance-measurement.pdf>.

[ETSI-IP6-WhitePaper]
ETSI, "ETSI White Paper No. 35: IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward", ISBN 979-10-92620-31-1, 2020.

[FACEBOOK]
FACEBOOK, "IPv6", 2020, <https://www.facebook.com/ipv6>.

[GOOGLE] GOOGLE, "IPv6 Adoption", 2020, <https://www.google.com/intl/en/ipv6/statistics.html>.

[I-D.ietf-opsec-v6]
Vyncke, E., Kk, C., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", draft-ietf-opsec-v6-21 (work in progress), November 2019.

[I-D.lmhp-v6ops-transition-comparison]
Lencse, G., Martinez, J., Howard, L., Patterson, R., and I. Farrer, "Pros and Cons of IPv6 Transition Technologies for IPv4aaS", draft-lmhp-v6ops-transition-comparison-05 (work in progress), July 2020.

[INFOCOM] Doan, T., "A Longitudinal View of Netflix: Content Delivery over IPv6 and Content Cache Deployments", 2020, <https://dl.acm.org/doi/abs/10.1109/INFOCOM41043.2020.9155367>.

[ISOC] Internet Society, "IPv6 Security FAQ", 2019, <https://www.internetsociety.org/wp-content/uploads/2019/02/Deploy360-IPv6-Security-FAQ.pdf>.

[MAPRG-IETF99]
Bajpai, V., "Measuring YouTube Content Delivery over IPv6", 2017, <https://www.ietf.org/proceedings/99/slides/slides-99-maprg-measuring-youtube-content-delivery-over-ipv6-00.pdf>.

[POTAROO] POTAROO, "IPv6 / IPv4 Comparative Statistics", 2020, <https://bgp.potaroo.net/v6/v6rpt.html>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, DOI 10.17487/RFC3756, May 2004, <https://www.rfc-editor.org/info/rfc3756>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[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>.

[RFC6036] Carpenter, B. and S. Jiang, "Emerging Service Provider Scenarios for IPv6 Deployment", RFC 6036, DOI 10.17487/RFC6036, October 2010, <https://www.rfc-editor.org/info/rfc6036>.

[RFC6180] Arkko, J. and F. Baker, "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", RFC 6180, DOI 10.17487/RFC6180, May 2011, <https://www.rfc-editor.org/info/rfc6180>.

[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>.

[RFC6540] George, W., Donley, C., Liljenstolpe, C., and L. Howard, "IPv6 Support Required for All IP-Capable Nodes", BCP 177, RFC 6540, DOI 10.17487/RFC6540, April 2012, <https://www.rfc-editor.org/info/rfc6540>.

[RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, DOI 10.17487/RFC6583, March 2012, <https://www.rfc-editor.org/info/rfc6583>.

[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>.

[RFC6883] Carpenter, B. and S. Jiang, "IPv6 Guidance for Internet Content Providers and Application Service Providers", RFC 6883, DOI 10.17487/RFC6883, March 2013, <https://www.rfc-editor.org/info/rfc6883>.

[RFC7381] Chittimaneni, K., Chown, T., Howard, L., Kuarsingh, V., Pouffary, Y., and E. Vyncke, "Enterprise IPv6 Deployment Guidelines", RFC 7381, DOI 10.17487/RFC7381, October 2014, <https://www.rfc-editor.org/info/rfc7381>.

[RIPE1] Huston, G., "Measuring IPv6 Performance", 2016, <https://ripe73.ripe.net/wp-content/uploads/presentations/35-2016-10-24-v6-performance.pdf>.

[RIPE2] RIPE, "IPv6 Security", 2019, <https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf>.

[W3TECHS] W3TECHS, "Historical yearly trends in the usage statistics of site elements for websites", 2020, <https://w3techs.com/technologies/history_overview/site_element/all/y>.

Appendix A. Summary of Questionnaire and Replies

This Appendix summarizes the questionnaire and the replies received.

1. Do you have plan to move more fixed or mobile or enterprise users to IPv6 in the next 2 years?

a. If yes, fixed, or mobile, or enterprise?

b. What're the reasons to do so?

c. When to start: already on going, in 12 months, after 12 months?

d. Which transition solution will you use, Dual-Stack, DS-Lite, 464XLAT, MAP-T/E?

2. Do you need to change network devices for the above goal?

a. If yes, what kind of devices: CPE, or BNG/mobile core, or NAT?

b. Will you migrate your metro or backbone or backhaul network to support IPv6?

Some answers below:

Answer 1: (1) Yes, IPv6 migration strategy relies upon the deployment of Dual Stack architecture. IPv4 service continuity designs is based on DS-Lite for fixed environments and 464XLAT for mobile environments. No plans to move towards MAP-E or MAP-T solutions for the time being. (2) Yes, it's a matter of upgrading CPE, routers (including BNGs), etc. Tunneling options (ISATAP, TEREDO, 6rd) will also be used for migration.

Answer 2: (1) Yes, at this moment we widely use IPv6 for mobile services while we are using DS-Lite for fixed services (FTTH and DSL). (2) We have no pressure to migrate to native IPv6 forwarding in the short term and it would represent a significant work without clear immediate benefit or business rationale. However we may see a future benefit with SRv6 which may justify in the long term a migration to native IPv6.

Answer 3: (1) Yes, fixed. The IP depletion topic is crucial, so we need to speed up the DS-Lite deployment and also Carrier Grade Nat introduction. (2) Yes, CGNAT introduction.

Answer 4: (1) No, we are rolling IPv6 users back to IPv4. DS-Lite. (2) No, it was already done. IPv6 works worse than IPv4. it is immature.

Answer 5: (1) Yes, all 3. Target is Dual-stack for fixed, mobile and enterprise. (2) Yes, we are adding specific services cards inside our FTTH equipment for dealing with CGNAT. Metro and backbone are already Dual Stack.

Answer 6: (1) Yes, Enterprises customer demand is high and the transition is on going through Dual-Stack. (2) No big plan for transport network.

Answer 7: No such requirements

Answer 8: (1) Yes, mobile. The Internet APN is not yet enabled for IPv6, this will be done soon. 464XLAT will be used to save on RFC1918 address space. (2) Yes, PGW; Metro is already IPv6 and Backbone is currently IPv4/MPLS. No native IPv6 planned as for now.

Answer 9: (1) Yes, Dual-Stack for all 3. Not all services are available on IPv6. IPv6 adoption has been stated from many years but still not finished. Dual-Stack is used. (2) No, at the moment it is 6PE solution. No plan to migrate on native IPv6.

Answer 10: (1) Yes, all 3. Ongoing transition with Dual-stack and 464XLAT. (2) No plan for Metro and Backbone.

Answer 11: No such requirements.

Answer 12: (1) Yes, mobile and fixed. To mitigate IPv4 exhaustion in 12 months, Dual-Stack is used. (2) No (hopefully). Managed by software upgrade.

Answer 13: (1) Yes, on Mobile and Fixed. Mobile: IPv4 exhaustion for the RAN transport and IPv6 roll out ongoing. Fixed: Enterprises are requesting IPv6 and also competitors are offering it. Mobile: dual stack and 6VPE; Enterprise: Dual Stack and 6VPE. (2) No, maybe only a software upgrade.

Answer 14: (1) Yes, fixed. IPv4 address depletion, on going, Dual-Stack with NAT444. (2) No.

Answer 15: (1) Yes, Mobile. Running out of private IPv4 address space and do not want to overlap addresses. Transition on going through 464XLAT. (2) Not yet, this is not the most pressing concern at the moment but it is planned.

Answer 16: No, already on Dual-Stack for many years. Discussing IPv6-only.

Answer 17: (1) Yes, all 3, strategy on going, Dual-Stack, MAP-T. (2) Yes, CPE, BR Dual-Stack.

Answer 18: (1) Yes, Mobile, due to address deficit. It would be very likely 464XLAT. (2) It is not clear at the moment. Still under investigation. CPE, Mobile Core, NAT. For IPv6 native support no plans for today.

Answer 19: No. Difficult to do it for enterprises, and don't really care for residential customers.

Answer 20: (1) Yes, fixed, mobile. IP space depletion. Mobile and Backbone are already done, Fixed is becoming Dual-Stack. (2) Yes, ordinary CPE and small routers. Some of them needs just software upgrade. Backbone done, no plan for metro and backhaul.

Answer 21: No such requirements

Answer 22: (1) Yes, mobile, we have few enterprise requests for IPv6; fixed already Dual-Stack. We are in the exhaustion point in public IPv4 usage in mobile so we need to move to IPv6 in the terminals. Dual-Stack deployment is ongoing. (2) No, all devices already support dual-stack mode. No migration needed. We already support IPv6 forwarding in our backbone.

Answer 23: No, already Dual-Stack

Answer 24: (1) Yes, fixed. DS-Lite. (2) Yes, BNG supporting CGNAT.

Answer 25: (1) Yes, fixed. DS-Lite will be deployed. (2) Yes.

Answer 26: (1) Yes, Mobile (Fixed already Dual-Stack). IPv4 depletion and Business customers are asking for it. Dual-Stack will be deployed. (2) No.

Answer 27: (1) Yes, Mobile. Dual-Stack is on going. (2) Yes, MBH, mobile core.

Answer 28: No such requirements.

Answer 29: (1) Yes, fixed and mobile, enterprise is not certain. IPv4 addressing is not enough, fixed and mobile should be started in 12 months. (2) Telco Cloud, BNG and PEs already support IPv6.

Answer 30: (1) Yes, all 3. Government has pushed. Dual-Stack for FBB in 12 months. (2) Yes, RGs have not good readiness, but not much could be done about it. PPPoE access does not create problem in access and aggregation. BNG should only change configuration.

Answer 31: (1) Yes, mobile for 5G sites. Plan to use IPv6 soon. 6VPE in the beginning, then migrate to Dual-stack. (2) IP BH devices already support IPv6.

Answer 32: No.

Answer 33: Yes, Enterprises. We are running short of IPV4 addresses. In our Internet Core IPV4/IPV6 Dual Stack was already introduced. The rollout of IPV6 services is slow and we started with business services. From customer perspective Dual Stack is still a "must have" and this will be true for many years to come. Another thought is related to regulatory obligations. Anyway a total switch from IPv4 to IPv6 will not be possible for many more years.

Answer 34: No, we have no plans to introduce new wave of IPv6 in our network.

Answer 35: (1) Yes. Fixed, Enterprise. IPv4 addressing is not enough. Dual Stack deployment is ongoing. (2) Yes, CPE for metro and backbone.

Answer 36: (1) Yes, Fixed, Enterprise. Dual-Stack. (2) Yes, CPE for IPv6 service delivery support.

Answer 37: Yes, mobile and enterprise. 6PE is deployed on the PEs, and dual-stack. The PE supports IPv6 by modifying the live network configuration or upgrading the software.

Answer 38: Yes, both home broadband and enterprise services support IPv6. IPv6 services are basic capabilities of communication networks. Currently 6RD, dual stack (native IPv6) in the future. The dual-stack feature does not require device changes. The home gateway is connected to the switch and the BNG. The Dual Stack can be supported through configuration changes. Both the metro and backbone networks use MPLS to provide bearer services and do not require IPv6 capabilities. IPv6 is not enabled on both the metro and backbone networks. IPv6 services are implemented through 6VPE.

Answer 39: (1) Yes, Enterprises B2B needs more IP addresses. Dual-Stack is already on going. (2) No, BNG/mobile core and NAT. Metro and Backbone already support today.

Answer 40: Not for now.

Authors' Addresses

Giuseppe Fioccola
Huawei Technologies
Riesstrasse, 25
Munich 80992
Germany

Email: giuseppe.fioccola@huawei.com

Paolo Volpato
Huawei Technologies
Via Lorenteggio, 240
Milan 20147
Italy

Email: paolo.volpato@huawei.com