

V60PS
Internet-Draft
Intended status: Informational
Expires: September 8, 2022

G. Fioccola
P. Volpato
Huawei Technologies
N. Elkins
Inside Products
J. Palet Martinez
The IPv6 Company
G. Mishra
Verizon Inc.
C. Xie
China Telecom
March 7, 2022

IPv6 Deployment Status
draft-ietf-v6ops-ipv6-deployment-05

Abstract

This document provides an overview of IPv6 deployment status and a view on how the transition to IPv6 is progressing among network operators and enterprises. It also aims to analyze the related challenges and therefore encourage actions and more investigations in those areas where the industry has not taken a clear and unified approach.

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 September 8, 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

March 2022

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	IPv4 vs IPv6: The Global Picture	5
2.1.	IPv4 Address Exhaustion	5
2.2.	IPv6 Users	6
2.3.	IPv6 Web Content	7
2.4.	IPv4 addresses per capita and IPv6 status	7
3.	A Survey on IPv6 Deployments	10
3.1.	IPv6 Allocations and Networks	10
3.2.	IPv6 among Network Operators	12
3.3.	IPv6 among Enterprises	14
3.3.1.	Government and Universities	15
3.4.	Observations on Industrial Internet	17
3.5.	Observations on Content and Cloud Service Providers	17
3.6.	Application Transition	18
4.	Towards an IPv6 Overlay Service Design	18
4.1.	IPv6 introduction	19
4.2.	IPv6-only Service Delivery	20
5.	IPv6-only Underlay Network Deployment	21
6.	IPv6 Benefits	23
7.	Common IPv6 Challenges	25
7.1.	Transition Choices	25
7.1.1.	Service Providers	25
7.1.2.	Enterprises and Industrial Internet	26
7.1.3.	Cloud and Data Centers	27
7.1.4.	CEs and user devices	28
7.2.	Government and Regulators	28
7.3.	Network Management and Operations	29
7.4.	Performance	29
7.4.1.	IPv6 packet loss and latency	30
7.4.2.	Customer Experience	30
7.5.	IPv6 security	31

7.5.1.	Protocols security issues	32
7.5.2.	IPv6 Extension Headers and Fragmentation	33
8.	Security Considerations	33
9.	Contributors	34
10.	Acknowledgements	34

11.	IANA Considerations	34
12.	References	34
12.1.	Normative References	34
12.2.	Informative References	36
Appendix A.	Summary of Questionnaire and Replies for network operators	42
Appendix B.	Summary of Questionnaire and Replies for enterprises	44
Authors' Addresses	45

[1.](#) Introduction

[RFC6036] described IPv6 deployment scenarios adopted or foreseen by a number of Internet Service Providers (ISPs) who responded to a technical questionnaire in early 2010. In doing that, [\[RFC6036\]](#) provided practices and plans expected to take place in the following years. Since the publication of [\[RFC6036\]](#), several other documents contributed to discuss the transition to IPv6 in operational environments. To name a few:

- [\[RFC6180\]](#) discussed IPv6 deployment models and transition mechanisms, recommending those that showed to be effective in operational networks.
- [\[RFC6883\]](#) provided guidance and suggestions for Internet content providers and Application Service Providers (ASPs).
- [\[RFC7381\]](#) introduced the guidelines of IPv6 deployment for enterprises.

It is worth mentioning here also [\[RFC6540\]](#) that not only recommended the support of IPv6 to all IP-capable nodes, but it was referenced in the IAB Statement on IPv6 [\[IAB\]](#), which represented a major step in driving the IETF as well as other Standard Developing Organizations (SDOs) to assume the use of IPv6 in their works.

In more recent times, organizations such as ETSI provided more

contributions to the use of IPv6 in operational environments, targeting IPv6 in different industry segments. As a result, [\[ETSI-IP6-WhitePaper\]](#), was published to provide an updated view on the IPv6 best practices adopted so far, in particular in the ISPs domain.

Considering all of the above, and after more than ten years since the publication of [\[RFC6036\]](#) it may be interesting to verify where the transition of the Internet to IPv6 currently stands, what major steps have been accomplished and what is still missing. Some reasons justify such questions:

- In some areas, the lack of publicly available IPv4 addresses forced both carriers and content providers to shift to IPv6 to support the introduction of new applications, in particular in wireless networks.
- Some governmental actions took place to encourage or even enforce, at different degrees, the adoption of IPv6 in certain countries.
- Looking at the global adoption of IPv6, this seems to have reached a threshold that justifies speaking of native, end-to-end IPv6 connectivity (between a user's device and a content on a site) at the IPv6 service layer.

This document intends to explode such statements, providing a survey of the status of IPv6 deployment and highlighting both the achievements and remaining obstacles in the transition to IPv6-only networks. The target is to give an updated view of the practices and plans already described in [\[RFC6036\]](#), to encourage further actions and more investigations in those areas that are still under discussion, and to present the main incentives for the adoption of IPv6. The expectation is that this process may help to understand what is missing and how to improve the current IPv6 deployment strategies of network operators, enterprises, content and cloud service providers.

The initial section of this document reports some data about the status of IPv6. The exhaustion of IPv4 as well as the measured adoption of IPv6 at the users' and the content's side will be

discussed. Comparing both IPv4 and IPv6, this latter has a higher growth rate. While this fact alone does not permit to conclude that the definitive transition to IPv6 is undergoing, at least testifies that a portion of the ICT industry has decided to invest and deploy IPv6 at large.

The next section provides a survey of IPv6 deployments in different environments, including ISPs, enterprises, cloud providers and universities. Data from some well-known analytics will be discussed. In addition, two independent polls among network operators and enterprises will also be presented.

Then, a section on IPv6 overlay service design will describe the IPv6 transition approaches for Mobile BroadBand (MBB), Fixed BroadBand (FBB) and Enterprise services. At present, Dual-Stack (DS) is the most deployed solution for IPv6 introduction, while 4G/LTE and Dual-Stack Lite (DS-Lite) seem the preferred ones for those players that have already enabled IPv6-only service delivery. A section on IPv6

underlay network deployment will also focus on the common approaches for the transport network.

The last parts of the document will analyze the incentives brought by IPv6 as well as the general challenges to be faced to move forward in the transition. Specific attention will be given to operational, performance and security issues. All these considerations will be input for the final section of the document that aims to highlight the areas still requiring improvement and some actions that the industry might consider to favor the adoption of IPv6.

[2.](#) IPv4 vs IPv6: The Global Picture

This section deals with some key questions related to IPv6, namely the status of IPv4 exhaustion, often considered as one of the triggers to switch to IPv6, the number of IPv6 end users, a primary measure to sense IPv6 adoption, and the percentage of websites reachable over IPv6. The former is constantly measured by the Regional Internet Registries (RIRs) and the next subsection provides an indication of where we currently stand. The utilization of IPv6 at both the end user's side and the content's side has also been monitored by several institutions worldwide as these two parameters

provide a first-order indication on the real adoption of IPv6.

[2.1.](#) IPv4 Address Exhaustion

According to [\[CAIR\]](#) there will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018. This poses the question on whether the IPv4 address space can sustain such a number of allocations and, consequently, if this is affecting the process of its exhaustion. The answer is not straightforward as many aspects have to be considered.

On one hand, the RIRs are reporting scarcity of available and still reserved addresses. Table 3 of [\[POTAR001\]](#) shows that the available pool of the five RIRs counts 5.2 million IPv4 addresses, while the reserved pool includes another 12 million, for a total of "usable" addresses equal to 17.3 million (-5.5% year over year, comparing 2021 against 2020). The same reference, in table 1, shows that the total IPv4 allocated pool equals to 3.685 billion addresses (+0.027% year over year). The ratio between the "usable" addresses and the total allocated brings to 0.469% of remaining space (from 0.474% at the end of 2020).

On the other, [\[POTAR001\]](#) again highlights the role of both NAT and the address transfer to counter the IPv4 exhaustion. NAT systems well fit in the current client/server model used by most of the available Internet applications, with this phenomenon amplified by

the general shift to cloud. Anyway, it should be noted that, in some cases, private address space cannot provide adequate address and the reuse of addresses may make the network even more complex. The transfer of IPv4 addresses also contributes to mitigate the need of addresses. As an example, [\[IGP-GT\]](#) and [\[NRO\]](#) show the amount of transfers to recipient organizations in the different regions. Cloud Service Providers (CSPs) appear to be the most active in buying available addresses to satisfy their need of providing IPv4 connectivity to their tenants. But, since each address blocks of Internet is licensed by a specific resource-holder and stored for the verification of the authenticity, frequent address transfer may affect the global assignment process.

[2.2.](#) IPv6 Users

The count of the IPv6 users is the key parameter to get an immediate understanding of the adoption of IPv6. Some organizations constantly track the usage of IPv6 by aggregating data from several sources. As an example, the Internet Society constantly monitors the volume of IPv6 traffic for the networks that joined the WorldIPv6Launch initiative [[WIPv6L](#)]. The measurement aggregates statistics from organizations such as [[Akm-stats](#)] that provides data down to the single network level measuring the number of hits to their content delivery platform. For the scope of this document, we follow the approach used by APNIC to quantify the adoption of IPv6 by means of a script that runs on a user's device [[CAIDA](#)]. To give a rough estimation of the relative growth of IPv6, the next table aggregates the total number of estimated IPv6-capable users at January 2022, and compares it against the total Internet users, as measured by [[POTAR002](#)].

	Jan 2018	Jan 2019	Jan 2020	Jan 2021	Jan 2022	CAGR
IPv6	513.07	574.02	989.25	1,136.28	1,207.61	23.9%
World	3,410.27	3,470.36	4,065.00	4,091.62	4,093.69	4.7%
Ratio	15.0%	16.5%	24.3%	27.8%	29.5%	18.4%

Figure 1: IPv6-capable users against total (in millions)

Two figures appear: first, the IPv6 Internet population is growing with a two-digits Compound Annual Growth Rate (CAGR), and second, the ratio IPv6 over total is also growing steadily.

[2.3.](#) IPv6 Web Content

[W3Tech] keeps track of the use of several technical components of websites. The utilization of IPv6 for websites is shown in the next table.

+-----+-----+-----+-----+-----+-----+-----+

Worldwide Websites	Jan 2018	Jan 2019	Jan 2020	Jan 2021	Jan 2022	CAGR
% of IPv6	11.4%	13.3%	15.0%	17.5%	20.6%	15.9%

Figure 2: Usage of IPv6 in websites

Looking at the growth rate, it may appear not particularly high. It has to be noted, though, that not all websites are equal. The largest content providers, which already support IPv6, generate a lot more IPv6-based content than small websites. [Csc6lab] measured at the beginning of January 2022 that out of the world top 500 sites ranked by [Alx], 203 are IPv6-enabled (+3.6% from January 2021 to January 2022). If we consider that the big content providers (such as Google, Facebook, Netflix) generate more than 50% of the total mobile traffic [SNDVN], and in some cases even more up to 65% ([ISOC1] [HxBld]), the percentage of content accessible over IPv6 is clearly more relevant than the number of enabled IPv6 websites.

Related to that, a question that sometimes arises is whether the content stored by content providers would be all accessible on IPv6 in the hypothetical case of a sudden IPv4 switch-off. Even if this is pure speculation, the numbers above may bring to state that this is likely the case. This would reinforce the common thought that, in quantitative terms, most of content is accessible via IPv6.

2.4. IPv4 addresses per capita and IPv6 status

The IPv4 addresses per capita ratio measures the quantity of IPv4 addresses allocated to a given country divided by the population of that country. It is a theoretical ratio, anyhow it provides an indication of the imbalanced distribution of the IPv4 addresses worldwide. It clearly derives from the allocation of addresses made in the early days of the Internet by the most advanced countries.

The sources for measuring the IPv4 addresses per capita ratio are the allocations done by the RIRs and the statistics about the world population. In our case, we take the distribution files of [POTAR002], which summarize the most useful information. We then

compare the obtained ratio against the measured adoption of IPv6. As

explained in [section 2.2](#), this is expressed as the number of IPv6 capable users over the total Internet population of the considered country. The result is shown in the following table, where some of countries with the highest number of IPv4 allocations are reported. The table is ordered based on the IPv4 addresses per capita ratio.

Country	IPv4 per capita	IPv6 deployment
United States of America	4.89	47.1%
Sweden	2.97	11.8%
Netherlands	2.93	35.5%
Switzerland	2.75	34.9%
Republic of Korea	2.19	17.1%
Australia	1.91	28.8%
Canada	1.85	32.4%
United Kingdom	1.65	33.2%
Belgium	1.62	62.0%
Japan	1.50	36.7%
Germany	1.48	53.0%
France	1.27	42.1%
Austria	1.24	29.2%
Italy	0.91	4.7%
Spain	0.69	3.0%
Poland	0.55	14.7%
Brazil	0.41	38.7%
Russian Federation	0.31	9.7%
China (*)	0.24	60.1%
India	0.03	76.9%

Figure 3: IPv4 per capita and IPv6 deployment

Internet-Draft

March 2022

(*) The IPv6 deployment information in China is derived from [\[CN-IPv6\]](#).

It is clear that a direct correlation between the two measures is not always straightforward. One may expect that a low IPv4 addresses per capita ratio should correspond to high IPv6 deployment. This is true for India and, relatively, for Brazil, but other countries such as the Russian Federation, Poland, Spain and Italy are still quite dependent on IPv4.

The opposite effect should apply for countries with a high value for same ratio. While this is true for Sweden and the Republic of Korea, which have a relatively low IPv6 deployment, for other countries at the top of the list this does not apply. The USA, Germany, France, Belgium all have a good level of IPv6 deployment, while other countries such the Netherlands, Switzerland, the UK, Canada, Australia, Japan are just following with around one third of their Internet population using IPv6.

The reasons for having high or medium-to-high IPv6 deployment may be quite different from country to country. For example, in West European countries such as Belgium, France, Germany the outcome depends on a mix of government and regulation activities which incentivized the adoption of IPv6 in the recent years. In some cases it has been industry self-regulation which created the traction for a bigger IPv6 adoption.

The IPv6 adoption in USA, China and India comes from different needs. Mobile operators have anticipated the usage of IPv6 to cope with the lack of available addresses (India) and to support new services and applications. In addition to that, all National governments have issued specific policies to bring IPv6 deployment forward.

[3.](#) A Survey on IPv6 Deployments

Right after the count of the IPv6 users, it is fundamental to understand the status of IPv6 in terms of concrete adoption in operational networks. This section deals with the status of IPv6 among carriers, service and content providers, enterprises and

research institutions.

3.1. IPv6 Allocations and Networks

RIRs are responsible for allocating IPv6 address blocks to ISPs, LIRs (Local Internet Registries) as well as enterprises or other organizations. An ISP/LIR will use the allocated block to assign addresses to their end users. For example, a mobile carrier will assign one or several /64 prefixes to the User Equipment (UE).

Fioccola, et al.

Expires September 8, 2022

[Page 10]

Internet-Draft

March 2022

Several analytics are available from the RIRs. Here we are interested to those relevant to IPv6. The next table shows the amount of individual allocations, per RIR, in the time period 2017-2021 [[APNIC2](#)].

Registry	Dec 2017	Dec 2018	Dec 2019	Dec 2020	Dec 2021	Cumulated	CAGR
AFRINIC	112	110	115	109	136	582	51%
APNIC	1,369	1,474	1,484	1,498	1,392	7,217	52%
ARIN	684	659	605	644	671	3,263	48%
LACNIC	1,549	1,448	1,614	1,801	730	7,142	47%
RIPE NCC	2,051	2,620	3,104	1,403	2,542	11,720	55%
Total	5,765	6,311	6,922	5,455	5,471	29,924	51%

Figure 4: IPv6 allocations worldwide

Overall, the trend is positive, witnessing the vivacity around IPv6. The decline of IPv6 allocations in 2020 (remarkable for RIPE NCC) and 2021 (in LACNIC), could be explained with the COVID-19 measures that may have affected the whole industry.

[APNIC2] also compares the number of allocations for both address families. Differently from what happened in 2020, when CAGR was higher for the IPv6 allocations, in 2021 IPv4 stayed a little ahead (53.6% versus 50.9%).

Address family	Dec 2017	Dec 2018	Dec 2019	Dec 2020	Dec 2021	Cumulated	CAGR
IPv6	5,765	6,311	6,922	5,455	5,471	29,924	50.9%
IPv4	8,091	9,707	13,112	6,263	7,829	45,002	53.6%

Figure 5: Allocations per address family

As noted, the pandemic may have influenced the ICT industry including the dynamic of the address allocations. The number of IPv4 allocations in 2021 includes many allocations of small address ranges (e.g. /24) [APNIC2]. On the contrary, a single IPv6 allocation is

large enough to cope with the need of an operators for many years. After an operator receives an IPv6 /30 or /32 allocation it is unlikely that a new request of addresses is repeated in the short term. Hence the two CAGR values in the table should not be compared directly as the weight of the allocations is different.

The next table is based on [APNIC3], [APNIC4] and shows the percentage of Autonomous System (AS) numbers supporting IPv6 compared to the total ASes worldwide. The number of IPv6-capable ASes increased from 24.3% in January 2018 to 38.7% in January 2022. This equals to 18% CAGR for IPv6-enabled networks, highlighting how IPv6 is growing faster than IPv4, since the CAGR value for the total of IPv6 and IPv4 networks grew of just 5%.

Advertised ASN	Jan 2018	Jan 2019	Jan 2020	Jan 2021	Jan 2022	CAGR
IPv6-capable	14,500	16,470	18,650	21,400	28,140	18%
Total ASN	59,700	63,100	66,800	70,400	72,800	5%
Ratio	24.3%	26.1%	27.9%	30.4%	38.7%	

Figure 6: Percentage of IPv6-capable ASes

The tables above provide an aggregated view of the allocations dynamic. Apart from the recent times influenced by the pandemic, the general trend related to IPv6 adoption is positive. What the aggregated view does not tell us is the split between the different types of organizations. The next sections of this chapter will zoom into each specific area to highlight the relative status.

[3.2.](#) IPv6 among Network Operators

Only a few public references describing the status of IPv6 in specific networks are available. An example is the case of Reliance Jio [[RlncJ](#)]. To understand the degree of adoption of IPv6 in the operators' domain, it is necessary to consult the data provided by those organizations that constantly track the usage of IPv6. Among the others, we have the Internet Society that constantly monitors the volume of IPv6 traffic for the networks that joined the WorldIPv6Launch initiative [[WIPv6L](#)] and Akamai [[Akm-stats](#)] that collects statistics both at a country level and at the single operator's network measuring the number of hits to their content delivery platform. In addition to them, the RIRs also provide

detailed information about the prefixes allocated and the ASes associated to each operator. Overall, the vast majority of the operators worldwide have enabled IPv6 and provide IPv6-based services even if the degree of adoption varies quite greatly based on local market demand, regulatory actions, and political decisions (e.g. [[RIPE3](#)] to look at the relative differences across the European market).

As it was proposed at the time of [[RFC6036](#)], also in the case of this document a survey was submitted to a group of service providers in Europe (see [Appendix A](#) for the complete poll), to understand the details about their plans about IPv6 and their technical preferences towards its adoption. Such poll does not pretend to give an exhaustive view on the IPv6 status, but to integrate the available data with some insights that may be relevant to the discussion.

The poll reveals that the majority of the operators interviewed has plans concerning IPv6 (79%). Of them, 60% has already ongoing

activities, while 33% is expected to start activities in a 12-months time-frame. The transition to IPv6 involves all business segments: mobile (63%), fixed (63%), and enterprises (50%).

The reasons to move to IPv6 vary. The majority of the operators that do have a plan for IPv6 perceives issues related to IPv4 depletion and prefer to avoid the use of private addressing schemes (48%) to save the NAT costs. Global IPv4 address depletion and the run out of private address space recommended in [\[RFC1918\]](#) are reported as the important drivers for IPv6 deployment. In some cases, the adoption of IPv6 is driven by innovation strategy (as the enabler of new services, 13%) or is introduced because of 5G/IoT, which play the role of business incentive to IPv6 (20%). In a few cases, respondents highlight the availability of National Regulatory policies requiring to enable IPv6 together with the launch of 5G (13%). Enterprise customers demand is also a reason to introduce IPv6 (13%).

From a technical preference standpoint, Dual-Stack is the most adopted solution, both in wireline (59%) and in cellular networks (39%). In wireline, the second most adopted mechanism is DS-Lite (19%), while in cellular networks the second preference goes to 4G/LTE (21%).

In the majority of the cases, the interviewed operators do not see any need to transition their network as a whole. They consider to touch or to replace only what it is needed. CE (47%), BNG (20%), CGN devices (33%), mobile core (27%) are the components that may be affected by transition or replacement. It is interesting to see that most of the network operators have no major plans to transition the

transport network (metro and backbone) soon, since they do not see business reasons. It seems that there is no pressure to move to native IPv6-only forwarding in the short term, anyway the future benefit of IPv6 may justify the shift in the long term.

More details about the answers received can be found in [Appendix A](#).

[3.3](#). IPv6 among Enterprises

As described in [\[RFC7381\]](#), enterprises face different challenges than operators. Some publicly available statistics also show that the

deployment of IPv6 lags behind other sectors.

[NST_1] provides estimations on deployment status of IPv6 for more than 1000 second level domains such as example.com, example.net or example.org belonging to organizations in the United States. The measurement encompasses many industries, including telecommunications, so that the term "enterprises" is a bit loose to this extent. In any case, it provides a first indication of IPv6 adoption in several US industry sectors. The analysis tries to infer whether IPv6 is supported by looking from "outside" a company's network. It takes into consideration the support of IPv6 to external services such as Domain Name System (DNS), mail and website. Overall, for around the 66.85% of the considered domains there is an active DNS Name Server (NS) v6 record but only 6.3% have IPv6 support for their websites and 21.2% have IPv6-based mail services as of January 2022.

[BGR_1] have similar data for China. The measurement considers 478 second or third level domains such as example.cn or example.com.cn. 74% have IPv6 support for DNS, 0% have IPv6-based mail services, 20% have IPv6-based websites.

[CNLABS_1] provides the status in India. Of the 104 measured domains, 51.9% are IPv6-enabled, 15.4% have IPv6 support in DNS, 16.3% have IPv6 support for the mail service.

A poll submitted to a group of large enterprises in North America (see [Appendix B](#)) show that the operational issues are likely to be more critical than for operators.

Looking at current implementations, almost one third has dual-stacked networks, while 20% declares that portions of their networks are IPv6-only. 35% of the enterprises are stuck at the training phase. In no cases the network is fully IPv6-based.

Speaking of training, the most critical needs are in the field of IPv6 security and IPv6 troubleshooting (both highlighted by the two thirds of respondents), followed by IPv6 fundamentals (57.41%).

Coming to implementation, the three areas of concern are IPv6 security (31.48%), training (27.78%), application conversion (25.93%). Interestingly, 33.33% of respondents think that all three areas are all simultaneously of concern.

The full poll is reported in [Appendix B](#).

[3.3.1](#). Government and Universities

This section focuses specifically on governments and academia, due to the relevance of both domains in the process of IPv6 adoption. The already mentioned organizations that estimates the IPv6 status provide a deep focus on IPv6 in the network domains associated with governmental and education-related agencies.

As far as governmental institutions or agencies are concerned, [\[NST 2\]](#) provides analytics on the degree of support that IPv6 gives to DSN, mail and websites across 1283 second level domains associated with US Federal agencies. These domains are in the form of example.gov or example.fed. The script used by [\[NST 2\]](#) have also been employed to measure the same analytics in other countries. For China [\[BGR 2\]](#) looks at 52 third level domains such as example.gov.cn. [\[CNLABS 2\]](#) provides statistics for 618 Indian government-related domains (ranging from the second to the fifth level). [\[IPv6Forum\]](#) analyzes 19 governmental domains connected to either the European Union or its member States.

Country	Domains analyzed	DNS	Mail	Website
China	52	0.0%	0.0%	98.1%
European Union (*)	19	47.4%	0.0%	21.1%
India	618	7.6%	6.5%	7.1%
United States of America	1283	87.1%	14.0%	51.7%

Figure 7: IPv6 support for external-facing services across governmental institutions

(*) Both EU and European governments domains are considered.

Looking at the USA, the support given by IPv6 to the services is higher than that in the enterprise sector discussed in the previous section. This is likely to depend on the directions set by [\[US-CIO\]](#) through the mandate to transition to IPv6. In the case of India, the degree of support seems still quite low. This is also true for China, with the notable exception of the percentage of IPv6-enabled government-related organizations websites.

Similar statistics are also available for higher education. [\[NST 3\]](#) measures the data coming from 346 second level domains of universities in the US, such as example.edu. [\[BGR 3\]](#) looks at 111 Chinese education-related domains such as example.edu.cn. [\[CNLABS 3\]](#) analyzes 100 domains in India (mostly third level), while [\[IPv6Forum\]](#) lists 118 universities in the European Union (second level).

Internet-Draft

March 2022

Country	Domains analyzed	DNS	Mail	Website
China	111	36.9%	0.0%	77.5%
European Union	118	83.9%	43.2%	35.6%
India	100	31.0%	54.0%	5.0%
United States of America	346	49.1%	19.4%	21.7%

Figure 8: IPv6 support for external-facing services across universities

Overall, the universities have wider support of IPv6-based services if compared with the other sectors. Apart from a couple of exceptions (e.g. the support of IPv6 mail in China and IPv6 web sites in India), the numbers shown in the table above indicate a good support of IPv6.

[3.4.](#) Observations on Industrial Internet

There are potential advantages for implementing IPv6 for IIoT (Industrial Internet of Things) applications, in particular the large IPv6 address space, the automatic IPv6 configuration and resource discovery.

However, there are still many obstacles that prevent its pervasive use. The key problems identified are the incomplete or immature tool support, the dependency on manual configuration and the poor knowledge of the IPv6 protocols among insiders. To advance and ease the use of IPv6 for smart manufacturing systems and IIoT applications in general, a generic approach to remove these pain points is

therefore, highly desirable.

[3.5.](#) Observations on Content and Cloud Service Providers

Both the number of addresses required to connect all of the virtual and physical elements in a Data Center and the necessity to overcome the limitation posed by [\[RFC1918\]](#) have been the drivers to adopt IPv6 in several CSP networks.

Fioccola, et al.

Expires September 8, 2022

[Page 17]

Internet-Draft

March 2022

Several public references, as reported in [Section 7.1.3](#), discuss how most of the major players find themselves at different stages in the transition to IPv6-only in their Data Center (DC) infrastructure. In some cases, the transition already happened and the DC infrastructure of these hyperscalers is completely based on IPv6. This can be considered a good sign because the end-to-end connectivity between a client (e.g. an application on a smartphone) and a server (a Virtual Machine in a DC) may be based on IPv6.

[3.6.](#) Application Transition

The preliminary step to take full benefit of the IPv6 capabilities is to write or adapt the application software for use in IPv6 networks (see, as an example, [\[ARIN-SW\]](#)).

It is worth mentioning Happy Eyeballs [\[RFC6555\]](#) and Happy Eyeballs 2 [\[RFC8305\]](#) as a major aspect of application transition and porting to IPv6. All host and network router OS's by default prefer IPv6 over IPv4.

Happy Eyeballs plays an important role and is extremely helpful when applications are migrated from IPv4 to IPv6 having a single DNS name with both A and AAAA record. In this way all applications can migrate to IPv6 as IPv6 is preferred over IPv4 and so all IPv6 dual-stacked hosts can communicate using same URL to the server via IPv6 and all IPv4 hosts can as well use the same URL to communicate via IPv4. Eventually when all host endpoints are dual-stacked, the application servers can migrate from dual stack to IPv6-only. For external connectivity to the internet, web proxy can be used providing 6to6 or 4to6 proxy to the internet. This allows application servers on the internal network to change to IPv6-only once all host endpoints are all dual-stacked.

At the current stage, the full support of IPv6 is not yet complete [[Wikipedia](#)], as issues remain in particular for applications known not to work properly behind NAT64.

[4.](#) Towards an IPv6 Overlay Service Design

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

Two approaches are usually considered [[ETSI-IP6-WhitePaper](#)], namely: (1) IPv6 introduction, and (2) IPv6-only. Depending on their specific plans and requirements, operators may consider either of the two or both. The usual approach sees them as two sequential stages, i.e. deal with IPv6 introduction first and then move to IPv6-only. In some cases, operators may instead jump directly to IPv6-only to

avoid the operational burden of a transient phase. IPv6 introduction 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 IPv6-only may occur. In this latter case, the service is delivered solely on IPv6, including the traffic originated from IPv4-based nodes. For this reason, the IPv6-only stage is also called IPv4aaS (IPv4 as a Service).

The consolidated approach foresees to enable IPv6 in the network (sometimes referred to as the underlay) and move progressively to the service layer. Recently, the attention has shifted to enabling IPv6 at the service layer (the overlay) leaving the transition of the network to IPv6 at a later stage. This relates to the increased adoption of the transition mechanisms described in this section.

[4.1.](#) IPv6 introduction

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

- o Enabling Dual-Stack [[RFC4213](#)] at the Customer Edge router (CE)
- o IPv6-in-IPv4 tunneling, e.g. with IPv6 Rapid Deployment (6rd) or Generic Routing Encapsulation (GRE).

Based on information provided by operators with the answers to the poll (Appendix A), Dual-Stack appears to be 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-IPv6-WhitePaper](#)]). Therefore, for operators that are willing to introduce IPv6 the most common approach is to apply the Dual-Stack transition solution, which appears more robust, and easier to troubleshoot and support.

With Dual-Stack, IPv6 can be introduced together with other network upgrades 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 the 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 CE has both IPv4 and IPv6 addresses 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-only hosts to access IPv4 servers. The backbone network underlay can also be IPv4 or IPv6.

Although the Dual-Stack IPv6 transition provides advantages in the IPv6 introductory stage, it does have few disadvantages in the long run, like the duplication of the network resources and states, as well as other limitations for network operation. It also means requiring more IPv4 addresses, so an increase in both Capital Expenses (CAPEX) and Operating Expenses (OPEX). Even if private addresses are being used via Carrier-Grade NAT (CGN), there is extra investment in the CGN devices, logs storage and helpdesk to track CGN-related issues.

For this reason, when IPv4 traffic is vanishingly small or when IPv6 usage increases to more than a given percentage, which highly depends on each network, it could be advantageous to switch to the IPv6-only stage with IPv4aaS. It is difficult to establish the criterion for switching (e.g. to properly identify the upper bound of the IPv4 decrease or the lower bound of the IPv6 increase). In addition to

the technical factors, the switch to IPv6-only may also include a loss of customers. Based on operational experience and some measurements of network operators participating in World IPv6 Launch [[WIPv6L](#)] where, at June 2021, out of 346 entries 108 exceed 50% of IPv6 traffic volume (31.2%), 72 overcome 60% (20.8%), while 37 go beyond 75% (10.7%), the consensus to move to IPv6-only is when IPv6 traffic volume is between 50% and 60%, which easily happens from since the moment IPv6 is deployed in networks where residential customers traffic is higher than business traffic (because major content providers, as already explained, already use IPv6).

[4.2.](#) IPv6-only Service Delivery

The second stage, named IPv6-only and including IPv4 support via IPv4aaS, can be a complex decision that depends on several factors, such as economic aspects, policy and government regulation.

[I-D.ietf-v6ops-transition-comparison] discusses and compares the technical merits of the most common transition solutions for IPv6-only service delivery, 464XLAT [[RFC6877](#)], DS-lite [[RFC6333](#)], Lightweight 4over6 (lw4o6) [[RFC7596](#)], MAP-E [[RFC7597](#)], and MAP-T [[RFC7599](#)], but without providing an explicit recommendation. As the poll highlights [Appendix A](#), the most widely deployed IPv6 transition solution in the MBB domain is 464XLAT while in the FBB space is DS-Lite.

Both of them are IPv6-only solutions providing IPv4aaS. IPv4aaS offers Dual-Stack service to users and allows an operator to run IPv6-only in the network (typically, the access network). It needs

to be observed that an increasing number of operators, also in the FBB area, tend to prefer 464XLAT over the other transition mechanisms, especially in the case of MBB/FBB convergence.

While it cannot be always the case, IPv6-only transition technologies such as 464XLAT require much less IPv4 public addresses [[I-D.ietf-v6ops-transition-comparison](#)], because they make a more efficient usage without restricting the number of ports per subscriber. This contributes to reduce troubleshooting costs and to remove some operational issues related to permanent black-listing of IPv4 address blocks when used via CGN in some services. For example, Sony Play Station Network or OpenDNS imply a higher rotation of IPv4

prefixes in CGN, until they get totally blocked, which means extra CAPEX in new IPv4 transfers.

IPv6-only may be facilitated by the natural upgrade or replacement of CEs because of newer technologies (triple-play, higher bandwidth WAN links, better WiFi technologies, etc.). The CAPEX and OPEX of other parts of the network may be lowered (for example CGN and associated logs) due to the operational simplification of the network.

In terms of addressing needs, for specific applications such as in the case of large mobile operators or large DCs, even the full private address space [[RFC1918](#)] is not large enough. Also, Dual-Stack likely leads to duplication of network resources and operations to support both IPv6 and IPv4, which increases the amount of state information in the network. 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.

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

[5.](#) IPv6-only Underlay Network Deployment

IPv6-only alone can be misinterpreted as not supporting IPv4. It can be referred to different portions of the network, to the underlay network, to the overlay network (services), as also mentioned in [[I-D.palet-v6ops-ipv6-only](#)].

As opposed to the IPv6-only service delivery (with IPv4aaS) discussed in the previous sections, the IPv6-only network means that the whole network (both operator underlay transport and customer traffic overlay) uses IPv6 as the network protocol for all traffic delivery, but some operators may do IPv6-only at the access network only. This can be accomplished on a case-by-case basis.

As a matter of fact, IPv4 reachability must be provided for a long time to come over IPv6 for IPv6-only endpoints. Most operators are leveraging CGN to extend the life of IPv4 instead of going with IPv4aaS.

When operators (both enterprises and service providers) start to migrate from an IPv4 core, MPLS LDPv4 core, SR-MPLSv4 core to introduce IPv6 in the underlay, they do not necessarily need to dual stack the underlay to maintain both IPv4 and IPv6 address families in the transport layer. Forwarding plane complexity on the Provider (P) core should be kept simple as a single protocol only core. An example could be Software Mesh Framework [[RFC5565](#)] which is based on a standard single protocol IPv4-Only or IPv6-Only for core where IPv4 packets can be tunneled over 4to6 MPLS software over an IPv6-Only core.

Hence, when operators decide to migrate to an IPv6 underlay, the Provider (P) core should be IPv4-only or IPv6-only while Dual-Stack is not the best choice. The underlay could be IPv6-only and allows IPv4 packets to be tunneled using VPN over an IPv6-only core and leveraging Advertising IPv4 Network Layer Routing Information (NLRI) with an IPv6 Next Hop [[RFC8950](#)]. Indeed, [[RFC8950](#)] specifies the extensions necessary to allow advertising IPv4 NLRI, Virtual Private Network Unicast (VPN-IPv4) NLRI, Multicast Virtual Private Network (MVPN-IPv4) NLRI with a Next Hop address that belongs to the IPv6 protocol. And also, [[I-D.ietf-bess-ipv6-only-pe-design](#)] allows dual-stacked functionality without having to dual-stack the interface and without any tunneling mechanisms, resulting in OPEX savings for the elimination of IPv4 addressing and BGP peering. This also enables the quick deployment of IPv6 in a core or Data Center network without provisioning IPv6 links with global unicast address, that can be a long process in very large networks.

Regarding the IPv6 underlay network deployment for Access Network (AN) Metro Edge BNG to NG edge, the current trend is to keep MPLS Data Plane IPv4-only and run IPv4/IPv6 Dual Stack to the Access Network (AN) to Customer RG edge node.

As operators do the transition in the future to IPv6 metro and backbone network, e.g. Segment Routing over IPv6 data plane (SRv6), they are able to start the elimination of IPv4 from the underlay transport network while continuing to provide overlay IPv4 services. Basically, as also showed by the poll among network operators, from a network architecture perspective, it is not recommended to apply Dual-Stack to the transport network per reasons mentioned above about the forwarding plane complexities.

If we consider IPv6-only to mean both operator underlay network and customer VPN traffic, that 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.

6. IPv6 Benefits

A comparison of the technical and operational characteristics of IPv4 and IPv6 should quite easily highlight the merits of the latter. On the other hand, the long path IPv6 is still taking to become the dominant network protocol shows that those merits are either not clear enough or not sufficient against other market, managerial or financial reasons. The scope of this section is to list what are generally considered the benefits of IPv6, following discussions at the IETF and other communities. The list below does not mean to be exhaustive; it tries to collect some facts about the use of IPv6.

1. Address space advantage: this is probably the most well-known characteristic of IPv6. The address space is orders of magnitude wider than IPv4's. With the emergence of new digital technologies, such as 5G, IoT and Cloud, new use cases have come into being, posing new requirements to IP networks. 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 to Internet technology and services. Other sections of this paper have already mentioned the efforts of both network and content providers to evolve their internal infrastructures to be IPv6-only to solve the issue of a constrained address space. From an operational perspective, the wide IPv6 address space avoids the typical renumbering activities that take place either when two networks merge or when an infrastructure needs to span across multiple geographic regions.
2. Government and regulation incentives: the shift to IPv6 is beneficial to create the market conditions to foster innovation and competition. This is, as an example, one of conclusions highlighted in [\[ARCEP\]](#): "This dearth of IPv4 addresses means that the internet will not stop working but it will stop growing. This shortage is also resulting in a significant increase in the price being charged for these addresses in the secondary market, which creates a real barrier to entry for new entrants to the internet. It has therefore become imperative, for the sake of competition and innovation, that all internet players switch over to IPv6". Governments have a huge responsibility in promoting

Internet-Draft

March 2022

IPv6 deployment. Some of them are 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 do not want to miss out on government related bids to evolve their infrastructures to be IPv6 capable. Any public incentives for technical evolution will be bonded to IPv6 capabilities of the technology itself. In this regard, in the United States, the Office of Management and Budget is calling for an implementation plan to have 80% of the IP-enabled resources on Federal networks be IPv6-only by 2025. If resources cannot be converted, then the Federal agency is required to have a plan to retire them. The Call for Comment is at [\[US-FR\]](#) and [\[US-CIO\]](#). In China, the government launched IPv6 action plan in 2017, which requires that networks, applications and terminal devices will fully support the adoption of IPv6 by the end of 2025 [\[CN\]](#).

3. New functionality and standard: it has been already mentioned the IAB statement [\[IAB\]](#), which asks the IETF, as well as other Standards Developing Organizations (SDOs), 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. [\[RFC6540\]](#) recommends that all networking standards assume the use of IPv6 and be written so they do not require IPv4. In addition, every RIR worldwide strongly recommends immediate IPv6 adoption. This is an incentive to network equipment vendors to endorse IPv6 and view it as the standards-based solution to the IPv4 address shortage. The introduction of new functionality is one of the technical benefit of IPv6 due to the flexible structure of the packet header. The IETF is currently active in defining operational recommendations for the usage of Extension Headers and Options left open by the base standards.
4. Future Proof: IPv6 was designed from scratch to be future-proof, despite some incompatibilities with IPv4. For example, mechanisms to translate back and forth from IPv4 to IPv6 are already in place in mobile networks worldwide. This allows to introduce newer generations of mobile services, as in the case of 5G applications. While exceptions may exist, IPv6 foresees the

absence of NAT along the network path. This allows an operator to remove the technical constraints of handling NAT and the relevant cost. A side effect to that, this approach brings the connectivity model back to the end-to-end client/server paradigm. Worth noting, the vast majority of terminals is IPv6-capable. Content is also greatly available on IPv6. The service

connectivity, from terminal to content, in particular in mobile networks, is reality.

[7.](#) Common IPv6 Challenges

There are some areas of improvement, that are often mentioned in the literature and during the discussions on IPv6 deployment. This section highlights these common IPv6 challenges in order 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 approaches that service providers and enterprises may take and the related challenges.

[7.1.1.](#) Service Providers

For fixed operators, the massive software upgrade of CEs to support Dual-Stack already started in most of service provider networks. On average, looking at the global statistics, the IPv6 traffic percentage is currently between 30% and 40% of IPv6. As highlighted earlier, all major content providers have already implemented Dual-Stack access to their services and most of them have implemented IPv6-only in their Data Centers. This aspect could affect the decision on the IPv6 adoption for an operator, but there are also other aspects like the current IPv4 addressing status, CE costs, CGN

costs and so on.

Fixed Operators with a Dual-Stack architecture, can start defining and apply a new strategy when reaching the limit in terms of number of IPv4 addresses available. This can be done through CGN or with an IPv6-only approach (IPv4aaS).

On the one hand, most of the fixed operators remain attached to a Dual-Stack architecture and have already employed CGN. In this case it is likely that CGN boosts their ability to supply IPv4 connectivity to CEs for more years to come. On the other hand, only few fixed operators have chosen to move to IPv6-only.

For mobile operators, the situation is quite different since, in some cases, mobile operators are already stretching their IPv4 address space since CGN translation levels have been reached and no more IPv4 public pool addresses are available.

Some mobile operators choose to implement Dual-Stack as first and immediate mitigation solution.

Other mobile operators prefer to move to IPv6-only solution (e.g. 464XLAT) since Dual-Stack only mitigates and does not solve completely the IPv4 address scarcity issue.

For both fixed and mobile operators the approach for the transition is not unique and this brings different challenges in relation to the network architecture and related costs. So each operator needs to do own evaluations for the transition based on the specific situation.

[7.1.2.](#) Enterprises and Industrial Internet

At present, the key driver for enterprises relies on upstream service providers. If they run out of IPv4 addresses, it is likely that they start providing native IPv6 and non-native IPv4. So for other networks trying to reach enterprise networks, the IPv6 experience could be better than the transitional IPv4 if the enterprise deploys IPv6 in its public-facing services. IPv6 also shows its advantages in the case of acquisition, indeed when an enterprise merges two networks which use IPv4 private addresses, the address space of the two networks may overlap and this makes the merge difficult. Since

several governments are introducing IPv6 policy, all the enterprises providing consulting service to governments are also required to support IPv6 and to show their technical expertise in the IPv6 arena.

Enterprises are shielded from IPv4 address depletion issues due to Enterprises predominantly using Proxy and Non internet routable private [[RFC1918](#)], thus do not have the business requirement or technical justification to migrate to IPv6. Enterprises need to find a business case and a strong motivation for IPv6 transition to justify additional CAPEX and OPEX. Also, since ICT is not the core business for most of the enterprises, ICT budget is often constrained and cannot expand considerably. However, there are examples of big enterprises that are considering IPv6 to achieve business targets through a more efficient IPv6 network and to introduce newer services which require future-proof IPv6 network architectures.

Enterprises worldwide, in particular small and medium-sized, are quite late to adopt IPv6, especially on internal networks. In most cases, the enterprise engineers and technicians don't know well how IPv6 works and the problem of application porting to IPv6 looks quite

difficult, even if technically is not a big issue. As highlighted in the relevant poll, the technicians may want to get trained but the management do not see a business need for adoption. This creates an unfortunate cycle where misinformation about the complexity of the IPv6 protocol and unreasonable fears about security and manageability combine with the perceived lack of urgent business needs to prevent adoption of IPv6. In 2019 and 2020, there has been a concerted effort by some grass roots non-profits working with ARIN and APNIC to provide training [[ARIN-CG](#)] [[ISIF-ASIA-G](#)].

For enterprises, the challenge is that of "First Mover Disadvantage". Compared to network operators that may feel the need of a network evolution towards IPv6, enterprises typically upgrade to new technologies and architectures, such as IPv6, only if it gains them revenue, and this is evident, at least in the short term.

As the most promising protocol for network applications, IPv6 is frequently mentioned in relation to Internet of Things and Industry 4.0. However, its industrial adoption, in particular in smart manufacturing systems, has been much slower than expected. Indeed, as for enterprises, it is important to provide an easy way to

familiarize system architects and software developers with the IPv6 protocol.

For Industrial Internet and related IIoT applications, it would be desirable to be able to implement a truly distributed system without dependencies to central components. In this regard the distributed IIoT applications can leverage the configuration-less characteristic of IPv6. In addition, it could be interesting to have the ability to use IP based communication and standard application protocols at every point in the production process and further reduce the use of specialized communication systems.

[7.1.3.](#) Cloud and Data Centers

Most CSPs have adopted IPv6 in their internal infrastructure but are also active in gathering IPv4 addresses on the transfer market to serve the current business needs of IPv4 connectivity. As noted in the previous section, most enterprises do not consider the transition to IPv6 as a priority. To this extent, the use of IPv4-based network services by the CSPs will last. Yet, CSPs are struggling to buy IPv4 addresses.

It is interesting to look at how much traffic in a network is going to Caches and Content Delivery Networks (CDNs). The response is expected to be an high percentage, at least higher than 50% in most of the cases. Since all the key Caches and CDNs are IPv6-ready [[Cldflr](#)], [[Akm](#)], [[Ggl](#)], [[Ntflx](#)], [[Amzn](#)], [[Mcrsft](#)], [[Vrzn](#)]. So the

percentage of traffic going to the key Caches/CDNs is a good approximation of the potential IPv6 traffic in a network.

The challenge for CSPs is related to the support of non-native IPv4 since most CSPs provide native IPv6. If, in the next years, the scarcity of IPv4 addresses becomes more evident, it is likely that the cost of buying an IPv4 address by a CSP could be charged to their customers.

[7.1.4.](#) CEs and user devices

It can be noted that most of the user devices (e.g. smartphones) are already IPv6-enabled since so many years. But there are exceptions, for example, smartTVs and Set-Top Box (STBs) typically had IPv6

support since few years ago, however not all the economies replace them at the same pace.

As already mentioned, ISPs who historically provided public IPv4 addresses to their customers generally still have those IPv4 addresses (unless they chose to transfer them). Some have chosen to put new customers on CGN but without touching existing customers. Because of the extremely small number of customers who notice that IPv4 is done via NAT444, it could be less likely to run out of IPv4 addresses and private IPv4 space. But as IPv4-only devices and traffic reduce, then the need to support private and public IPv4 become less. So the complete support of CEs to IPv6 is also an important challenge and incentive to overcome Dual-Stack towards IPv6-only with IPv4aaS [[ANSI](#)].

[7.2.](#) Government and Regulators

The global picture shows that the deployment of IPv6 worldwide is not uniform at all [[G_stats](#)], [[APNIC1](#)]. Countries where either market conditions or local regulators have stimulated the adoption of IPv6 show clear sign of growth.

As an example, zooming into the European Union area, countries such as Belgium, France and Germany are well ahead in terms of IPv6 adoption. The French National Regulator, Arcep, can be considered a good reference of National support to IPv6. [[ARCEP](#)] introduced an obligation for the operators awarded with a license to use 5G frequencies (3.4–3.8GHz) in Metropolitan France to be IPv6 compatible. As stated, "the goal is to ensure that services are interoperable and to remove obstacles to using services that are only available in IPv6, as the number of devices in use continues to soar, and because the RIPE NCC has run out of IPv4 addresses". A slow adoption of IPv6 could prevent new Internet services to widespread or create a barrier to entry for newcomers to the market. "IPv6 can help

to increase competition in the telecom industry, and help to industrialize a country for specific vertical sectors".

A renewed industrial policy might be advocated in other countries and regions to stimulate IPv6 adoption. As an example, in the United States, the Office of Management and Budget is also calling for IPv6 adoption [[US-FR](#)], [[US-CIO](#)]. China is another example of govern

supporting a country-wide adoption.

7.3. Network Management and Operations

There are important IPv6 complementary solutions related to Operations, Administration and Maintenance (OAM) that look not so complete compared to IPv4. Network Management System (NMS) has a central role in the modern networks for both network operators and enterprises and its transition is a fundamental challenge. This is because some IPv6 products are not field-proven as for IPv4 even if traditional protocols (e.g. SNMP, RADIUS) already supports IPv6. In addition, incompatible vendor roadmap for the development of new NMS features affects the confidence of network operators or enterprises. For example, YANG is the configuration language for networking but in the real world the data modeling is still vendor dependent.

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 transition. 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 some cases also replaced. This may introduce more complexity and costs for the transition.

7.4. Performance

People tend to compare the performance of IPv6 versus IPv4 to argue or motivate the IPv6 transition. In some cases, IPv6 behaving "worse" than IPv4 may be used as an argument for avoiding the full adoption of IPv6. However, there are some aspects where IPv6 is filling the gap to IPv4. 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. While performance is undoubtedly an important issue to consider and worth further investigation, reality is that a definitive answer cannot be found on what IP version performs better. Depending on the specific use case and application, IPv6 is better; in others the same applies to IPv4.

[7.4.1.](#) IPv6 packet loss and latency

[APNIC5] provides a measurement of both the failure rate and RTT of IPv6 compared against IPv4. Both measures are based on scripts that employs the three-way handshake of TCP. As such, the measurement of the failure rate does not provide a direct measurement of packet loss (that would need an Internet-wide measurement campaign). Said that, despite IPv4 is still performing better, the difference seems to have decreased in recent years. Two reports, namely [\[RIPE1\]](#) and [\[APRICOT\]](#), discussed the associated trend, showing how the average worldwide failure rate of IPv6 is still a bit worse than IPv4. Reasons for this effect may be found in endpoints with an unreachable IPv6 address, routing instability or firewall behavior. Yet, this worsening effect may appear as disturbing for a plain transition to IPv6.

[APNIC5] also 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. Regions (e.g. Western Europe, Northern America, Southern Asia) and Countries (e.g. US, India, Germany) with an advanced deployment of IPv6 (e.g. >45%) are showing that IPv6 has better performance 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 CDNs are also available [\[MAPRG\]](#), [\[INFOCOM\]](#). The TCP connect time is still higher for IPv6 in both cases, even if the gap has reduced over the analysis time window.

[7.4.2.](#) Customer Experience

It is not totally clear if the Customer Experience is in some way perceived as better when IPv6 is used instead of IPv4. In some cases it has been publicly reported by IPv6 content providers, that users have a better experience when using IPv6-only compared to IPv4 [\[ISOC2\]](#). This could be explained because in the case of an IPv6 user connecting to an application hosted in an IPv6-only Data Centers, the connection is end-to-end, without translations. Instead, when using IPv4 there is a NAT translation either in the CE or in the service provider's network, in addition to IPv4 to IPv6 (and back to IPv4) translation in the IPv6-only content provider Data Center. [\[ISOC2\]](#),

Internet-Draft

March 2022

[FB] provide reasons in favor of IPv6. In other cases, the result seems to be still slightly in favor of IPv4 [[INFOCOM](#)], [[MAPRG](#)], even if the difference between IPv4 and IPv6 tends to vanish over time.

[7.5](#). IPv6 security

Another point that is sometimes considered as a challenge when discussing the transition to IPv6 is related to the Security. [[RFC9099](#)] analyzes the operational security issues in several places of a network (enterprises, service providers and residential users). It is also worth considering the additional security issues brought into existence by the applied IPv6 transition technologies used to implement IPv4aaS, e.g. 464XLAT, DS-Lite. Some hints are in the paper [[ComputSecur](#)].

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. 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 [[ISOC3](#)], 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. However, this is turning also in the other way around, as with more

IPv6 deployment there may be older IPv4 flaws not discovered or even not resolved anymore by vendors.

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.

[7.5.1.](#) 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:

- o Basic IPv6 protocol (Basic header, Extension Headers, Addressing)
- o IPv6 associated protocols (ICMPv6, NDP, MLD, DNS, DHCPv6)
- o 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 add 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.

[7.5.2](#). IPv6 Extension Headers and Fragmentation

IPv6 Extension Headers imply some issues, in particular their flexibility also means an increased complexity, indeed security devices and software must process the full chain of headers while firewalls must be able to filter based on Extension Headers. Additionally, packets with IPv6 Extension Headers may be dropped in the public Internet. Some documents, e.g. [[I-D.hinden-6man-hbh-processing](#)], [[I-D.bonica-6man-ext-hdr-update](#)], [[I-D.peng-v6ops-hbh](#)] analyze and provide guidance regarding the processing procedures of IPv6 Extension Headers.

There are some possible attacks through EHs, for example RH0 can be used for traffic amplification over a remote path and it is deprecated. Other attacks based on Extension Headers are based on IPv6 Header Chains and Fragmentation that could be used to bypass filtering, but to mitigate this effect, Header chain should go only in the first fragment and the use of the IPv6 Fragmentation Header is forbidden in all Neighbor Discovery messages.

Fragment Header is used by IPv6 source node to send a packet bigger than path MTU and the Destination host processes fragment headers. There are several threats related to fragmentation to pay attention to e.g. overlapping fragments (not allowed) resource consumption while waiting for last fragment (to discard), atomic fragments (to be isolated).

A lot of additional functionality has been added to IPv6 primarily by adding Extension Headers and/or using overlay encapsulation. All of these expand the packet size and this could lead to oversized packets that would be dropped on some links. It is important to investigate the potential problems with oversized packets in the first place. Fragmentation must not be done in transit and a better solution needs to be found, e.g. upgrade all links to bigger MTU or follow specific recommendations at the source node.

[[I-D.vasilenko-v6ops-ipv6-oversized-analysis](#)] analyzes available standards for the resolution of oversized packet drops.

[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.

Fioccola, et al.

Expires September 8, 2022

[Page 33]

Internet-Draft

March 2022

[9.](#) Contributors

Sebastien Lourdez
Post Luxembourg
Email: sebastien.lourdez@post.lu

[10.](#) Acknowledgements

The authors of this document would like to thank Brian Carpenter, Fred Baker, Alexandre Petrescu, Barbara Stark, Haisheng Yu(Johnson), Dhruv Dhody, Gabor Lencse, Shuping Peng, Daniel Voyer, Daniel Bernier, Hariharan Ananthakrishnan, Donavan Fritz, Igor Lubashev, Erik Nygren, Eduard Vasilenko and Xipeng Xiao for their comments and review of this document.

[11.](#) IANA Considerations

This document has no actions for IANA.

[12.](#) References

[12.1.](#) Normative References

[I-D.ietf-v6ops-transition-comparison]

Lencse, G., Martinez, J. P., Howard, L., Patterson, R., and I. Farrer, "Pros and Cons of IPv6 Transition Technologies for IPv4aaS", [draft-ietf-v6ops-transition-comparison-02](#) (work in progress), March 2022.

[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>>.
- [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>>.
- [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>>.

[RFC8950] Litkowski, S., Agrawal, S., Ananthamurthy, K., and K. Patel, "Advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop", [RFC 8950](#), DOI 10.17487/RFC8950, November 2020, <<https://www.rfc-editor.org/info/rfc8950>>.

[RFC9099] Vyncke, E., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", [RFC 9099](#), DOI 10.17487/RFC9099, August 2021, <<https://www.rfc-editor.org/info/rfc9099>>.

[12.2](#). Informative References

[Akm] Akamai, "IPv6 Adaptation", <<https://www.akamai.com/us/en/multimedia/documents/product-brief/ipv6-adaptation-product-brief.pdf>>.

[Akm-stats] Akamai, "IPv6 Adoption Visualization", 2021, <<https://www.akamai.com/uk/en/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp>>.

[Alx] Alexa, "The top 500 sites on the web", 2021, <<https://www.alexa.com/topsites>>.

[Amzn] Amazon, "Announcing Internet Protocol Version 6 (IPv6) support for Amazon CloudFront, AWS WAF, and Amazon S3 Transfer Acceleration", <<https://aws.amazon.com/es/about-aws/whats-new/2016/10/ipv6-support-for-cloudfront-waf-and-s3-transfer-acceleration/>>.

[ANSI] ANSI/CTA, "ANSI/CTA Standard Host and Router Profiles for IPv6", 2020, <<https://shop.cta.tech/products/host-and-router-profiles-for-ipv6>>.

- <<https://stats.labs.apnic.net/ipv6>>.
- [APNIC2] APNIC2, "Addressing 2021", 2022,
<<https://blog.apnic.net/2022/01/19/ip-addressing-in-2021/>>.
- [APNIC3] APNIC, "BGP in 2020 - The BGP Table", 2021,
<<https://blog.apnic.net/2021/01/05/bgp-in-2020-the-bgp-table/>>>.
- [APNIC4] APNIC, "BGP in 2021 - The BGP Table", 2022,
<<https://blog.apnic.net/2022/01/06/bgp-in-2021-the-bgp-table/>>>.
- [APNIC5] APNIC, "Average RTT Difference (ms) (V6 - V4) for World (XA)", 2022, <<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>>.
- [ARCEP] ARCEP, "Arcep Decision no 2019-1386, Decision on the terms and conditions for awarding licences to use frequencies in the 3.4-3.8GHz band", 2019,
<https://www.arcep.fr/uploads/tx_gsavis/19-1386.pdf>.
- [ARIN-CG] ARIN, "Community Grant Program: IPv6 Security, Applications, and Training for Enterprises", 2020,
<https://www.arin.net/about/community_grants/recipients/>.
- [ARIN-SW] ARIN, "Preparing Applications for IPv6",
<https://www.arin.net/resources/guide/ipv6/preparing_apps_for_v6.pdf>.
- [BGR_1] BIIGROUP, "China Commercial IPv6 and DNSSEC Deployment Monitor", 2022,
<<http://218.2.231.237:5001/cgi-bin/generate>>.
- [BGR_2] BIIGROUP, "China Government IPv6 and DNSSEC Deployment Monitor", 2022,
<http://218.2.231.237:5001/cgi-bin/generate_gov>.
- [BGR_3] BIIGROUP, "China Education IPv6 and DNSSEC Deployment Monitor", 2022,
<http://218.2.231.237:5001/cgi-bin/generate_edu>.

-
- [CAIDA] APNIC, "Client-Side IPv6 Measurement", 2020, <<https://www.cmand.org/workshops/202006-v6/slides/2020-06-16-client-side.pdf>>.
- [CAIR] Cisco, "Cisco Annual Internet Report (2018-2023) White Paper", 2020, <<https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>>.
- [Cldflr] Cloudflare, "Understanding and configuring Cloudflare's IPv6 support", <<https://support.cloudflare.com/hc/en-us/articles/229666767-Understanding-and-configuring-Cloudflare-s-IPv6-support>>.
- [CN] China.org.cn, "China to speed up IPv6-based Internet development", 2017, <http://www.china.org.cn/business/2017-11/27/content_41948814.htm>.
- [CN-IPv6] National IPv6 Deployment and Monitoring Platform, "Active IPv6 Internet users", 2022, <<https://www.china-ipv6.cn/#/activeconnect/simpleInfo>>.
- [CNLABS_1] CNLABS, "Industry IPv6 and DNSSEC Statistics", 2022, <https://cnlabs.in/IPv6_Mon/generate_industry.html>.
- [CNLABS_2] CNLABS, "Industry IPv6 and DNSSEC Statistics", 2022, <https://cnlabs.in/IPv6_Mon/generate_gov.html>.
- [CNLABS_3] CNLABS, "Industry IPv6 and DNSSEC Statistics", 2022, <https://cnlabs.in/IPv6_Mon/generate_industry.html>.
- [ComputSecur] Computers & Security (Elsevier), "Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64", DOI 10.1016/j.cose.2018.04.012, 2018.
- [Csc6lab] Cisco, "World - Display Content Data", 2022, <<https://6lab.cisco.com/stats/>>.
- [ETSI-IP6-WhitePaper] ETSI, "ETSI White Paper No. 35: IPv6 Best Practices,

Internet-Draft

March 2022

- [FB] Saab, P., "Facebook IPv6 Experience", 2015,
<<https://youtu.be/An7s25FSK0U>>.
- [G_stats] Google, "Google IPv6 Per-Country IPv6 adoption", 2021,
<<https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption>>.
- [Ggl] Google, "Introduction to GGC",
<<https://support.google.com/interconnect/answer/9058809?hl=en>>.
- [HxBld] HexaBuild, "IPv6 Adoption Report 2020", 2020,
<<https://hexabuild.io/assets/files/HexaBuild-IPv6-Adoption-Report-2020.pdf>>.
- [I-D.bonica-6man-ext-hdr-update]
Bonica, R. and T. Jinmei, "Inserting, Processing And
Deleting IPv6 Extension Headers", [draft-bonica-6man-ext-hdr-update-07](#) (work in progress), February 2022.
- [I-D.hinden-6man-hbh-processing]
Hinden, R. M. and G. Fairhurst, "IPv6 Hop-by-Hop Options
Processing Procedures", [draft-hinden-6man-hbh-processing-01](#) (work in progress), June 2021.
- [I-D.ietf-bess-ipv6-only-pe-design]
Mishra, G., Mishra, M., Tantsura, J., Madhavi, S., Yang,
Q., Simpson, A., and S. Chen, "IPv6-Only PE Design for
IPv4-NLRI with IPv6-NH", [draft-ietf-bess-ipv6-only-pe-design-00](#) (work in progress), September 2021.
- [I-D.palet-v6ops-ipv6-only]
Martinez, J. P., "IPv6-only Terminology Definition",
[draft-palet-v6ops-ipv6-only-05](#) (work in progress), March
2020.
- [I-D.peng-v6ops-hbh]
Peng, S., Li, Z., Xie, C., Qin, Z., and G. Mishra,
"Processing of the Hop-by-Hop Options Header", [draft-peng-](#)

[v6ops-hbh-06](#) (work in progress), August 2021.

[I-D.vasilenko-v6ops-ipv6-oversized-analysis]

Vasilenko, E., Xipeng, X., and D. Khaustov, "IPv6 Oversized Packets Analysis", [draft-vasilenko-v6ops-ipv6-oversized-analysis-01](#) (work in progress), September 2021.

[IAB]

IAB, "IAB Statement on IPv6", 2016,
<<https://www.iab.org/2016/11/07/iab-statement-on-ipv6/>>.

Fioccola, et al.

Expires September 8, 2022

[Page 39]

Internet-Draft

March 2022

[IGP-GT]

Internet Governance Project, Georgia Tech, "The hidden standards war: economic factors affecting IPv6 deployment", 2019, <<https://via.hypothes.is/https://www.internetgovernance.org/wp-content/uploads/IPv6-Migration-Study-final-report.pdf>>.

[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>>.

[IPv6Forum]

IPv6Forum, "Estimating IPv6 & DNSSEC External Service Deployment Status", 2022, <<https://www.ipv6forum.com/IPv6-Monitoring/index.html>>.

[ISIF-ASIA-G]

ISIF Asia, "Internet Operations Research Grant: IPv6 Deployment at Enterprises. IIESoc. India", 2020, <<https://isif.asia/2020-grantees/>>.

[ISOC1]

Internet Society, "State of IPv6 Deployment 2018", 2018, <<https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/>>.

[ISOC2]

Internet Society, "Facebook News Feeds Load 20-40% Faster Over IPv6", 2015, <<https://www.internetsociety.org/blog/2015/04/facebook-news-feeds-load-20-40-faster-over-ipv6/>>.

[ISOC3]

Internet Society, "IPv6 Security FAQ", 2019, <<https://www.internetsociety.org/wp->

<content/uploads/2019/02/Deploy360-IPv6-Security-FAQ.pdf>>.

- [MAPRG] 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>>.
- [Mcrsft] Microsoft, "IPv6 for Azure VMs available in most regions", <<https://azure.microsoft.com/en-us/updates/ipv6-for-azure-vm/>>.
- [NRO] NRO, "Internet Number Resource Status Report", 2021, <<https://www.nro.net/wp-content/uploads/NRO-Statistics-2021-Q3-FINAL.pdf>>.

Fioccola, et al.

Expires September 8, 2022

[Page 40]

Internet-Draft

March 2022

- [NST_1] NIST, "Estimating Industry IPv6 and DNSSEC External Service Deployment Status", 2022, <<https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com>>.
- [NST_2] NIST, "Estimating USG IPv6 and DNSSEC External Service Deployment Status", 2022, <<https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov>>.
- [NST_3] NIST, "Estimating University IPv6 and DNSSEC External Service Deployment Status", 2022, <<https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-edu>>.
- [Ntflx] Netflix, "Enabling Support for IPv6", <<https://netflixtechblog.com/enabling-support-for-ipv6-48a495d5196f>>.
- [POTAR001] POTAR00, "IP Addressing through 2021", 2022, <<https://www.potaroo.net/ispcol/2022-01/addr2021.html>>.
- [POTAR002] POTAR00, "IPv6 Resource Allocations", 2022, <<https://www.potaroo.net/bgp/iso3166/v6cc.html>>.
- [RFC5565] Wu, J., Cui, Y., Metz, C., and E. Rosen, "Softwire Mesh

Framework", [RFC 5565](#), DOI 10.17487/RFC5565, June 2009, <<https://www.rfc-editor.org/info/rfc5565>>.

[RFC6555] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", [RFC 6555](#), DOI 10.17487/RFC6555, April 2012, <<https://www.rfc-editor.org/info/rfc6555>>.

[RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", [RFC 8305](#), DOI 10.17487/RFC8305, December 2017, <<https://www.rfc-editor.org/info/rfc8305>>.

[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>>.

[RIPE3] RIPE, "IPv6", 2021, <https://www.ripe.net/participate/meetings/roundtable/26-january-2021/ipv6_roundtable_-jan-2021.pdf>.

[RlncJ] Reliance Jio, "IPv6-only adoption challenges and standardization requirements", 2020, <<https://datatracker.ietf.org/meeting/109/materials/slides-109-v6ops-ipv6-only-adoption-challenges-and-standardization-requirements-03>>.

[SNDVN] SANDVINE, "Sandvine releases 2020 Mobile Internet Phenomena Report: YouTube is over 25% of all mobile traffic", 2020, <<https://www.sandvine.com/press-releases/sandvine-releases-2020-mobile-internet-phenomena-report-youtube-is-over-25-of-all-mobile-traffic>>.

[US-CIO] The CIO Council, "Memorandum for Heads of Executive Departments and Agencies. Completing the Transition to Internet Protocol Version 6 (IPv6)", 2020, <<https://www.cio.gov/assets/resources/internet-protocol-version6-draft.pdf>>.

- [US-FR] Federal Register, "Request for Comments on Updated Guidance for Completing the Transition to the Next Generation Internet Protocol, Internet Protocol Version 6 (IPv6)", 2020, <<https://www.federalregister.gov/documents/2020/03/02/2020-04202/request-for-comments-on-updated-guidance-for-completing-the-transition-to-the-next-generation>>.
- [Vrzn] Verizon, "Verizon Digital Media Services announces IPv6 Compliance", <<https://www.verizondigitalmedia.com/blog/verizon-digital-media-services-announces-ipv6-compliance/>>.
- [W3Tech] W3Tech, "Historical yearly trends in the usage statistics of site elements for websites", 2021, <https://w3techs.com/technologies/history_overview/site_element/all/y>.
- [Wikipedia] Wikipedia, "Comparison of IPv6 support in common applications", <https://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_common_applications>.
- [WIPv6L] World IPv6 Launch, "World IPv6 Launch - Measurements", 2021, <<https://www.worldipv6launch.org/measurements/>>.

Appendix A. Summary of Questionnaire and Replies for network operators

A survey was proposed to more than 50 service providers in the European region during the third quarter of 2020 to ask for their plans on IPv6 and the status of IPv6 deployment.

Fioccola, et al.

Expires September 8, 2022

[Page 42]

Internet-Draft

March 2022

40 people, representing 38 organizations, provided a response. This appendix summarizes the results obtained.

Respondents' business

	Convergent	Mobile	Fixed
Type of operators	82%	8%	11%

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

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

- b. What are 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?

Answer 1.A (38 respondents)

	Yes	No		
Plans availability	79%	21%		
	Mobile	Fixed	Enterprise	Don't answer
Business segment	63%	63%	50%	3%

Answer 1.B (29 respondents)

Even this was an open question, some common answers can be found.

14 respondents (48%) highlighted issues related to IPv4 depletion. The reason to move to IPv6 is to avoid private and/or overlapping addresses.

For 6 respondents (20%) 5G/IoT is a business incentive to introduce IPv6.

4 respondents (13%) also highlight that there is a National regulation request to enable IPv6 associated with the launch of 5G.

4 respondents (13%) consider IPv6 as a part of their innovation strategy or an enabler for new services.

4 respondents (13%) introduce IPv6 because of Enterprise customers demand.

Answer 1.C (30 respondents)

	On-going	In 12 months	After 12 months	Don't answer
Timeframe	60%	33%	0%	7%

Answer 1.D (28 respondents for cellular, 27 for wireline)

Transition in use	Dual-Stack	464XLAT	MAP-T	Don't answer
Cellular	39%	21%	4%	36%

Transition in use	Dual-Stack	DS-Lite	6RD/6VPE	Don't answer
Wireline	59%	19%	4%	19%

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

- If yes, what kind of devices: CE, or BNG/mobile core, or NAT?
- Will you migrate your metro or backbone or backhaul network to support IPv6?

Answer 2.A (30 respondents)

	Yes	No	Don't answer		
Need of changing	43%	33%	23%		

	CEs	Routers	BNG	CGN	Mobile core
What to change	47%	27%	20%	33%	27%

Answer 2.B (22 respondents)

	Yes	Future	No
Plans for transition	9%	9%	82%

Appendix B. Summary of Questionnaire and Replies for enterprises

The Industry Network Technology Council (INTC) developed the following poll to verify the need or willingness of medium-to-large US-based enterprises for training and consultancy on IPv6 (<https://industry.netcouncil.org/>).

54 organizations provided an answer.

Question 1. How much IPv6 implementation have you done at your organization? (54 respondents)

None	16.67%
Some people have gotten some training	16.67%
Many people have gotten some training	1.85%
Web site is IPv6 enabled	7.41%
Most equipment is dual-stacked	31.48%
Have an IPv6 transition plan for entire network	5.56%
Running native IPv6 in many places	20.37%
Entire network is IPv6-only	0.00%

Question 2. What kind of help or classes would you like to see INTC do? (54 respondents)

Classes/labs on IPv6 security	66.67%
Classes/labs on IPv6 fundamentals	55.56%
Classes/labs on address planning/network conf.	57.41%
Classes/labs on IPv6 troubleshooting	66.67%
Classes/labs on application conversion	35.19%
Other	14.81%

Question 3. As you begin to think about the implementation of IPv6 at your organization, what areas do you feel are of concern? (54 respondents)

Security	31.48%
Application conversion	25.93%
Training	27.78%
All the above	33.33%
Don't know enough to answer	14.81%
Other	9.26%

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

Fioccola, et al.

Expires September 8, 2022

[Page 45]

Internet-Draft

March 2022

Nalini Elkins
Inside Products
36A Upper Circle
Carmel Valley CA 93924
United States of America

Email: nalini.elkins@insidethestack.com

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

Email: jordi.palet@theipv6company.com

Gyan S. Mishra
Verizon Inc.

Email: gyan.s.mishra@verizon.com

Chongfeng Xie
China Telecom

Email: xiechf@chinatelecom.cn

Fioccola, et al.

Expires September 8, 2022

[Page 46]