Workgroup: V6OPS
Internet-Draft:
draft-ietf-v6ops-ipv6-deployment-08
Obsoletes: 6036 (if approved)
Published: 20 October 2022
Intended Status: Informational
Expires: 23 April 2023
Authors: G. Fioccola, Huawei Technologies
P. Volpato, Huawei Technologies
N. Elkins, Inside Products
J. Palet Martinez, The IPv6 Company
G. Mishra, Verizon Inc.
C. Xie, China Telecom

IPv6 Deployment Status

Abstract

This document provides an overview of IPv6 deployment status in 2022. Specifically, it looks at the degree of adoption of IPv6 in the industry, analyzes the remaining challenges and proposes further investigations in areas where the industry has not yet taken a clear and unified approach in the transition to IPv6. It obsoletes RFC 6036.

Status of This Memo

Copyright Notice

Table of Contents

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 have contributed to the IPv6 transition discussion in operational environments. To name a few:

- [RFC6180] discussed IPv6 deployment models and transition mechanisms, recommending those proven 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.

[RFC6540] recommended the support of IPv6 to all IP-capable nodes. 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) towards using 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 ISP domain.

Considering all of the above, and after more than ten years since the publication of [RFC6036] it is useful to assess the status of the transition to IPv6. Some reasons include:

- In some areas, the lack of 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 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, at least at the IPv6 service layer.

This document aims to provide a survey of the status of IPv6 deployment and highlight both the achievements and remaining obstacles in the transition to IPv6 networks (and its coexistence with continued IPv4 services). 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.

This document is intended for a general audience interested to understand the status of IPv6 in different industries and network domains. People who provide or use network services may find it useful for the transition to IPv6. Also, people developing plans for IPv6 adoption in an organization or in an industry may find information and references for their analysis. Attention is given to the different stages of the transition to IPv6 networks and services. In particular, a terminology on the use of "IPv6-only" is provided, considering IPv6-only networks and services as the final stage of such transition.

The topics discussed in this document are organized into four main chapters.

Section 2 reports data about the status of IPv6.

Section 3 provides a survey of IPv6 deployments in different environments, including ISPs, enterprises, cloud providers and universities.

Section 4 describes the IPv6 transition approaches for Mobile BroadBand (MBB), Fixed BroadBand (FBB) and Enterprise services.

Section 5 analyzes the general challenges to be solved in the IPv6 transition. Specific attention will be given to operations, performance and security issues.

1.1. Terminology

This section defines the terminology regarding the usage of IPv6-only expressions within this document. The term IPv6-only is defined in relation to the specific scope it is referring to. In this regard, it may happen that only part of a service, of a network or even part of a node is in an IPv6-only scope and the rest is not.

Below are listed the most used terms in relation to the different scopes:

IPv6-only interface: It means that the interface of a node is configured to forward only IPv6. This denotes that just part of the node can be IPv6-only since the rest of the interfaces of the same node may work with IPv4 as well. A Dual-Stack interface is not an IPv6-only interface.

IPv6-only node: It means that the node uses only IPv6. All interfaces of the host only have IPv6 addresses.

IPv6-only service: It is used if between the host's interface and the interface of the content server, all packet headers of the service session are IPv6.

IPv6-only overlay: It is used if between the end points of the tunnels, all inner packet headers of the tunnels are IPv6. For example, IPv6-only overlay in fixed network means that the encapsulation is only IPv6 between the interfaces of the Provider Edge (PE) nodes or between the WAN interface of the Customer Edge (CE) node and the Broadband Network Gateway (BNG) facing interface of CGN.

IPv6-only underlay: It is used if the data plane and control plane are IPv6, but not necessarily management plane. For example, IPv6-only underlay in fixed network means that the underlay network protocol is only IPv6 between any Provider Edge (PE) nodes but they can be Dual-Stack in overlay. SRv6 is an example of IPv6-only underlay.

IPv6-only network: It is used if every node in this network is IPv6-only. No IPv4 should exist in an IPv6-only network. In particular, IPv6-only network's data plane, control plane, and management plane must be IPv6. All PEs must be IPv6-only. Therefore, if tunnels exist among PEs, both inner and outer headers must be IPv6. For example, IPv6-only access network means that every nodes in this access network must be IPv6-only and similarly IPv6-only backbone network means that every nodes in this backbone network must be IPv6-only.

IPv4 as a Service (IPv4aaS): It means that IPv4 service support is provided by means of transition mechanism, therefore there is a combination of encapsulation/translation + IPv6-only overlay + decapsulation/translation. For an IPv6-only network, connectivity to legacy IPv4 is either non-existent or provided by IPv4aaS mechanisms.

Note that IPv6-only definitions are also discussed in [I-D.palet-v6ops-ipv6-only].

2. IPv6: The Global Picture

This section deals with some key questions related to IPv6 namely: (1) the status of IPv4 exhaustion, often considered as one of the triggers to switch to IPv6, (2) the number of IPv6 end users, a primary measure to sense IPv6 adoption, (3) the percentage of websites reachable over IPv6 and (4) a report on IPv6 public actions and policies.

These parameters are monitored by the Regional internet Registries (RIRs) and other institutions worldwide as they provide a first-order indication on the 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 may affect 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 [POTAROO1] 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, [POTAROO1] again highlights the role of both address transfer and Network Address Translation (NAT) to counter the IPv4 exhaustion. The transfer of IPv4 addresses can be done under the control or registration of a RIR or on the so-called grey market where third parties operate to enable the buy/sell of IPv4 addresses. In all cases, a set of IPv4 addresses is "transferred" to a different holder that has the need to expand their address range. 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 IPv4 addresses to satisfy their need of providing IPv4 connectivity to their tenants. NAT systems provide a means to absorb at least a portion of the demand of public IPv4 addresses as they enable the use of private addressing in internal networks while limiting the use of public addresses on their WAN-facing side. In the case of NAT, architectural and operational issues remain. Private address space cannot provide adequate address span, especially for large organizations, and the reuse of addresses may make the network more complex. In addition, multiple levels of address translation may coexist in a network, e.g. Carrier-Grade NAT (CGN) [RFC6264] based on two stages of translation. This comes with an economic and operational burden, as discussed later in this document.

2.1.1. 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 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 this regard, [POTAROO2] provides distribution files. The next table compares the IPv4 addresses per capita ratio of a certain country with relative adoption of IPv6, expressed as the number of IPv6 capable users in the considered country. 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 1: IPv4 per capita and IPv6 deployment

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

A direct correlation between low IPv4 per capita and high IPv6 adoption is not immediate. For example, countries like the Russian Federation, Poland, Spain and Italy have lower IPv4 per capita ratio than countries like the U.S.A, Germany, France, even if their IPv6 adoption rate is also lower. Looking at the countries with higher IPv6 adoption, this appears related to several factors in addition to the lack of IPv4 addresses, including local regulation and market-driven actions.

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, the approach used by APNIC to quantify the adoption of IPv6 by means of a script that runs on a user's device [CAIDA] is considered. 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 [POTAROO2].

	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 2: 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 3: 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 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. IPv6 public actions and policies

As previously noted, the worldwide deployment of IPv6 is not uniform [G_stats], [APNIC1]. It is worth noticing that, in some cases, higher IPv6 adoption in a certain country has been achieved as a consequence of actions taken by the local government through regulation or incentive to the market. Looking at the European Union area, countries such as Belgium, France and Germany are well ahead in terms of IPv6 adoption. In the case of Belgium, the Belgian Institute for Postal services and Telecommunications (BIPT) acted to mediate an agreement between the local ISPs and the government to limit the use of Carrier-Grade NAT (CGN) systems and of public IPv4 addresses for lawful investigations in 2012 [BIPT]. The agreement limited the use of one IPv4 address per 16 customers behind NAT. The economic burden sustained by the ISPs for the unoptimized use of NAT induced the shift to IPv6 and its increased adoption in the latest years. In France, the National Regulator (Autorite de regulation des communications electroniques, or Arcep) introduced an obligation for the mobile carriers awarded with a license to use 5G frequencies (3.4-3.8GHz) in Metropolitan France to be IPv6 compatible [ARCEP]. 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". Increased IPv6 adoption in Germany depended on a mix of industry and public actions. Specifically, the Federal Office for Information Technology (under the Federal Ministry of the Interior) issued over the years a few recommendations on the use of IPv6 in the German public administration. The latest guideline in 2019 constitutes a high-level roadmap for mandatory IPv6 introduction in the federal administration networks [GFA]. In the United States, the Office of Management and Budget is also calling for IPv6 adoption [US-FR], [US-CIO]. These documents define a plan to have the 80% of the US Federal IP-capable networks based on IPv6-only by the year 2025. China is another example of government which is supporting a country-wide IPv6 adoption [CN]. In India, the high adoption of IPv6 took origin from the decision of Reliance Jio to move to IPv6 in their networks [RelJio]. In addition, the Department of Telecommunications (under the Ministry of Communications and Information Technology) issued guidelines for the progressive adoption of IPv6 in public and private networks. The latest one dates 2021 [IDT] and fosters further moves to native IPv6 connection services.

3. A Survey on IPv6 Deployments

This section discusses the status of IPv6 adoption in operational networks.

3.1. IPv6 Allocations

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. The following 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

The trend shows the steady progress of IPv6. The decline of IPv6 allocations in 2020 and 2021 may be due to COVID-19 pandemic. It also happens to IPv4 allocations.

[APNIC2] also compares the number of allocations for both address families. The CAGR looks quite similar in 2021 but a little higher for the IPv4 allocations in comparison to the IPv6 allocations (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

The reason may be that the IPv4 allocations in 2021 include 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 operator for long period. 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 Systems (AS) 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. In comparison, the CAGR for the total of IPv6 and IPv4 networks is 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. The next subsections will zoom into each specific domain to highlight its relative status.

3.2. IPv6 among Internet Service Providers

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 their plans about IPv6 and their technical preferences towards its adoption. Although such poll does not give an exhaustive view on the IPv6 status, it provides some insights that are relevant to the discussion.

The poll reveals that the majority of the ISPs 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. Global IPv4 address depletion and the run out of private address space recommended in [RFC1918] are reported as the important drivers for IPv6 deployment (48%). In a few cases, respondents cite the requirement of national IPv6 policies and the launch of 5G as the reasons (13%). Enterprise customers demand is also a reason to introduce IPv6 (13%).

From a technical preference standpoint, Dual-Stack is the most adopted solution, in both wireline (59%) and cellular networks

(39%). In wireline, the second most adopted mechanism is DS-Lite (19%). In cellular networks, the second preference is 464XLAT (21%).

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 ISPs. Publicly available reports show how the enterprise deployment of IPv6 lags behind ISP deployment [cmpwr].

[NST_1] provides estimations on deployment status of IPv6 for domains such as example.com, example.net or example.org in the United States in 2022. The measurement encompasses many industries, including telecommunications, so the term "enterprises" is a bit loose in this context. 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. [BGR_1] has similar data for China while [CNLABS_1] provides the status in India.

Country	Domains analyzed	DNS	Mail	Website
China	478	74.7%	0.0%	19.7%
India	104	51.9%	15.4%	16.3%
United States of America	1070	66.8%	21.2%	6.3%

Figure 7: IPv6 support for external-facing services across enterprises (Jan 2022)

A poll submitted to a group of large enterprises in North America (see Appendix B) shows that the operational issues are even more critical than for ISPs.

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 case is the network 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%). 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 the IPv6 adoption of governments and academia.

As far as governmental agencies are concerned, [NST_2] provides analytics on the degree of IPv6 support for DNS, mail and websites across second level domains associated with the US federal agencies. These domains are in the form of example.gov or example.fed. The script used by [NST_2] has also been employed to measure the same analytics in other countries: China [BGR_2], India [CNLABS_2] and the European Union [IPv6Forum].

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 8: IPv6 support for external-facing services across governmental institutions (Jan 2022)

(*) Both EU and country specific domains are considered.

USA's IPv6 support is higher than other countries. This is likely due to the IPv6 mandate set by [US-CIO]. In the case of India, the degree of support seems still quite low. This is also true for China, with the notable exception of high percentage of IPv6-enabled websites for government-related organizations.

Similar statistics are also available for higher education. [NST_3] measures the data from second level domains of universities in the US, such as example.edu. [BGR_3] looks at Chinese education-related domains. [CNLABS_3] analyzes domains in India (mostly third level), while [IPv6Forum] lists universities in the European Union (second level).

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 9: IPv6 support for external-facing services across universities (Jan 2022)

Overall, the universities have wider support of IPv6-based services compared to 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 in academia.

3.4. Observations on Industrial Internet

In an industrial environment, OT (Operational technology) refers to the systems used to monitor and control processes within a factory or production environment, while IT (Information technology) refers to anything related to computer technology and networking connectivity.

There are potential advantages for using IPv6 for Industrial Internet of Things (IIoT), in particular the large IPv6 address space, the automatic IPv6 address 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. To promote the use of IPv6 for smart manufacturing systems and IIoT applications a generic approach to remove these pain points is highly desirable.

3.5. Observations on Content and Cloud Service Providers

The high number of addresses required to connect the virtual and physical elements in a Data Center and the necessity to overcome the limitation posed by [RFC1918] have been the drivers to the adoption of IPv6 in several CSP networks.

Several public references, as reported in Section 5.1.3, 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.

3.6. Application Transition

The transition to IPv6 requires that the application software is adapted for use in IPv6-based networks ([ARIN-SW] provides an example). The use of transition mechanisms like 464XLAT is essential to support IPv4-only applications while they evolve to IPv6. Depending on the transition mechanism employed some issues may remain. For example, in the case of NAT64/DNS64 the use of literal IPv4 addresses, instead of DNS names, will fail, unless mechanisms such as Application Level Gateways (ALG) are used. This issue is not present in 464XLAT (see [RFC8683]).

It is worth mentioning Happy Eyeballs [RFC8305] as a relevant aspect of application transition to IPv6.

4. IPv6 deployment scenarios

The scope of this section is to discuss the network and service scenarios applicable for the transition to IPv6. Most of their definitions have been provided in Section 1.1. This clause is intended to focus on their technical and operational characteristics. The sequence of scenarios described here does not have necessarily to be intended as a roadmap for the IPv6 transition. Depending on their specific plans and requirements, service providers may either adopt the scenarios proposed in a sequence or jump directly to a specific one.

4.1. Dual-Stack

Based on answers provided by operators to the poll (Appendix A), Dual-Stack [RFC4213] appears to be currently the most widely deployed IPv6 solution (about 50%, see both Appendix A and the statistics reported in [ETSI-IP6-WhitePaper]).

With Dual-Stack, IPv6 can be introduced together with other network upgrades and many parts of network management and Information Technology (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. The cost and effort on the network management and IT systems upgrade are moderate. The benefits are to start using IPv6 and save NAT costs.

Although Dual-Stack may provide advantages in the introductory stage, it does have a few disadvantages in the long run, like the duplication of the network resources and states. It also requires more IPv4 addresses, thus increasing both Capital Expenses (CAPEX) and Operating Expenses (OPEX). For example, even if private addresses are used with 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 IPv6 usage exceeds certain threshold, it may be advantageous to switch to start a transition to a next scenario. For example, the process may start with the IPv6-only overlay stage and IPv4aaS, as described hereinafter. 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 the next scenarios may also cause a loss of customers. Based on feedbacks of network operators participating in World IPv6 Launch [WIPv6L] in June 2021, 108 out of 346 operators exceed 50% of IPv6 traffic volume (31.2%), 72 exceed 60% (20.8%), while 37 exceed 75% (10.7%). The consensus to move to IPv6-only might be reasonable when IPv6 traffic volume is between 50% and 60%.

4.2. IPv4 as a Service and IPv6-only Overlay

As defined in Section 1.1, IPv6-only is generally associated with a scope, e.g. IPv6-only overlay or IPv6-only underlay.

The IPv6-only overlay denotes that the overlay tunnel between the end points of a network is based only on IPv6. It can be used to ensure IPv4 support via IPv4aaS and it can be a complex decision that depends on several factors, such as economic aspects, policy and government regulation.

[I-D.ietf-v6ops-transition-comparison] compares the merits of the most common transition solutions for IPv6-only service delivery, i.e. 464XLAT [RFC6877], DS-lite [RFC6333], Lightweight 4over6 (lw4o6) [RFC7596], MAP-E [RFC7597], and MAP-T [RFC7599], but does not provide an explicit recommendation. However, the poll in Appendix A indicates that the most widely deployed IPv6 transition solution in the Mobile Broadband (MBB) domain is 464XLAT while in the Fixed Broadband (FBB) domain is DS-Lite.

Both are IPv4aaS solutions by leveraging IPv6-only overlay. IPv4aaS offers Dual-Stack service to users and allows an ISP to run IPv6-only in the network (typically, the access network).

While it may not always be the case, IPv6-only transition technologies such as 464XLAT require far fewer IPv4 addresses [I-D.ietf-v6ops-transition-comparison], because they make a more efficient usage without restricting the number of ports per subscriber. This helps 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.

IPv6-only overlay may be facilitated by the natural upgrade or replacement of CEs because of newer technologies (tripe-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.

For applications with a large number of users (e.g. large mobile operators) or a large number of hosts (e.g. large DCs), even the full private address space [RFC1918] is not enough. Also, Dual-Stack will likely lead to duplication of network resources and operations to support both IPv6 and IPv4, which increases the amount of state information in the network. This suggests that for scenarios such as MBB or large DCs, IPv6-only overlay could be more efficient from the start of the IPv6 introduction.

So, in general, when the Dual-Stack disadvantages outweigh the IPv6-only complexity, it makes sense to transit to IPv6-only overlay. Some network operators already started this process, as in the case of [TMus], [RelJio] and [EE].

4.3. IPv6-only Underlay

As opposed to IPv6-only overlay and IPv4aaS, discussed in the previous sections, IPv6-only underlay network uses IPv6 as the network protocol for all traffic delivery. Both the control and data planes are IPv6-based. The definition of IPv6-only underlay needs to be associated with a scope in order to identify the domain where it is applicable, such as IPv6-only access network or IPv6-only backbone network.

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

When both enterprises and service providers begin to transit from an IPv4/MPLS backbone to introduce IPv6 in the underlay, they do not necessarily need to dual-stack the underlay. Forwarding plane complexity on the Provider (P) nodes of the ISP core should be kept simple as a single protocol only backbone. An example could be Softwire Mesh Framework [RFC5565]. This is based on IPv6 as the only protocol for the core network where IPv4 packets can be tunneled with 4to6 MPLS softwire encapsulation over the IPv6-only backbone.

Hence, when operators decide to transit to an IPv6 underlay, the ISP backbone should be 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 backbone 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.

Therefore, IPv6-only underlay network deployment for access and backbone network, seems not the first option and the current trend is to keep IPv4/MPLS Data Plane and run IPv4/IPv6 Dual-Stack to edge nodes.

As ISPs do the transition in the future to IPv6-only access 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 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 related to the forwarding plane complexities.

4.4. IPv6-only

IPv6-only is the final stage of the IPv6 transition and it happens when a complete network, end-to-end, no longer has IPv4. No IPv4 address is configured for network management or anything.

Since IPv6-only means that both underlay network and overlay services are only IPv6, it will take longer to happen.

5. Common IPv6 Challenges

This section lists common IPv6 challenges in order to encourage more investigations. Despite IPv6 has already been well-proven in production, there are some challenges to consider. In this regard, it is worth noting that [ETSI-GR-IPE-001] also discusses gaps that still exist in IPv6 related use cases.

5.1. Transition Choices

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 carrier's or the enterprise's context, such as the IPv6 network design that fits the service requirements, the network operations and the deployment strategy.

This section briefly highlights the approaches that service providers and enterprises may take and the related challenges.

5.1.1. 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 around 40%. 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 factors like the current IPv4 address shortage, 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 may be done through CGN or with an IPv4aaS approach.
>
> Most of the fixed operators remain attached to a Dual-Stack architecture and many 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. Indeed, only few fixed operators have chosen to move to an IPv6-only scenario.

For mobile operators, the situation is quite different since, in some cases, mobile operators are already stretching their IPv4 address space. The reason is that CGN translation limits 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 IPv4aaS solutions (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 bring 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.

5.1.2. Enterprises and Industrial Internet

At present, the challenge for enterprises mainly relies on upstream service providers. Often, the enterprise connectivity depends on the services provided by their upstream provider. As pointed out in Section 3, enterprises may benefit deploying IPv6 in their public-facing services. IPv6 also shows its advantages in the case of merger and acquisition, to avoid overlapping of the two address spaces. In addition, since several governments are introducing IPv6 policy, all the enterprises providing consulting service to governments are also required to support IPv6.

Enterprises are shielded from IPv4 address depletion issues due to their prevalent use of Proxy and private addressing [RFC1918], thus do not have the business requirement or technical justification to transit to IPv6. Enterprises need to find a business case and a strong motivation for IPv6 transition to justify additional CAPEX and OPEX. Also, since Information and Communication Technologies (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 IPv6 network architecture.

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 do not know well how IPv6 works and the problem of application porting to IPv6 looks quite difficult, even if technically the issue is not overly complicated. 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 ARIN and APNIC initiatives to provide training [ARIN-CG] [ISIF-ASIA-G].

As the most promising protocol for network evolution, 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.

Advances in cloud-based platforms and developments in artificial intelligence (AI) and machine learning (ML) allow OT (Operational technology) and IT (Information technology) systems to integrate and migrate to a centralized analytical, processing, and integrated platform, which must act in real-time. The limitation is that manufacturing companies have diverse corporate cultures and the adoption of new technologies may lag as a result.

For Industrial Internet and related IIoT applications, it would be desirable to leverage the configuration-less characteristic of IPv6 to automatically manage and control the IoT devices. 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.

5.1.3. 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.

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.

5.1.4. 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 IPv4aaS solution [ANSI].

5.2. 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 support 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 may be 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.

Availability of both systems and training is necessary in areas such as IPv6 addressing. IPv6 addresses can be assigned to an interface through different means, such as Stateless Auto-Configuration (SLAAC) [RFC4862], stateful and stateless Dynamic Host Control Protocol (DHCP) [RFC8415]. IP Address Management (IPAM) systems may contribute to handle the technical differences and automate some of the configuration tasks, such as the address assignment or the management of DHCP services.

5.3. 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 has already filled (or 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.

5.3.1. 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 slightly in favor of IPv6. 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. 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.

5.3.2. 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], [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.

5.4. IPv6 security and privacy

An important point that is sometimes considered as a challenge when discussing the transition to IPv6 is related to the security and privacy. [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 by the applied IPv6 transition technologies used to implement IPv4aaS (e.g. 464XLAT, DS-Lite) [ComputSecur].

The security aspects have to be considered to keep at least the same or even a better level of security as it exists nowadays in an IPv4 network environment. The autoconfiguration features of IPv6 will require some more attention. Router discovery and address autoconfiguration may produce unexpected results and security holes. IPsec protects IPv6 traffic at least as well as it does IPv4, and the security protocols for constrained devices (IoT) are designed for IPv6 operation.

IPv6 was designed to restore the end-to-end model of communications with all nodes on networks using globally unique addresses. But, considering this, IPv6 may imply privacy concerns, due to greater visibility on the Internet. IPv6 nodes can (and typically do) use privacy extensions [RFC8981] to prevent any tracking of their burned-in MAC address(es), which are easily readable in the original modified EUI-64 interface identifier format. But, on the other hand, stable IPv6 interface identifiers ([RFC8064]) were developed and this can also affect privacy.

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 of 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, with more IPv6 deployment, IPv6 will also benefit from this process in the long run.

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.

5.4.1. Protocols security issues

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

* Basic IPv6 protocol (Basic header, Extension Headers, Addressing)

* IPv6 associated protocols (ICMPv6, NDP, MLD, DNS, DHCPv6)

* Internet-wide IPv6 security (Filtering, DDoS, Transition Mechanisms)

ICMPv6 is an integral part of IPv6 and performs error reporting and diagnostic functions. 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.

5.4.2. IPv6 Extension Headers and Fragmentation

IPv6 Extension Headers provide a hook for interesting new features to be added, and are more flexible than IPv4 Options. This does add some complexity, and in particular some security mechanisms may require to process the full chain of headers, and some firewalls may require to filter packets based on their Extension Headers. Additionally, packets with IPv6 Extension Headers may be dropped in the public Internet [RFC7872]. Some documents, e.g. [I-D.ietf-6man-hbh-processing], [I-D.ietf-v6ops-hbh], [I-D.bonica-6man-ext-hdr-update], analyze and provide guidance regarding the processing procedures of IPv6 Extension Headers.

Defence against possible attacks through Extension Headers is necessary. For example, the original IPv6 Routing Header type 0 (RH0) was deprecated because of possible remote traffic amplification. In addition, it is worth mentioning that unrecognized Hop-by-Hop Options Header and Destination Options Header will not be considered by the nodes if they are not configured to deal with it [RFC8200]. Other attacks based on Extension Headers may be 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 [RFC6980].

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).

The operational implications of IPv6 Packets with Extension Headers are further discussed in [RFC9098].

6. Security Considerations

This document has no impact on the security properties of specific IPv6 protocols or transition tools. In addition to the discussion above in Section 5.4, the security considerations relating to the protocols and transition tools are described in the relevant documents.

7. Contributors

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

8. Acknowledgements

The authors of this document would like to thank Brian Carpenter, Fred Baker, Alexandre Petrescu, Fernando Gont, 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.

9. IANA Considerations

This document has no actions for IANA.

10. References

10.1. 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", Work in Progress, Internet-Draft, draft-ietf-v6ops-transition-comparison-04, 23 May 2022, <https://www.ietf.org/archive/id/draft-ietf-v6ops-transition-comparison-04.txt>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., 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, É., 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>.

10.2. 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>.

[APNIC1] APNIC, "IPv6 Capable Rate by country (%)", 2022, <https://stats.labs.apnic.net/ipv6>.

[APNIC2] APNIC2, "IP 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 Décision n° 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>.

[BIPT] Belgian Institute for Postal services and Telecommunications, "IPv6 in Belgium", 2017, <https://www.ripe.net/participate/meetings/roundtable/september-2017/government-roundtable-meeting-bahrain-26-september-2017/presentations/belgium-experience-bahrain-roundtable.pdf>.

[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>.

[cmpwr] Compuware, "Impact on Enterprises of the IPv6-Only direction for the US Federal Government", 2020, <https://mydigitalpublication.com/article/Impact+on+Enterprises+of+the+IPv6-Only+Direction+for+the+U.S.+Federal+Government/3702828/664279/article.html>.

[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, <https://doi.org/10.1016/j.cose.2018.04.012>.

[Csc6lab] Cisco, "World - Display Content Data", 2022, <https://6lab.cisco.com/stats/>.

[EE] EE, "IPv6-only devices on EE mobile", 2017, <https://indico.uknof.org.uk/event/38/contributions/489/attachments/612/736/Nick_Heatley_EE_IPv6_UKNOF_20170119.pdf>.

[ETSI-GR-IPE-001] ETSI, "ETSI GR IPE 001: IPv6 Enhanced Innovation (IPE) Gap Analysis", 2021, <https://www.etsi.org/deliver/etsi_gr/IPE/001_099/001/01.01.01_60/gr_IPE001v010101p.pdf>.

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

[FB] Saab, P., "Facebook IPv6 Experience", 2015, <https://youtu.be/An7s25FSK0U>.

[GFA] German Federal Government Commissioner for Information Technology, "IPv6-Masterplan für die Bundesverwaltung", 2019, <https://media.frag-den-staat.de/files/foi/531501/

de-government-ipv6-masterplan-v100-entwurf_konvertiert.pdf>.

[Ggl] Google, "Introduction to GGC", <https://support.google.com/interconnect/answer/9058809?hl=en>.

[G_stats] Google, "Google IPv6 Per-Country IPv6 adoption", 2021, <https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption>.

[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", Work in Progress, Internet-Draft, draft-bonica-6man-ext-hdr-update-07, 24 February 2022, <https://www.ietf.org/archive/id/draft-bonica-6man-ext-hdr-update-07.txt>.

[I-D.ietf-6man-hbh-processing] Hinden, R. M. and G. Fairhurst, "IPv6 Hop-by-Hop Options Processing Procedures", Work in Progress, Internet-Draft, draft-ietf-6man-hbh-processing-03, 13 October 2022, <https://www.ietf.org/archive/id/draft-ietf-6man-hbh-processing-03.txt>.

[I-D.ietf-bess-ipv6-only-pe-design] Mishra, G. S., Mishra, M. P., Tantsura, J., Madhavi, S., Yang, Q., Simpson, A., and S. Chen, "IPv6-Only PE Design for IPv4-NLRI with IPv6-NH", Work in Progress, Internet-Draft, draft-ietf-bess-ipv6-only-pe-design-03, 24 September 2022, <https://www.ietf.org/archive/id/draft-ietf-bess-ipv6-only-pe-design-03.txt>.

[I-D.ietf-v6ops-hbh] Peng, S., Li, Z., Xie, C., Qin, Z., and G. Mishra, "Operational Issues with Processing of the Hop-by-Hop Options Header", Work in Progress, Internet-Draft, draft-ietf-v6ops-hbh-01, 18 April 2022, <https://www.ietf.org/archive/id/draft-ietf-v6ops-hbh-01.txt>.

[I-D.palet-v6ops-ipv6-only] Martinez, J. P., "IPv6-only Terminology Definition", Work in Progress, Internet-Draft, draft-palet-v6ops-ipv6-only-05, 9 March 2020, <https://www.ietf.org/archive/id/draft-palet-v6ops-ipv6-only-05.txt>.

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

[IDT]
Indian Department of Telecommunications, "Revision of IPv6 Transition Timelines", 2021, <https://dot.gov.in/revision-ipv6-transition-timelines-2021>.

[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.V., "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-vms/>.

[NRO] NRO, "Internet Number Resource Status Report", 2021, <https://www.nro.net/wp-content/uploads/NRO-Statistics-2021-Q3-FINAL.pdf>.

[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>.

[POTAROO1] POTAROO, "IP Addressing through 2021", 2022, <https://www.potaroo.net/ispcol/2022-01/addr2021.html>.

[POTAROO2] POTAROO, "IPv6 Resource Allocations", 2022, <https://www.potaroo.net/bgp/iso3166/v6cc.html>.

[RelJio] 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>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[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>.

[RFC6264] Jiang, S., Guo, D., and B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition", RFC 6264, DOI 10.17487/RFC6264, June 2011, <https://www.rfc-editor.org/info/rfc6264>.

[RFC6980] Gont, F., "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery", RFC 6980, DOI 10.17487/RFC6980, August 2013, <https://www.rfc-editor.org/info/rfc6980>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6

Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/info/rfc7872>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[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>.

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

[RFC8683] Palet Martinez, J., "Additional Deployment Guidelines for NAT64/464XLAT in Operator and Enterprise Networks", RFC 8683, DOI 10.17487/RFC8683, November 2019, <https://www.rfc-editor.org/info/rfc8683>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RFC9098] Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. Liu, "Operational Implications of IPv6 Packets with Extension Headers", RFC 9098, DOI 10.17487/RFC9098, September 2021, <https://www.rfc-editor.org/info/rfc9098>.

[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>.

[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>.

[TMus] T-Mobile US, "Going IPv6-only", 2018, <https://pc.nanog.org/static/published/meetings/NANOG73/1645/20180625_Lagerholm_T-Mobile_S_Journey_To_v1.pdf>.

[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>.

[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.

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?

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

b. Will you start the transition of 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://industrynetcouncil.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
80992 Munich
Germany

Email: giuseppe.fioccola@huawei.com

Paolo Volpato
Huawei Technologies
Via Lorenteggio, 240
20147 Milan
Italy

Email: paolo.volpato@huawei.com

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
28420 La Navata - Galapagar, Madrid
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