Internet Engineering Task Force (IETF)
Request for Comments: 9386
Obsoletes: 6036
Category: Informational
ISSN: 2070-1721

G. Fioccola
P. Volpato
Huawei Technologies
J. Palet Martinez
The IPv6 Company
G. Mishra
Verizon Inc.
C. Xie
China Telecom

April 2023

# IPv6 Deployment Status

## Abstract

This document provides an overview of the status of IPv6 deployment 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

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

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

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9386.

## Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction
  1.1. Terminology
2. IPv6: The Global Picture
  2.1. IPv4 Address Exhaustion
    2.1.1. IPv4 Addresses per Capita and IPv6 Status
  2.2. IPv6 Users

2.3. IPv6 Web Content
2.4. IPv6 Public Actions and Policies
3. A Survey on IPv6 Deployments
3.1. IPv6 Allocations
3.2. IPv6 among Internet Service Providers
3.3. IPv6 among Enterprises
3.3.1. Government and Universities
4. IPv6 Deployment Scenarios
4.1. Dual-Stack
4.2. IPv6-Only Overlay
4.3. IPv6-Only Underlay
4.4. IPv4-as-a-Service
4.5. IPv6-Only
5. Common IPv6 Challenges
5.1. Transition Choices
5.1.1. Service Providers: Fixed and Mobile Operators
5.1.2. Enterprises
5.1.3. Industrial Internet
5.1.4. Content and Cloud Service Providers
5.1.5. CPEs and User Devices
5.1.6. Software Applications
5.2. Network Management and Operations
5.3. Performance
5.3.1. IPv6 Packet Loss and Latency
5.3.2. Customer Experience
5.4. IPv6 Security and Privacy
5.4.1. Protocols' Security Issues
6. IANA Considerations
7. Security Considerations
8. References
8.1. Normative References
8.2. Informative References
Appendix A. Summary of Questionnaire and Replies for Network Operators
Appendix B. Summary of Questionnaire and Replies for Enterprises
Acknowledgements
Contributors
Authors' Addresses

## 1. Introduction

[RFC6036] describes IPv6 deployment scenarios that were adopted or foreseen by a number of Internet Service Providers (ISPs) who responded to a technical questionnaire in early 2010, and [RFC6036] also provides practices and plans that were 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] discusses IPv6 deployment models and transition mechanisms, recommending those proven to be effective in operational networks.

* [RFC6883] provides guidance and suggestions for Internet content providers and Application Service Providers (ASPs).

* [RFC7381] introduces the guidelines of IPv6 deployment for enterprises.

[RFC6540] recommends 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 and other Standards Development 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 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 in understanding 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, 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 and analytics about the status of IPv6.

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

* Section 4 describes the IPv6 deployment approaches for Mobile Broadband (MBB), Fixed Broadband (FBB), and enterprises.

* Section 5 analyzes the general challenges to be solved in the IPv6 transition. Specific attention is 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, a network, or even a node is in an IPv6-only scope, and the rest is not. The most used terms in relation to the different scopes are listed below:

IPv6-only interface:
: 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:
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 a fixed network means that the encapsulation is only IPv6 between the interfaces of the Provider Edge (PE) nodes or between the Customer Provider Edge (CPE) node and the Broadband Network Gateway (BNG).

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

IPv6-only network:
It is used if every node in this network is IPv6-only. IPv4 should not exist in an IPv6-only network. In particular, an 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, an IPv6-only access network means that every node in this access network must be IPv6-only, and similarly, an IPv6-only backbone network means that every node in this backbone network must be IPv6-only.

IPv4-as-a-Service (IPv4aaS):
IPv4 service support is provided by means of a transition mechanism; therefore, there is a combination of encapsulation/translation + IPv6-only underlay + 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 [IPv6-ONLY-DEF].

## 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 about

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] (January 2022) shows that the available pool of the five RIRs at the end of 2021 counted 5.2 million IPv4 addresses, while the reserved pool included another 12.1 million, for a total of 17.3 million IPv4 addresses (-5.5% year over year, comparing 2021 against 2020). Table 1 of [POTAROO1] shows that the total IPv4 allocated pool equaled 3.685 billion addresses (+0.027% year over year). The ratio between the available addresses and the total allocated was brought to 0.469% of the remaining IPv4 address space (from 0.474% at the end of 2020).

On the other hand, [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 an RIR or on the so-called grey market, where third parties operate to enable the buying/selling 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 an 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.

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 tables compare the number of IPv4 addresses available per person in a certain country (IPv4 address per capita) against the relative adoption of IPv6 in the same country (expressed as the number of IPv6-capable users in the considered country). The table shows just a subset of the data available from [POTAROO2]. In particular, the following table provides the data for the 25 most populated countries in the world. The table is ordered based on the IPv4 addresses per capita ratio, and the data refer to 1 January 2022.

| Country | IPv4 per Capita | IPv6 Deployment |
|---|---|---|
| United States of America | 4.89 | 47.1% |

| | | |
|---|---|---|
| United Kingdom | 1.65 | 33.2% |
| Japan | 1.50 | 36.7% |
| Germany | 1.48 | 53.0% |
| France | 1.27 | 42.1% |
| Italy | 0.91 | 4.7% |
| South Africa | 0.46 | 2.4% |
| Brazil | 0.41 | 38.7% |
| Russian Federation | 0.31 | 9.7% |
| China | 0.24 | 60.1%(*) |
| Egypt | 0.24 | 4.3% |
| Mexico | 0.23 | 41.8% |
| Turkey | 0.20 | 0.2% |
| Vietnam | 0.17 | 48.0% |
| Iran (Islamic Republic) | 0.15 | 0.1% |
| Thailand | 0.13 | 40.8% |
| Indonesia | 0.07 | 5.0% |
| Philippines | 0.05 | 13.8% |
| India | 0.03 | 76.9% |
| Pakistan | 0.03 | 2.1% |
| United Republic of Tanzania | 0.02 | 0.0% |
| Nigeria | 0.02 | 0.2% |
| Bangladesh | 0.01 | 0.3% |
| Ethiopia | 0.00 | 0.0% |
| Democratic Republic of Congo | 0.00 | 0.1% |

Table 1: IPv4 per Capita and IPv6 Deployment for the Top 25 Most Populated Countries in the World (as of January 2022)

(*) 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, yet some indications emerge. For example, some countries, such as Brazil, China, and India, have clearly moved towards IPv6 adoption. As discussed later, this appears related to several factors in addition to the lack of IPv4 addresses, including local regulation and market-driven actions. The 5 countries at the top of the table, with relative high availability of IPv4 addresses, have also shown a good level of IPv6 adoption. In other cases, a relative scarcity of IPv4 addresses has not meant a clear move towards IPv6, as several countries listed in the table still have low or very low IPv6 adoption.

## 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 World IPv6 Launch initiative [WIPv6L]. The measurement aggregates statistics from organizations, such as [Akm-stats], that provide 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 as of 1 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% |

Table 2: IPv6-Capable Users against Total Users (in Millions) as of January 2022

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

## 2.3. IPv6 Web Content

[W3Techs] keeps track of the use of several technical components of websites worldwide through different analytical engines. The utilization of IPv6 for websites is shown in the next table, where the percentages refer to the websites that are accessible over IPv6.

| 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% |

Table 3: Usage of IPv6 in Websites (as of January 2022)

Looking at the growth rate, it may not appear 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. At the beginning of January 2022, [Csc6lab] measured that out of the world's top 500 sites, 203 are IPv6 enabled (+3.6% from January 2021 to January 2022). If we consider that the big content providers (such as Google, Facebook, and 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. Of that 50% of all mobile traffic, it would be interesting to know what percentage is IPv6. Unfortunately, this information is not available.

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 the 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 certain countries has been achieved as a consequence of actions taken by the local governments through regulation or incentive to the market. Looking at the European Union area, some 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 (3.4-3.8 GHz) in Metropolitan France to be IPv6 compatible [ARCEP]. As stated in [ARCEP] (translated from French),

> 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 from spreading widely or create a barrier to entry for newcomers to the market. Per [ARCEP] (translated from French), "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 road map 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 80% of the US federal IP-capable networks based on IPv6-only by the year 2025. China is another example of a government that 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 IPv6 connection services.

## 3. A Survey on IPv6 Deployments

This section discusses the status of IPv6 adoption in service provider and enterprise networks.

## 3.1. IPv6 Allocations

RIRs are responsible for allocating IPv6 address blocks to ISPs, Local Internet Registries (LIRs), and 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 from 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% |

Table 4: IPv6 Allocations Worldwide (as of January 2022)

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

Table 5: Allocations per Address Family (as of January 2022)

The reason may be that the IPv4 allocations in 2021 included 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.

The next table is based on [APNIC3] and [APNIC4] and shows the percentage of Autonomous Systems (ASes) 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% of the 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% | |

Table 6: Percentage of IPv6-Capable ASes (as of January 2022)

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

A survey was submitted to a group of service providers in Europe during the third quarter of 2020 (see Appendix A for the complete poll) to understand their plans about IPv6 and their technical preferences regarding its adoption. Although this poll does not give an exhaustive view on the IPv6 status, it provides some insights that are relevant to the discussion.

The poll revealed that the majority of ISPs interviewed had plans concerning IPv6 (79%). Of them, 60% had ongoing activities already, while 33% were expected to start activities in a 12-month timeframe. The transition to IPv6 involved all business segments: mobile (63%), fixed (63%), and enterprise (50%).

The reasons to move to IPv6 varied. Global IPv4 address depletion and the run out of private address space recommended in [RFC1918] were reported as the important drivers for IPv6 deployment (48%). In a few cases, respondents cited the requirement of national IPv6 policies and the launch of 5G as the reasons (13%). Enterprise customer demand was also a reason to introduce IPv6 (13%).

From a technical preference standpoint, Dual-Stack [RFC4213] was the most adopted solution in both wireline (59%) and cellular networks (39%). In wireline, the second most adopted mechanism was Dual-Stack Lite (DS-Lite) [RFC6333] (19%). In cellular networks, the second preference was 464XLAT [RFC6877] (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 the deployment status of IPv6 for domains such as example.com, example.net, or example.org in the United States. 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 websites. [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% |

Table 7: IPv6 Support for External-Facing Services across Enterprises (as of January 2022)

A poll submitted to a group of large enterprises in North America in early 2021 (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. Additionally, 35% of the enterprises did not implement IPv6 at all or are stuck at the training phase. In no case is the network fully based on IPv6.

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 address planning / network configurations (57.41%).

Coming to implementation, the three areas of concern are IPv6 security (31.48%), training (27.78%), and application conversion (25.93%), and 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 adoption of IPv6 in 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 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, e.g., China [BGR_2], India [CNLABS_2], and the European Union [IPv6Forum]. For this latter analytic, some post-processing is necessary to filter out the non-European domains.

| 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% |

Table 8: IPv6 Support for External-Facing Services across Governmental Institutions (as of January 2022)

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

IPv6 support in the US 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 a 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_1] analyzes domains in India (mostly third level), while [IPv6Forum] lists universities in the European Union (second level), again after filtering the non-European domains.

| 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% |

Table 9: IPv6 Support for External-Facing Services across Universities (as of January 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 websites in India), the numbers shown in the table above indicate good support of IPv6 in academia.

# 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 the related definitions have been provided in Section 1.1. This clause is intended to focus on the technical and operational characteristics. The sequence of scenarios described here does not necessarily have to be intended as a road map 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 the poll answers provided by network operators (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 IT systems can still work in IPv4. This avoids a 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 help desk to track CGN-related issues.

For this reason, when IPv6 usage exceeds a certain threshold, it may be advantageous to start a transition to the next scenario. For example, the process may start with the IPv4aaS stage, 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 the feedback of network operators participating in the 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%), and 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. 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. Tunneling provides a way to use an existing IPv4 infrastructure to carry IPv6 traffic. IPv6 or IPv4 hosts and routers can tunnel IPv6 packets over IPv4 regions by encapsulating them within IPv4 packets. The approach with IPv6-only overlay helps to maintain compatibility with the existing base of IPv4, but it is not a long-term solution.

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 IPv6-only solutions.

### 4.3. IPv6-Only Underlay

The IPv6-only underlay network uses IPv6 as the network protocol for all traffic delivery. Both the control and data planes are based on IPv6. 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 the IPv6-only access network or IPv6-only backbone network.

When both enterprises and service providers begin to transition 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 backbone with a single protocol. Hence, when operators decide to transition to an IPv6 underlay, the ISP backbone should be IPv6-only because Dual-Stack is not the best choice. The underlay could be IPv6-only and allow IPv4 packets to be tunneled using a VPN over an IPv6-only backbone while leveraging [RFC8950], which specifies the extensions necessary to allow advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 next hop.

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

As ISPs do the transition in the future to an IPv6-only access network or backbone network, e.g., Segment Routing over IPv6 (SRv6) data plane, they start the elimination of IPv4 from the underlay transport network while continuing to provide IPv4 services.

Basically, as also shown 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. IPv4-as-a-Service

IPv4aaS can be used to ensure IPv4 support, and it can be a complex decision that depends on several factors, such as economic aspects, policy, and government regulation.

[RFC9313] compares the merits of the most common transition solutions for IPv4aaS, i.e., 464XLAT [RFC6877], DS-Lite [RFC6333], Lightweight 4over6 (lw4o6) [RFC7596], Mapping of Address and Port with Encapsulation (MAP-E) [RFC7597], and Mapping of Address and Port using Translation (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, it is DS-Lite.

Both are IPv4aaS solutions that leverage IPv6-only underlay. 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 [RFC9313], because they are more efficient and do not restrict the number of ports per subscriber. This helps to reduce troubleshooting costs and to remove some operational issues related to permanent block listing of IPv4 address blocks when used via CGN in some services.

IPv4aaS may be facilitated by the natural upgrade or replacement of CPEs because of newer technologies (triple-play, higher bandwidth WAN links, better Wi-Fi 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 deployments with a large number of users (e.g., large mobile operators) or a large number of hosts (e.g., large Data Centers (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, IPv4aaS 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 transition to IPv4aaS. Some network operators have already started this process, as in the case of [TMus], [RelJio], and [EE].

### 4.5. 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 else.

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

## 5. Common IPv6 Challenges

This section lists common IPv6 challenges, which have been validated and discussed during several meetings and public events. The scope

is to encourage more investigations. Despite that 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, an enterprise, or a CSP may perceive quite a complex task with 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 is an important challenge and may depend on factors specific to the context, such as the IPv6 network design that fits the service requirements, the network operations, and the deployment strategy.

The subsections below briefly highlight the approaches that the different parties may take and the related challenges.

### 5.1.1. Service Providers: Fixed and Mobile Operators

For fixed operators, the massive software upgrade of CPEs to support Dual-Stack already started in most of the service provider networks. On average, looking at the global statistics, the IPv6 traffic percentage is currently around 40% [G_stats]. As highlighted in Section 3.2, 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, CPE costs, CGN costs, and so on.

* Fixed operators with a Dual-Stack architecture can start defining and applying a new strategy when reaching the limit in terms of the 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 CPEs 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 a 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 the IPv4 address scarcity issue completely.

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; therefore, each operator needs to do their own evaluations for the transition based on the specific situation.

### 5.1.2. Enterprises

At present, the usage of IPv6 for enterprises often relies on upstream service providers, since the enterprise connectivity depends on the services provided by their upstream provider. Regarding the

enterprises' internal infrastructures, IPv6 shows its advantages in the case of a merger and acquisition, because it can be avoided by the overlapping of the two address spaces, which is common in case of IPv4 private addresses. In addition, since several governments are introducing IPv6 policies, all the enterprises providing consulting services to governments are also required to support IPv6.

However, enterprises face some challenges. They are shielded from IPv4 address depletion issues due to their prevalent use of proxy and private addressing [RFC1918]; thus, they do not have the business requirement or technical justification to transition to IPv6. Enterprises need to find a business case and a strong motivation to transition to IPv6 to justify additional CAPEX and OPEX. Also, since Information and Communication Technologies (ICTs) are not the core business for most of the enterprises, the 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 that require IPv6 network architecture.

Enterprises worldwide, in particular small- and medium-sized enterprises, are quite late to adopt IPv6, especially on internal networks. In most cases, the enterprise engineers and technicians do not have a great experience with IPv6, and the problem of application porting to IPv6 looks quite difficult. As highlighted in the relevant poll, the technicians may need to be trained, but the management does not see a business need for adoption. This creates an unfortunate cycle where the perceived complexity of the IPv6 protocol and concerns about security and manageability combine with the 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].

#### 5.1.3. Industrial Internet

In an industrial environment, Operational Technology (OT) refers to the systems used to monitor and control processes within a factory or production environment, while Information Technology (IT) refers to anything related to computer technology and networking connectivity. IPv6 is frequently mentioned in relation to Industry 4.0 and the Internet of Things (IoT), affecting the evolution of both OT and IT.

There are potential advantages for using IPv6 for the Industrial Internet of Things (IIoT), in particular, the large IPv6 address space, the automatic IPv6 address configuration, and resource discovery. However, its industrial adoption, in particular, in smart manufacturing systems, has been much slower than expected. There are still many obstacles and challenges that prevent its pervasive use. The key problems identified are the incomplete or underdeveloped 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. 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 and IT 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 configurationless 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.

#### 5.1.4. 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.

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.

Several public references, as reported hereinafter, 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.

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 a high percentage, at least higher than 50% in most of the cases, since all the key Caches and CDNs are ready for IPv6 [Cldflr] [Ggl] [Ntflx] [Amzn] [Mcrsft]. So the percentage of traffic going to the key Caches/CDNs is a good approximation of the potential IPv6 traffic in a network.

The challenges for CSPs are mainly related to the continuous support of IPv4 to be guaranteed, since most CSPs already completed the transition to IPv6-only. 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.

#### 5.1.5. CPEs and User Devices

It can be noted that most of the user devices (e.g., smartphones) have been IPv6 enabled for many years. But there are exceptions, for example, for the past few years, smart TVs have typically had IPv6 support; 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 (i.e., the preferred CGN solution for carriers), it could be less likely to run out of IPv4 addresses and private IPv4 space. But as IPv4-only devices and traffic reduce, the need to support private and public IPv4 lessens. So to have CPEs completely support IPv6 serves as an important challenge and incentive to choose IPv4aaS solutions [ANSI] over Dual-Stack.

#### 5.1.6. Software Applications

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 (ALGs) 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.

### 5.2. Network Management and Operations

There are important IPv6 complementary solutions related to Operations, Administration, and Maintenance (OAM) that look less mature compared to IPv4. A Network Management System (NMS) has a central role in the modern networks for both network operators and enterprises, and its transition is a fundamental issue. This is because some IPv6 products are not as field proven as IPv4 products, even if conventional protocols (e.g., SNMP and RADIUS) already support IPv6. In addition, an incompatible vendor road map for the development of new NMS features affects the confidence of network operators or enterprises.

An important factor is represented by the need for training the network operations workforce. Deploying IPv6 requires that 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], or by using the stateful Dynamic Host Configuration Protocol (DHCP) [RFC8415]. IP Address Management (IPAM) systems may contribute by handling the technical differences and automating 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 comprehensive measurement campaigns are providing up-to-date information. While performance is undoubtedly an important issue to consider and worth further investigation, the 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 Round-Trip Time (RTT) of IPv6 compared against IPv4. Both measures are based on scripts that employ the three-way handshake of TCP. As such, the measurement of the failure rate does not provide a direct measurement of packet loss (which would need an Internet-wide measurement campaign). That said, despite that 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, and Southern Asia) and countries (e.g., US, India, and Germany) with an advanced deployment of IPv6 (e.g., greater than 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 relate to 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 connection 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 Center, the connection is end to end, without translations. Instead, when using IPv4, there is a NAT translation either in the CPE 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] and [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 and 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 Media Access Control (MAC) address(es), which are easily readable in the original modified 64-bit Extended Unique Identifier (EUI-64) interface identifier format. On the other hand, stable IPv6 interface identifiers [RFC8064] were developed, and this can also affect privacy.

As reported in [ISOC3], in comparing IPv6 and IPv4 at the protocol level, one may probably conclude that the increased complexity of IPv6 will result 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. It is also worth mentioning that most vulnerabilities nowadays are caused by human beings and are in the application layer, not the IP layer.

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. The 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 how the 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]. [RFC3756] says to use IPsec, but it is impractical and not used; on the other hand, SEcure Neighbor Discovery (SEND) [RFC3971] is not widely available. It is worth mentioning that applying host isolation may address many of these concerns, as described in [ND-CONSIDERATIONS].

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

#### 5.4.1.1. 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. In particular, some security mechanisms may require processing the full chain of headers, and some firewalls may require filtering packets based on their extension headers. Additionally, packets with IPv6 extension headers may be dropped in the public Internet [RFC7872]. Some documents, e.g., [HBH-PROCESSING], [HBH-OPT-HDR], and [IPv6-EXT-HDR], analyze and provide guidance regarding the processing procedures of IPv6 extension headers.

Defense 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 [RFC5095]. In addition, it is worth mentioning that the 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. To mitigate this effect, the initial IPv6 header, the extension headers, and the upper-layer header must all be in the first fragment [RFC8200]. Also, the use of the IPv6 fragment header is forbidden in all Neighbor Discovery messages [RFC6980].

The fragment header is used by the IPv6 source node to send a packet bigger than the 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 the last fragment (to discard), and atomic fragments (to be isolated).

The operational implications of IPv6 packets with extension headers are further discussed in [RFC9098].

## 6. IANA Considerations

This document has no IANA actions.

## 7. 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.

## 8. References

### 8.1. Normative References


[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, ., 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>.

[RFC9313] Lencse, G., Palet Martinez, J., Howard, L., Patterson, R., and I. Farrer, "Pros and Cons of IPv6 Transition Technologies for IPv4-as-a-Service (IPv4aaS)", RFC 9313, DOI 10.17487/RFC9313, October 2022, <https://www.rfc-editor.org/info/rfc9313>.

## 8.2. Informative References

[Akm-stats] Akamai, "IPv6 Adoption Visualization", 2023, <https://www.akamai.com/uk/en/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization>.

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

[ANSI] ANSI, "Host and Router Profiles for IPv6", ANSI/CTA 2048-A, October 2020, <https://shop.cta.tech/products/host-and-router-profiles-for-ipv6>.

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

[APNIC2] Huston, G., "IP addressing in 2021", January 2022, <https://blog.apnic.net/2022/01/19/ip-addressing-in-2021/>.

[APNIC3] Huston, G., "BGP in 2020 - The BGP Table", January 2021, <https://blog.apnic.net/2021/01/05/bgp-in-2020-the-bgp-table/>.

[APNIC4] Huston, G., "BGP in 2021 - The BGP Table", January 2022, <https://blog.apnic.net/2022/01/06/bgp-in-2021-the-bgp-table/>.

[APNIC5] APNIC Labs, "Average RTT Difference (ms) (V6 - V4) for World (XA)", <https://stats.labs.apnic.net/v6perf/XA>.

[APRICOT] Huston, G., "IPv6 Performance Measurement", February 2020, <https://2020.apricot.net/assets/files/APAE432/ipv6-performance-measurement.pdf>.

[ARCEP] ARCEP, "Proposant au ministre charg des communications lectroniques les modalits et les conditions d’attribution d’autorisations d’utilisation de frquences dans la bande 3,4 - 3,8 GHz", [Decision on the terms and conditions for awarding licenses to use frequencies in the 3.4  3.8 GHz band], Dcision n° [Decision No.] 2019-1386, November 2019, <https://www.arcep.fr/uploads/tx_gsavis/19-1386.pdf>.

[ARIN-CG] ARIN, "2020 ARIN Community Grant Program Recipients: IPv6 Security, Applications, and Training for Enterprises", 2020, <https://www.arin.net/about/community_grants/recipients/2020>.

[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", December 2021, <http://218.2.231.237:5001/cgi-bin/generate>.

[BGR_2] BIIGROUP, "China Government IPv6 and DNSSEC Deployment Monitor", December 2021, <http://218.2.231.237:5001/cgi-bin/generate_gov>.

[BGR_3] BIIGROUP, "China Education IPv6 and DNSSEC Deployment Monitor", December 2021, <http://218.2.231.237:5001/cgi-bin/generate_edu>.

[BIPT] Vannieuwenhuyse, J., "IPv6 in Belgium", September 2017, <https://www.ripe.net/participate/meetings/roundtable/september-2017/government-roundtable-meeting-bahrain-26-september-2017/presentations/belgium-experience-bahrain-roundtable.pdf>.

[CAIDA] Huston, G., "Client-Side IPv6 Measurement", June 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", March 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] Elkins, N., "Impact on Enterprises of the IPv6-Only Direction for the U.S. Federal Government", <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", November 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", (in Chinese), 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, "Government IPv6 and DNSSEC Statistics", 2022, <https://cnlabs.in/IPv6_Mon/generate_gov.html>.

[ComputSecur] Lencse, G. and Y. Kadobayashi, "Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64", Computers and Security, Volume 77, Issue C, pp. 397-411, DOI 10.1016/j.cose.2018.04.012, August 2018, <https://doi.org/10.1016/j.cose.2018.04.012>.

[Csc6lab] Cisco, "Display global data", 2023, <https://6lab.cisco.com/stats/>.

[EE] Heatley, N., "IPv6-only Devices on EE Mobile", January 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, "IPv6 Enhanced Innovation (IPE) Gap Analysis", ETSI GR IPE 001, V1.1.1, August 2021, <https://www.etsi.org/deliver/etsi_gr/IPE/001_099/001/01.01.01_60/gr_IPE001v010101p.pdf>.

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

[FB] "Paul Saab Facebook V6 World Congress 2015", YouTube video, 25:32, posted by Upperside Conferences, March 2015, <https://youtu.be/An7s25FSK0U>.

[GFA] German Federal Government Commissioner for Information Technology, "IPv6-Masterplan fr die Bundesverwaltung", [IPv6 Master Plan for the Federal Administration], November 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 Statistics", <https://www.google.com/intl/en/ipv6/statistics.html>.

[HBH-OPT-HDR] 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-04, 10 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-v6ops-hbh-04>.

[HBH-PROCESSING] Hinden, R. and G. Fairhurst, "IPv6 Hop-by-Hop Options Processing Procedures", Work in Progress, Internet-Draft, draft-ietf-6man-hbh-processing-07, 6 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-hbh-processing-07>.

[HxBld] HexaBuild, "IPv6 Adoption Report 2020: The IPv6 Internet is the Corporate Network", November 2020, <https://hexabuild.io/assets/files/HexaBuild-IPv6-Adoption-Report-2020.pdf>.

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

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

[IGP-GT] Kuerbis, B. and M. Mueller, "The hidden standards war: economic factors affecting IPv6 deployment", DOI 10.1108/DPRG-10-2019-0085, February 2019, <https://www.emerald.com/insight/content/doi/10.1108/DPRG-10-2019-0085/full/html>.

[INFOCOM] Doan, T., Bajpai, V., and S. Crawford, "A Longitudinal View of Netflix: Content Delivery over IPv6 and Content Cache Deployments", IEEE INFOCOM 2020, IEEE Conference on Computer Communications, pp. 1073-1082, DOI 10.1109/INFOCOM41043.2020.9155367, July 2020, <https://dl.acm.org/doi/abs/10.1109/INFOCOM41043.2020.9155367>.

[IPv6-EXT-HDR] 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://datatracker.ietf.org/doc/html/draft-bonica-6man-ext-hdr-update-07>.

[IPv6-ONLY-DEF] Palet Martinez, J., "IPv6-only Terminology Definition", Work in Progress, Internet-Draft, draft-palet-v6ops-ipv6-only-05, 9 March 2020, <https://datatracker.ietf.org/doc/html/draft-palet-v6ops-ipv6-only-05>.

[IPv6Forum] IPv6Forum, "Estimating IPv6 & DNSSEC External Service Deployment Status", 2023, <https://www.ipv6forum.com/IPv6-Monitoring/index.html>.

[ISIF-ASIA-G] India Internet Engineering Society (IIESoc), "IPv6 Deployment at Enterprises", March 2022, <https://isif.asia/ipv6-deployment-at-enterprises/>.

[ISOC1] Internet Society, "State of IPv6 Deployment 2018", June 2018, <https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/>.

[ISOC2] York, D., "Facebook News Feeds Load 20-40% Faster Over IPv6", April 2015, <https://www.internetsociety.org/blog/2015/04/facebook-news-feeds-load-20-40-faster-over-ipv6/>.

[ISOC3] Gont, F., "IPv6 Security Frequently Asked Questions (FAQ)", January 2019, <https://www.internetsociety.org/wp-content/uploads/2019/02/Deploy360-IPv6-Security-FAQ.pdf>.

[MAPRG] Bajpai, V., "Measuring YouTube Content Delivery over IPv6", IETF 99 Proceedings, July 2017, <https://datatracker.ietf.org/meeting/99/materials/slides-99-maprg-measuring-youtube-content-delivery-over-ipv6-00>.

[Mcrsft] Microsoft, "IPv6 for Azure VMs available in most regions", September 2016, <https://azure.microsoft.com/en-us/updates/ipv6-for-azure-vms/>.

[ND-CONSIDERATIONS] Xiao, X., Vasilenko, E., Metz, E., Mishra, G., and N. Buraglio, "Selectively Applying Host Isolation to Simplify IPv6 First-hop Deployment", Work in Progress, Internet-Draft, draft-ietf-v6ops-nd-considerations-00, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-

v6ops-nd-considerations-00>.

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

[NST_1] NIST, "Estimating Industry IPv6 & DNSSEC External Service Deployment Status", 2023, <https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com>.

[NST_2] NIST, "Estimating USG IPv6 & DNSSEC External Service Deployment Status", 2023, <https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov>.

[NST_3] NIST, "Estimating University IPv6 & DNSSEC External Service Deployment Status", 2023, <https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-edu>.

[Ntflx] Aggarwal, R. and D. Temkin, "Enabling Support for IPv6", July 2012, <https://netflixtechblog.com/enabling-support-for-ipv6-48a495d5196f>.

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

[POTAROO2] POTAROO, "IPv6 Resource Allocations", March 2023, <https://www.potaroo.net/bgp/iso3166/v6cc.html>.

[RelJio] Chandra, R., "IPv6-only adoption challenges and standardization requirements", IETF 109 Proceedings, November 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>.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007, <https://www.rfc-editor.org/info/rfc5095>.

[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", October 2016, <https://ripe73.ripe.net/wp-content/uploads/presentations/35-2016-10-24-v6-performance.pdf>.

[RIPE2] RIPE, "IPv6 Security", January 2023, <https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf>.

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

[TMus] Lagerholm, S., "Going IPv6 Only", June 2018, <https://pc.nanog.org/static/published/meetings/NANOG73/1645/20180625_Lagerholm_T-Mobile_S_Journey_To_v1.pdf>.

[US-CIO] Vought, R., "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)", March 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>.

[W3Techs] W3Techs, "Historical yearly trends in the usage statistics

of site elements for websites", 2023,
<https://w3techs.com/technologies/history_overview/
site_element/all/y>.

[WIPv6L] World IPv6 Launch, "Measurements", June 2022,
<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.

In this survey, 40 people, representing 38 organizations, provided responses. This appendix summarizes the results obtained.

Respondents' business:

| Convergent | Mobile | Fixed |
|---|---|---|
| 82% | 8% | 11% |

Table 10: Type of Operators

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

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

B. What are the reasons to do so?

C. When to start: already ongoing, in 12 months, or after 12 months?

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

Answers for 1.A (38 respondents)

| Yes | No |
|---|---|
| 79% | 21% |

Table 11: Plan to Move to IPv6 within 2 Years

| Mobile | Fixed | Enterprise | No Response |
|---|---|---|---|
| 63% | 63% | 50% | 3% |

Table 12: Business Segment

Answers for 1.B (29 respondents)

Even though 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.

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

* 4 respondents (13%) highlighted that there is a national regulation request to associate and enable IPv6 with the launch of 5G.

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

* 4 respondents (13%) introduced IPv6 because of enterprise customer demand.

Answers for 1.C (30 respondents)

| Ongoing | In 12 months | After 12 months | No Response |
|---|---|---|---|
| 60% | 33% | 0% | 7% |

Table 13: Timeframe

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

| Dual-Stack | 464XLAT | MAP-T | No Response |
|---|---|---|---|
| 39% | 21% | 4% | 36% |

Table 14: Transition in Use: Cellular

| Dual-Stack | DS-Lite | 6RD/6VPE | No Response |
|---|---|---|---|
| 59% | 19% | 4% | 19% |

Table 15: Transition in Use: Wireline

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

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

B. Will you start the transition of your metro, backbone, or backhaul network to support IPv6?

Answers for 2.A (30 respondents)

| Yes | No | No Response |
|---|---|---|
| 43% | 33% | 23% |

Table 16: Need to Change

| CPEs | Routers | BNG | CGN | Mobile core |
|---|---|---|---|---|
| 47% | 27% | 20% | 33% | 27% |

Table 17: What to Change

Answers for 2.B (22 respondents)

| Yes | Future | No |
|---|---|---|
| 9% | 9% | 82% |

Table 18: Plans for Transition

## 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/> in early 2021.

54 organizations provided answers.

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% |
| Website is IPv6 enabled | 7.41% |
| Most equipment is dual-stacked | 31.48% |
| Have an IPv6 transition plan for entire network | 5.56% |
| Running IPv6-only in many places | 20.37% |
| Entire network is IPv6-only | 0.00% |

Table 19: IPv6 Implementation

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% |

Table 20: Help/Classes from INTC

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% |

Table 21: Areas of Concern for IPv6 Implementation

## 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, Gbor 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.

## Contributors

Nalini Elkins
Inside Products
Email: nalini.elkins@insidethestack.com

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

## 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

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