ETSI White Paper No. 35

IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward

First edition – August 2020

ISBN No. 979-10-92620-31-1

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

Contributing organizations and authors

CAICT	Zhiruo Liu
China Telecom	Chongfeng Xie, Cong Li
Cisco	Patrick Wetterwald, Pascal Thubert, Francois Clad
Hewlett-Packard Enterprise	Yanick Pouffary
Huawei	Giuseppe Fioccola, Xipeng Xiao, Georgios Karagiannis, Shucheng(Will) Liu
KPN	Eduard Metz
Luxembourg University	Latif Ladid
Portugal Telecom	Jose Cananao, Jose Palma
Post Luxembourg	Sébastien Lourdez
Telefonica	Luis M. Contreras

Contents

Executive Summary

Over 1.2 billion Internet netizens are using IPv6 today without even knowing it. India has over 358 million IPv6 users with 60% penetration and China has over 200 million while the US has over 143 million. Brazil reached 50 million. Japan has 43 million and Germany has over 30 million. Some countries are topping 60% IPv6 penetration. The remaining 40% lies in the hands of the enterprise world to fulfil the complete adoption of IPv6 enabling the ultimate switch to IPv6-Only Internet, allowing thereby the deprecation of the IPv4 Internet as recommended recently by the US Government, reducing thereby the maintenance of two Internets. The management of the enterprises should look at reducing CAPEX and OPEX by studying the best practices of the top Internet technology enterprises that have already implemented IPv6-Only in-house with far greater benefits expected by the adoption of IPv6.

This White Paper focuses on the lessons learned from IPv6 best practices, use cases, benefits and deployment challenges and makes recommendations to ease adoption and motivate the industry in view of large-scale deployment of IoT, 4G/5G, IoT Cloud Computing benefiting from the restoration of the end-to-end model.

Since the ETSI ISG IP6 is reaching the end of its mandate, this is a perfect time to review and summarize the work achieved by this group and report in this whitepaper the main aspects of the deployment of IPv6.

The major findings of this White Paper are:

- IPv6 is becoming a priority, due the exhaustion of the IPv4 address space since 2010, for the Information and Communications Technology (ICT) industry, since technologies like 5G, cloud, IoT require its use, governments and standard bodies demand it, and the device – network – content communication value chain are calling for its adoption.
- IPv6 is growing faster than IPv4 in all measures including number of users, percentage of content, and amount of traffic. This testifies that the key Internet industry players have decided strategically to invest and deploy IPv6 in large-scale to sustain the Internet growth.
- IPv6 transition solutions for Mobile BroadBand (MBB), Fixed BroadBand (FBB) and enterprise services are ready. Dual-Stack is the recommended solution for IPv6 introduction, while 464XLAT and Dual stack Lite (DS-Lite) are recommended for IPv6-only service delivery.
- A large number of cloud service providers and operators have successfully deployed and used IPv6. A significant number of companies have started to move to or plan for an IPv6-only service delivery. Therefore, there is a need for an increased sharing of knowledge and experience in this area. Several practical guidelines for IPv6 deployment and IPv6 use cases are provided in this White Paper.
- Vertical applications such as autonomous vehicles, smart grid, industrial factory automation, process control, and building automation will greatly benefit from IPv6-enabled machine-to-machine communications. Over the last decade, Standards Development Organizations (SDOs) like the Internet Engineering Task Force (IETF), ETSI and International Electrotechnical Commission (IEC) have been developing new technologies that are specific to IPv6 for constrained environments, low-power radio communications and massive onboarding and security in many working groups dedicated to the IPv6 Internet of Things (IoT).

- IPv6 Enhanced Innovations for future technologies like 5G, Low-Power radios, SDN/NFV, Deterministic Networking, Cloud Computing, will greatly benefit the whole industry, in particular demand chain stakeholders (such as governments, end users, enterprises as well as Internet Service Providers/Network Operators) and also supply chain stakeholders (such as the Internet and Telecommunication vendors as well as vertical industry suppliers). Furthermore, IPv6 enables overlay techniques that abstract the underneath technologies and provide a continuous reliable service in virtualized environments at scale.

1 Background

1.1 Why should IPv6 become a priority again?

As 5G communications and Internet of Things (IoT) emerge in many industry verticals, a scalable IP technology is required with no constraint in number of addresses and no connectivity constraints. To serve those needs, the networking industry has initiated a global effort to transition to Internet Protocol version 6 (IPv6). For example, the Internet Architecture Board (IAB) at the Internet Engineering Task Force (IETF) issued in November 2016, an "IAB Statement on IPv6" [1], stating that "IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6". Similarly, 3GPP is considering mandating IPv6 in 5G Standalone (SA). In addition, major governments like those of the USA and China will issue new policies and requirements for IPv6 [OMB][APNIC_2]. Since the end of 2017, the Chinese government has strongly pushed forward the development of IPv6 nationwide, and great progress has been made thanks to the involvement of Chinese operators. IPv6 connectivity services are now provided to Chinese customers, and the total amount of IPv6 users dramatically increased: there are now 330 million IPv6 users in China, as per the latest China Academy of Information and Communications Technology (CAICT) statistics of 2019.

Some people may still want to ask the classic question: "Users do not care about IPv4 or IPv6, and migrating to IPv6 involves a lot of cost and difficulties, so why should we do it now"?

The short answer is: IPv6 is growing faster than IPv4, in all measures such as number of users, percentage of content, and amount of traffic. This means that despite all the doubt, cost and difficulties, the collective wisdom of the networking industry has selected IPv6 for the future.

Moreover, it is worth noting that, the "device – network – content" communication chain is now ready for IPv6. This is different from the last wave of the IPv6 deployment campaign around 2011 that was triggered by Regional Internet Registries (RIRs) running out of IPv4 addresses. Devices and content were not IPv6 ready at that time, but they are ready now. Therefore, when operators move more subscribers to use IPv6, they can immediately profit from several IPv6 benefits, e.g. reducing Capital Expenses (CAPEX) and Operational Expenses (OPEX), by eliminating Network Address Translation (NAT)/ Carrier Grade NAT (CGNAT) tax and the complexity it brings forth.

Several stakeholders, such as governments, end users, enterprises and as well Internet service providers/operators are considering deploying and/or applying IPv6. Once deployed, IPv6 can open the door to new opportunities in network operations & management and to offer enhanced services. It is expected that IPv6 can become unavoidable and the value of IPv4 assets (about $20 per IP) can be repurposed.

This White Paper will elaborate on this point and provide pragmatic recommendations about IPv6 implementation and transition techniques, and IPv6 transition and operation strategy.

In particular, this White Paper focuses on the IPv6 adoption and shows how the IPv6 deployment and use, has increased in the last 5 years. IPv6 is in a key stage of deployment, and since ETSI ISG IP6 is reaching the end of its journey, this is a perfect time to review the work achieved by this group and report in this White Paper the main aspects of the IPv6 technology.

After providing a short overview of the ISG IP6 work, see Annex 1, emphasis will be provided to

1) the IPv6 progress in the last 5 years,

2) the IPv6 service design for Mobile BroadBand (MBB), Fixed BroadBand (FBB) and enterprises,

3) IPv6 transition solutions from operator's perspective,

4) IPv6 network operations,

5) examples of advanced industry applications of IPv6,

6) IPv6 use cases from the real world,

7) IPv6 enhanced innovation and the way forward and finally recommendations towards ETSI and Industry.

1.2 Goals of this White Paper

The target audience of this White Paper is the whole IPv6 ecosystem, particularly operator personnel, vertical industries and enterprise personnel that are planning to deploy IPv6 in their network infrastructures. Besides answering the important question of "why IPv6 should be a renewed priority now", this White Paper focuses on the following goals:

- To review the work achieved by the ETSI ISG IP6.
- To present the progress of IPv6 over the past 5 years, from various standpoints – user devices, networks, contents, etc.
- To discuss the IPv6 design, deployment and management options, along with a few recommendations drawn from operational experience.
- To elaborate on IPv6 benefits, and how IPv6 can contribute to shape the future of IP networks and services.

Even though IPv6 standards have been ratified for a long time, the level of features implementation is not universal, but the reality is that there are many practical challenges and issues which may arise. This White Paper also documents common challenges and issues one may encounter while deploying IPv6, and how those challenges and issues have been addressed by others. The knowledge and experience from these IPv6 deployment best cases can be used as practical guidelines during the IPv6 deployment process.

Networking field is in constant evolution, and now core technologies such as wireless, virtualization and cloud fabrics were not as mature or even did not exist when IPv6 was initially introduced, in the mid-1990s. Since then, IPv6 has evolved, and keeps evolving, to meet the new challenges as they arise. New technologies are introduced at the IETF with a strong focus for security and backward compatibility that enables new IPv6 capabilities to be deployed over legacy infrastructures. This is how IPv6 prepares for the future while respecting the past of existing technologies, deployed networks and human skills as a continuous development. Although, it is important to be mentioned that the IAB at the IETF issued in

November 2016, an “IAB Statement on IPv6” [1], stating that “IETF will stop requiring IPv4 compatibility in new or extended protocols”.

2 IPv6 progress in the last 5 years

Before focusing on the IPv6 progress in the last 5 years, a short overview of the ETSI ISG IP6 work will be provided. More details are given in Annex 1. The ISG IP6 documents published by the ETSI ISG IP6 are:

- IPv6 Deployment in the Enterprise (see ETSI GR IP6 001 V1.1.1 [IP6-1]);
- Generic migration steps from IPv4 to IPv6 (see ETSI GR IP6 006 V1.1.1 [IP6-2]);
- IPv6-based Internet of Things Deployment of IPv6-based Internet of Things (see ETSI GR IP6 008 V1.1.1 [IP6-3)];
- IPV6-based Industrial Internet Leveraging 6TISCH Technology (see ETSI GR IP6 009 V1.1.1 [IP6-4]);
- IPv6-based SDN and NFV; Deployment of IPv6-based SDN and NFV (see ETSI GR IP6 010 V1.1.1 [IP6-5]);
- IPv6-Based 5G Mobile Wireless Internet; Deployment of IPv6-Based 5G Mobile Wireless Internet (see ETSI GR IP6 011 V1.1.1 [IP6-6]);
- 6TiSCH Interoperability Test Specifications (see ETSI GR IP6 017 V1.1.1 [IP6-7]).

The remainder of this section describes IPv6 progress in the last 5 years in terms of:

- Devices supporting IPv6
- Content (web sites, cloud services) supporting IPv6
- Networks supporting IPv6
- Number of IPv6 users
- Amount of IPv6 traffic
- IPv6 standardization progress

The above listed topics cover the end-to-end IPv6 communication chain. The takeaway of this section is IPv6 is growing fast in every major aspect (user devices, networks, contents), and more importantly, IPv6 is growing much faster than IPv4.

2.1 Devices supporting IPv6

All the Operating Systems (OS) for hosts support IPv6. Most CPEs also support IPv6, in particular:

- Mobile devices (e.g., the UEs) support Dual-Stack and 464XLAT, which represents the combination of stateful and stateless translation and is one of the most popular IPv6 transition techniques for Mobile Broadband, see also ETSI GR IP6 011 V1.1.1 [IP6-6];

- Fixed CPEs use to support Dual-Stack, Dual stack Lite (DS-Lite) and IPv6 Rapid Deployment (6RD) as required by [RFC 7084] "Basic Requirements for IPv6 Customer Edge Routers", see also ETSI GR IP6 006 V1.1.1 [IP6-2]. But since May 2019, [RFC 7084] has been updated by [RFC 8585]. Therefore, other useful transition techniques like 464XLAT must also be supported on new fixed CPEs;
- Enterprise CPEs support Dual-Stack and other IPv6 transition techniques, see ETSI GR IP6 001 V1.1.1 [IP6-1] and ETSI GR IP6 006 V1.1.1 [IP6-2].

Operators could combine the IPv6 upgrade of deployed CPEs with other CPE upgrade opportunity/necessity (e.g. for a new user) and select the most efficient IPv6 transition technique that satisfy their needs and requirements.

2.2 Content (web sites, cloud services) supporting IPv6

Figure 1 is based on [W3Tech] and it shows that the percentage of content (represented by websites) supporting IPv6 is increasing from 5% in January 2015 to 15% in January 2020.

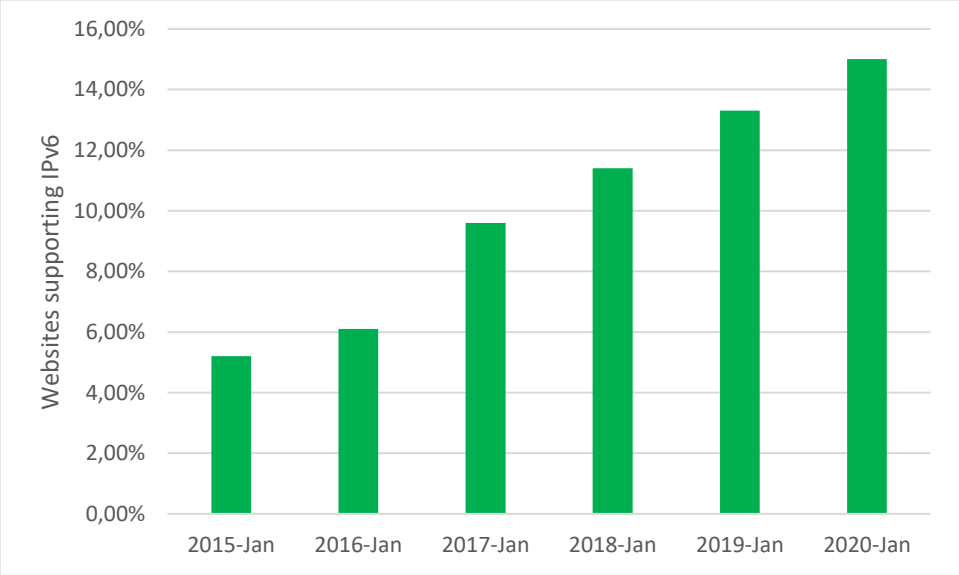

Figure 1: Percentage of websites supporting IPv6 (CAGR 24%), based on [W3Tech]

The Compound Annual Growth Rate (CAGR) is impressive at 24% for websites supporting IPv6. Although 15% of websites supporting IPv6 in January 2020 may seem low, it should be noted that a big website generates a lot more content and traffic than a small website, and because the biggest content providers have all enabled IPv6, the percentage of IPv6-reachable content is much greater than 15%, and is growing fast. Indeed, several operators with Dual-Stack deployment report that 40-50% of their traffic is IPv6 (see

Operator 1 in the “Use Case” section). Therefore, it can be concluded that 40-50% of the overall content is IPv6.

2.3 Networks supporting IPv6

Table 1 is based on [POTAROO] and shows the percentage of ASes supporting IPv6 increases from 21.1% in January 2015 to 27.5% in January 2020. This equals to 15.19% CAGR for IPv6 enabled networks. This also shows that the number of networks supporting IPv6 is growing much faster than the ones supporting IPv4, since the total (IPv6 and IPv4) networks grow at 9.23% CAGR.

Table 1: Percentage of ASes supporting IPv6, based on [POTAROO]

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

2.4 Number of IPv6 users

Figure 2 is based on [APNIC_1] and shows the growth of the number of IPv6 Users for some countries, from January 2015 to January 2020. In particular, the CAGR for India is at 413.70%, for Brazil the CAGR is at 226.90%, for USA, the CAGR is at 33.90% and for Japan, the CAGR is at 31.20%.

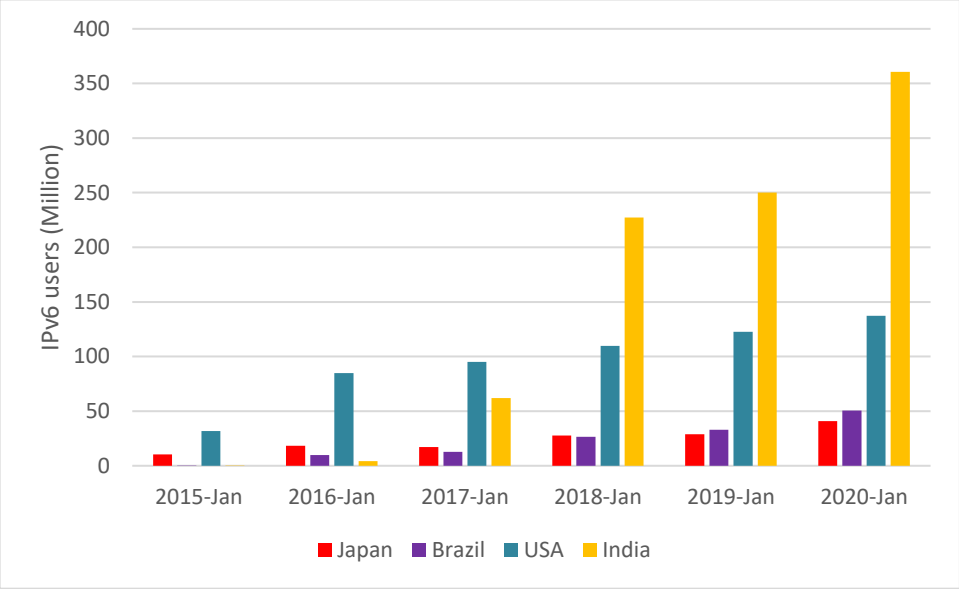

Figure 2: Number of IPv6 users for some countries (Million), based on [APNIC_1]

Table 2 is based on [APNIC_1] and it shows that worldwide, the percentage of IPv6 users (i.e., IPv6/total ratio) grows from 3.22% in January 2015 to 24.33% in January 2020, at a 67.9% CAGR. At the same time, the total number of users (IPv6 + IPv4) grows at a 12% CAGR. Therefore, it can be concluded that the number of IPv6 users is growing much faster than the number of IPv4 users.

Table 2: Number of IPv6 users worldwide (Million), based on [APNIC_1]

worldwide users	2015-Jan	2016-Jan	2017-Jan	2018-Jan	2019-Jan	2020-Jan	**CAGR**
IPv6 users	74.24	179.42	290.68	513.68	574.02	989.25	**67.90%**
Total user	2303.09	3246.15	3339.37	3410.28	3470.37	4065.21	**12.00%**
% IPv6 user	3.22%	5.53%	8.70%	15.06%	16.54%	24.33%	

2.5 Amount of IPv6 traffic

Statistics about IPv6 traffic are scarce as most operators do not publish such statistics. However, from the few operators that disclosed their IPv6 traffic, it can be deduced that the IPv6 traffic is growing faster than the IPv4 traffic, see as well ETSI GR IP6 006 V1.1.1 [IP6-2] and ETSI GR IP6 011 V1.1.1 [IP6-6].

- Operator 1 in the "IPv6 Use Cases in the Real World" section reported that IPv6 traffic in their network is 25% in 2018, 32% in 2019, and 40% in 2020.

- Operator 3 in the same section, reported that IPv6 grew from 0% in mid-2018 to about 7% in late 2019.

2.6 IPv6 standardization progress

In the last 5 years, ETSI IP6 ISG published 7 Group Reports (GRs), which are briefly introduced in Annex 1.

Furthermore, it is important to note that the IAB at the IETF issued in November 2016, an "IAB Statement on IPv6" [1], stating that the "IETF will stop requiring IPv4 compatibility in new or extended protocols". Future IETF protocol work will then optimize for and depend on IPv6".

The IETF focuses on IPv6 enhancements, in the following working groups:

- IPv6 over Networks of Resource-constrained Nodes (6lo) WG, to enable IPv6 connectivity over constrained node networks
- Low-Power Wide-Area Network (LPWAN) WG, to enable IPv6 connectivity over extremely constrained Low-Power Wide-Area technologies
- 6TiSCH WG, to enable IPv6 over Time-slotted Channel Hopping (TSCH) for industrial applications.
- Routing Over Low power and Lossy networks (ROLL) WG that designs the RPL routing protocol for scalable IPv6 IoT.

In addition, the following three IETF working groups are involved in the documentation of IPv6 management procedures and protocols:

- Source Packet Routing in Networking (Spring) WG, focusing on Segment Routing (SR) and SRv6 standardization.
- IPv6 maintenance (6man) WG, whose works include: (1) updated version of the IPv6 specification [RFC 8200]; (2) 16 RFCs (since 2015) reviewing the basic components of the IPv6 protocols (e.g. fragments, MTU, headers, node requirements, etc.).
- v6ops WG: improvement of already available mechanisms, such as 464XLAT and SLAAC. It also develops guidelines for the deployment and operation of new and existing IPv6 networks.

3 IPv6 service design for Mobile, Fixed broadband and enterprises

Based on discussions with several operators, it was observed that the following information was used during the process of rolling out IPv6 services for MBB (Mobile broadband), FBB (Fixed broadband) and enterprises:

- The IPv6 service design
- The deployment strategy, and
- The service and network operations

This section discusses

1) the IPv6 service design, with focus on the transition solution, i.e. NAT (Network Address Translation) issues,

(2) the IPv6 prefix and address assignment at the CPEs,

(3) IPv6 packet transport are also part of the IPv6 service design. More Details related to the latter two topics are provided in Annex 2.

In the next section we take an operator-centric perspective. In particular, when describing IPv6 for enterprise, the focus is on how operators provide IPv6 services for enterprises (WAN side). The introduction of deploying IPv6 inside enterprise networks (LAN side) is provided in the subsection entitled "IPv6 deployment inside enterprise networks".

3.1 IPv6 transition solutions from operator perspective

As emphasized in ETSI GR IP6 006 V1.1.1 [IP6-2], there are several IPv6 transition solutions available, see Annex 1 also. In particular, ETSI GR IP6 006 V1.1.1 [IP6-2] classifies these IPv6 transition solutions in two groups: (A) the IPv4 to IPv6 transition technologies used to provide IPv6 connectivity and (B) IPv4 to IPv6 transition technologies used for providing IPv4 connectivity.

The IPv4 to IPv6 transition technologies used to provide IPv6 connectivity, mentioned in ETSI GR IP6 006 V1.1.1 [IP6-2] are:

(1) Dual-Stack,

(2) Configured tunnels (6in4),

(3) Generic Routing Encapsulation (GRE),

(4) IPv6 Rapid Deployment (6rd),

(5) Native IPv6 behind NAT44 CPEs (6a44),

(6) Intra-Site Automatic Tunnel Addressing Protocol (ISATAP),

(7) Connection of IPv6 Domains via IPv4 Clouds (6to4),

(8) Tunneling IPv6 over UDP through NATs (Teredo),

(9) IPv6 over IPv4 without Explicit Tunnels (6over4),

(10) Anything In Anything (AYIYA),

(11) IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP).

The IPv4 to IPv6 transition technologies used for providing IPv4 connectivity, described in ETSI GR IP6 006 V1.1.1 [IP6-2] are:

(1) Stateless IP/ICMP Translation Algorithm (SIIT),

(2) Stateful NAT64,
(3) Combination of Stateful and Stateless Translation (464XLAT),
(4) Dual-Stack Lite (DS-Lite),
(5) Mapping of Address and Port – Encapsulation (MAP-E),
(6) Mapping of Address and Port – Translation (MAP-T).

Selecting the right IPv6 transition solution can be complex. It is unrealistic to assume that all these technologies will be widely adopted. The choice of the IPv6 transition solution depends on several factors, usually driven by market and applied policy.

In addition to the two groups of IPv6 transition solutions introduced in ETSI GR IP6 006 V1.1.1 [IP6-2], this whitepaper provides as well a classification based on the two stages (see also [RFC 6036], [RFC 7381]) of an IPv6 transition process: (1) *IPv6 introduction* and (2) *IPv6-only*. Note that both those IPv6 transition process stages are related to service delivery perspective and not to a network underlay perspective.

The *IPv6 introduction* stage is to enable the deployment of an IPv6 service in an originally-IPv4 network. IPv6 services are delivered on top of or alongside IPv4 service. With an IPv4/IPv6 dual-stack pattern, this stage is to gain experience with IPv6. In this stage, the IPv6 traffic volume is assumed to start small compared to IPv4 traffic, depending on the available IPv6 content. Even in this stage, it is expected that over time, the IPv6 traffic volume will gradually increase.

When the IPv6 traffic increases to a certain limit then a move to the IPv6-only stage can take place, where the service for subscribers is delivered solely on IPv6. This means that the CPE has only an IPv6 address at the WAN side and uses an IPv6 connection to the operator gateway, e.g. Broadband Network Gateway (BNG) or Packet Gateway (PGW) / User Plane Function (UPF). However, the hosts and content servers can still be IPv4 and/or IPv6. For example, NAT64 can enable IPv6 hosts to access IPv4 servers. The backbone network underlay can also be IPv4 or IPv6. The service delivery architecture is purely IPv6, at least for the access part, and IPv4 services are provided over IPv6.

Note that when to switch from IPv6 introduction to IPv6-only can be a complex decision that depends on several factors, such as economic factors, policy and government regulation.

The two IPv6 transition stages are described in more details in the following subsections. However, it is worth mentioning that in some scenarios (e.g. MBB) IPv6-only stage could be more efficient from the start since the IPv6 introduction phase with Dual-Stack may consume more resources (for example CGNAT costs).

3.1.1 For IPv6 introduction

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

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

[RFC 7381] recommends that: "dual-stack when you can, tunnel when you must". Dual-Stack is more robust, and easier to troubleshoot and support. Based on information provided by operators it can be stated that Dual-Stack is currently the most widely deployed IPv6 solution, for MBB, FBB and enterprises,

accounting for about 50% of all IPv6 deployments, see Figures 3 & 4 and the information given in [RESEARCH]. Therefore, for operators that are willing to introduce IPv6 it is recommended to apply the Dual-Stack transition solution. Note that the actual deployment strategy is further discussed in the "Deployment and Operations" subsection.

Although the Dual-Stack IPv6 transition is a good solution to be followed in the IPv6 introduction stage, it does have few disadvantages in the long run (as described in the "deployment and operations" section). Therefore, when IPv6 increases to a certain limit, it is recommended to switch to the IPv6-only stage.

3.1.2 For IPv6-only service delivery

This section discusses the possible IPv6-only transition solutions, and the process of selecting one of them to fit the need.

[LMHP-V6OPS] discusses and compares the technical merits of the most common transition solutions for IPv6-only service delivery, 464XLAT, DS-lite, Lightweight 4over6 (lw4o6), MAP-E, and MAP-T, but without providing an explicit recommendation.

Based on discussions with operators and experts the following recommendations on the selection of IPv6 transition technologies are provided.

Figure 3 and Figure 4 are based on the documents referenced in [RESEARCH] and show that, besides Dual-Stack, the most widely deployed IPv6 transition solution for MBB is 464XLAT, see Figure 3, and for FBB is DS-Lite, see Figure 4, both of which are IPv6-only solutions.

ISP (name)	Country	Transition Mechanism (NAT64/464xlat, 6rd, DS-Lite, Dual Stack, ...)	Network Type (mobile, DSL, fiber, cable, satellite,...)
	US	?	Mobile
	BT	Dual Stack	Mobile
	GB	464XLAT	Mobile
	TT	Dual Stack	Mobile
	DE	464XLAT, NAT64	mobile (2G,3G,4G)
	DE	Dual Stack	mobile (2G,3G,4G)
	EE	dual stack	mobile
	TW	Dual Stack	Mobile
	VN	dual stack	LTE
	NO	Dual stack	3GPP
	FR	Dual-stack	Mobile
	PL	464XLAT	Mobile
	IN	464XLAT	Mobile
	CA	NAT64/464XLAT	Wireless
	US	464XLAT	mobile
	US	464XLAT, NAT64	mobile
	SE	Dual stack	3GPP
	AU	464XLAT	mobile
	DK,SE	Dual stack	3GPP
	US	Dual-stack	mobile

Figure 3: IPv6 solutions deployed in MBB

ISP (name)	Country	Transition Mechanism (NAT64/464xlat, 6rd, DS-Lite, Dual Stack, ...)	Network Type (mobile, DSL, fiber, cable, satellite,...)
	DK,NO	6RD	Fibre
	US	6rd	AT&T Old PPPoE ADSL
	US	Native IPv6 (Dual Stack)	802.1x "IPDSL" over
	CH	DS-Lite	DOCSIS
	US	Dual Stack MAP-T (EFT)	DOCSIS
	US	dual stack	DOCSIS
	CR	Dual-stack	Docsis, Fiber, GPON
	DE	Dual Stack	dsl/vdsl
	IE	dual stack	VDSL2 & FTTH
	GR	Dual-Stack, DS-Lite	DSL
	NO	Dual stack	DOCSIS
	TW	Dual stack	VDSL, FTTH
		dual stack, DS-Lite	fibre?
	DE	DS-Lite	DOCSIS
	DE	Dual Stack and NAT64	WIFI
	DE	DS-Lite	DSL/FTTB
	MA	Dual-Stack	Fiber
	UA	dual stack	fibre, ETTH
	DE	Dual Stack	DSL
	CZ	DS-Lite	DSL
	ES	dual stack, DS-Lite	fibre
	FR	Dual-stack	ADSL, VDSL, Fibre
	PL	DS-Lite	DSL and fibre
	SK	DS-Lite	DSL
	GR	Dual-stack / lw4o6	xDSL
	BE	dual stack	DSL
	DE	DS-Lite	DOCSIS
	AR	Dual stack	DOCSIS, GPON
	RO	Dual Stack	FTTH
	IN	MAP-T, Dual-stack	DOCSIS
	UK	Dual Stack	DSL + Fibre
	CH	6rd	DSL and fibr
	AT	DS-Lite	mostly DOCSIS
	CZ	Dual-stack	DSL
	SI	Dual Stack	xDSL/FTTH/GPON/P2P
	BE	dual stack	DOCSIS
	NO	Dual stack	GPON, DOCSIS, xDSL, 3GPP
	EE	dual stack	DSL/FTTH
	DE	Dual Stack	xDSL/FTTH/GPON/P2P
	DE	DS-Lite	DOCSIS
	CZ	DS-Lite	DOCSIS
	RO	DS-Lite	DOCSIS
	HU	DS-Lite	DOCSIS
	PL	DS-Lite	DOCSIS
	SK	DS-Lite	DOCSIS
	IE	DS-Lite	Docsis
	NL	DS-Lite	Docsis

Figure 4: IPv6 solutions deployed in FBB

Based on discussions with operators and experts the following recommendations are provided for the selection of the transition solution:

- If CPEs support 464XLAT, then use 464XLAT; this holds for MBB, FBB and enterprises.
- For the situations that FBB and enterprise CPEs do not support 464XLAT, then DS-Lite can be considered as the second-best choice.

The rationales of deriving the above listed recommendations are elaborated below.

First, for MBB, the IPv6 hosts (e.g. the Apps on the UE) behind the IPv6-only CPE (i.e. the User Equipment (UE) itself) can natively access IPv6 websites or services. However, in order to access IPv4 websites, NAT64 and DNS64 are needed. NAT64 [RFC 6146] is needed to accomplish the translation. DNS64 [RFC6147] is likely needed too, assuming DNS queries are required, see Figure 5. Note that Figure 5 shows how an IPv6-only host accesses an IPv4 website.

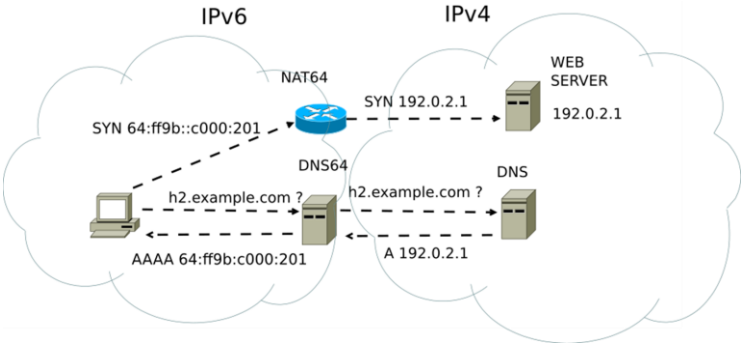

Figure 5: NAT64 + DNS64: how they work (from Wiki)

Second, NAT64 + DNS64 is not sufficient for all scenarios. For example, when an IPv6-only UE is serving as a hotspot, some tethering devices may only support IPv4. To support such IPv4 hosts behind an IPv6-only CPE, 464XLAT [RFC 6877] is a suitable choice, because 464XLAT consists of a client side NAT46 (CLAT) at the CPE and a provider side NAT64 (PLAT), see Figure 6. PLAT is identical to the one described in the first case, while CLAT at the CPE can translate the IPv4 traffic from the IPv4 hosts into IPv6 traffic. So with 464XLAT, this second scenario effectively becomes the first scenario. At the provider side, NAT64 is the only NAT, and both IPv4 and IPv6 hosts behind the IPv6-only CPE will work, for any kinds of websites.

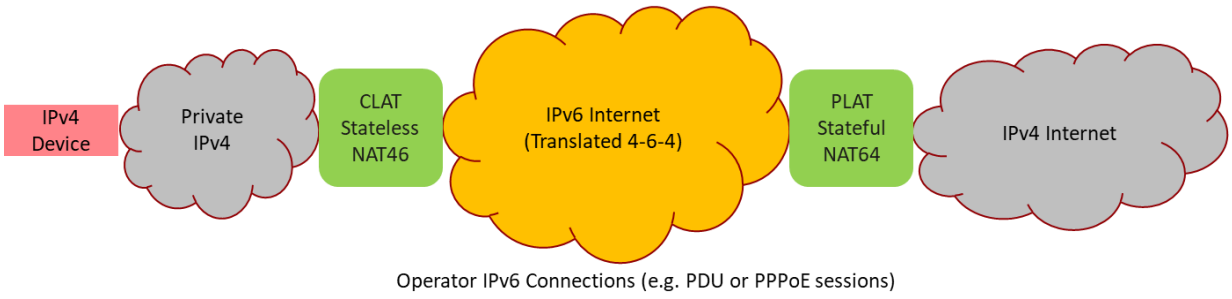

Figure 6: Overview of the 464XLAT

Note that most of the mobile UE OSes support the client part of 464XLAT (provider part of 464XLAT is not relevant to mobile OSes). Furthermore, according to [LMHP-V6OPS], mobile OSes generally do not support other IPv6-only transition solutions. Consequently, 464XLAT can be considered to be effectively the only IPv6-only solution for MBB.

For FBB and enterprises, if the CPEs support 464XLAT, in particular CLAT, then it is the recommended IPv6-only solution. In this way MBB, FBB and enterprises can apply the same solution, and NAT64 will be the only NAT. This can simplify network operations and management and reduce OPEX.

However, it is important to be mentioned that according to [RFC 7084] the required IPv6 transition solutions are Dual-Stack, DS-lite and 6RD. Meaning that there are retail fixed CPEs that are not required to support 464XLAT. In May 2019, [RFC 8585] updated [RFC 7084] that requires the support of other IPv6-only transition solutions, including 464XLAT. This means that for operators who would need to deploy an IPv6-only solution for FBB and enterprises in the future, 464XLAT can be the first option to consider.

If the operators' CPEs do not support 464XLAT, then the DS-Lite IPv6 transition solution is a viable alternative. It is important to mention that many existing fixed IPv6-only deployments use DS-Lite, possibly due to the fact that DS-Lite was the first IPv6-only transition solution that was published, indeed DS-Lite [RFC 6333] was published in Aug. 2011, while 464XLAT [RFC 6877] was published in April 2013. Figure 7 provides an overview of the DS-Lite architecture. The IPv6 traffic will be transported natively; IPv4 traffic will be tunneled from Basic Bridging Broadband (B4) to Address Family Transition Router (AFTR), where traffic will be decapsulated and NATted. The solution is comparable to 464XLAT in terms of technical merit, but it is different from the IPv6-only solution used for MBB. This could mean that operators will need to deploy two different NATs, NAT64 for MBB and NAT44 for FBB.

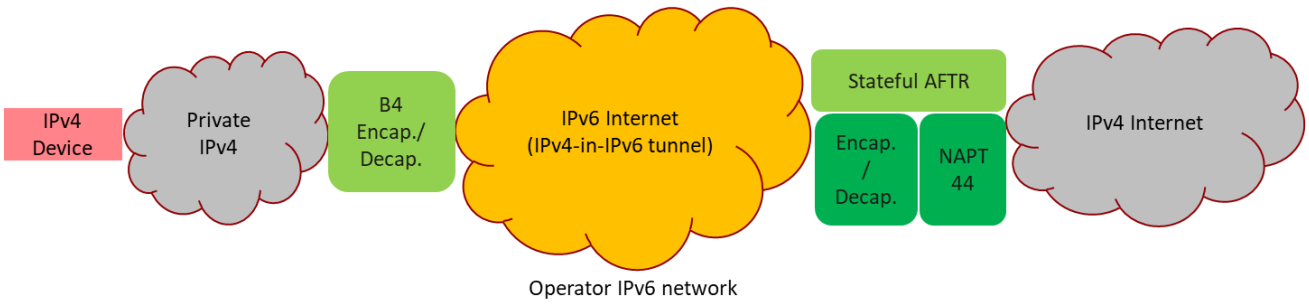

Figure 7: Overview of DS-Lite architecture

Based on the above discussion we recommend Dual-Stack as the IPv6 transition solution for IPv6 introduction in the early-stage, and 464XLAT / DS-Lite for the IPv6-only service delivery.

Note that MAP-E and MAP-T have clear technical merit for the FBB scenario, but they are rarely deployed (see Figures 3 and 4).

During the process of applying the selected IPv6 transition solutions, some common issues can be encountered. Based on discussions with operators and experts the following common issues and their solutions are identified:

- Issue_1: DNSSEC (DNS security) aware hosts may consider DNS64 AAAA records tampered and reject them, because DNS64 indeed change the destination's A record (IPv4) into an AAAA record (IPv6)
    - Solution: Any security-aware host must also be upgraded to be translation-aware and the DNS64 function should be accomplished locally. In addition, the host needs to be able to learn the WKP (Well-Known Prefix) or the right NSP (Network-Specific Prefix) in order to use NAT64 [RFC7051].
- Issue_2: NAT64 deployment may cause website providers/suppliers to deduce that there is no need for websites to support IPv6.
    - Solution: End to end IPv6 avoids NAT and therefore, websites can profit from reduced latency, see ETSI GR IP6 011 V1.1.1 [IP6-6], and should upgrade to IPv6. According to ETSI GR IP6 011 V1.1.1 [IP6-6], it can be observed that for all four USA mobile network operators:
        - Round Trip Time (RTT), DNS lookup Webpage Page Load Time (PLT) experiments on Content Delivery Network Provider 1's content delivery infrastructure show that IPv6 based mobile networks outperform IPv4 based mobile networks deployed by the same cellular mobile network operator.

          Content Delivery Network (CDN) RTT performance for mobile content can be improved when IPv6 networks are used, due to the fact that in-path middle-boxes for IPv6 address translation deployed by cellular carriers are not anymore needed

3.2 IPv6 prefix and address assignment at the CPEs

One of the key differences between the IPv6 prefix and address assignment from the IPv4 prefix and address assignment at the CPE is the possibility to use SLAAC (StateLess Address Auto Configuration) [RFC 4862] in IPv6. In IPv4, hosts must obtain IP addresses from a DHCP server. In IPv6, hosts generate the "interface identifier" (last 64 bits) of their IPv6 address by means of SLAAC. This was originally done by prepending a prefix to the 48-bit MAC address. In this way, hosts located on the same link can communicate with each other without a router or a DHCP server. If a router is available on the same link, then the hosts will also get a prefix from the router and prepend it to the interface identifier, to form a globally routable IPv6 address. The purpose of SLAAC is to enable plug-and-play feature.

Therefore, when acquiring IPv6 addresses for MBB, FBB and enterprise CPEs, the main difference from acquiring IPv4 address is the possibility to use SLAAC.

Annex 2 describes the details of the MBB and FBB IPv6 prefix and address assignment procedures, including message sequence charts.

Based on discussions with operators and experts the following IPv6 prefix and address assignment issues and solutions can be identified.

3.2.1 For MBB UEs

- Issue_3: In the case of a modem, Point-to-Point Protocol v6 (PPPv6) was used historically to connect modem (MT) and terminal (TE) and it was possible to transfer configuration parameters by using PPP. Currently, a non-PPP MT-TE connection is getting more popular for performance reasons.
    - Solution: Proprietary methods can be used to transfer parameters, such as Maximum Transmission Unit (MTU), DNS, default Gateway. Other approaches are supporting the TE to request such parameters using stateless DHCP. It is recommended to use standardized solutions for the MT-TE connection.

3.2.2 For FBB RGs

An FBB Residential Gateway (RG) may use PPP Over Ethernet (PPPoE) or Internet Protocol over Ethernet (IPoE) to establish connections to Broadband Network Gateway (BNG). This White Paper focuses, as example, only on the PPPoE approach.

The following IPv6 prefix and address assignment issues and solutions are identified.

- Issue_4: SLAAC is stateless – due to the fact that hosts do not inform the router when they join a LAN, router would not be aware of the IP addresses of new appearing hosts in time. The Initial traffic to unknown hosts could be dropped. This could happen even when the traffic is the response to the host's request
    - Solution: This can be solved by using the solution "Gratuitous Neighbor Discovery" (similar to IPv4 gratuitous ARP), proposed in [Linkova]. Please note however, that currently [Linkova] is an individual IETF draft.
- Issue_5: If any dynamic allocation for interface IDs is adopted, then the IPv6 address used for traceability need to be logged and maintained. Since these IP addresses contain dynamic interface IDs, this information has to be logged. Otherwise, if something unexpected occurs, it will not be possible to identify which IPv6 addresses have been applied.
    - Solution: Stateful DHCP is an efficient solution for such environment, as the IPv6 address for each host is logged.

3.2.3 For Enterprise CPEs

This section only discusses how an operator provides IPv6 addresses and prefixes to the enterprise CPEs. How to deploy IPv6 inside enterprise networks is discussed in ETSI GR IP6 001 V1.1.1 [IP6-1] and the "IPv6 deployment inside enterprise networks" section of this White Paper.

For Small and Medium Enterprises (SMEs) that connect to operators via Digital Subscriber Line (DSL) or Fiber to the X (FTTX), the IPv6 address and prefix assignment is exactly the same as in the FBB case. In this section we focus on larger enterprises whose CPEs connect to operator's PE routers via direct links (i.e. not a tunnel).

Enterprise CPEs' IPv6 addresses are manually configured. An enterprise with a single ISP may use IPv6 address space allocated from its provider. This is known as Provider Aggregable (PA). For larger enterprises (typically multi-homed to multiple providers), PA space will not be practical. They should apply directly to their Regional Internet Registry (RIR) for what is known as a provider-independent (PI) prefix allocation. This type of allocation comes with an annual operational cost.

3.3 IPv6 Packet Transport

After the subscriber CPEs acquire IPv6 addresses and the right NAT solutions are deployed, the end points can conceptually communicate with each other. But in reality, packets must be able to reach the destinations. To do so, one can either:

- Support Dual-Stack network to transport IPv6 & IPv4 packets natively, or
- Tunnel IPv6 packets over IPv4 or MPLS to a point where IPv6 packets can be natively transported again.

It is important to emphasize that:

- The choice between Dual-Stack and tunneling is applicable for the backbone networks. In mobile backhaul networks and fixed broadband metro networks, all packets from the users are encapsulated in GPRS Tunneling Protocol (GTP) or PPPoE tunnels (IPoE is not discussed in this White Paper). User traffic that can be IPv6 or IPv4 is invisible to such networks.

The above are key points associated with IPv6 packet transport. Below are some common issues encountered by operators and their suggested solutions:

- Issue_6: Tunneling typically results in a decrease of the Path-MTU. This, when coupled with the widespread dropping of Internet Control Message Protocol (ICMP) error messages leads to the so-called "black-holes", where packets are dropped without any reason reported.
    - Solution: reduce the Path-MTU, either by means of TCP Maximum Segment Size (MSS) "clamping" or use the IPv6 minimum MTU (1280 bytes) at the end-nodes.
- Issue_7: Extension headers of IPv6 could be very long. That could create a problem for Application-Specific Integrated Circuit (ASIC)-based Packet Forwarding Engines (PFEs). If PFEs are not capable of parsing up to TCP/UDP layer then several new features such as load balancing, filtering for security or QoS will not be able to support.
    - Solution: important to observe the "key buffer" length that is used for header parsing – if this is too large, it could create unresolvable problems even for small chain of extension headers. IPv6 is very demanding to ASICs.

3.4 IPv6 deployment inside enterprise networks

The previous section discussed operators providing IPv6 connectivity services for enterprises. This section discusses IPv6 deployment inside the enterprise networks.

ETSI GR IP6 001 V1.1.1 [IP6-1] provides guidelines and recommendations on IPv6 deployment in the enterprise. For more details see Annex 1. In particular, the provided guidelines and recommendations include the steps that need to be followed by Enterprises in order to deploy IPv6. These steps relate to:

(1) Transition deployment models,
(2) Enterprise Design Considerations - Building a cross functional team,
(3) Preparation and Assessment Phase,
(4) IPv6 address plan,
(5) Address Management and
(6) Routing considerations.

In addition, an example is provided on how these guidelines can be applied in IPv6 Data Centers. Other topics that are considered are (a) key elements that can be used to build an IPv6 Internet Presence in Enterprises and (b) Security;

One of the key derived conclusions is that there is no single recipe for IPv6 transformation. Each enterprise is unique and depends on its unique business goals, long-term vision and constraints. It is critical to put in place a joint Business & IT Task Force. This will help ensuring a smooth path toward IPv6. A pragmatic roadmap for an IPv6 transition, while also developing clear business benefits that can be achieved through the transition, is needed.

4 IPv6 deployment & operations

Existing infrastructure including CPEs, networks, and management systems are mostly based on IPv4. The IPv6 transition solutions discussed in the previous sections cannot be deployed overnight. Therefore, a practical deployment strategy is needed. In addition, it is important to be aware of how to operate the IPv6 network and services, since they need to be planned before the IPv6 services are deployed. These two topics are discussed in this section.

4.1 IPv6 deployment strategy

Multiple operators and [RFC 6036], [RFC 7381] provided many practical advices. The key points that can be applied as guidelines for IPv6 transition, are summarized below:

- Clearly separate IPv6 transition into 2 stages: (1) IPv6 introduction and (2) IPv6-only. These 2 stages have different purposes and require different solutions. IPv6 introduction is to gain experience with IPv6 and to accommodate future services, e.g. IoT, Vehicle to X (V2X). As previously discussed in this White Paper, Dual-Stack is generally the most suitable solution. In this stage, the IPv6 traffic may start low, compared to IPv4, but it will increase faster than IPv4. When

the IPv6 traffic increases to a certain limit then a move to the IPv6-only stage can take place, where service for subscribers is delivered solely on IPv6, so as to simplify network operations and to reduce CAPEX and OPEX. In this stage, the 464XLAT is likely the most suitable solution, although DS-Lite can be a viable alternative for FBB. It is notable that in some scenarios, the IPv6-only stage can be the starting point for subscribers' IPv6 service, e.g. in MBB, to speed up the IPv6 transition process and reduce costs.

- Align people and organization's views: switching services from IPv4 to IPv6 will affect many people and organizations inside companies and organizations. People may be reluctant to support changes they are not familiar with. Therefore, it is very important to communicate frequently in order to align people and organization's views. It is also important to provide training to relevant people so that they are open for the IPv6 transition.
- Audit IPv6 capability of the infrastructure: IPv6 affects all the components of any communication service chain, from the terminals to the websites, from the CPEs to the service platforms, from the user applications to the information system. Which devices already support IPv6, which devices need upgrade, must be carefully audited, and necessary upgrade must be planned and executed.
- Introduce IPv6 support together with other types of network upgrade to reduce cost. For example, when part of the network reaches its end-of-life status and needs to be replaced, IPv6 capabilities are to be supported by the replacing equipment.
- Use DNS as the switch to turn on/off IPv6 services for the end users, because the hosts decide whether to use IPv6 depending on the presence of IPv6 AAAA records from DNS queries.

Following the previous discussion, more information is provided regarding the costs and benefits of the IPv6 introduction stage and the IPv6-only stage.

4.1.1 IPv6 introduction stage

As discussed previously in this White Paper, it is recommended that organizations that have not yet introduced IPv6 start to introduce IPv6 by applying the Dual-Stack solution. The costs can be considered as being moderate while the benefits are clear:

- Cost
    - If IPv6 is introduced together with other network upgrade, the additional CAPEX is low.
    - With Dual-Stack, many parts of network management and IT systems can still work in IPv4. This avoids major upgrade of such systems to support IPv6, which is possibly the most difficult task in IPv6 transition. In other words, the cost and effort on the network management and IT system upgrade are moderate.
- Benefits
    - Accommodating future services: future services requiring IPv6 addresses, e.g., IoT or V2X, can be smoothly supported.

- Saving NAT cost: today, the biggest content and most of the CDN providers support IPv6. Moreover, hosts are mostly Dual-Stack enabled and can support IPv6. Therefore, when operators introduce Dual-Stack, a fairly large amount of traffic (40%-50%) can be IPv6, without requiring CGNAT. As CGNAT is expensive, with per Gbps cost that is 3-5 times of a router cost based on typical vendor pricing, the saving can be in the range of millions of dollars.

4.1.2 IPv6-only stage

Even though Dual-Stack is a good choice in the IPv6 introduction stage, it has some disadvantages in the long run:

- Dual-Stack will likely lead to duplication of several activities, once in IPv6 and another time in IPv4, in e.g. network operations (e.g. both IPv6 & IPv4 FCAPS) and legal interception. This might increase the CAPEX and OPEX.
- Dual-Stack increases the amount of state information in the network;
- Dual-Stack still requires IPv4 addresses to be assigned. In some cases, even when using private addresses, such as 10.0.0.0/8, the address pool is not large enough, e.g. for large mobile operators or large DCs with server virtualization.

However, transitioning to IPv6-only also has the following difficulties:

- The need to upgrade network management and IT systems to support IPv6. This may be one of the most difficult and time-consuming tasks during the whole IPv6 transition process, because network management and IT systems tend to have longer lifecycles than networks, and therefore are older and more difficult to upgrade;
- In IPv6-only stage, NAT64 will be used instead of NAT44. However, NAT64 can be generally more expensive than NAT44 based on current vendor pricing. Moreover, Internet providers and operators generally have more experience with NAT44 than with NAT64.

When the Dual-Stack disadvantages outweigh the IPv6-only complexity, it makes sense to transition to IPv6-only. This topic is for further study.

4.2 IPv6 Network Operations

The key tasks in IPv6 network operations serve three main purposes which can be consider as the Key Performance Indicators (KPIs) for Internet providers and operators: SLA, TTM & budget.

1. For SLA (service level agreement)
    a. IPv6 fault management: when there are network issues, new engineer skills and tools are needed to troubleshoot and solve the problems;
    b. IPv6 security management: IPv6 will introduce new security risks that make networks and services vulnerable. Such risks are to be analyzed and dealt with.

2. For TTM (time to market)
    a. IPv6 configuration: service delivery teams must be trained for IPv6; New service provisioning tools are needed;
    b. IPv6 accounting: new software (e.g., for new user identity information, new IPv6 MIBs) and new engineer skills;
    c. IPv6 performance monitoring: new software and skill training for people.
3. For budget (CAPEX & OPEX) compliance
    a. IPv6 may require new devices, and more state information in devices. Such CAPEX increase must be accounted for. However, IPv6 can be piggybacked (done in parallel) on equipment renewal and CAPEX should not be a big issue in this case;
    b. IPv6 introduces additional complexity in the networks during the transition period. Therefore, it will increase OPEX.

ETSI GR IP6 001 V1.1.1 [IP6-1] and [RFC 7381] focused on these key tasks, although from an enterprise perspective. We welcome operators' contributions on this topic.

The above are key points for IPv6 network operations. Below are some common issues encountered by operators and the suggested solutions. They are either contributed by operators or are extracted from a large number of RFCs and IPv6 white papers. They are put here in a single place for easier reference.

4.2.1 Security issues and solutions

The issues and solutions described in this section are based on discussions and contributions coming from operators and experts:

- Issue_8: the algorithm specified in [RFC 1858] can prevent an overlapping fragment attack on an upper-layer protocol (e.g., TCP) for IPv4 but not for IPv6. This is because the fragmentable part of the IPv6 packet can contain extension headers. Consequently, a malicious attacker can bypass a firewall using overlapping fragments. See [RFC 5722] for detail.
    - Solution: [RFC5722] updates the IPv6 specification to explicitly forbid overlapping fragments. In this way, the IPv6 nodes transmitting datagrams that need to be fragmented must not create overlapping fragments. When reassembling an IPv6 datagram, if one or more fragments are determined to be overlapping fragments, the entire datagram must be silently discarded. Implementing RFC 5722 will solve this issue.
- Issue_9: In order to decrease the probability of Denial of Service (DDoS) DDOS attacks, it is a common practice for IPv4 to filter out ICMP packets. Full ICMPv6 filtering is not possible, because it would break path MTU discovery and slow down all hosts.
    - Solution: Rate limit ICPMv6 messages that could not be filtered – see [RFC4890] for more details. Implementing RFC 4890 will solve this issue.
- Issue_10: "MAC address inserted into IP address" generate a list of associated security issues – see RFC 7721 [RFC7721] for problem discussion: correlation of activities, location tracking, address scanning, vendor-specific vulnerabilities exploitation.
    - Solution: a number of solutions exist: [RFC4941] (update in progress by [FGONT]) "periodically change the interface ID", [RFC3972] "cryptographically generated

addresses", [RFC7217] "semantically opaque", RFC 8064 "please, do not use stable ID!", Microsoft "random" (effectively RFC 4941, but without regeneration address over time), DHCPv6. RFC 7217 is probably the best choice, because it is stable, and can be easily configured on different subnets.

- Issue_11: DDOS attacks on Neighbor Discovery (ND) protocol, since the neighbor cache could be easily exhausted [RFC 6583]. Thus, could as well happen as a result of normal operation, for example: inventory system scan.
    - Solution: Vendors should limit resources for ND cache. Customers should test products (CPE, RG, Routers) to check that particular product is not vulnerable;
    - [RFC 8505] provides a proactive cache setup for IPv6 that prepares the ND cache at the router before it is needed. This avoids the gap that is introduced in IPv4 by the ARP lookup and in IPv6 by the ND Address Resolution, upon the first packet from the outside. If this method is generalized in the whole subnet, then the multicast lookup is no more used, and the ND/ARP cache DDOS attack vulnerability is eliminated.

4.2.2 OAM (Operations, Administration, and Maintenance)

The key point in this section is, most existing OAM tools already support IPv6, while new OAMs being defined by the IETF have not yet considered IPv6 support.

- Existing OAM tools (ping, traceroute, BFD, MPLS OAM, Pseudowire OAM, TWAMP, STAMP, ITU-T Y.1731, IEEE 802.1ag, IEEE 802.3ah, TCPDUMP, IPFIX, sFlow, mirroring) are fully compliant with IPv6 for more than a decade. Moreover, SRv6 OAM can be supported using legacy IPv6 OAM tools.

- New OAM tools such as iOAM [NTF], iFit [IFIT-FRAMEWORK], Alternate Marking [RFC 8321] [IPv6-ALT-MARK] are in the process of active development for the last few years. They touch data plane (especially iOAM/iFit), therefore some typical issues are anticipated. See [IFIT-FRAMEWORK] for details.

5 Examples of industry applications of IPv6

5.1 IIOT (Industrial IOT)

Converging Networks for the Industrial Internet

Operational Technology (OT) often refers to Industrial networks, which focus on highly reliable, secure and deterministic networking. In OT environments, deterministic networks are characterized as providing a guaranteed bandwidth with extremely low packet loss rates, bounded latency, and low jitter. OT networks are typically used for monitoring systems and supporting control loops, as well as movement detection systems for use in process control (i.e., continuous manufacturing) and factory automation (i.e., discrete manufacturing), and protection systems in the SmartGrid.

Due to its different goals, OT has evolved in parallel but in a manner that is radically different from Information Technology/Information and Communications Technology (IT/ICT), which relies on selective queuing and discarding of IP packets to achieve end-to-end flow control over the Internet.

IPv6 can contribute to the convergence of IT and OT. Having a single standardized way to communicate with widely deployed new IOT devices is a guaranty of success. IPv6 has evolved since its inception to support the new industrial communication requirements. The IETF and its working groups have added numerous new standards that allows IP networks to meet the demanding objectives of OT communications. In this regard it is possible to list the following IETF working groups: Detnet, 6loWPAN, 6lo, 6Tisch, LPWAN, IPWAVE.

The IETF has also developed a new routing protocol targeting specifically the IOT domain called RPL (Routing for low Power and Lossy networks) [RFC 6550]. This new routing protocol has rapidly become one of the most deployed IGPs worldwide. This is because it is widely used in the smart metering domain where each and every meter is an IPv6 router. An average smart metering system overpassed easily a million of meters, leading to hundreds of millions of IPv6 routers worldwide. It expanded over the year to reach also the substation automation field by connecting the small electrical substations together with sensors along a distribution line. This type of network forms a FAN (Field Area Network) and offers all the necessary connectivity for the utilities.

Figure 8: Example of FAN (Field Area Network) [FAN] Courtesy of Kyoto University, Nissin Systems, ROHM

Using IPv6 allows to respect the end-to-end principle and to avoid the multiplication and deployment of numerous IOT gateways. It will reduce the OPEX and avoid the deployment of complex network management systems.

The IETF is not the only standardization organization looking at easing the deployment of IPv6. The IEC have published a technical report (IEC TR 62357-200:2015) for the power automation domain. This technical report describes the transition strategies, covering impact on applications, communication stack, network nodes, configuration, address allocation, cyber security and the related management. It considers backward compatibility and shows concepts as well as necessary transition paths to IPv6 from IPv4 where necessary, for a number of protocols in the IEC 61850 framework.

It covers the communication systems of the electrical substations, control center, maintenance center, energy management systems, synchrophasor-based grid stability systems, bulk energy generation, distributed energy generation (renewables), energy storage and load management.

As mentioned, the number of wireless devices increases in the industrial environments. Today, most of them are connected using standards like Wireless Hart and ISA 100.11a. The latest is using IPv6 for its addressing scheme. But the demand for a larger scalability and more determinism is emerging. Even if 6TiSCH has already filled up a gap in the standardization landscape, a new IETF working group is now looking at reliable wireless communication. It is called RAW standing for Reliable and Available Wireless. For details on IPv6 and IoT, please see ETSI GR IP6 008 V1.1.1 [IP6-3], ETSI GR IP6 009 V1.1.1 [IP6-4] and ETSI GR IP6 017 V1.1.1 [IP6-7].

5.2 RAW (Reliable and Available Wireless)

RAW (Reliable and Available Wireless) is a new Working Group at the IETF, with a goal to approach deterministic networking over paths that include wireless segments. The wireless and wired media are fundamentally different at the physical level, and a RAW solution has to address the additional issues of less consistent transmissions, energy conservation and shared spectrum efficiency.

While deterministic networking solutions apply to both wireless and wired, there has been recent industry interest for wireless applications which were not initially included in the DetNet use cases. One critical application is Aeronautical Data Communications. The Aeronautical standards work on a physical layer and data link layer for data communications is reaching maturity and there is significant interest in IP connectivity applications. Other examples of potential wireless applications include industrial, pro audio and video, gaming, and edge robotics.

Due to uncontrolled interferences, including obstacles in the Fresnel zone, co-channel energy and the self-induced multipath fading, a single radio link can never be trusted over the long term for reliability and availability; this is why wireless technologies have been lagging behind efforts for deterministic on wired systems at both the IEEE with TSN and at the IETF with DetNet. Recent efforts with 3GPP 5G and Wi-Fi 6 indicate that wireless is finally catching up at the lower layers and that it becomes possible for the IETF to extend DetNet for wireless segments that are capable of scheduled wireless transmissions.

IP leverages routing protocols to compute alternate routes and provide a reliable delivery in the face of a node or a link failure. In a serial path, intermediate network Nodes such as routers, switches, base stations, and APs, wire bundles and the air medium itself can become single points of failure. To achieve high availability, it is thus required to compute physically link- and node-disjoint paths; in the wireless space, it is also required to use the highest possible degree of diversity in the transmission to combat the causes of transmission loss. The highest degree of diversity is obtained when different transmission media are used in parallel, e.g., combining wired and wireless paths, and/or different wireless technologies. This is why the RAW problem must be handled at the IP layer, in a fashion that can observe diverse paths and technologies, so as to use the most relevant one(s) at any point of time.

The radio conditions may change faster than a centralized routing can adapt and reprogram the network, e.g., when the routing function operates in a distant controller, and connectivity is slow and limited. To address this issue, RAW separates the route computation time scale at which a complex path is

recomputed from the packet forwarding time scale at which the forwarding decision is taken for an individual packet. RAW operates at the forwarding time scale.

The goal for RAW is to leverage advanced IPv6 technologies such as In-situ Operations, Administration, and Maintenance (IOAM), Segment Routing (SRv6) and Bit Indexed Explicit Replication (BIER) to steer traffic across diverse and redundant paths in order to ensure a reliable delivery at all times, even in the face of loss over one particular wireless segment.

5.3 DataCenter fabrics

DataCenter (DC) networking started as an extension to traditional Layer-2 switching, but it became evident over time that IP routing was a more appropriate technology, with richer routing features and forwarding functionalities for, e.g., wide Equal Cost Multipath (ECMP) over possibly a hundred of feasible successors, overlay networks, and L7 proxies.

This is why over the recent years DataCenter routing has been migrating to IP for both the overlay and the underlay. Though IPv4 and IPv6 are both feasible, and supported by the new DataCenter IGPs such as RIFT [RIFT], IPv6 adds a number of benefits including:

- Avoiding private addresses [RFC 1918] and the related problems, e.g., when interconnecting networks that originally grew separately and may reuse the same address space
- High scalability for dense Virtual Machine deployments with both IPv6 autoconfiguration and centralized addressing management capabilities
- A better (virtual) host-to-router interface with [RFC 8505] that enables the fabric to learn the VM addresses and follow their mobility across the fabric
- Source Address protection and validation with RFC 3971/3972 and / or [AP-ND]

The reference model for DC fabrics, often called Canonical Clos or Fat tree, is getting traction beyond the core DC networks in the enterprise and campus networks. This is because the high amount of ECMP enables both failure tolerance without complex fast reroute, and near non-blocking properties.

6 IPv6 Use Cases from the Real World

This section provides use cases of IPv6 deployments as experienced by various types of stakeholders involved in these deployments. Several ETSI ISG IP6 published documents have as well described several use cases of IPv6 deployments, see Annex 1.

6.1 Network Operator 1 in Europe

6.1.1 Current status of IPv6 deployment and traffic growth

This Operator from Europe shared the status of IPv6 deployment and the transition experience. Although the IP backbone had already been upgraded, the massive old CPE software updates and the new hardware CPE placement started at the end of 2013 to support dual stack for the fixed network access, copper and fiber. It took two years (late 2016) to achieve 90% of the fixed network accesses. In 2020 they have almost 100% dual-stack support in fixed access CPEs.

In late 2016, in their ISP, providing dual connectivity, in a normal internet usage pattern, 30% of the generated traffic was using IPv6 connectivity (70% via IPv4). It is interesting to see that by 2016 all major content internet players and all user devices mainstream operating systems had already implemented dual stack. In late 2018 these values dropped to 25/75. One year later (2019), it has smoothly growing to around a stable 32/68 relation. What they are observing today is that this percentage has grown to 40/60 (this was achieved during COVID pandemic peak, thanks to an abnormal increase in multimedia traffic, indeed the normal IPv6 traffic growth places this relation just before COVID in around 37/63).

6.1.2 IPv6 transition experience and thoughts

On the fixed access side, operator's IPv6 adoption decision was done in 2013 and was based on the dual-stack model. It seemed the most economic at the time with less disruption on client's service. At the same time, other mitigation measures like IPv4 pool usage optimization, network consolidation and address space acquisition were also taken. That leads them up to 2020, where, in fixed access network, they are now facing the public ipv4 address space exhaustion point. The next steps are being analyzed very carefully, but as a temporary mitigation measure CGNAT will be used, since previous investment had already been done in this platform.

On the mobile side, there is still no IPv6 implementation. NAT translation levels have been reached, and no more IP public pool addresses are available. The new constraints of national regulator lawful interception, Voice over Long-Term Evolution (VoLTE) and the new 5G 3GPP release implementations are seen as major drivers for IPv6. At this point, the first mitigation solution is to implement Dual-Stack.

Nevertheless, one of the major concerns is to adopt the same transition model towards IPv6 networks and translation model for IPv4 networks, for both fixed and mobile, to reduce the OPEX by using the same transport backbone node types and by consolidating operations teams.

6.2 Network Operator 2 in Europe

6.2.1 Benefits of Segment Routing V6 deployment in transport network

This operator decided to implement the SRv6 protocol on top of IPv6 infrastructure in his new transport network. As the adoption of IPv6 grows in operators' networks, it offers the opportunity to install and use new related protocols. Segment Routing v6 (SRv6) protocol is a typical case as it is totally constructed around IPv6 and integrates smoothly in existing IPv6 deployments. As a cousin of the MPLS-based Segment Routing (SR-MPLS), its purpose is the building of traffic engineered transport paths defined with segments

lists. When the SR-MPLS uses MPLS labels for referencing segments, SRv6 leverages dedicated IPv6 Routing Headers, called Segment Routing headers [RFC8754]. IPv6 header usage leads in some advantages. Standard IPv6 routing is used for forwarding IPv6 packets even if some legacy routers in the network do not run the SRv6 features. Using an IPv6 Routing Header offers more possibilities for the further use case application such as instructions coding, meaning it would be possible to chain instructions for building enhanced services, expressed as Ipv6 addresses in the Routing Header. Regarding these different advantages, simplification of the protocol stack and the further flexibility of SRv6 protocol, SRv6 will offer the foundations for installing various types of services in the transport network: Fixed services such as 3Play and Mobile services such 5G slices.

6.2.2 Delivery of 3Play Internet service over SRv6

The 3Play Internet service is delivered from the BNG to the End User through a PPPoE session. A Layer2 service is built on the Transport Network from the BNG to the OLT where the End User is connected. The user data are encapsulated in SRv6 packets at PE and forwarded in the IPv6 Transport Network using a primary path. In case of failure, a backup path has been pre-configured in the network and will be used for forwarding the user data. In this service use case, the SRv6 technology replaces the legacy MPLS technology.

The scheme below describes the service principle:

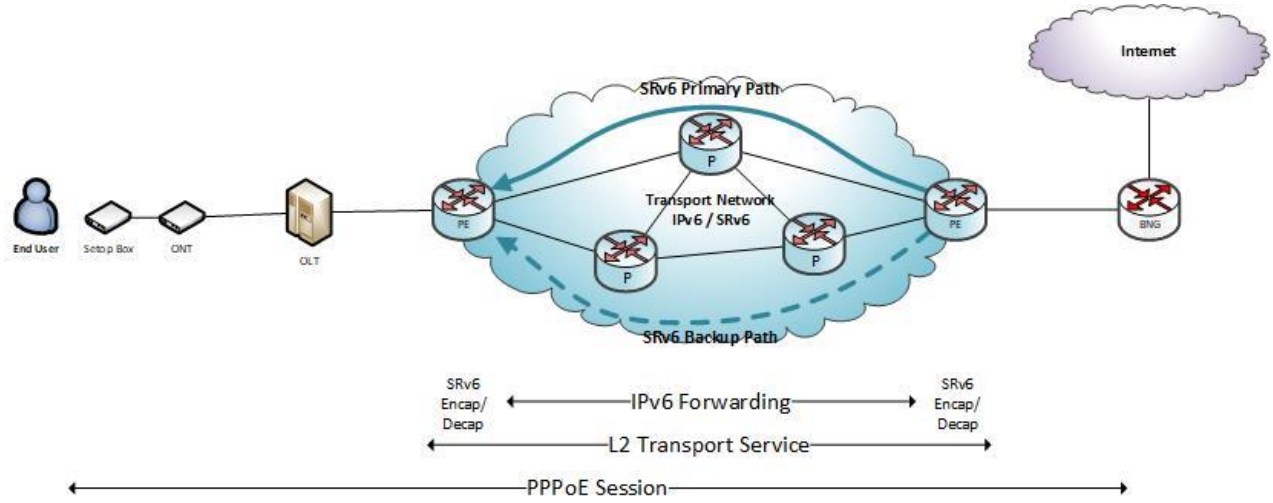

Figure 9: 3Play Internet service over SRv6 for Network Operator 2

This Operator is also investigating the use of BIERv6 for the 3Play service over SRv6 and in particular for delivering IPTV in their offer.

6.3 Network Operator 3 in Asia

6.3.1 Current status of IPv6 deployment

This operator in China provides both mobile and wireline communication service to their customers, in addition, it also provides cloud computing services.

As mentioned above, the Chinese government has been actively promoting the deployment of IPv6 for a long time. Under this circumstance, the operator started the IPv6 commercial trial in two cities in 2009 and achieved the first IPv6 commercialization in China. In 2013, the scale of IPv6-deployment was enlarged to 21 cities. Moreover, in 2015, the operator enabled IPv6 capability on LTE networks in some regions and began to provide IPv4/IPv6 dual-stack access services to mobile users.

Up to now, IPv6 commercial deployment has been fully completed in every part of the network infrastructure, including Metro Area Network (MAN), mobile network, backbone network, Internet Data Center (IDC), etc. More than 13,000 devices and 19,000 links in these networks were replaced or upgraded. Meanwhile, the quantity of users with IPv6 addresses and the number of active connections has increased significantly. This operator has about 330 million mobile users, the statistics of CAICT in December 2019 shows that, 274 million terminals are assigned IPv6 addresses and there are 240 million active connections. Of the 179 million optical broadband users, 114 million have obtained IPv6 addresses and there are 55 million active connections. Herein, IPv6 active connections are defined as the number of users who have obtained an IPv6 address and have access IPv6 service at least once within a month.

In addition to enabling IPv6 in the network, the operator also deployed IPv6 in its own cloud resource pools Cloud computing is a new scenario compared to the transition to IPv6 ten years ago. Currently, 75 cloud resource pools support IPv6 with 25 IPv6-capable cloud products, such as cloud hosting, load balancing, and cloud storage. The deployment of IPv6 in cloud computing provides the ICT/IT industry with a broader space for business development and technological innovation. As a result, the operator has been providing a full range of IPv6-enabled products and services including dedicated lines, virtual networks, clouds, and IDC for about 1,000 government and enterprise customers in various industries.

6.3.2 Challenges

Although the upgrading of the network infrastructure has been completed, the overall improvement of IPv6 traffic still faces many challenges. The following figures show the IPv6 traffic and proportion in fixed and mobile networks. In the past year, IPv6 traffic has increased rapidly, but the overall IPv6 traffic still accounts for less than 10% of the total traffic. One of the reasons is that the transition of OTT (e.g., Over-The-Top) is slower than operators. The transition of OTT services to IPv6, especially large OTT services, is one of the important factors that determines the ration of IPv6 traffic. Some OTTs have concerns about network performance and security when migrating services to IPv6, although these issues have little impact in practice.

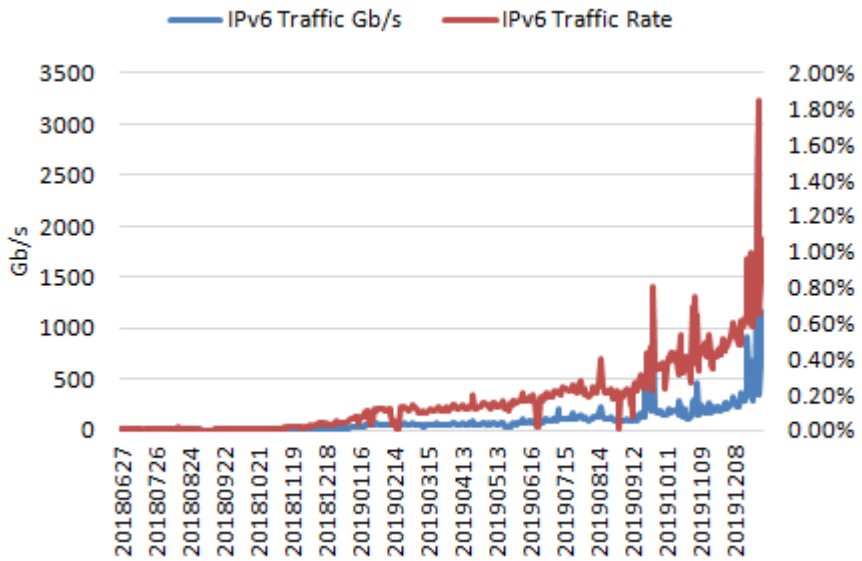

Figure 10: IPv6 traffic data for the fixed network

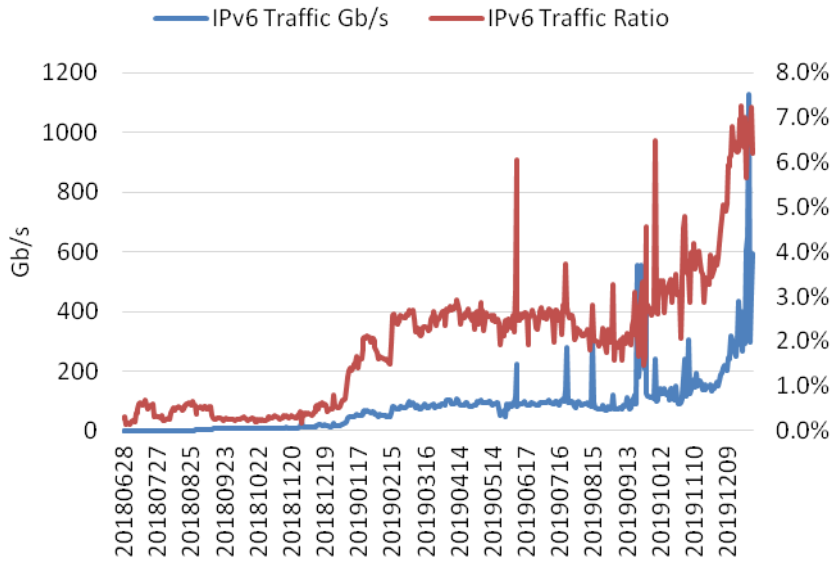

Figure 11: IPv6 traffic data for the mobile network

In addition, IPv6 development still faces the difficulty of IPv6 support in some home Customer Premise Equipment (CPE). Although the operator has developed a complete and mature IPv6 access solutions for different customers, and IPv6 has been implemented in the operator's customized home router. However, operators do not have the power to customize every home router, and there are still a large number of home routers not customized by operators in the existing network. The CPE purchased from the free market by the users accounts for more than half of the total. This factor has caused a huge obstacle to the further increase in the number of IPv6 users, which in turn has affected the penetration of IPv6 in fixed networks and the growth in IPv6 traffic.

6.4 Mobile Operator 1 in North America

This Mobile Operator in the Unites States was running out of IPv4 addresses and needed an IPv6 transition strategy. Their solution was 464XLAT, an IPv6-only solution.

As described in the previous sections, 464XLAT is an IPv6 transition technology documented in RFC 6877, which builds on previous technologies such as NAT64 and DNS64. The problem for this operator with just using NAT64 and DNS64 was that specific applications, such as those with IPv4 literals in URLs, could not function through NAT64. By using 464XLAT this operator was able to keep these applications working and provide native IPv6 connectivity where possible.

In 2014, after launching this solution on several million phones this mobile operator has seen up to 30% of all traffic on these phones be native IPv6, and the number has grown a lot. A report of 2019 shows how close this mobile operator is to attaining 100% IPv6 adoption.

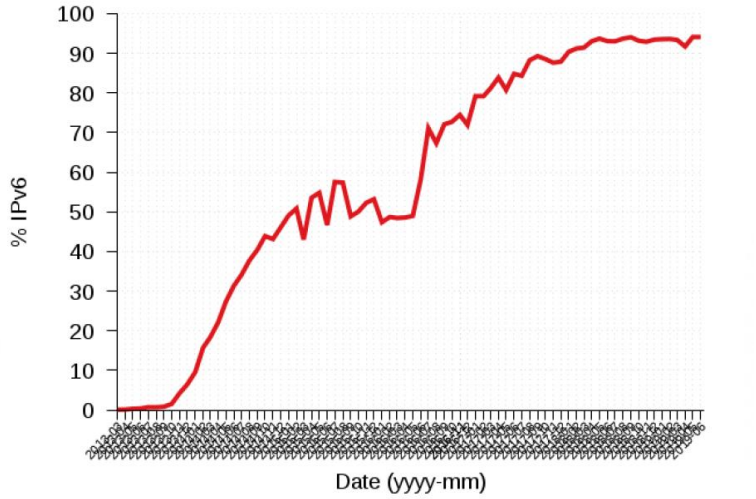

Figure 12: IPv6 adoption for Mobile Operator 1

This mobile operator stated in several presentations that 464XLAT allows for full functionality on IPv6-only networks. Dual-Stack does not solve the IPv4 number scarcity issue while NAT64/DNS64 is very good, but not good enough for full IPv4 replacement (web and email work, but some applications do not work). So 464XLAT is the best solution this operator followed since it solves IPv4 numbering issue by not assigning IPv4 to clients and decouples edge growth from IPv4 availability. In addition, IPv4-only applications (including those with IPv4 literals in URLs) work on an IPv6-only network because 464XLAT translates IPv4 on the phone to IPv6 on the network.

IPv6 deployment is achievable as the experience of this operator shows and it did not spend any CapEx on IPv6. The operator only introduces 464XLAT on new phones, so they do not disrupt any existing services, leverage normal phone Quality Assurance (QA) process. They also had some Innovative thinking to reduce deployment costs (e.g. hash 128 bit numbers into 32 bit fields in billing records). In the end they consider that IPv6 will save money in the network (less NAT/CGN, no need to buy IPv4 addresses.

APNIC shared the measurement for this mobile operator. The following graph shows that this mobile operator has a better connection failure rate in comparison with country average.

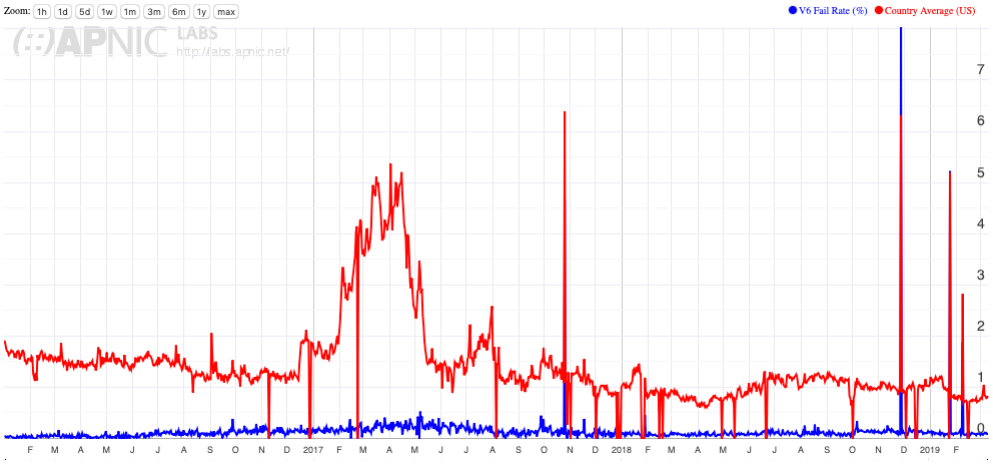

Figure 13: Connection failure rate for Mobile Operator 1

6.5 Content Provider 1 Worldwide

6.5.1 IPv6-only infra DC

The main reason for IPv6 deployment given by this Content Provider is related to the issue that they had run out of private 10.0.0.0/8 space [RFC 1918] for their Data Centers. Assigning large prefixes (/24) to each rack was wasteful but made all the tooling and summarization easier (/25 is what they could have re-numbered but with not enough savings and too much code assumed racks are /24). At this point, to overcome this dilemma, this Content Provider decided to go for IPv6 and allocate a /64 network per rack, which seems a little excessive but efficient in terms of routing table lookups in ASICs and ECMP implementation for IPv6, despite the initial problems they had for the lack of proper IPv6 support.

Over the past few years, this Content Provider has been transitioning its data center infrastructure from IPv4 to IPv6. They began by dual-stacking the internal network, adding IPv6 to all IPv4 infrastructure, and decided that all new data center clusters would be brought online as IPv6-only. They then worked on moving all applications and services running in their data centers to use and support IPv6. Today, 99% of the internal traffic is IPv6 and half of their clusters are IPv6-only. They anticipate moving their entire fleet to IPv6 and retiring the remaining IPv4 clusters over the next few years.

Globally, however, only a percentage of the users of this Content Provider have IPv6 support. So they needed a way to serve users with access only to IPv4 internet while they operate an IPv6-only infrastructure within their data centers. Traffic requests to the Content Provider often pass through a series of load balancers before landing on a server. Since these load balancers act as a proxy, it is possible to let them maintain partial IPv4 support. This allows to keep everything in the data center IPv6-only while still serving IPv4 traffic.

6.5.2 Supporting IPv4 through load balancers

When IPv4 traffic finishes in IPv6-only Clusters, a possibility can be the use of RFC5549 and advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop. An alternative is RFC7755 that specifies SIIT-DC (Stateless IP/ICMP Translation for IPv6 Data Center Environments), a sort of "464XLAT" for Data Centers. But, neither SIIT [RFC7755] nor [RFC5549] have been used in the case described of this Content Provider that employed a different approach.

The solution chosen by this Content Provider was to take their IPv6-only data center clusters and made a series of changes to the software load balancers to include the support for IPv4 external requests (all internal requests are IPv6-only). All requests enter the network through a series of network devices and are routed to a load balancer server using Border Gateway Protocol (BGP). They run two software load balancers: A Layer 4 load balancer (L4LB/shiv) that operates on TCP/IP, and a Layer 7 load balancer (L7LB/proxygen) that operates on HTTP/HTTPS.

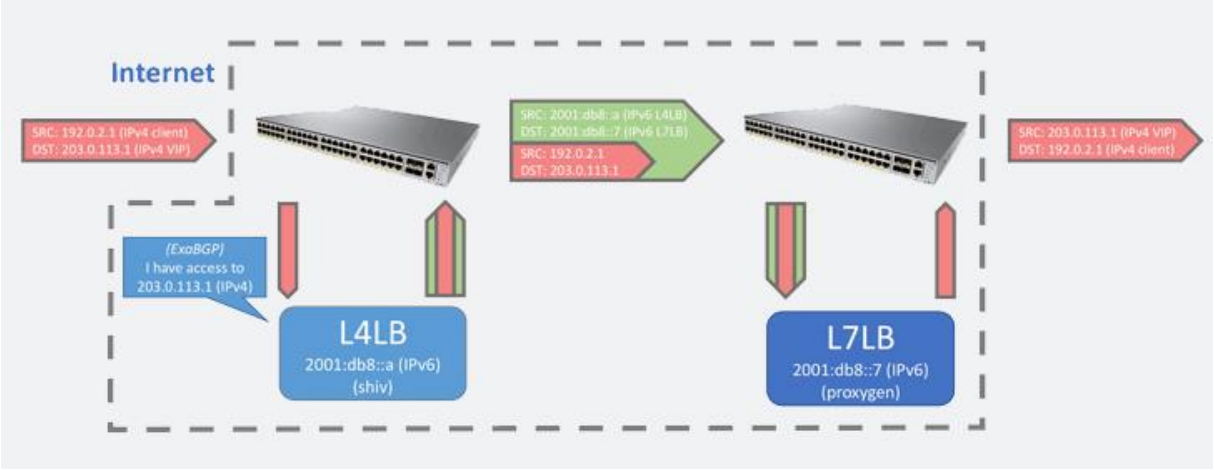

Figure 14: IPv6-only data center for Content Provider 1

The incoming requests are routed to a L4LB server using BGP and the L4LB announces its publicly routable virtual IP addresses (VIPs) that can be both IPv6 and IPv4. In case of IPv6 requests everything is handled in the IPv6-only cluster but in case of IPv4 requests some considerations need to be made.

When an IPv4 packet arrives, the L4LB dual-stack server uses a routable IPv4 address as the BGP next-hop, while if L4LB is an IPv6-only server it can use an IPv4 link-local address as the BGP next-hop. IPv4 link-local addresses are assigned from address block 169.254.0.0/16. The IPv4 packet is routed to L4LB by using the IPv4 address or the IPv4 link-local. The use of link-local address is possible since the L4LB is in the same rack of the frontend router. But after that, L4LB needs to forward the request to the specific chosen L7LB. L4LB and L7LB have no routable IPv4 address and are not in the same rack, so IPv4 link-local cannot be used and IPv6 is required. So L4LB encapsulates IPv4 traffic inside IPv6 through IP tunneling by using IPVS (IP Virtual Server) to forward traffic to the L7LB. Finally, the L7LB receives the request, decapsulates it, and sends a response directly back to the client in IPv4 via the frontend router.

While they have a few years until their IPv4 data center clusters are fully phased out, they are now in a position where they can move the rest of the infrastructure to IPv6-only without cutting off people whose internet does not yet support IPv6. And, when they no longer need this feature, they can easily turn it off.

6.6 Enterprise 1 Worldwide

6.6.1 Towards IPv6-only Single Stack Network

The declared goal of this big Enterprise is to have their end-users be IPv6-only. All corporate and VPN networks are dual-stack, but their ultimate goal is to run a single stack in the network. Of course, it won't happen overnight because they have a huge environment. They are now focusing on having a single stack in the network. It won't happen immediately, but they are working on it. There are four things that drove their decision to move to IPv6-only on their internal network.

1) First, IPv4 address depletion. They needed to offer publicly routable addresses to external customers, so, starting from 2011, they renumbered to private addresses (10/8 space). However, they can foresee based on the consumption and requirements a sliding date of depletion in two to three years. They don't have any large blocks like /16s or /17s left. They have smaller blocks, but people like the larger blocks to help them manage devices like virtual machines. Currently, they have a need for quite a lot of IPv4 address space which they don't have in a continuous format. They are also working on reclaiming IPv4 space that is not heavily used in their internal network, but they know that there is a point in the not-so-distant future that they will run out of IPv4, and they need to be prepared for it.

2) The second reason they are moving to IPv6-only is because they know that running a dual-stack network makes it more complex including troubleshooting time, security and QoS policies. Dual-Stacking also does not remove their reliance on NAT44 which they have to leverage heavily. While Dual-Stack was good to have experience with deploying and operating IPv6, it keeps dependent on IPv4. Ultimately, everywhere where they can they will do IPv6-only.

3) The third reason is that everyone uses private IPv4. This makes acquisitions quite difficult as they must insert and operate more NAT in their environments to enable communication between environments and the acquired companies.

4) The fourth reason is the industry pressure. The pressure from the other Partners to enforce IPv6 was great. It made them much more aware of IPv6 since they need to prepare IPv6-only test environment which would enable Partners to verify correct functioning for interworking.

One of the first things they needed towards the adoption of IPv6 was an address plan. People say IPv6 is difficult because it is hard to read, but that's not true, indeed the prefix can help to know which part of the world it is from, so, locally, it is possible to work with only one aggregated prefix and what changes is the bits after it. With IPv4 there was no such possibility. They also had to make an important decision about the method of address assignment. They went for stateless DHCPv6 with IPv6 stateless address SLAAC and RDNSS (Recursive DNS Server) on network segments and this was driven by the mixed level of support of DHCPv6 and RDNSS by user, infrastructure and IoT devices. The next thing to do is testing since

they had to make sure the features, they needed were available in existing hardware and software that they put in the network. Another important aspect is the extensive training of the engineering staff. The industry is still not fluent in IPv6 but that's no surprise considering the global levels of IPv6 adoption, so much goes in making a single stack-only network.

The benefit of IPv6-only is losing dependency on the legacy protocol. Getting out of those restrictions means they won't have to do multiple layers of NAT in internal network as they are doing today. There is an undisturbed traffic flow. They have observed internally faster network connections, because IPv6 is not disrupted by NAT, and they assume that the code in network devices that supports IPv6 is newer and it seems to be written in a better way. They still must find a better way to measure this but that's their observation to date. The real benefit of IPv6 is when it's a single-stack network. From a broader perspective, deploying IPv6 can contribute to better traffic flow on the Internet, because the IPv4 Internet routing table is big. There is a general worry that the fragmentation of IPv4 space could potentially lead to slowing down the IPv4 traffic. While the IPv6 routing table is better organized, getting to your destination could be faster.

They want to get as much user traffic as they can on IPv6. The real driver is that for users on the IPv6-only segments, they want to avoid sending traffic through NAT64 and DNS64 as much as possible. Anyway, NAT64 and DNS64 are essential to make sure that users can continue working in IPv6-only environment. Even when all their internal services are enabled with IPv6, the Internet will still be IPv4-only to a certain degree.

IPv6 can be overwhelming and their advice is to take the deployment bit by bit. Focus on things that give the biggest benefit, the biggest learning, the biggest impact on the largest group of users. Finally, Dual-Stack is only a temporary solution. The ultimate solution is IPv6-only.

6.7 Utility Company 1 in North America

6.7.1 Field Area Network for Electric Distribution Network and smart metering

In the domain of the Internet of Things, in the past few years there was a rapid evolution of the electrical grid. It started by the changes in the smart metering infrastructure. Mainly, all utilities around the world pushed by regional regulations have set up plans to move their metering system to a fully remote operable infrastructure. There are now hundreds of millions of smart meters deployed and the majority of them is based on IPv6 networks.

Open-standards-based IPv6 architecture for smart-grid last-mile infrastructures has been developed in support of a number of advanced smart-grid applications (meter readout, demand-response, telemetry, and grid monitoring and automation) and the related multiservice platform has been deployed by a Utility Company in North America.

Last-mile networks have gained considerable momentum over the past few years because of their prominent role in the smart-grid infrastructure. These networks support a variety of applications including not only electricity usage measurement and management, but also advanced applications such as demand/response (DR), which gives users the opportunity to optimize their energy usage based on real-

time electricity pricing information; distribution automation (DA), which allows distribution monitoring and control; and automatic fault detection, isolation and management.

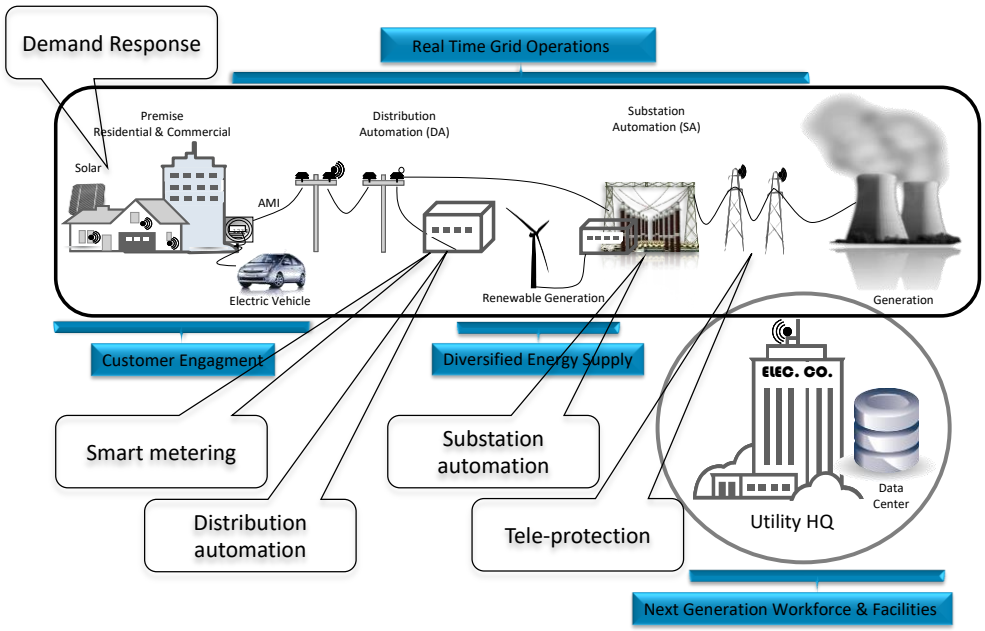

Figure 15: Electric Distribution Network and smart metering for Utility Company 1

Field Area Networks (FANs), which is the combination of local devices attached to a Field Area Router (FAR) offering the backhaul WAN interface(s), have emerged as a central component of the smart-grid network infrastructure. In fact, they can serve as backhaul networks for a variety of other electric grid control devices, multitenant services (gas and water meters), and data exchanges to home-area network (HAN) devices, all connected through a variety of wireless or wired-line technologies. This has created the need for deploying IPv6, enabling the use of open standards that provide the reliability, scalability, high security, internetworking, and flexibility required to cope with the fast-growing number of critical applications for the electric grid that distribution power networks need to support.

One application being run over FANs is meter reading, where each meter periodically reports usage data to a utility headend application server. The majority of meter traffic was thus directed from the meter network to the utility network in a multipoint-to-point (MP2P) fashion. With the emergence and proliferation of applications such as DR, distributed energy resource integration and EV charging, it is expected that the traffic volume across FANs would increase substantially and traffic patterns and bi-directional communication requirements would become significantly more complex. In particular, FANs are expected to support a number of use cases that take advantage of network services: communication with an individual meter, communication among DA devices, HAN applications, EV charging, multitenant services, security, network management, multicast services.

The FAN network is based on an open stack implementing the IPv6 protocol suite. One example of this is the WI-SUN alliance stack. This stack fully relies on IPv6 networks and allows the successful deployment of new applications in the electric distribution network.

7 IPv6 Enhanced Innovation and the Way Forward

7.1 IPv6-only perspectives

IPv6 adoption is no longer optional. The global transition to IPv6 is happening and has been underway for years. All Internet technical standard bodies and network equipment vendors have endorsed IPv6 and view it as the standards-based solution to the IPv4 address shortage. Consider the unequivocal statement made by APNIC some years ago: “IPv6 is the only means available for the sustained ongoing growth of the Internet, and [we urge] all Members of the Internet industry to move quickly towards its deployment.” In fact, every Internet registry worldwide strongly recommends immediate IPv6 adoption.

Back in November 2016, The Internet Architecture Board (IAB), following discussions in the Internet Engineering Task Force (IETF), advises its partner Standards Development Organizations (SDOs) and organizations that the pool of unassigned IPv4 addresses has been exhausted, and as a result it is seeing an increase in both dual-stack (that is, both IPv4 and IPv6) and IPv6-only deployments, a trend that will only accelerate. Therefore, networking standards need to fully support IPv6.

The IETF, as well as other SDOs, need to ensure that their standards do not assume IPv4. The IAB expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6. This is already true for most IoT-related protocols such as 6LoWPAN and RPL.

Preparation for this transition requires ensuring that many different environments are capable of operating completely on IPv6 without being dependent on IPv4 (see RFC 6540). It is recommended that all networking standards assume the use of IPv6 and be written so they do not require IPv4. It is also recommended that existing standards be reviewed to ensure they will work with IPv6 and use IPv6 examples. Backward connectivity to IPv4, via dual-stack or any other IPv6 transition technique, will be needed for some time. The key issue for SDOs is to remove any obstacles in their standards which prevent or slow down the transition in different environments.

In addition, the IETF has found it useful to add IPv6 to its external resources (e.g., Web, mail) and to also run IPv6 on its conference network since this helps our participants and contributors and also sends the message that they are serious about IPv6. That approach might be applicable to other SDOs.

So, the industry is encouraged to develop strategies for IPv6-only operation. Over time, numerous technical and economic stop-gap measures have been developed in an attempt to extend the usable lifetime of IPv4, but all of these measures add cost and complexity to network infrastructure and raise significant technical and economic barriers to innovation. It is widely recognized that full transition to IPv6 is the only viable option to ensure future growth and innovation in Internet technology and services.

Several large networks and data centers have already evolved their internal infrastructures to be IPv6-only. Forward looking large corporations are also working toward migrating their enterprise networks to

IPv6-only environments. The technical, economic and security benefits of operating a single, modern, and scalable network infrastructure are the driving forces for such evolution.

7.1.1 Government wide Responsibilities

Governments have a huge responsibility in promoting IPv6 deployment within their countries. There are example of governments already adopting policies to encourage IPv6 utilization or enforce increased security on IPv4. In this regard it is possible to mention the concrete transition recommendations that have been announced in March 2020 by the US Office of Management Bureau (OMB). The memorandum updates guidance on the Federal government's operational deployment and use of IPv6 [OMB] and it strongly suggests the completion of the transition to IPv6.

So, even without funding the IPv6 transition, governments can impose the Public Offices (e.g., Municipalities, Police, School, Health Care) to add IPv6 compatibility for every connectivity, service or products bid. This will encourage the ISP and product manufacturer who don't want to miss out on government related bids to evolve their infrastructure to be IPv6 capable. This will create a positive loop where the ISP will want to maximize the return on investment and will shift as many users as possible to use the IPv6.

Any public incentives for technical evolution will have to be bonded to IPv6 capabilities of the technology itself (e.g., subsidize Fiber to the Home (FTTH) binding it to IPv6 adoption).

Some governments also force a policy for a maximum number of user NATted on a single IPv4 address, for security reason (e.g., 16 users per public IPv4), while IPv6 has no limitation in this perspective.

Countries ready for the Digital Transformation and all the related present and future use cases will need to be IPv6 ready to tackle them, and governments have to play their role in guiding this transition.

It is relevant to highlight the ITU resolution 180 (REV. DUBAI, 2018) [ITU RES 180] on Promoting deployment and adoption of IPv6 to facilitate the transition from IPv4 to IPv6

ITU resolution invites Member States to:

1. to continue to promote specific initiatives at the national level, which foster interaction with governmental, private and academic entities and civil society for the purposes of the information exchange necessary for the deployment and adoption of IPv6 in their respective countries;
2. to encourage, with support from the ITU regional offices, the RIRs and other regional organizations in coordinating research, dissemination and training actions with participation by governments, industry and the academic community in order to facilitate the deployment and adoption of IPv6 within the countries and in the region, and to coordinate initiatives between regions to promote its deployment worldwide;
3. to develop national policies to promote the technological update of systems in order to ensure that the public services provided utilizing the IP protocol and the communications infrastructure and relevant applications of the Member States are compatible with IPv6;

4. to encourage manufacturers to supply to the market fully-featured customer premises equipment that supports IPv6 in addition to IPv4;
5. to raise awareness among information service providers on the importance of making their services available over IPv6.

7.1.2 Enhancing cybersecurity

Industry guidance and best practices for the secure deployment of IPv6 have been well documented. While the knowledge base of how to secure IPv6 has matured significantly, the understanding of how IPv6 enables more efficient approaches to overall security is often overlooked. For example, organizations that develop IPv6 addressing plans that are highly correlated with their network security architecture are finding a significant reduction in the complexity of their security configurations.

Adopting and enforcing the IPv6-only policy worldwide by deploying the single stack of IPv6, turning off IPv4, and setting a plan to sunset IPv4 completely will also reduce the overall cybersecurity threats and attacks based on IPv4. Organizations worldwide, big or small, have to deal with constant cyberattacks and data breaches. And the situation can only get worse since the IPv6 adoption rate is increasing and running in parallel with IPv4. This is effectively doubling the overall attack vectors. Adopting an IPv6-only policy will consequently reduce this effect and improve the overall situation.

7.2 Benefits of IPv6

7.2.1 IPv6 Promotion

As a new generation of network protocols for the Internet, IPv6 has existed for more than 25 years. During the past, by the joint efforts of global network community, its base specification became mature after several revisions and polish and the stability of the IPv6 protocol makes it possible for wide deployment of IPv6 in the world. Moreover, with the emergence of new digital technologies, such as 5G, IOT and cloud, etc., new use cases have come into being and posed more new requirements for IPv6 deployment. Herein, some of the new requirements are listed:

- **Network Programming**, since operators need to deliver service fast and provide tailored service to meet the specific requirements of customers. This requires the capability for an application to encode any complex program as a set of individual functions distributed through the network. In this regard, as based on IPv6 data plane, SRv6 programmability concept is relevant.
- **Low Latency**, with the rising of latency-sensitive applications, the network is required to process data with minimal delay and jitter. To achieve this goal, the delay-sensitive data should be forwarded along paths that are not overloaded or new queue technique are needed to optimize latency. IPv6 can easily be integrated with low latency techniques.

- **Network Slicing**, some enhanced services require dedicated network resources to achieve isolation from other services in the network, and the number of such enhanced services can be greater than the number of traffic classes with QoS. This put forward the requirement to create multiple unique logical and virtualized networks, namely slicing, over a common infrastructure. Both SRv6 and the end-to-end model of IPv6 allow network slicing.
- **IoT**, such as NB-IoT, has been widely deployed during the past several years. Indeed a strong requirement of IoT is related to the addressing and reachability of devices. In this case, the whole 128-bits address enables more flexibility and can be allocated without using NAT, and some IOT applications even require the IPv6 address remain unchanged during the lifetime of the device, so they can access and control the devices easily via IPv6 address.

7.2.2 SRv6 networking technology

IPv6 brings new opportunities. New technologies will benefit greatly from the end to end model restored by IPv6 such as 5G, IoT, SDN/NFV and Cloud Computing for the Enterprise. In this regard SRv6 (Segment Routing over IPv6 data plane), described in RFC8754, is gaining a lot of interest in the SDOs

The native reachability of IPv6 in combination with SR (Segment Routing) technology adds interesting proprieties. Compared with SR-MPLS, SRv6 has significant advantages especially in the large-scale networking scenario. The main advantages are: IP Route Aggregation (for the native IP feature of route aggregability compared to MPLS), End-to-end Service Auto-start (for the native IPv6 reachability compared to MPLS), on-Demand Upgrade (since only the relevant devices need to be upgraded to enable SRv6 while all other devices only need to support IPv6 forwarding). The incremental deployment is the key for smooth transition to SRv6.

The SRv6 architecture is a promising solution to support end-to-end per-flow SR policies applied to IPv6 Data Plane to reach connectivity, resiliency, path preference, traffic engineering and service selection. SRv6 allows a fine granularity in the programming interface and the number of differentiated flows/policies does not impact the state that is necessary in the network. This introduces interesting scalability properties.

SRv6 programmability concept [SRV6-PROG] represents the capability of a network operator to enforce a network program comprising a sequence of network instructions (functions), which is encoded within the IPv6 packet headers. These functions are distributed among the SRv6 capable nodes in the network. The IPv6 packet carrying the network instructions explicitly tells the network about the precise SRv6 nodes that need to be traversed and the SRv6 function that must be executed on each of them. The network instruction is called SRv6 segment and identified by a SRv6 Segment Identifier (SID). A SRv6-capable source node can insert a single SID into the IPv6 header or multiple SIDs into the Segment Routing Header (SRH). SRv6 SIDs are encoded in an IPv6 packet as 128-bit IPv6 addresses. Typically, a header of the IPv6 packet contains a list of segments.

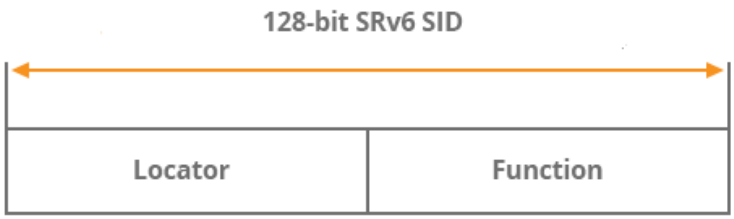

Figure 16: 128-bit SRv6 SID including Locator and Function

SRv6 SIDs are structured as a 128-bit IPv6 address consisting of two parts. The first most significant bits (the length is variable) represent an address of a particular SRv6 node. This part is called a Locator and it is used for routing in SRv6 networks. Remaining SID bits identify the function that is executed locally on a particular node, specified by the locator bits.

SRv6 programmability also enables Protocols Simplification that is another strong characteristic since it is possible to avoid some protocols given that their functions can be encoded as function of the SID. An example is the stateless service programming capability described in [SR-SERVICE-PROG].

SRv6 is also a candidate technology to achieve the new requirements of [ENHANCED-VPN] services in terms of isolation, performance guarantee, dynamic management and so on.

SRv6 allows a very fine granularity of traffic differentiation policies while still ensuring the scalability necessary to operators. A multitude of applications are carried over the network, which have varying needs for network bandwidth, latency, jitter, and packet loss, etc. Some new emerging applications (e.g. 5G) have very demanding performance requirements. However, in current networks, the network and applications are decoupled, that is, the network is not aware of the applications' requirements in a fine granularity. Therefore, it is difficult to provide truly fine-granularity traffic operations for the applications and guarantee their SLA requirements.

SRv6 was meant from inception to be extended in the future and evolve with the network needs. Recent proposals include SRv6 compressed segment list encoding [SRH-COMP], in particular SRv6 micro-segment [USID] and G-SRv6 for compression [GSRV6]. The goal of these drafts is to enable a more concise expression of the network programming steps for a better scalability (e.g. to address multi-domain 5G deployments). Another relevant proposal is the Application-aware IPv6 Networking (APN6) [APN6-FRAMEWORK], [APN6-USE-CASES] that aims to use the IPv6 encapsulation to convey the application characteristic information such as application identification and its network performance requirements into the network, to facilitate service provisioning, perform application-level traffic steering and network resource adjustment.

7.3 IPv6 Enhanced Innovation

In the 5G and cloud era, IPv6 fundamentally solves the problem of global IPv4 address depletion. The emerging businesses, such as automatic driving, industrial automation, immersive services (e.g. VR/AR), Internet of things, etc., need massive, high-quality and smart connections, which requirements for IPv6

enhanced innovation with enhanced network experience assurance, and network automation & intelligence.

7.3.1 5G and Cloud era raise new challenges to IP networks

With the rapid development of digital economy and traffic growth, cloud and 5G are often seen as key pillars of a new digital economy. 5G networks and cloud computing resources are meant to facilitate the development of new services and applications which in turn raise new requirements for the network in the following three aspects:

- Numerous connections: With the development of 5G and cloud, IoT and virtual nodes will bring hundreds of billions of links, requiring numerous addresses.
- High-quality connection: Cloud AR / VR service with delay <20ms and bandwidth 50-100Mbps; Autonomous driving with delay 5-20ms and bandwidth 5-20Mbps; Industrial automation with time delay 1-10ms and bandwidth 1-10Mbps, etc.
- Smart connections: With the popularity of the cloud, the service opening period ranges from months to hours, fault location cost from hours to minutes, etc.

Figure 17: The 5G and Cloud Era Raises New Challenges to IP Network

Commercial Service Providers (CSP) will have to address these new requirements (e.g., requirements raised by mobile gaming, immersive services, videoconferencing, etc.) as well as new enterprise services using hybrid clouds.

- The cloud paradigm allows consumers and enterprises to build new services in reduced time, creating compute resources on the fly with the possibility for them to auto-scale according to the success/utilization of the service.
- The enhanced IPv6 technology is the key to support this new range of services in environments where network automation techniques are introduced to enable quick transport service delivery and scaling, choosing the best access technologies and granting SLA over time.

(a) Cloud network integration

With the development of cloud computing technology and industry, more and more businesses and data have been moved to the cloud. There are a lot of IT infrastructure resources that can provide computing and storage capabilities on the network. If each cloud is a fragmented island between each other and cannot serve users as a whole IT resource pool, it cannot become a part of ICT infrastructure.

The carrier network of cloud computing infrastructure mainly includes the intra-cloud network, inter-cloud network and user's access network to connect to the cloud. Today, these three network parts cannot form a whole network and it is not possible to realize the end-to-end control of resources.

Therefore, Cloud Network Integration aims to promote the integration of Cloud and Network, realizing on demand resource allocation, and at the same time, the optimized use of resources. The IPv6-only paradigm and also the homogeneous underlay and overlay, enabled by SRv6, can allow this Cloud Network Integration so that end-to-end OAM and service creation and provisioning are much more simplified and flexible.

(b) 5G bearer network

Compared with the previous mobile communication systems, 5G diversified application scenarios need to meet more extreme performance requirements and put forward new challenges to the transmission network, mainly reflected in low latency, mobility and massive connectivity.

For the low delay service, the link delay can be reduced by reducing the transmission path to some extent by deploying the service on the access side close to the user. However, it is not enough to rely on the nearby deployment of the service. In addition, it also needs to be able to provide the low delay technical support in the bearer network. Compared with 3G / 4G, the sinking deployment of 5G gateway can effectively optimize the solution of the delay problem, but at the same time, it also introduces the problem that the terminal may switch frequently between gateways in the process of mobile, which brings great challenges to the mobility. 5G large connection will bring great challenges to the signaling process of control plane and the transmission overhead of user plane. 5G network connection density may reach million / square kilometers. At this time, a huge amount of context information and signaling process will bring a great burden to the bearer network.

The above new challenges brought the new technologies enabled by IPv6, such as SRv6, which introduces better granularity traffic differentiation and guarantee strict SLA requirements.

7.3.2 IPv6 + Protocol Innovation + AI: IPv6 enhanced innovations promoting the development of Internet

Based on IPv6, the Internet needs to be combined with innovative technologies to develop an enhanced IPv6 network. IPv6 and all the new generation technologies based on IPv6 (IPv6 based protocol innovation and adding AI, cloud and network convergence, service telemetry, …) drive the transformation of network service, stimulating business and business model innovation, and accelerating the pace of enterprise digitalization.

- **IPv6 + protocol innovation: stimulate business innovation and provide user experience guarantee.**

IPv6 message design provides sufficient support for network loading new applications in the future. This feature allows IPv6 related protocols to continue to evolve, making IPv6 infinitely possible. For example, Segment Routing over IPv6 (SRv6) is a source routing technology. With the extension header of IPv6, it allocates segments for each node or link, and the header node combines these segments to form segment sequence (segment path), which guides the packets to forward according to segment sequence, so as to realize the programming ability of the network. Therefore, the protocol innovation represented by SRv6 (e.g. SRv6 SID compression), BIER for IPv6 network, APN6, etc., will help IP network gradually meet the needs of 5G bearer and cloud network integration. Provide IPv6 enabling for cloud leased line, video cloud, game acceleration, cloud office and other scenarios, and provide agile differentiated network services for different business, clients and cloud reconstruction scenarios.

- **IPv6 + AI: lower maintenance cost.**

Artificial intelligence, including machine learning and natural language processing, provides a broader network intelligent scheme for the network. Meanwhile, the scalability and flexibility of IPv6 facilitate network data collection for AI. With the assist of AI, IPv6 network are able to have intelligent application opportunities in 5G, private line service, home broadband and other business scenarios, such as IPv6 based intelligent routing, network fault analysis, root cause analysis and positioning, self-healing and prediction, network resource arrangement and management, IPv6 intelligent security, etc.

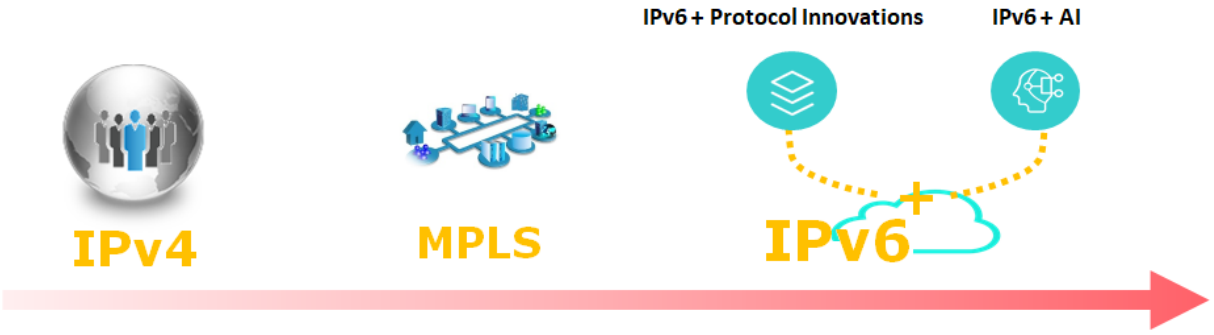

Figure 18: IPv6 enhanced innovation promoting the development of network

The development of network has gone through phases for the requirements of different eras. To meet the new requirements brought by 5G and cloud, IPv6 based protocol innovation (IPv6 + protocol innovation) and IPv6 adding AI (IPv6+AI) , are IPv6 enhanced innovations, which can be abbreviated as “IPv6 +”, represented by protocols innovations such as SRv6, etc., combined with network analysis, intelligent tuning, and other network intelligent innovation technologies, to realize intelligent path planning, service speed opening, operation and maintenance automation, quality visualization, SLA assurance, application perception, etc.

8 Recommendations towards ETSI & industry

As described in this White Paper and as being actively promoted in ETSI ISG IP6, the deployments of IPv6 provides the strong base for all the new technologies and new services evolution (5G, IoT, Cloudification, etc.).

IPv6 has indeed proven that it is the way to the future:

- Traffic, users, content are growing faster in IPv6 and there is the good support today from OSes, devices and applications
- SDOs (3GPP, IETF) have decided to put more efforts on IPv6 technology and IPv6 will have more functionality in the future: this will increase the technical advantages against IPv4
- Many governments are starting to push for IPv6
- IPv6-only has been successfully deployed in some scenarios, such as mobile network, and it is the time for industry to consider it in the coming future.
- The user device – network – content communication chain is ready for IPv6, and companies that have deployed IPv6 have had success in moving more and more users and traffic to IPv6

Given this background and given that IPv6 enhanced innovations for new technologies such as 5G, IoT, cloud computing will bring many new opportunities for the industry, it is beneficial for ETSI to start a new ISG to study and promote such opportunities. We also call on all parties to actively participate in this effort, as IPv6 is bringing a new era to the networking industry, and it is up to us to maximize the potential of this new era with the enhanced innovations.

Annex A: A brief review of relevant ISG IP6 GRs

IPv6 Deployment in the Enterprise, ETSI GR IP6 001 V1.1.1 [IP6-1]

This GR published on June 2017, outlines the motivation for the deployment of IPv6 within enterprises, the objectives, the benefits, the risks, the challenges, the technology guidelines, the different choices that arise when designing IPv6-only or dual-stack enterprise network, step-by-step process, the addressing plan, and the milestones.

Moreover, it provides guidelines and recommendations on IPv6 deployment in the enterprise. The provided guidelines and recommendations include the steps that need to be followed by Enterprises in order to deploy IPv6. These steps relate to:

(1) Transition deployment models,
(2) Enterprise Design Considerations - Building a cross functional team,
(3) Preparation and Assessment Phase,
(4) IPv6 address plan,
(5) Address Management
(6) Routing considerations.

In addition, an example is provided on how these guidelines can be applied in IPv6 Data Centers. Other topics that are considered are (a) key elements that can be used to build an IPv6 Internet Presence in Enterprises and (b) Security;

One of the key derived conclusions of this GR is that there is no single recipe for IPv6 transformation. Each enterprise is unique and depends on its unique business goals, long-term vision and constraints. It is critical to put in place a joint Business & IT Task Force. This will help ensuring a smooth path toward IPv6. A pragmatic roadmap for an IPv6 transition, while also developing clear business benefits that can be achieved through the transition, is needed.

Generic migration steps from IPv4 to IPv6, ETSI GR IP6 006 V1.1.1 [IP6-2]

This GR published in November 2017, outlines the generic transition steps from IPv4 to IPv6, including the transition necessity, principles and technology guidelines, generic transition steps, security implications and the generic step-by-step process.

The IPv4 to IPv6 transition technologies are used for one of the following goals: (a) providing IPv6 connectivity and (b) providing IPv4 connectivity (usually by multiplexing multiple devices in the same IPv4 address). This GR briefly describes the transition technologies used to satisfy each of these two goals. In particular, the IPv4 to IPv6 transition technologies used to provide IPv6 connectivity are:

(1) Dual-Stack,
(2) Configured tunnels (6in4),
(3) Generic Routing Encapsulation (GRE),
(4) IPv6 Rapid Deployment (6rd),
(5) Native IPv6 behind NAT44 CPEs (6a44),
(6) Intra-Site Automatic Tunnel Addressing Protocol (ISATAP),
(7) Connection of IPv6 Domains via IPv4 Clouds (6to4),

(8) Tunnelling IPv6 over UDP through NATs (Teredo),
(9) IPv6 over IPv4 without Explicit Tunnels (6over4),
(10) Anything In Anything (AYIYA),
(11) IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP).

Moreover, the IPv4 to IPv6 transition technologies used for providing IPv4 connectivity, described in this GR are:

- Stateless IP/ICMP Translation Algorithm (SIIT),
- Stateful NAT64,
- Combination of Stateful and Stateless Translation (464XLAT),
- Dual-Stack Lite (DS-Lite),
- Mapping of Address and Port – Encapsulation (MAP-E)
- Mapping of Address and Port – Translation (MAP-T).

Furthermore, this GR provides examples of IPv4 to IPv6 transition scenarios deployed by Operators in France, China and United States. Moreover, this GR discusses IPV4 to IPv6 transition pitfalls, which are: (1) tunneling issue denoted as "black-holes", where dropped packets are observed, due the decrease of Path-MTU and the dropping of ICMP error messages, (2) dual-stack issue, where long delays to establish TCP connections are observed, caused by the use of dual-stack nodes.

IPv6-based Internet of Things Deployment of IPv6-based Internet of Things, ETSI GR IP6 008 V1.1.1 **[IP6-3]**

This GR published in June 2017, outlines the motivation for IPv6 in IoT, the technical challenges to address IoT on constrained devices and networks, the impact on the IPv6 technology and protocols, the technology guidelines, the step by step process, the benefits and the risks, as applicable to IoT domains. These IoT domains are including: M2M, Energy, Industrial, Mining, Oil and gas, Smart city, Transportation (including EVs), etc. In this context, IPv6-based IoT, refers to the connectivity network layers needed to support the communication between things.

The key driver for the introduction of IPv6 in IoT, is the large address space that IPv6 is providing. However, other drivers can be identified, such as auto-configuration, security and flow identification (i.e., usage of the 3-tuple of the Flow Label, Source Address, and Destination Address fields), and as well that IPv6 is being a future proof technology.

As impact of the IoT on the IPv6 technology and protocols, the following protocols and concepts can be identified:

(1) Routing Protocols: Routing over Low Power and Lossy Networks (Roll),

(2) Transport protocols: Constrained Restful Environments (CoRE),

(3) IPv6 Neighbour Discovery,

(4) Adaptation Layers: IPv6 over Networks of Resource-constrained Nodes (6Lo)

(5) Low Power and Wide Area Networking (LPWAN).

This GR describes briefly the Deterministic Networking DetNet/6TiSCH concept as a specific market deployment consideration in the Industrial Internet.

As lessons learned, this GR provides information about the use of IPv6 for the Smart Grid domain, focusing on: (1) Power Automation use case and (2) Field Area Network use case for Electric Distribution Network and smart metering. Moreover, this GR lists several advantages of using IPv6 network services when deploying IoT. The mentioned IPv6 network services are:

(1) Unique device's addressing,

(2) Address auto-configuration,

(3) Media independency,

(4) Routing,

(5) Data Integrity, Confidentiality and Privacy,

(6) Multicast,

(7) Quality of Services (QoS),

(8) Network Segmentation and isolation,

(9) Time Distribution

(10) Management.

IPV6-based Industrial Internet Leveraging 6TISCH Technology, ETSI GR IP6 009 V1.1.1 [IP6-4]

This GR published in March 2017, outlines a general architecture for an Industrial Internet, providing motivation for the deployment and technical guidelines with a focus on deterministic and low power technologies, for a prospective IPv6-based Industrial Internet leveraging deterministic wireless technology. In particular, this GR elaborates on deterministic networking in wired and wireless environments, for application in the Industrial Internet.

The key attributes of deterministic networking are:

- time synchronization on all the nodes, often including source and destination,
- the centralized computation of network-wide deterministic paths,
- new traffic shapers within and at the edge to protect the network
- hardware for scheduled access to the media.

Both wired and wireless networks are evolving towards more determinism, in particular with work done at the IEEE 802.1 for bridged Ethernet networks, and at IEEE 802.15 for Low-power Wireless PANs. However, the techniques used in wired and wireless environments are largely different. The Deterministic Networking (DetNet) working group at the IETF is now considering the establishment of end-to-end paths with Deterministic properties from the perspective of Layer 3, hopefully to be applied at 6TiSCH for the particular case of LWPANs.

In particular, this GR defines that the applicability of the various techniques proposed, really depends on the use case and the imposed requirements on the underlying IPv6 network. As future work, this GR

proposes that enabling determinism on wired and wireless networks separately is certainly not the end of the journey. Future activities need to focus on solutions to maintain deterministic properties at the interconnection of wired and wireless networks.

IPv6-based SDN and NFV; Deployment of IPv6-based SDN and NFV, ETSI GR IP6 010 V1.1.1 [IP6-5]

This GR published in December 2017, outlines the motivation for the deployment of IPv6-based Cloud Computing, the objectives, the technology guidelines, the step-by-step process, the benefits, the risks, the challenges and the milestones. SDN/NFV concepts and technologies can be used to enable network programmability and accelerate and optimize the deployment of the IPv4 to IPv6 transition strategies. An IPv4 to IPv6 transition powered by SDN could lower the deployment and operational costs by decoupling the data plane and control plane, and by providing unified data plane devices/entities. Moreover, it enables the development of native IPv6 services through the availability of open Northbound APIs.

During the IPv6 transition period, the network will go through three stages: IPv4-only network, dual-stack network and IPv6-only network. The target is that the network should support both IPv4 services and IPv6 services at each stage. This GR describes some of the key issues related to the deployment of the IPv4 to IPv6 transition strategies, such as (1) evolving from one IPv4 to IPv6 transition scenario to another will require that the network should support both IPv4 services and IPv6 services at each stage, (2) coexistence of multiple transition mechanisms is costly and can add significant complexity to an already complex environment, (3) scattered address pools, where different address pools need to be used when configuring devices that support multiple transition mechanisms, (4) extensibility, which can be realized by offering open and programmable ways to easily add these new features without modifying existing device hardware. The SDN/NFV concepts can be used to solve some of the implications caused by these issues.

This GR introduces as well an open IPv6 Architecture, powered by SDN, and the application of SDN and NFV to support network programmability. In particular, in the IPv6 transition scenarios, the SDN help the ISP to guide IPv4 / IPv6 traffic to the appropriate network function (or virtual network function) automatically, the NFV allows the ISP to deploy virtual IPv4 / IPv6 network function in the same infrastructure.

IPv6-Based 5G Mobile Wireless Internet; Deployment of IPv6-Based 5G Mobile Wireless Internet, ETSI GR IP6 011 V1.1.1 [IP6-6]

This GR published in October 2018, outlines the motivation for the deployment of IPv6-based 5G Mobile Internet, the objectives, the technology guidelines, the step-by-step process, the benefits, the risks, the challenges and the milestones for this deployment. With the rapid development of the 5G network infrastructure, and as well as other technology enablers such as IoT, mobile Internet, cloud computing, Software Defined Networking (SDN), virtualization, smart home and Internet of vehicles, there is a consensus between different stakeholders that the demand of Internet is no longer limited to the exhausting IP address, but extends to the end-to-end interconnection and permanently stable IP address. One of the main challenges associated with the above is associated with how gradually to stop IPv4, deploy IPv6 in full scale and start using the Internet of the 21st century.

This GR briefly describes the main IPv6 transition strategies that are being discussed by Mobile Network Operators (MNOs), which are: (1) IPv4 only, (2) Coexistence of IPv4 and IPv6, (3) IPv6 only, (4) Enhanced IPv6 only + NAT64 and (5) Enhanced IPv6 only + 464XLAT.

The best cases on IPv6 transition strategies in cellular networks presented in this GR are associated with mobile operators, content delivery network providers and social media providers. In particular the best cases deployed by Operators, are: (a) two examples by Operators in USA, (b) four examples by Operators in Europe and (c) two examples by Operators in China. Moreover, two best cases examples deployed by Content Delivery Networks providers and one best case example deployed by a Social media provider are presented in this GR;

One of the key lessons learned is that the sooner a cohesive strategy for 5G and IPv6 is developed and applied into among others in standardization and research, the sooner the benefits and risks of using IPv6 in 5G will be verified and validated. 5G will help vertical industries to achieve the IoT vision of ubiquitously connected, highly reliable, ultra-low latency services for massive number of devices. Furthermore, IPv6 can enable the scalability required by the IoT and can provide enhancements to IPv4 based solutions in the field of for example, mobility support, stateless address auto-configuration, support of constraint devices and security.

6TiSCH Interoperability Test Specifications, ETSI GR IP6 017 V1.1.1 [IP6-7]

This GR published in January 2019, aims to provide guidelines for performing 6TiSCH Conformance and Interoperability Tests. The Conformance and Interoperability test methodologies used in this GR are based on the well-established test methodologies, presented in ETSI EG 202 237 and ETSI EG 202 568. Conformance Testing aims at verifying whether a product correctly implements a particular standardized protocol. Thus, it establishes whether or not the protocol Implementation Under Test (IUT) meets the requirements specified for the protocol itself. Interoperability Testing aims at checking whether a product works with other similar products. Thus, it proves that end-to-end functionality between (at least) two devices (from different vendors) is, as required by the standard(s) implemented on those devices.

This GR provides:

- The testbed architecture showing which IETF 6TiSCH systems and components are involved, and how they are going to inter-work in the interoperation focus.
- The configurations used during test sessions, including the relevant parameter values of the different layers (IEEE 802.15.4e TSCH and RPL).
- The interoperability test descriptions, describing the scenarios, which the participants will follow to perform the tests.
- The guidelines for participants on how to use the *golden device* to test against their implementation.

Annex B: IPv6 prefix & address assignment at the CPEs: Message Sequence Charts

B.1 IPv6 prefix and address assignment at the CPEs

As already described in the main body of this whitepaper, the key difference from acquiring IPv6 addresses for MBB, FBB and enterprise CPEs, from acquiring IPv4 address is the use of SLAAC.

A difference that needs as well to be emphasized is the concept of the stateful DHCP versus the stateless DHCP. The typically used DHCP, is the stateful DHCP server that stores and maintains information per host, e.g., the IP address of each host, while in Stateless DHCP, the information per host is not maintained, but it uses information that is common to all hosts, e.g., a DNS server's address. In Stateful DHCP, the server must keep track of information per host, e.g., the IP address of each host, while in Stateless DHCP, the information is common to all hosts and need not to be tracked per host. That is why it is called stateless.

B.1.1. For MBB UEs

The figure below shows the step-by-step procedure of how a UE acquires an IPv6 address and establishes an IPv6 connection to the mobile gateway. Note that the steps not relevant to IPv6 are ignored.

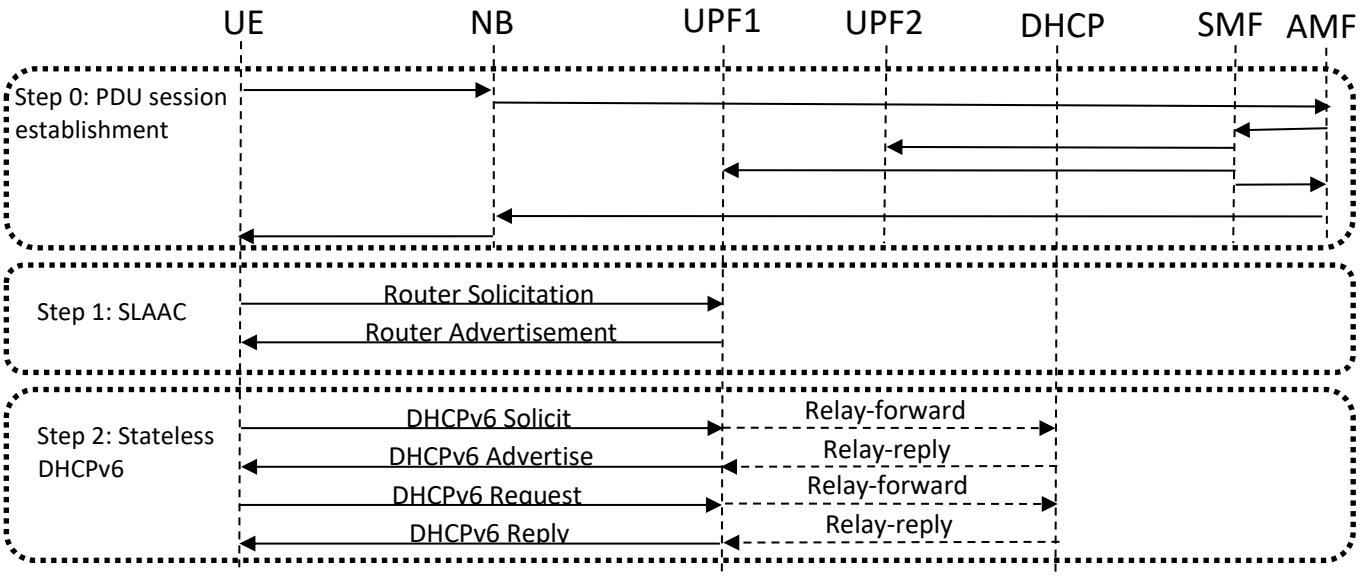

Figure B.1: IPv6 address acquisition at MBB CPE

- Step 0: Everything is the same as in IPv4, except that the PDU session type will be IPv4v6 (Dual-Stack) or IPv6

- Step 1: SLAAC is initiated by UE. The User Plane Function (UPF), (that corresponds to Packet Data Network (PDN) gateway in 4G) advertises Interface ID that UE should use to avoid address duplication and the need for Duplicate Address Detection (DAD). In particular, International Mobile Subscriber Identity (IMSI) is prohibited to be used as Interface ID.

  For SLAAC: Router Advertisement [RFC 4861] from UPF would deliver to UE some important parameters like MTU, default router, and DNS.

- Step 2: If UE needs other parameters, then the UE would initiate stateless DHCPv6 [RFC 8415]. Between [RFC 6459] and [RFC 7849], the recommendation of stateless DHCPv6 has changed from "not needed" to "mandatory". The primary reason is a need for Prefix Delegation (PD) – UE can be a CPE (hot spot) with LAN behind it. The Prefix Exclude Option for DHCPv6-based Prefix Delegation is mandatory. The purpose is to use the same aggregated prefix for both WAN and LAN. Another reason to prioritize DHCP is the popularity of 464XLAT which needs PREFIX64 that is typically delivered via DHCP.

  If the UE receives the same parameters at different stages, e.g. from both SLAAC and DHCP, then the earlier stage would take priority.

  When UE is acting as a hot spot, parameters received on the WAN (MTU, DNS, RA) should be advertised on the LAN only if WAN is active.

B.1.2 For FBB RGs

A FBB RG may use PPPoE or IPoE to establish connection to BNG. This White Paper focuses on PPPoE and ignores IPoE to limit the size.

RGs will use the following procedure to obtain an IPv6 address and establish IPv6 connectivity at the WAN side to the operator network:

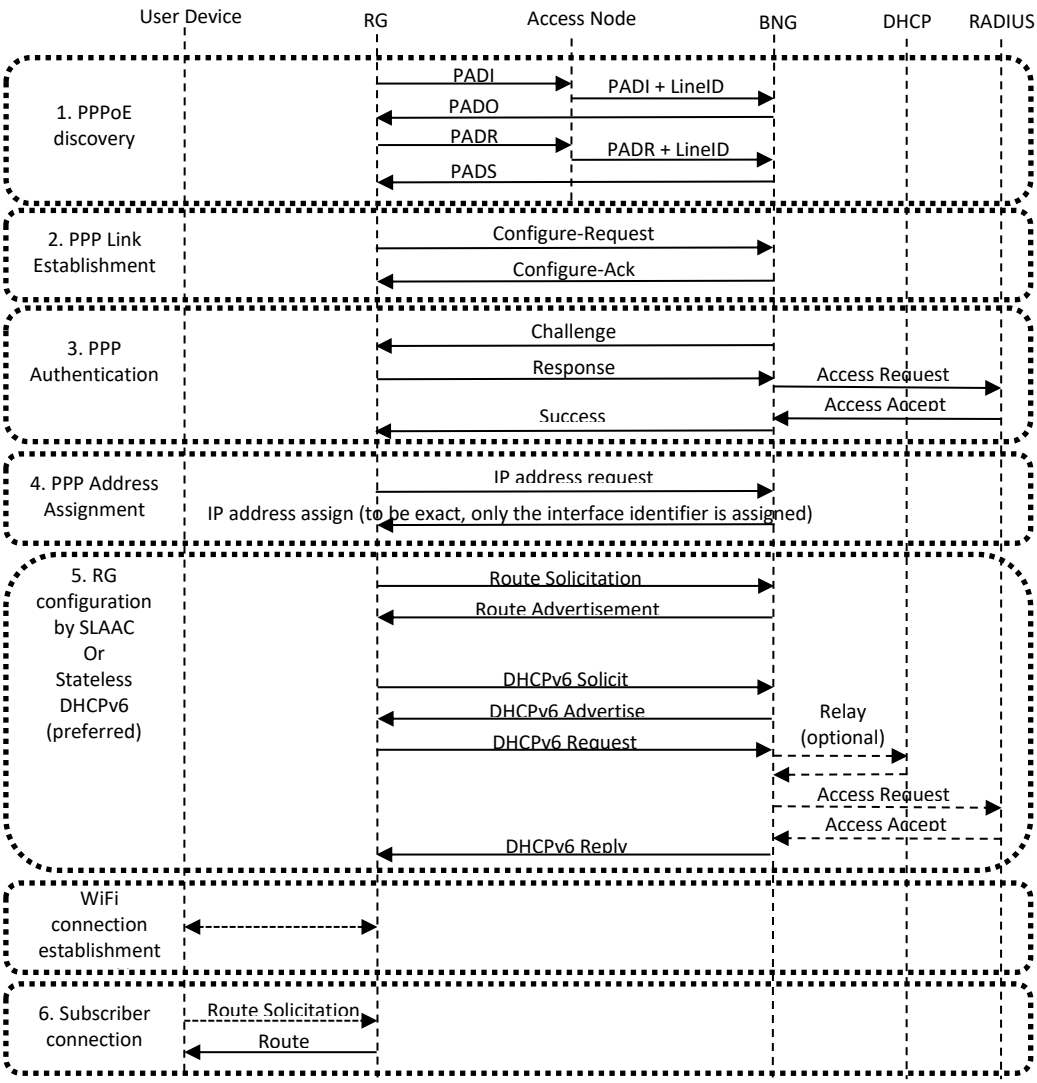

Figure B.19 Example of an IPv6 prefix assignment procedure by CPE

- In steps 1-3, the RG establishes PPP connection with BNG; this process is the same for IPv6 and IPv4.

- In step 4, the RG uses IPv6CP [RFC 5072] to negotiate the interface identifier with the BNG. The interface identifier will then be used to generate the IPv6 address via SLAAC in step 5.

- In step 5, the RG uses SLAAC to generate an IPv6 address for the WAN connection. It is also possible to get some parameters by SLAAC (DNS, Default gateway), but the primary method is to get these and other parameters by Stateless DHCPv6 [RFC 8415]. Other parameters include Prefix Delegation for the LAN behind the RG, Session Initiations Protocol (SIP) server address, TR-069/CWMP (CPE WAN Management Protocol) server address.

- Step 6: the RG can announce itself as a router to LAN hosts only after WAN link initialization is finished (chapter 3.2.1 of [RFC 7084]). A simplified procedure of SLAAC is recommended for

user/hosts addresses assignment with minimal parameters configuration (MTU, DNS, and Default Router).

Annex C: List of Abbreviations

- 464XLAT - Combination of Stateful and Stateless Translation
- 6a44 - Native IPv6 behind NAT44 CPEs
- 6in4 - Configured tunnels (6in4),
- 6lo - IPv6 over Networks of Resource-constrained Nodes
- 6man- IPv6 Maintenance
- 6over4 - IPv6 over IPv4 without Explicit Tunnels
- 6rd - IPv6 Rapid Deployment
- 6tisch - IPv6 over the TSCH mode of IEEE 802.15.4e
- 6to4 - Connection of IPv6 Domains via IPv4 Clouds
- AFTR - Address Family Transition Router
- AYIYA - Anything In Anything
- ASIC - Application-Specific Integrated Circuit
- B4 - Basic Bridging Broadband
- CAICT - China Academy of Information and Communications Technology
- CAPEX – Capital Expenses
- CG NAT – Carrier-Grade NAT
- CAGR- Compound Annual Growth Rate
- CDN - Content Delivery Network
- CLAT - client side NAT46
- CPE - Customer Premises Equipment
- DAD - Duplicate Address Detection
- DC - DataCenter
- DDOS - Denial-of-Service
- DetNet - Deterministic Networking
- DSL - Digital Subscriber Line
- DNS – Domain Name System
- DNSSEC - DNS security
- DS-Lite - Dual stack Lite
- ECMP - Equal Cost Multipath
- FBB - Fixed BroadBand
- FTTH - Fiber to the Home
- FTTX - Fiber to the X
- GRE - Generic Routing Encapsulation
- GR - Group Report
- GTP - GPRS Tunnelling Protocol
- IAB - Internet Architecture Board
- ICT - Information and Communications Technology
- ICMP - Internet Control Message Protocol
- IEC – International Electrotechnical Commission
- IETF - Internet Engineering Task Force
- IMSI - International Mobile Subscriber Identity
- IoT - Internet of Things

- IT - Information Technology
- IP6 - IPv6 Integration
- IPv6 - Internet Protocol version 6
- IPv6CP - IPv6 Control Protocol
- ISATAP - Intra-Site Automatic Tunnel Addressing Protocol
- KPI - Key Performance Indicator
- LPWAN- Low Power Wide Area Network
- lw4o6 - Lightweight 4over6
- MAP-E - Mapping of Address and Port – Encapsulation
- MAP-T - Mapping of Address and Port – Translation
- MBB - Mobile BroadBand
- MT – modem
- MSS - Maximum Segment Size
- NAT – Network Address Translation
- ND – Neighbor Discovery
- NSP - Network-Specific Prefix
- OMB - US Office of Management Bureau
- OPEX – Operational Expenses
- OS - Operating System
- OT - Operational Technology
- OTT – Over The Top
- PA - Provider Aggregable
- PEF - Packet Forwarding Engines
- PDN - Packet Data Network
- PFEs - Packet Forwarding Engines
- PLAT - provider side NAT64
- PLT - Webpage Page Load Time
- PPPoE - PPP Over Ethernet
- PPPv6 - Point-to-Point Protocol v6
- RAW - Reliable and Available Wireless
- RDNSS - Recursive DNS Server
- RIR - Regional Internet Registry
- ROLL - Routing Over Low power and Lossy networks
- RPL - Routing for low Power and Lossy networks
- RTT – Round Trip Time
- Standalone – SA
- SDO - Standard Development Organization
- SIIT - Stateless IP/ICMP Translation Algorithm
- SIP – Session Initiation Protocol
- SPRING - Source Packet Routing in Networking
- TE - Terminal
- Teredo - Tunnelling IPv6 over UDP through NATs
- TSCH - Time Slotted Channel Hopping
- UE – User Equipment

- V2X - Vehicle to X
- WKP - Well-Known Prefix

Annex D: References

[1] INTERNET ARCHITECTURE BOARD: STATEMENT ON IPV6 https://www.iab.org/2016/11/07/iab-statement-on-ipv6/

[APNIC_2] https://blog.apnic.net/2019/06/06/100-by-2025-china-getting-serious-about-ipv6/

[IP6-1] ETSI GR IP6 001 V1.1.1 (2017-06): "IPV6 DEPLOYMENT IN THE ENTERPRISE". https://www.etsi.org/deliver/etsi_gr/IP6/001_099/001/01.01.01_60/gr_ip6001v010101p.pdf

[IP6-2] ETSI GR IP6 006 V1.1.1 (2017-11): "GENERIC MIGRATION STEPS FROM IPV4 TO IPV6". https://www.etsi.org/deliver/etsi_gr/IP6/001_099/006/01.01.01_60/gr_ip6006v010101p.pdf

[IP6-3] ETSI GR IP6 008 V1.1.1 (2017-06): "IPV6-BASED INTERNET OF THINGS DEPLOYMENT OF IPV6-BASED INTERNET OF THINGS". https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_ip6008v010101p.pdf

[IP6-4] ETSI GR IP6 009 V1.1.1 (2017-03): "IPV6-BASED INDUSTRIAL INTERNET LEVERAGING 6TISCH TECHNOLOGY". https://www.etsi.org/deliver/etsi_gr/IP6/001_099/009/01.01.01_60/gr_ip6009v010101p.pdf

[IP6-5] ETSI GR IP6 010 V1.1.1 (2017-12): "IPV6-BASED SDN AND NFV; DEPLOYMENT OF IPV6-BASED SDN AND NFV". https://www.etsi.org/deliver/etsi_gr/IP6/001_099/010/01.01.01_60/gr_ip6010v010101p.pdf

[IP6-7] ETSI GR IP6 017 V1.1.1 (2019-01): https://www.etsi.org/deliver/etsi_gr/IP6/001_099/017/01.01.01_60/gr_IP6017v010101p.pdf

[RESEARCH] LIST OF LINKS USED TO FILL IN THE TABLES IN THE FIGURES:

https://www.altibox.no/privat/bredband/ipv6/

https://indico.uknof.org.uk/event/38/contribution/8/material/slides/1.pdf

https://pc.nanog.org/static/published/meetings/NANOG71/1452/20171004_Gottlieb_Mapping_Of_Address_v1.pdf

http://labs.comcast.com/world-ipv6-launch-four-years-later

https://www.heise.de/newsticker/meldung/IPv4-Daemmerung-Telekom-testet-IPv6-only-Kommunikation-im-Mobilfunk-4150047.html

https://www.heise.de/newsticker/meldung/Telekom-startet-IPv6-Einfuehrung-im-Mobilfunknetz-2741029.html

https://telekomhilft.telekom.de/t5/All-IP-das-digitale-Netz/IPv4-oder-DualStack/td-p/2614214

https://bb6-ie.blogspot.com/2018/08/updates-to-eir-fibre-ipv6-support.html

https://www.emome.net/channel?chid=911

http://ipv6.forthnet.gr/

https://www.lrz.de/services/netz/ipv6/

https://www.marwan.ma/index.php/services/connectivites/ipv6

https://www.netcologne.de/privatkunden/ipv6

https://twitter.com/zajdee/status/1156496837437771776

https://www.nextinpact.com/brief/ipv6-active-pour-10---des-clients-mobiles-orange-et-sosh-426.htm

https://assistance.orange.fr/livebox-modem/toutes-les-livebox-et-modems/installer-et-utiliser/piloter-et-parametrer-votre-materiel/le-parametrage-avance-reseau-nat-pat-ip/gerer-votre-adresse-ip/ipv6-chez-orange_238184-528413

https://www.ripe.net/participate/meetings/regional-meetings/ipv6-day-denmark/presentations/4-tomasz-ipv6_day_kopenhagen_v4.pdf

https://www.root.cz/zpravicky/slovensky-orange-nasadil-ipv6-na-dsl-za-ipv4-chce-99-eur/

https://www.internetsociety.org/resources/deploy360/2014/case-study-how-romanias-rcsrds-deployed-ipv6/

https://blog.apnic.net/2017/02/07/reliance-jio-boosts-india-past-20-ipv6-capability/

https://labs.ripe.net/Members/richard_patterson/connecting-5-million-users-to-ipv6

https://arstechnica.com/information-technology/2016/08/sky-will-push-all-subscribers-onto-ipv6-network-by-summer-2016/

https://help.sonic.com/hc/en-us/articles/236083487-Fusion-IPv6-Tool

https://www.telekom.si/zasebni-uporabniki/ponudba/internet/internetne-storitve/protokol-ipv6

https://blog.apnic.net/2017/01/13/TELSTRAS-FIVE-YEAR-MOBILE-IPV6-PLAN-BECOMES-REALITY/

https://online.ptc.org/assets/uploads/papers/ptc17/PTC17_Sun_APNIC%20WS_Yeung.pdf

https://conference.apnic.net/data/39/5-mf-motohashi-201503-apricot-dslite-deployment_1425422341.pdf

http://www.mynewsdesk.com/se/tre/pressreleases/tre-framtidssaekrar-naetet-med-naesta-generations-internetprotokoll-ipv6-2365944

https://forums.verizon.com/t5/Fios-Internet/IPv6-for-Residential-Customers/td-p/831549

https://community.ziggo.nl/internetverbinding-102/dual-stack-ipv6-43692

[RFC 1858] https://datatracker.ietf.org/doc/rfc1858/

[RFC 1918] https://datatracker.ietf.org/doc/rfc1918/

[RFC 3972] https://datatracker.ietf.org/doc/rfc3972/

[RFC 4861] https://datatracker.ietf.org/doc/rfc4861/

[RFC 4862] https://datatracker.ietf.org/doc/rfc4862/

[RFC 4890] https://datatracker.ietf.org/doc/rfc4890/?include_text=1

[RFC 4941] https://datatracker.ietf.org/doc/rfc4941/

[RFC 4942] https://datatracker.ietf.org/doc/rfc4942/

[RFC 5072] https://datatracker.ietf.org/doc/rfc5072/

[RFC 5549] https://datatracker.ietf.org/doc/rfc5549/

[RFC 5722] https://datatracker.ietf.org/doc/rfc5722/

[RFC 6036] https://datatracker.ietf.org/doc/rfc6036/

[RFC 6146] https://datatracker.ietf.org/doc/rfc6146/

[RFC 6147] https://datatracker.ietf.org/doc/rfc6147/

[RFC 6333] https://datatracker.ietf.org/doc/rfc6333/

[RFC 6459] https://datatracker.ietf.org/doc/rfc6459/

[RFC 6540] https://datatracker.ietf.org/doc/rfc6540/

[RFC 6583] https://datatracker.ietf.org/doc/rfc6583/

[RFC 6877] https://datatracker.ietf.org/doc/rfc6877/

[RFC 7051] https://datatracker.ietf.org/doc/rfc7051/

[RFC 7084] https://datatracker.ietf.org/doc/rfc7084/

[RFC 7217] https://datatracker.ietf.org/doc/rfc7217/

[RFC 7381] https://datatracker.ietf.org/doc/rfc7381/

[RFC 7721] https://datatracker.ietf.org/doc/rfc7721/

[RFC 7755] https://datatracker.ietf.org/doc/rfc7755/

[RFC 7849] https://datatracker.ietf.org/doc/rfc7849/

[RFC 8064] https://datatracker.ietf.org/doc/rfc8064/

[RFC 8200] https://datatracker.ietf.org/doc/rfc8200/

[RFC 8321] https://datatracker.ietf.org/doc/rfc8321/

[RFC 8415] https://datatracker.ietf.org/doc/rfc8415/

[RFC 8585] https://datatracker.ietf.org/doc/rfc8585/

[RFC 8754] https://datatracker.ietf.org/doc/rfc8754/

[SRV6-PROG] https://datatracker.ietf.org/doc/draft-ietf-spring-srv6-network-programming/

[SR-SERVICE-PROG] https://datatracker.ietf.org/doc/draft-ietf-spring-sr-service-programming/

[NTF] https://datatracker.ietf.org/doc/draft-ietf-opsawg-ntf/

[IFIT-FRAMEWORK] https://datatracker.ietf.org/doc/draft-song-opsawg-ifit-framework/

[IPv6-ALT-MARK] https://datatracker.ietf.org/doc/draft-ietf-6man-ipv6-alt-mark/

[ENHANCED-VPN] https://datatracker.ietf.org/doc/draft-ietf-teas-enhanced-vpn

[LMHP-V6OPS] https://datatracker.ietf.org/doc/draft-lmhp-v6ops-transition-comparison/

[LINKOVA] https://datatracker.ietf.org/doc/draft-linkova-6man-grand/

[FGONT] https://datatracker.ietf.org/doc/draft-fgont-6man-rfc4941bis

[RIFT] https://datatracker.ietf.org/doc/draft-ietf-rift-rift/

[AP-ND] https://datatracker.ietf.org/doc/draft-ietf-6lo-ap-nd/

[SRH-COMP] https://datatracker.ietf.org/doc/draft-filsfilscheng-spring-srv6-srh-comp-sl-enc

[USID] https://datatracker.ietf.org/doc/draft-filsfils-spring-net-pgm-extension-srv6-usid

[GSRV6] https://datatracker.ietf.org/doc/draft-cl-spring-generalized-srv6-for-cmpr

[APN6-FRAMEWORK] https://datatracker.ietf.org/doc/draft-li-apn6-framework

[APN6-USE-CASES] https://datatracker.ietf.org/doc/draft-li-apn6-problem-statement-usecases

[ITU RES 180] https://www.itu.int/en/council/Documents/basic-texts/RES-180-E.pdf

[APNIC_1] https://stats.labs.apnic.net/

[APNIC_2] https://blog.apnic.net/2019/06/06/100-by-2025-china-getting-serious-about-ipv6/

[AMS-IX] https://stats.ams-ix.net/index.html

[IX.BR] https://ix.br/

[WIKI] https://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems

[W3TECH] https://w3techs.com/technologies/overview/site_element

[HURRICANE ELECTRIC] https://bgp.he.net/

[POTAROO] https://bgp.potaroo.net/index-v6.html

[ISOC_1] https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[ISOC_2] https://www.internetsociety.org/resources/deploy360/2014/case-study-t-mobile-us-goes-ipv6-only-using-464xlat/

[ISOC_3] https://www.internetsociety.org/resources/deploy360/2014/case-study-facebook-moving-to-an-ipv6-only-internal-network/

[3GPP] https://www.3gpp.org/ftp/tsg_ct/tsg_ct/TSGC_78_Lisbon/Docs/

[OMB] HTTPS://WWW.CIO.GOV/ASSETS/RESOURCES/INTERNET-PROTOCOL-VERSION6-DRAFT.PDF

[McKillop] https://teamarin.net/2019/04/03/microsoft-works-toward-ipv6-only-single-stack-network/

[FAN] http://www.dco.cce.i.kyoto-u.ac.jp/en/PL/PL_2019_01.html

[IPV6-PARAMETERS] HTTPS://WWW.IANA.ORG/ASSIGNMENTS/IPV6-PARAMETERS/IPV6-PARAMETERS.XHTML

Acknowledgement

The authors would like to acknowledge the contributions from

- Hui Tian, CAICT
- Weiqiang Cheng, China Mobile
- Ming Feng, China Telecom
- Clarence Filsfils, Cisco
- Zhenbin Li (Robin), Chenxi Wang, Eduard Vasilenko, Paolo Volpato, Stefano Giachetti, Aldo Artigiani, Huawei
- Mariusz Krukowski, T-Mobile Poland
- and other contributors who choose to be anonymous.

Their contributions make this whitepaper possible, and greatly improve its quality.

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org