ETSI GR IP6 011 V1.1.1 (2018-10)

IPv6-Based 5G Mobile Wireless Internet; Deployment of IPv6-Based 5G Mobile Wireless Internet

Disclaimer

Reference
DGR/IP6-0011

Keywords
5G, internet, IPv6, mobile

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) IPv6 Integration (IP6).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document 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.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Alcatel-Lucent Strategic White Paper (April 2015): "464XLAT in mobile networks IPv6 migration strategies for mobile networks".

[i.2] IETF RFC 6342 (December 2011): "Mobile Networks Considerations for IPv6 Deployment".

[i.3] ETSI GR IP6 006: "Generic migration steps from IPv4 to IPv6".

[i.4] NGMN Alliance (version 1.0): "NGMN 5G White paper", 17 February 2015.

[i.5] 3GPP TR 22.891 (V14.1.0): "Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)", September 2016.

[i.6] 3GPP TR 22.861 (V14.0.0): "Feasibility Study on New Services and Markets Technology Enablers for Massive Internet of Things; Stage 1 (Release 14)", June 2016.

[i.7] 3GPP TR 22.862 (V14.0.0): "Feasibility Study on New Services and Markets Technology Enablers - Critical Communications; Stage 1 (Release 14)", June 2016.

[i.8] 3GPP TR 22.863 (V14.0.0): "Feasibility Study on New Services and Markets Technology Enablers - Enhanced Mobile Broadband; Stage 1 (Release 14)", June 2016.

[i.9] 3GPP TR 22.864 (V14.0.0): "Feasibility Study on New Services and Markets Technology Enablers - Network Operation; Stage 1 (Release 14)", June 2016.

[i.10] 3GPP TR 23.799 (V0.5.0): "Study on Architecture for Next Generation System (Release 14)", December 2016.

[i.11] ETSI TS 123 501 (V15.2.0): "5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15)".

[i.12] ETSI TS 123 502 (V15.2.0): "5G; Procedures for the 5G System (3GPP TS 23.502 version 15.2.0 Release 15)".

[i.13] 3GPP TR 33.899 (V0.2.0): "Study on the security aspects of the next generation system (Release 14)", May 2016.

[i.14] 3GPP TR 38.913 (V0.3.0): "Study on Scenarios and Requirements for Next Generation Access Technologies (Release 14)", March 2016.

[i.15] Recommendation ITU-R M.2083 (September 2015): "IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond".

[i.16] ITU-R report M.2135 (December 2009): "Guidelines for evaluation of radio interface technologies for IMT-Advanced".

[i.17] IETF RFC 3316 (April 2003): "Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts".

[i.18] IETF RFC 7084 (November 2013): "Basic Requirements for IPv6 Customer Edge Routers".

[i.19] IETF RFC 7066 (November 2013): "IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts".

[i.20] IETF RFC 6434 (December 2011): "IPv6 Node Requirements".

[i.21] IETF RFC 7278 (June 2014): "Extending an IPv6 /64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link".

[i.22] IETF RFC 7445 (March 2015): "Analysis of Failure Cases in IPv6 Roaming Scenarios".

[i.23] IETF RFC 6459 (January 2012): "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)".

[i.24] IETF RFC 4213 (October 2005): "Basic Transition Mechanisms for IPv6 Hosts and Routers".

[i.25] IETF RFC 1918 (February 1996): "Address Allocation for Private Internets".

[i.26] ITU-T, Study Group 13, TD 208 (PLEN/13): "Report on Standards Gap Analysis", December 2015.

NOTE: Available at http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Documents/T13-SG13-151130-TD-PLEN-0208%21%21MSW-E.docx.

[i.27] R, Chandler and ARIN staff: "The introduction of IPv6 to the 3GPP Standards and Mobile Networks", ARIN wiki, last modified on 20 June 2015.

NOTE: Available at https://getipv6.info/display/IPv6/3GPP+Mobile+Networks.

[i.28] IETF RFC 3633 (December 2003): "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".

[i.29] IETF RFC 3769 (June 2004): "Requirements for IPv6 Prefix Delegation".

[i.30] IETF RFC 7755 (February 2016): "SIIT-DC: Stateless IP/ICMP Translation for IPv6 Data Center Environments".

[i.31] Internet Society Deploy360 (June 2014): "Case Study: T-Mobile US Goes IPv6-only Using 464XLAT".

NOTE: Available at http://www.internetsociety.org/deploy360/resources/case-study-t-mobile-us-goes-ipv6-only-using-464xlat/.

[i.32] NANOG 61 (June 2014): "464XLAT: Breaking Free of IPv4", C. Byrne.

NOTE: Available at https://www.nanog.org/sites/default/files/wednesday_general_byrne_breakingfree_11.pdf.

[i.33] IETF RFC 6877 (April 2013): "464XLAT: Combination of Stateful and Stateless Translation".

[i.34] APNIC 34, IPv6 at Verizon Wireless, August 2012.

NOTE: Available at https://www.apnic.net/wp-content/uploads/2017/01/vzw_apnic_13462152832-2.pdf.

[i.35] IETF RFC 6674 (July 2012): "Gateway-Initiated Dual-Stack Lite Deployment".

[i.36] IPv6 council meeting at Nokia Antwerp, Belgium (May 2016): "Telenet Update", C. Wuyts.

NOTE: Available at https://www.ipv6council.be/IMG/pdf/03_IPv6_Council_-_Telenet_Update_-_may2016.pdf.

[i.37] IPv6 Council (May 2016): "IPv6 in eir", R. Chandler.

NOTE: Available at https://www.ipv6council.be/IMG/pdf/05_eir-ipv6-v4.pdf.

[i.38] 4th Technical GRNOG Meeting (2 December 2016): "IPv6 for COSMOTE GR", G. Manousakis.

NOTE: Available at https://www.grnog.gr/4th-technical-meeting/?lang=en.

[i.39] IETF RFC 6333 (August 2011): "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion".

[i.40] IETF RFC 6346 (August 2011): "The Address plus Port (A+P) Approach to the IPv4 Address Shortage".

[i.41] IETF RFC 6555 (April 2012): "Happy Eyeballs: Success with Dual-Stack Hosts".

[i.42] P. Saab: "Facebook IPv6 Strategy", Keynote speech at V6 World 2015 "Unleashing the Power" Conference, 17 March 2015.

[i.43] IETF RFC 5549 (May 2009): "Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop".

[i.44] Lightreading, 2015: "Facebook: IPv6 Is a Real-World Big Deal", G. Brown.

NOTE: Available at http://www.lightreading.com/ethernet-ip/ip-protocols-software/facebook-ipv6-is-a-real-world-big-deal/a/d-id/718395.

[i.45] ACM MobiCom'16, October 03-07 2016, New York City, USA: "A case for faster mobile web in cellular IPv6 networks", U. Goel, M. Steiner, MP. Wittie, M. Flack, S. Ludin.

NOTE: Available at https://origin-www.moritzsteiner.de/papers/Mobicom_IPv6.pdf.

[i.46] ETSI GR IP6 008: "IPv6-based Internet of Things Deployment of IPv6-based Internet of Things".

[i.47] 5GPP (V1.0): "5G Vision: The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services", February 2015.

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Partnership Project
5G	5th Generation
5G-PPP	5G Infrastructure Public Private Partnership
AMF	Access and Mobility Function
APN	Access Point Names
APNIC	Asia Pacific Network Information Centre
AUSF	AUthentication Server Function
BGP	Border Gateway Protocol
CDN	Content Delivery Network
CGN	Carrier Grade NAT
CG-NAT	Carrier-Grade NAT (Network Address Translation)
CLAT	Customer-side transLATor
CORE	Core Network
CP	Control Plane
CSFB	Circuit Switched FallBack
DN	Data Network
DNS	Directory Name Server
DS	Dual-Stack
EPS	Evolved Packet System

FG	Focus Group
FTTH	Fiber To The Home
GET	HTTP GET used to request data from a specified resource
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
HLR	Home Location Register
H-PCF	Home-PCF
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IMT	International Mobile Telecommunications
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPVS	IP Virtual Server
ISP	Internet Service Provider
ITU-R	International Telecommunication Union - Radiocommunication Sector
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN	Local Area Network
MAN	Metropolitan Area Network
MN	Mobile Node
MNG	Mobile Network Gateway
MNO	Mobile Networks Operator
NAT	Network Address Translation
NEO	Network Operations
NGMN	Next Generation Mobile Network
OAM	Operations, Administration, and Maintenance
PCF	Policy Control Function
PDN	Packet Data Network
PDP	Packet Data Protocol
PGW	Packet data network GateWay
PLAT	Provider-side transLATor
PLT	Page Load Time
PPP	Point to Point Protocol
RAT	Radio Access Technologies
RFC	Request For Comments
RTT	Round Trip Time
RUM	Real User Monitoring
SDN	Software Defined Networking
SGSN	Serving GPRS Support Node
SMF	Session Management Function
TCP	Transmission Control Protocol
TD	Temporary Document
TM Forum	Tele Management Forum
TSG RAN	Technical Specifications Group Radio Access Network
TWAG	Trusted Wireless LAN Access Gateway
UDM	Unified Data Management
UE	User Equipment
UP	User Plane
VoIP	Voice over IP
VoLTE	Voice over Long Term Evolution
V-PCF	Visited-PCF
VPN	Virtual Private Network
WI	Work Item
WLAN	Wireless Local Area Network

4 IPv6-based 5G Mobile Wireless Internet

4.0 Introduction

The fifth generation of mobile technology (5G) will address the demands and business contexts of 2020 and beyond. Moreover, it is expected that:

1) the future European society and economy will strongly rely on 5G infrastructure;

2) its impact will go far beyond existing wireless access networks with the aim for communication services, reachable everywhere, all the time, and faster; and

3) 5G technology will be adopted and deployed globally in alignment with developed and emerging markets' needs.

According to [i.47], several key drivers and disruptive capabilities will help the adoption and deployment of 5G globally.

In particular, regarding the key drivers, 5G will ensure user experience continuity in challenging situations such as high mobility (e.g. in trains), and very dense or sparsely populated areas, and journeys covered by heterogeneous technologies. At the same time 5G will be the key enabler for the Internet of Things (IoT) by providing a platform to connect a massive number of sensors, rendering devices and actuators with stringent energy and transmission constraints, see Figure 1. In addition, new mission critical services will be deployed, requiring very high reliability, global coverage and/or very low latency, which are up to now handled by specific networks, typically public safety, will become natively supported by the 5G infrastructure.

Moreover, it is expected that 5G will integrate networking, computing and storage resources into one programmable and unified infrastructure, which will allow for an optimized and more dynamic usage of all distributed resources, and the convergence of fixed, mobile and broadcast services. This unification will also enable 5G to support multi tenancy models, enabling operators and other players to collaborate in new ways.

5G will leverage on the cloud computing concepts and will stimulate paving the way for virtual pan European operators relying on nationwide infrastructures.

Another important key driver is that 5G is being designed to be a sustainable and scalable technology. This can be realized by firstly, the telecom industry will stimulate and work towards a drastic energy consumption reduction and energy harvesting. Moreover, sustainable business models for all Information and Communication Technology (ICT) stakeholders will be enabled by cost reductions through human task automation and hardware optimization.

One of the most important key drivers is that 5G will create an ecosystem for technical and business innovation. This will be enabled by the fact that network services will rely more and more on software, the creation and growth of start-ups in the sector will be encouraged. Furthermore, the 5G infrastructures will provide network solutions and involve vertical markets such as automotive, energy, food and agriculture, city management, government, healthcare, smart manufacturing, public transportation, water management.

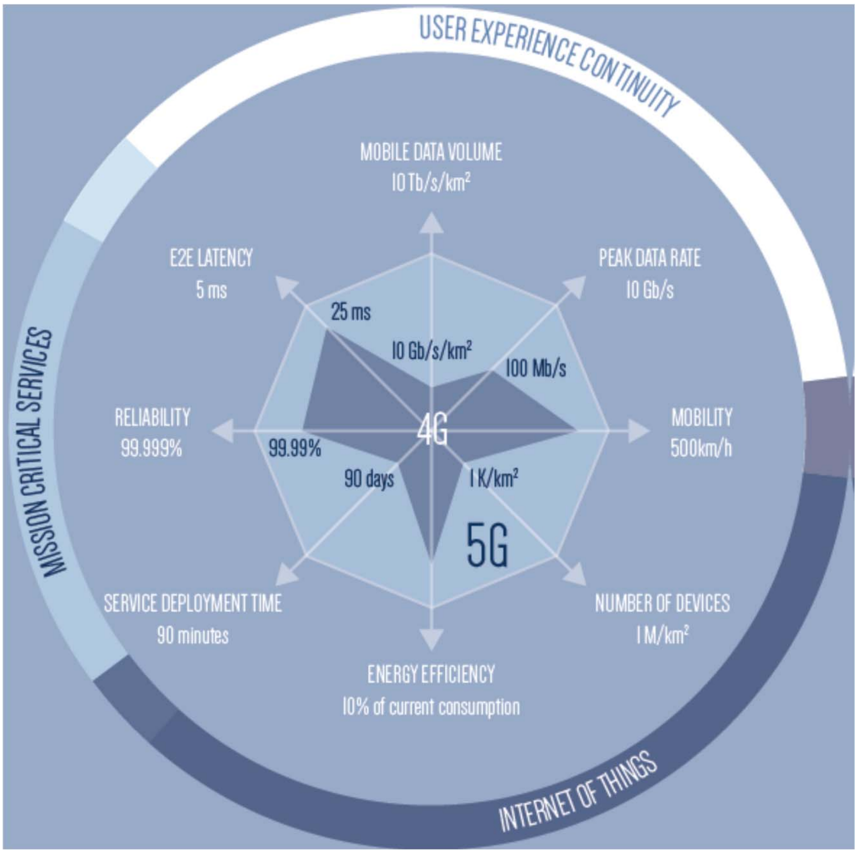

Figure 1: 5G Key drivers and disruptive capabilities, copied from [i.47]

Moreover, 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. Moreover, it has a higher requirement for the security, management, maintenance as well as the operation of the next generation Internet. 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.

4.1 IPv6 Transition Strategies in Mobile Networks

Currently several IPv6 transition strategies can be identified. The main IPv6 transition strategies that are being discussed by Mobile Network Operators (MNOs), see e.g. [i.1] are listed below. More details on mobile networks considerations for IPv6 deployment are described in [i.2], see also clause 4.2.5 of the present document.

- **IPv4 only:** delays the introduction of IPv6 to a later date and remain an all-IPv4 network. Over the long term, it is expected that this transition strategy will lead to problems and increased costs for the MNO. Due to the increase in traffic, see 5G requirements, there will be an increased demand for IP addresses and on using NAT in the carriers' network, denoted as Carrier Grade Network Address Translation (CG-NAT). In particular, all traffic to and from the Internet will have to pass CG-NAT. Furthermore, growth in bandwidth demand can only be handled with increased CG-NAT capacity, which has a higher cost. It means that the MNO is unable to benefit from the increasing ratio of IPv6-to-IPv4 Internet traffic. This mechanism works only for DNS-based applications and IPv4-only.

- **Coexistence of IPv4 and IPv6:** requires the use of a dual-stack, introducing IPv6 in the network next to IPv4. For a MNO, this approach is a less desirable option because dual-stack networks are more complex to deploy, operate, and manage. Furthermore, this option also requires an address management solution for both IPv4 and IPv6 addresses.

- **IPv6 only:** introduces IPv6 in the network and remove IPv4 completely. This approach can provide benefits for a MNO, because IPv6-only networks are simpler to deploy, operate, and manage. Moreover, an address management solution is required only for IPv6 addresses. Therefore, this option has no impact on scale, charging, and roaming because only a single bearer with a single stack is required. However, the problem with this approach is that many UE (User Equipment) devices, websites, and applications still only work on IPv4. When moving to an IPv6-only network may lead to inferior service for MNO customers, resulting in customer dissatisfaction.

- **Enhanced IPv6 only + NAT64:** in addition to offering IPv6 only, also IPv4 is offered as a service over IPv6 for DNS-based applications. For the MNO, benefits from the advantages of the IPv6 only strategy and at the same time, there is no impact on scale, charging, and roaming as only a single bearer with a single stack is required. DNS64 (Domain Name System 64) also embeds IPv4 Internet destinations in IPv6 addresses. However, non-DNS applications are not supported and will be broken, which could result in a lower quality service for the operator's customers.

- **Enhanced IPv6 only + 464XLAT:** this strategy benefits from the advantages provided by the IPv6 only + NAT64 solution and at the same time it solves the drawback associated with the support of non-DNS applications. In particular, For IPv4-only, non-DNS applications, IPv4 packets are translated to IPv6 packets by the UE and subsequently are translated back to IPv4 packets by a central CG-NAT64, which is deployed behind the PGW (PDN Gateway).

More details on the IPv4 to IPv6 transition are provided in ETSI GR IP6 006 [i.3].

4.2 World Wide 5G Initiatives

4.2.0 Introduction

This clause briefly describes main world wide 5G initiatives. Currently, only the 5G initiatives and architectures proposed by Next Generation Mobile Network (NGMN) Alliance, Third Generation Partnership Project (3GPP), Internet Engineering Task Force (IETF), 5G Infrastructure Public Private Partnership 5G-PPP and the Focus Group on network aspects of IMT-2020 (FG IMT 2020) are briefly presented.

4.2.1 Next Generation Mobile Networks (NGMN)

NGMN alliance (https://www.ngmn.org/home.html) is a mobile telecommunication association that consists of mobile operators, vendors, manufacturers and research institutes. The main objective of the alliance is to ensure the successful commercial launch of existing and future mobile broadband networks through a roadmap of technology and user trials. NGMN was founded by major operators in 2006 and can be considered as an open forum that evaluates candidate technologies in order to develop a common view for current and for next evolution of wireless networks. The alliance supports and cooperates with standards organizations like 3GPP, TeleManagement Forum (TM Forum) - and the Institute of Electrical and Electronics Engineers (IEEE) and provides them with requirements coming from mobile operators.

The 5G architecture developed by NGMN is shown in Figure 8 of [i.4]. It consists of:

1) 5G devices that can be of any type, from a wearable device up to a car or robot;

2) different Radio Access Technologies (RATs); and

3) the following four layers:

   - end to end management and orchestration layer;

   - business application layer that consists of use cases, business models and value proposition;

   - business enablement layer that consists of library of modular network functions and value enabling capabilities;

   - infrastructure resources layer that consists of access nodes, central and edge cloud nodes, and networking nodes.

4.2.2 3rd Generation Partnership Project (3GPP)

The 3rd Generation Partnership Project (3GPP) started several activities in defining the 5G Next Generation Network/System, which focus on the network and the next generation access technologies for the radio.

The 3GPP Next Generation Network/System work is split in three releases: Release 14, Release 15 and Release 16.

The time line for the three releases is shown in Table 1.

The three-stage methodology as defined by ITU-T, is applied in 3GPP:

- Stage 1 is an overall service description from the user's standpoint.
- Stage 2 is an overall description of the organization of the network functions to map service requirements into network capabilities.
- Stage 3 is the definition of switching and signalling capabilities needed to support services defined in stage 1.

Table 1: Time line for Release 14, 15 and 16 on Next Generation Networks/Systems

Release	Stage 1 freeze	Stage 2 freeze	Stage 3 freeze
Release 14	June 2016	September 2016	March 2017
Release 15	June 2017	December 2017	June 2018
Release 16	December 2018	June 2019	December 2019

In Release 14, the stage 1 study [i.5] has been initiated by 3GPP SA1 which focuses on a feasibility study on new services and markets technology enablers associated with the 5G Next Generation Network/System and it identifies the use cases to be considered by 3GPP in this area. This 3GPP SA1 study describes 74 use cases. The potential service requirements and as well as the potential operational requirements related to each of these use cases are briefly described.

As a result of the 3GPP TR 22.891 study [i.5], 3GPP SA1 started four other study documents that provide more details on use cases and requirements in the following areas:

- Massive Internet of Things [i.6].
- Critical communications [i.7].
- Enhanced Mobile Broadband (eMBB) [i.8].
- Network Operations (NEO) [i.9], which focuses on how 3GPP network operators can support network operations such as network slicing, multi-network connectivity, network capability exposure.

The Release 14 Stage 2 activities focus on the 3GPP Study on Architecture for Next Generation System and are driven by 3GPP SA2 and are documented in 3GPP TR 23.799 [i.10]. The 3GPP Release 15 Stage 2 specifications started in 2017 and are documented in ETSI TR 123 501 [i.11] and ETSI TS 123 502 [i.12].

The Release 14 security activities are driven by 3GPP SA3 and are focusing on the study on the security aspects of the next generation system, which is documented in 3GPP TR 33.899 [i.13].

In addition to the above, 3GPP Technical Specifications Group Radio Access Network (TSG RAN) focuses on 3GPP TR 38.913 [i.14] and it will be focusing on a new approved work item that aims to develop a new radio access technology to meet the use cases defined in 3GPP TR 38.913 [i.14].

3GPP TR 38.913 [i.14] is a study of the scenarios and requirements for next generation access technologies taking into account the ITU-R IMT-2020 requirements [i.15] and [i.16]. The families of the usage scenarios for IMT 2020 and beyond included in 3GPP TR 33.899 [i.13] are:

- enhanced Mobile Broadband (eMBB);
- massive Machine Type Communications (mMTC);
- Ultra-Reliable and Low Latency Communications (URLLC).

The Non-Roaming 5G System Architecture in reference point representation defined in 3GPP TR 23.799 [i.10] and ETSI TS 123 501 [i.11] is provided in Figure 2.

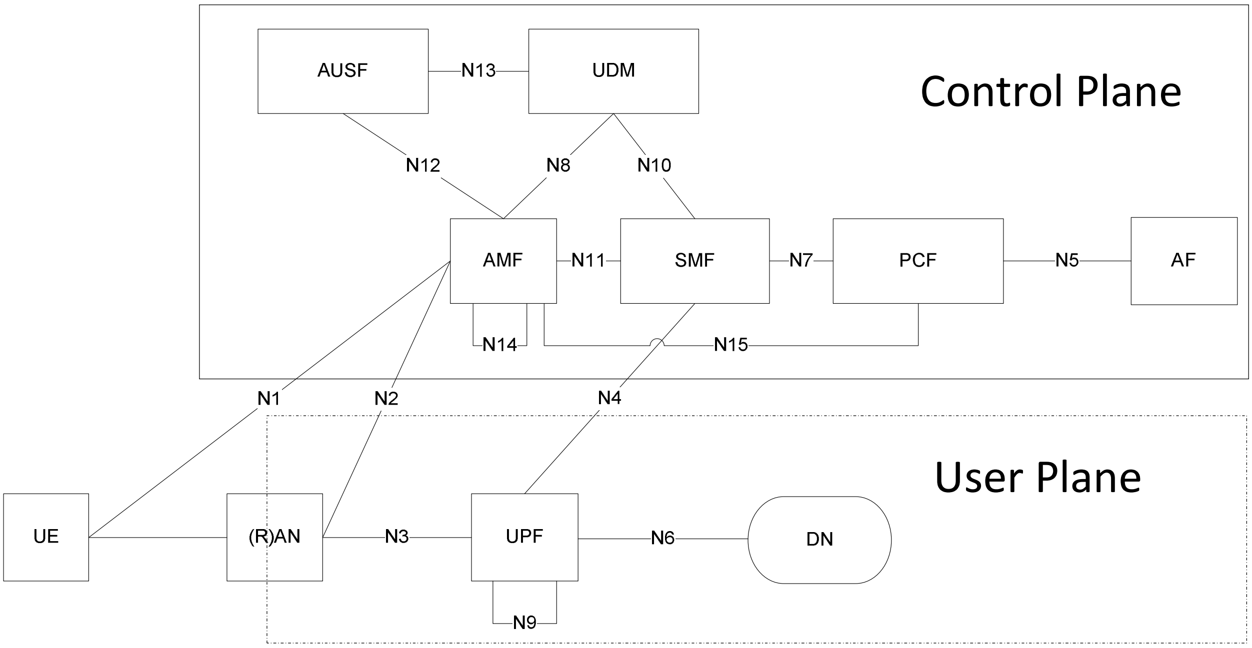

Figure 2: Non-Roaming 5G System Architecture in reference point representation, based on ETSI TS 123 501 [i.11]

The reference points used in the 5G System Architecture are the following ones:

- **N1:** Reference point between the User Equipment (UE) and the Control Plane (CP) functions.
- **N2:** Reference point between the RAN and the CP functions.
- **N3:** Reference point between the RAN and the User Plane (UP) functions.
- **N4:** Reference point between the CP functions and the UP (User Plane) functions.
- **N5:** Reference point between the CP functions and an Application Function.
- **N6:** Reference point between the UP functions and a Data Network (DN).
- **N7:** Reference point between the Session Management function (SMF) and the Policy Control function (PCF).
- **N7r:** Reference point between the Visited-PCF (V-PCF) and the Home-PCF (H-PCF).
- **N8:** Reference point between Unified Data Management (UDM) and Access and Mobility Management function (AMF).
- **N9:** Reference point between two Core User Plane Functions (UPFs).
- **N10:** Reference point between UDM and SMF.
- **N11:** Reference point between AMF and SMF.
- **N12:** Reference point between AMF and Authentication Server function (AUSF).
- **N13:** Reference point between UDM and AUSF.
- **N14:** Reference point between two AMFs.
- **N15:** Reference point between the PCF and the AMF in case of non-roaming scenario, V-PCF and AMF in case of roaming scenario.

- **N16:** Reference point between two SMFs, (in roaming case between V-SMF and the H-SMF).

4.2.3 Internet Engineering Task Force (IETF)

The mission of the IETF is to make Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. IETF is specifying the IPv4 and IPv6 protocol suites which are documented in several RFCs (Request for Comments). Moreover, IETF is providing recommendations on the IPv4 - IPv6 transition, for details see ETSI GR IP6 006 [i.3]. In addition to this IETF is also providing guidelines for operators and other mobile cellular stakeholders on how to apply and use IPv6 in mobile cellular systems.

In particular, the main RFCs that provide considerations for IPv6 deployment in mobile networks are listed below:

- Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts [i.17].
- Basic Requirements for IPv6 Customer Edge Routers [i.18].
- Mobile Networks Considerations for IPv6 Deployment [i.2].
- IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS) [i.23].
- IPv6 Node Requirements [i.20].
- IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts [i.19].
- Extending an IPv6/64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link [i.21].
- Analysis of Failure Cases in IPv6 Roaming Scenarios [i.22].

A summary of the recommendations provided on IETF RFC 6342 [i.2] and IETF RFC 6459 [i.23] that focus on IPv6 in mobile networks and in the 3GPP EPS, respectively, is provided below.

The main mobile networks considerations for IPv6 deployment described in IETF RFC 6342 [i.2] are the following ones:

- Due to the fact that mobile service providers are willing to conserve their available IPv4 pool while deploying IPv6 it implies that there is a need for network address translation in mobile networks. Mobile networks can make use of the IETF dual stack model specified in IETF RFC 4213 [i.24].
- Placement of NAT functionality in mobile networks: Two types can be considered, for private IPv4 address pool management, the centralized and distributed models:
  - The distributed model archives a good operation efficiency, since each Mobile Network Gateway (MNG) can manage its own NET10 pool [i.25], and reuse the available private IPv4 pool avoiding the issues associated with the non-unique private IPv4 addresses for the MNs without additional protocol mechanisms. The MNG is the Mobile Node (MN)'s default router, which provides IP address management. Furthermore, the distributed model also augments the "subscriber management" functions at an MNG, such as readily enabling NAT session correlation with the rest of the subscriber session state.
  - By using the centralized IP address management the mobile service providers can continue their legacy architecture by placing the NAT at a common node. Moreover, the centralized model can also achieve private IPv4 address reuse but it needs additional enhancements, such as additional protocol extensions to differentiate overlapping addresses at the common NAT and as well as to integrate with the policy and billing infrastructure.
- IPv6-only mobile network deployments: This deployment model is can be considered to be feasible in the LTE (Long Term Evolution) architecture for a mobile network operator's own services and applications. However, the following considerations need to be taken into account:
  - existing MNs still expect IPv4 address assignment;
  - roaming, which is unique to mobile networks, requires that a provider support IPv4 connectivity when its (outbound) users roam into a mobile network that is not IPv6- enabled;
  - a provider needs to support IPv4 connectivity for (inbound) users whose MNs are not IPv6-capable;

- IPv6-IPv4 interworking is necessary for IPv6-only MNs to access the IPv4 Internet.

- Fixed-Mobile Convergence: Fixed and mobile networks impose different requirements on the IPv6 deployments. IETF RFC 6342 [i.2] shows that harmonization of functions may be possible across the access networks. However, the service provider's core network is perhaps better-suited for converged network architecture. Similar gains in convergence are feasible in the service and application layers.

The key conclusions derived in IETF RFC 6459 [i.23] regarding the use of IPv6 in 3GPP EPS are the following ones.

The 3GPP network architecture and specifications define appropriate PDP context types that enable IPv4 and IPv6 connections. A Packet Data Protocol (PDP) context is the equivalent of a virtual connection between the User Equipment (UE) and a Packet Data Network (PDN) using a specific gateway.

It is important that main 3GPP mobile network entities, such as the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) are supporting the IETF dual stack model and connectivity.

Regarding devices and applications it is recommended that while they are being upgraded to support IPv6, they can start leveraging the IPv6 connectivity provided by the networks while maintaining the ability to fall back to IPv4.

4.2.4 5G Infrastructure Public Private Partnership (5G-PPP)

The 5G Infrastructure Public Private Partnership (https://5g-ppp.eu/) has been initiated by the European Commission and industry manufacturers, telecommunications operators, service providers, SMEs and researchers. The main objective of 5G-PPP is to deliver solutions, architectures, technologies and standards for the ubiquitous next generation communication infrastructures of the coming decade. The 5G-PPP initiative stimulates the development of a shared vision for the next generation of communications infrastructure beyond 2020, which include actions for leveraging 5G research to improve competitiveness and innovation in order to stimulate economic growth and more job creation in other industrial sectors.

The 5G-PPP brings a long term commitment from both the private and the public actors to invest in achieving these objectives and the PPP will play a key role in formulating the research and innovation priorities to be supported in European Horizon 2020 research and development programme.

The 5G architecture developed by 5G-PPP is shown in Figure 3. It consists of RATs that can support Device to Device, Moving Networks, Massive Machine Communications using Wireless Access, Wireless front haul, Wired front haul and backhaul. Moreover, in addition to RATs, the 5G architecture can support internet of things (ephemeral) networks. An aggregation network, which forms the core network, provides local, regional, national connectivity between the RATs, the ephemeral network and the Internet. The aggregation network consists of centralized functions and Operations Administration and Management (OAM) functions.

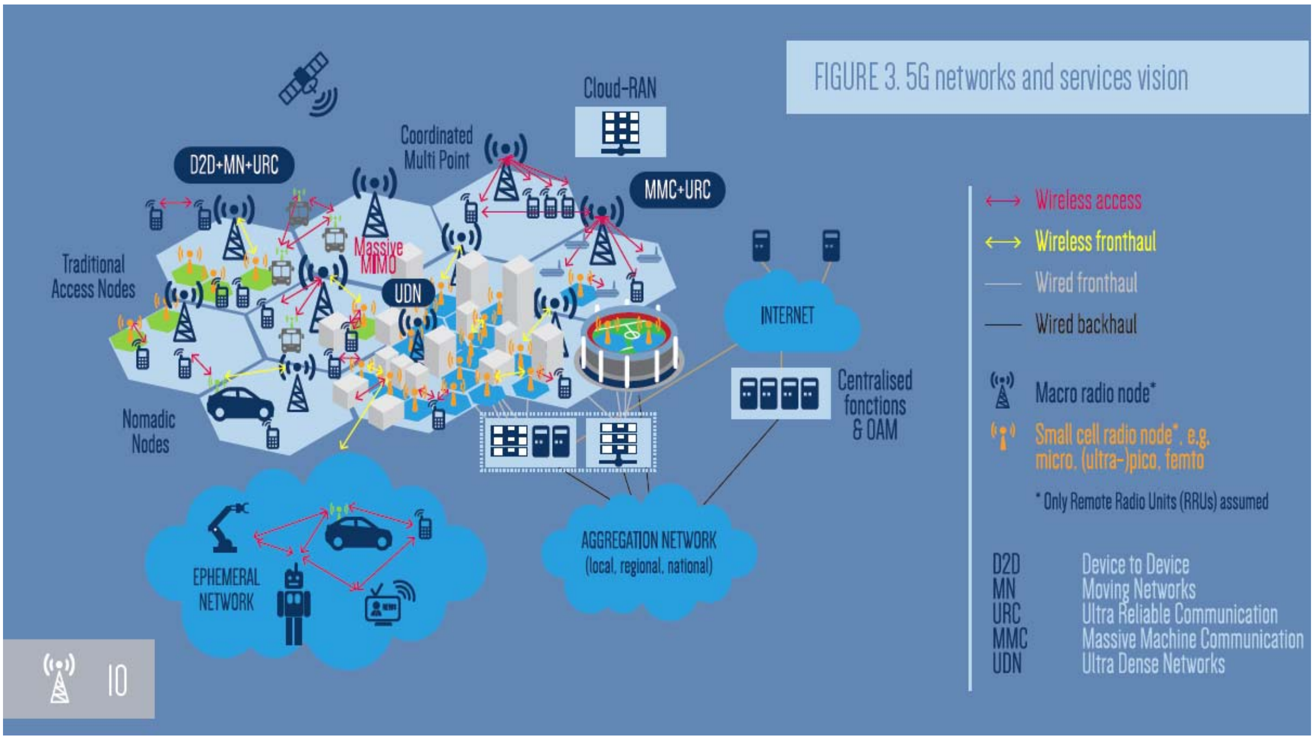

Figure 3: 5G Architecture, copied from [i.47]

4.2.5 Focus Group on network aspects of IMT-2020 (FG IMT 2020)

The Focus Group on network aspects of IMT-2020 (FG IMT 2020) (http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx) has been established in May 2015, by its parent ITU-T Study Group 13, having as main goal to analyse how emerging 5G technologies will interact in future networks as a preliminary study into the networking innovations required to support the development of 5G systems. In December 2015, the FG IMT 2020 received an extension to its lifetime, having the following specific tasks and areas of work:

- Explore demonstrations or prototyping with other groups, notably the open-source community.
- Enhance aspects of network softwarization and information-centric networking.
- Continue to refine and develop the IMT-2020 network architecture.
- Continue to study fixed-mobile convergence.
- Continue to study network slicing for the front haul/backhaul network.
- Continue to define new traffic models and associated aspects of Quality of Service (QoS) and operations, administration and management applicable to IMT-2020 networks.

An important outcome of the FG IMT 2020 activities is that the ITU-T standardization activity group will be able to prioritize the alignment of 5G deliverables with those of ITU-R, ensuring that standardization work on the network aspects of 5G is informed by the progression of its radio-transmission systems.

The 5G architecture developed by FG IMT-2020 is depicted in Figure 3 of TD 208 [i.26]. This architecture consist of four main layers:

1) Applications;
2) Control plane that includes the Network & Service Orchestration and the Unified Control;
3) The data plane includes RATs, front haul/backhaul, transport networks and convergent data functions; and
4) The Integrated Network and Service Management that influences and manages also all the other three layers.

4.3 Best Cases on IPv6 Transition Strategies in Cellular Networks

4.3.0 Introduction

This clause describes several best cases on IPv6 strategies that have been successfully applied in cellular systems. There are few initiatives that are monitoring and documenting the IPV6 deployments in cellular networks. One of them is the IPv6 Forum (http://www.ipv6forum.com/), which promotes the deployment of IPv6 by organizing events and workshops where cellular network representatives are presenting achievements and possible IPv6 roadmaps. Another initiative is the Internet Society, which via the Deploy360 Programme (http://www.isoc.org/deploy360) provides information about IPv6 deployments and IPv6 statistics. In addition, it maintains a list with other initiatives that provide IPv6 statistics, see https://www.internetsociety.org/deploy360/ipv6/statistics.

World IPv6 Launch related statistics http://www.worldipv6launch.org/measurements/:

- APNIC related statistics, measured via user's computers http://stats.labs.apnic.net/ipv6.
- Daily IPv6 Statistics https://www.vyncke.org/ipv6status/.

[i.27] provides a brief description on the IPv6 introduction in 3GPP standards and mobile networks. IPv6 was first introduced into the 3GPP standards with release 99 (in year 1999), but unfortunately, was not widely implemented by equipment vendors or deployed by Mobile Network Operators. The 3GPP Release 9 (started in 2009) is considered a minor update to Release 8. However, the main change related to the IPv6 deployment is that it introduced support in GPRS for dual-stack IPv4v6 PDP contexts on a single shared radio access bearer. Furthermore, Release 9 also resolved the anomalous situation with Release 8 where dual-stack was supported for LTE access but not supported for GPRS access. The 3GPP Release 10 introduced DHCPv6-Prefix Delegation, based on IETF RFC 3769 [i.29] and IETF RFC 3633 [i.28]), to the 3GPP standards.

In the context of 3GPP IP Multimedia Subsystem (IMS), the Voice over LTE (VoLTE) system implements Voice over IP (VoIP) using IMS instead of using Circuit Switched Fallback (CSFB). IPv6 support was in IMS from the start. It is straightforward to use IPv6 with VoLTE. In particular, IMS requires a separate APN from the Internet Access Point Name (APN) therefore the inter-RAT and roaming issues with Internet access APNs do not arise. It is important to note that IPv6 is mandatory with VoLTE. All VoLTE phones have Radio Interface Layers that support IPv6. It is emphasized that the evolution to VoLTE should act as a further stimulus to user-plane IPv6 deployment because the User Equipment will require at least two IP addresses at the Packet Data Network Gateway (PGW), one for Internet access and the other for VoLTE.

One of the content providers listed on 6th of June 2016, some examples of using IPv6 to solve real-world business problems:

- Content/Service providers are in the process of migrating their Internet-connected X1 set-top box to IPv6-only.
- Several ISPs are now using IPv6-only interfaces for managing network devices such as cable modems and VOIP gateways. This enables them to assign unique addresses per device, even for many tens of millions of devices. This also frees up IPv4 addresses for residential users.
- Several mobile networks are using IPv6-only for Android handsets (and hopefully Apple iOS handsets soon) by using NAT64+DNS64 for access to legacy IPv4 content. Providing access to content over IPv6 is faster than IPv4 in these environments due to being able to bypass the NAT64 gateway. In particular, the *Operator in USA 1*, now experiences that for IPv6-enabled handsets between 65 % and 73 % (off-peak vs. peak) of all bits transferred use native IPv6 and only the remainder uses their NAT64 gateway.
- Several social media providers, are moving to IPv6-only data centres. This enables them to eliminate needing to also manage IPv4 within their data centres. In some cases, access to servers over IPv4 can be provided through technologies such as IETF RFC 7755 [i.30], which specifies a stateless IP/ICMP Translation Algorithm in an IPv6 Internet Data Center.
- Several virtual hosting providers have experimented with, or already offer lower-cost offerings for IPv6-only virtual machines. It is expected that this may become increasingly common considering that cloud service providers run out of IPv4 address space and therefore, start moving infrastructure and management interfaces primarily to IPv6-only. IPv4 access can then be provided as a service or through gateways.

4.3.1 Operators in USA: Example 1

According to [i.31] and [i.32], the *Operator in USA 1* in the USA was running out of IPv4 addresses and therefore needed an IPv6 transition strategy. The solution that the *Operator in USA 1* adopted in 2014 was the use of 464XLAT and IPv6-only solutions. In particular, 464XLAT is an IPv6 transition technology documented in IETF RFC 6877 [i.33], which builds on previous technologies such as NAT64 and DNS64. By using 464XLAT, IPv4 packets are translated to IPv6 on the customer-side translator (CLAT) and back to IPv4 on the provider-side translator (PLAT). The key issue for the *Operator in USA 1* with just using NAT64 and DNS64 was that specific applications, such as instant messaging apps could not function properly through NAT64. By using 464XLAT solution, the *Operator in USA 1* was able to keep these applications working, and provide native IPv6 connectivity where possible.

Operator in USA 1 has taken a lead by deploying an IPv6-only network for Android, and other providers are likely to follow, once Android iOS also supports IPv6-only. In a publication is shown that the percentage of requests over IPv6 dual stack sites coming from the *Operator in USA 1* on a known *Content Delivery Network Provider* has increased from June 2013 to May 2016 with 53,3 %.

Currently, this operator in USA announced that in new 5G deployments only the IPv6-only solution will be applied. Concerning IPv6 deployments, a significant increase in the IPv6 deployments in the *Operator in USA 1* mobile network took place from March 2013 to August 2018, with 93%, see http://www.worldipv6launch.org/measurements/.

4.3.2 Operators in USA: Example 2

The *Operator in USA 2*, is a broadband telecommunications company and the largest USA wireless communications service provider as of September 2014.

The *Operator in USA 2* Wireless, introduced IPv6 since the date that they started deploying 4G (LTE) in USA in 4Q 2010. The use of IPv6 is significantly increasing every year. In a publication is shown that the increase in percent of requests over IPv6 to dual-stack sites on a known *Content Delivery Network Provider* when using the *Operator in USA 2* wireless infrastructure, from June 2013 to May 2016 with 71.5%. The *Operator in USA 2* provides both IPv6 and IPv4 addressing to all of its devices connected to its LTE network [i.34]. For devices with no IPv6 support or not connected by LTE, the *Operator in USA 2* provides only IPv4 addressing - resulting in the devices using *Operator in USA 2*'s IPv4 network. Thus, in the *Operator in USA 2* network, the choice of addressing on the device is based on whether the device is connected to the LTE network or not, see Slide 5 in [i.34]. In particular, there are two different methods in which the *Operator in USA 2* routes packets from IPv6 devices:

1) via IPv6 network with no stateful middleboxes; and

2) via IPv4-in-IPv6 tunnels using Gateway Initiated Dual-Stack Lite (DS Lite) [i.35] software on the phone.

Concerning IPv6 deployments, the IPv6 traffic in the *Operator in USA 2* mobile network increased from September 2014 to August 2018, with 88 %, see http://www.worldipv6launch.org/measurements/.

4.3.3 Operators in Europe Example 1

The *Operator in Europe 1*, i.e. is a Mobile Operator mainly operating in Europe, the *Operator in Europe* 1's IPv6 program started nearly 7 years ago. Incrementally planned and deployed IPv6, where already in 2013 the entire core network has been IPv6 enabled. Moreover, since 2013, the *Operator in Europe 1*'s Highs speed Internet over Fibre deployed infrastructure is IPv6 enabled and launched with live customers. According to [i.36] currently, nearly 70 % of the *Operator in Europe 1*'s residential users are IPv6 enabled. Furthermore, the management of peripherals is done for 91 % through IPv6. Regarding, IPv6 at modem-only installs there is currently no policy on enabling IPv6. However, some individual tests have been done, running without any problems. The Field trials are going on in 2016, having as goal to enable IPv6 at modem-only installs by the end of 2016.

Concerning the IPv6 deployments, the IPv6 traffic in the *Operator in Europe 1* mobile network increased from February 2014 to August 2018, with 68 %, see http://www.worldipv6launch.org/measurements/.

4.3.4 Operators in Europe Example 2

The *Operator in Europe 2*, i.e. is a mobile operator that operates in Europe. According to [i.37] the main service that *Operator in Europe 2* introduced IPv6 is the Fixed Broadband Next Generation Access. In particular, all FTTH (Fibre To The Home) and VDSL2 (Very high-speed Digital Subscriber Line 2) connections are IPv6 capable. This applies to wholesale, retail and managed customers.

The future the *Operator in Europe* 2 mobile operator developments that will support IPV6 are expected to be the following [i.37]:

- Guest-WiFi/WLAN through TWAG (Trusted Wireless Access Gateway), where each User Equipment gets a /64 prefix.
- IMS for VoIP and VoLTE (Voice over LTE).
- Mobile Internet data APN supports 464XLAT, where Home Location Register (HLR) provisioning update is needed to allow all subscribers to use the IPv6 based APN protocol.

This operator is a late starter in IPv6 deployments. However, the IPv6 traffic in the *Operator in Europe 2* mobile IPv6 increased from April 2017 to August 2018, to 40 %, see http://www.worldipv6launch.org/measurements/

4.3.5 Operators in Europe Example 3

The *Operator in Europe 3* is a mobile operator that operates in Europe. The *Operator in Europe 3* started introducing IPv6 deployments in their mobile network in 2011. Some key deployment steps followed by the *Operator in Europe 3* are provided below, see e.g. [i.38]:

- May 2011:
  - GGSN servicing IPv6 only, single stack APN setup;
  - open source NAT 64;
  - IPv6 only access was a success.
- February 2012:
  - SGSN Software upgrade to support dual stack.
- July 2012:
  - GGSN upgrade to support dual stack.
- August 2012:
  - HLR software upgrade to support dual stack APN type.
- November 2012:
  - LTE introduction with dual stack support APN;
  - LTE dongle v4/v6 success.
- February 2013:
  - Dual stack connection success over single PDP from mobile handset.
- End 2013
  - Configuration homogenization;
  - IP Core network readiness;
  - IPv4/IPv6 type for APN "Internet".
- 2014:
  - Testing with roaming partners.
- July 2015:
  - Mass market "Internet" APN dual stack configured on all production infrastructure.

- January 2016:
  - All new subscribers provisioned with Dual Stack configuration.
- February - April 2016:
  - All users IPv6 configured;
  - Customer Care Training.
- September 2016:
  - Samsung™ support for IPv6.
- Future:
  - Apple™ support;
  - IPV6 only with NAT64/DNS64.

Since January 2016, all new subscribers are provisioned with IPv6 dual stack [i.24]. This resulted in a significant increase in the IPv6 traffic in the *Operator in Europe 3* mobile network from September 2016 to August 2018 with 48 %, see http://www.worldipv6launch.org/measurements/

The IPV6 transition mechanism used is the Dual Stack, which consists of IPv6 and Private IPv4 with Port Address Translation.

4.3.6 Operators in Europe Example 4

According to [i.3], the *Operator in Europe 4*, i.e. uses for fixed networks as the base recommendation for IPv4 to IPv6 transition, the IPv6 dual-stack [i.24]. Moreover, DS-Lite [i.39] is used as the Group-wise recommendation to ensure IPv4 service continuity while A+P [i.40] is used as the CGN exit strategy. For mobile networks, IPv6 only + NAT64 is deployed in some affiliates of the Group.

According to ETSI GR IP6 006 [i.3], as per 2016, there are around 1,5 million *Operator in Europe 4* subscribers that are supported/delivered using IPv6 connectivity.

Concerning the IPv6 deployments, the IPv6 traffic in the *Operator in Europe 4* mobile network increased from September 2016 to August 2018 with 40 %, see http://www.worldipv6launch.org/measurements/

4.3.7 Operators in China: Example 1

The *Operator in China 1* is a fixed and mobile operator that operates in China. In particular, the *Operator in China 1* plays a main role in the market of fixed networks in China. According to ETSI GR IP6 006 [i.3], the *Operator in China 1* started deploying IPv6 in its 4G mobile networks with dual stack in 2 provinces since May 2015, and more than 60 % of the online 4G users are IPv6-enabled. Currently, the backbone network of the *Operator in China 1* is 100 % IPv6 deployed, while the percentage of IPv6 deployment is 70 % in Metropolitan Area Network (MAN).

In September 2018, the IPv6 *Operator in China 1* counted 100 million IPv6 online subscribers. Moreover, by September 2018 the whole *Operator in China 1* 4G mobile network started to provide IPv6 access services and the IPv6 penetration rate for 4G is nearly 60 %.

The *Operator in China 1* is using a broad set of IPv6 transition technologies. They are even the proposer/proponent of Lightweight 4over6. For the IPv4 to IPv6 transition the *Operator in China 1* is implementing dual-stack, DS-Lite and NAT444, see ETSI GR IP6 006 [i.3].

4.3.8 Operators in China: Example 2

According to ETSI GR IP6 006 [i.3], the number of IPv6 users/customers represents 2-3 % of the total number of the *Operator in China 2*, i.e. users/customers. The IPv6 transition technology that the *Operator in China 2* is using, is the dual-stack.

4.3.9 Content Delivery Network Providers Example 1

The *Content Delivery Network Provider 1* is one of the USA companies that supports content delivery using an IPv6 content delivery infrastructure. In particular, in the *Content Delivery Network Provider 1*'s content delivery infrastructure, the content delivery servers are deployed so deeply inside several cellular ISPs' networks that the end-to-end communication between mobile devices and the *Content Delivery Network Provider 1*'s servers, mostly do not go outside the cellular network. More details on the used *Content Delivery Network Provider 1*'s IPv6 based content delivery infrastructure is provided in clause 4.3.12.

4.3.10 Content Delivery Network Providers Example 2

The *Content Delivery Network Provider 2* is a USA company that helps enhancing web performance and security. In particular, it provides a content delivery network, Internet security services and distributed domain name server services. The *Content Delivery Network Provider 2* is sitting between the visitor and the *Content Delivery Network Provider 2* user's hosting provider and acting as a reverse proxy for websites.

In a publication, the *Content Delivery Network Provider 2*, shows that in the year 2016 more than 4 million *Content Delivery Network Provider 2* sites are using IPv6 (which is 98,01 % of the total the *Content Delivery Network Provider 2* sites). The IPv6 traffic through the *Content Delivery Network Provider 2* and supported by operator's mobile networks varies from 2 % to 6 % per operator.

Moreover, in terms of devices, mobile traffic is 50 % more likely to use IPv6 than desktop traffic, where 21,4 % of mobile traffic uses IPv6 traffic, whereas only 13,6 % of desktop traffic is over IPv6.

In the last months of the year 2016, the *Content Delivery Network Provider 2* enabled IPv6 for around 100 000 sites a day, monitoring how their systems are operated and how the traffic behaved. From these measurements was derived that visitors connecting over IPv6 were able to connect and load pages in 27 % less time than visitors connecting over IPv4.

According to the same publication, the IPv6 enabled sites are faster compared to the IPv4 enabled ones, for two reasons:

- several major operating systems and browsers impose anywhere from a 25 ms to 300 ms artificial delay [i.41] on connections made over IPv4;
- mobile networks will not need to perform extra IPv4 to IPv6 and IPv6 to IPv4 translations to connect visitors to IPv6 enabled sites if the mobile phone is only assigned an IPv6 address.

4.3.11 Social Media Providers Example 1

Social Media Provider 1 is heavily involved on realizing the transition from IPv4 to IPv6 due to following reasons, see [i.42]:

- Not efficient to maintain two stacks in the entire network.
- It is more efficient to handle two stacks at the edge of the network and one internally.
- Stop engineers from continually writing IPv4 only code that will need to be modified later.
- Push the industry to move faster and re-prioritize IPv6.

The *Social Media Provider 1* focused lately on providing:

1) IPv6 only for host - host communication; and
2) deployed a number of IPv6-only clusters in 2014, such as frontend (web client), Service Cluster (newsfeed) and development in (C++), by:
    a) forcing engineers to work without IPv4; and
    b) enabled IPv6 VPN for remote access.

According to [i.42], the IPv6 Internet traffic, as seen by the *Social Media Provider 1*, is doubling each year. However, [i.42] identified several reasons of why and how IPv4 is required for an IPv6-only network:

- IPv4 internet traffic is still being terminated in IPv6-only clusters, since not all IPv4 traffic can be forwarded up to the edge;
- the access layer still uses IPv4; this is due to the fact that it requires no special hardware or software and it allows the *Social Media Provider 1* developers to implement stateless and simple solutions for IPv4, while being used only for Boarder Gateway Protocol (BGP) peering/routing;
- same IETF RFC 1918 [i.25] IPv4 address block is used for every cluster that is built and therefore not consuming any new IPv4 space within the *Social Media Provider 1* network;
- implemented IPv4 in IPv6 tunnelling for IPVS -Linux 3.18;
- using IPv4 link-local addresses on Linux hosts and rack switches by peering with the top of rack switch to inject IPv4 routes and being completely stateless and without requiring any special hardware;
- being forced to use IPv4 for interconnects in the *Social Media Provider 1* fabric clusters, without implementing IETF RFC 5549 [i.43] and where two peering sessions per interconnect are applied:
  - IPv4 BGP session using reusable IETF RFC 1918 [i.25] space;
  - IPv6 BGP session using unique allocations;
- vendors are not moving fast enough to satisfy the IPv6 transition needs of the *Social Media Provider 1*.

The results of the *Social Media Provider 1* experiments shown in [i.42] conclude that the mobile performance in terms of HTTP GET completion and Total Request time, is much higher on IPv6 networks compared to IPv4. From these experiments it can be seen that the IPv6 connections are as 40 % faster than IPv4. However, in [i.42] it was as well recommended that more active research is needed in this area to identify what causes these differences. For example, one of the reasons could be that the CG-NAT introduces significant delays in the end to end latency.

In [i.44], which is an article published later than [i.42], it was revealed that the *Social Media Provider 1*'s announced that IPv6 accounts for almost 50 % of the *Social Media Provider 1*'s 4G smart phone traffic in the USA and predicted that it will come to dominate IPv4 as major networking and Internet companies continue to push the IPv6 technology. Moreover, it was emphasized that after extensive testing and analysis it has been showed that IPv6 is 15 % faster than IPv4 for the *Social Media Provider 1* users and highlighted the removal of NAT devices from the forwarding path as the most significant reason for this improvement.

Based on the above results, the *Social Media Provider 1* recommends and stimulates more mobile network operators [i.42] to deploy IPv6 in order to realize the following objectives:

- improve latency to the user;
- better experience over all;
- more IPv6 enabled users means more traffic, since it gives incentive to content providers to enable IPv6;
- improved peer-peer between phones.

4.3.12 Example of Web Performance Improvement in Cellular Networks using IPv6

This clause is based on [i.45] and shows an example of improvements on the Web performance in USA cellular mobile networks from the point of view of the *Content Delivery Network Provider 1*'s content delivery infrastructure when using IPv6 networks.

As mentioned in clause 4.3.10, the content delivery servers in the *Content Delivery Network Provider 1*'s content delivery infrastructure are deployed so deeply inside several cellular mobile ISP networks that the end-to-end communication between mobile devices and the *Content Delivery Network Provider 1*'s servers, mostly do not go outside the cellular mobile network. In particular, the way of the *Content Delivery Network Provider 1*'s content delivery infrastructure is deployed, it enabled the authors of [i.45] to view the end-to-end cellular ecosystem between mobile devices and cellular gateways and evaluate how content is delivered over cellular IPv6 networks from the perspective of content providers, mobile network operators (ISPs), and other content delivery networks (CDNs).

The study in [i.45] mainly investigates the IPv6 performance across several factors that influence Web performance on cellular networks. In order to compare the IPv6 and IPv4 networks three types of experiments were accomplished and documented in [i.45]:

1) RTT (Round Trip Time) of the communication between clients and CDN (Content Delivery Networks), see Figures 4 and 5 in [i.45].

2) DNS Lookup Time distribution needed to resolve names from cellular Domain Name Servers for different cellular USA mobile network operators, see Figure 6 in [i.45].

3) Webpage Page Load Time (PLT) distribution for dual-stack in different cellular USA mobile network operators, see Figure 7 in [i.45].

For details on the scenarios used and the definition of the applied performance metrics, see [i.45].

Some highlights on the experimental setup are as follows. [i.45] provided the assessment of the IPv6 performance for 4 major USA cellular mobile network operators, i.e. *Operator in USA 1*, *Operator in USA 2*, *Operator in USA 3* and *Operator in USA 4*. Moreover, [i.45] provided a comparison between IPv6 native, IPv4, and NAT64/DS Lite deployments. During these experiments, the *Content Delivery Network Provider's 1* CDN infrastructure has been used, where a significant dataset was collected, consisting of millions of data points capturing the measured IPv6 and IPv4 performance, during the months of January 2015 - August 2015.

In order to compare the Web performance perceived by end-users on IPv6 and IPv4 networks, the authors of [i.45] used the *Content Delivery Network Provider 1*'s Real User Monitoring (RUM) system, see e.g. https://www.akamai.com/us/en/resources/real-user-monitoring.jsp. Moreover, the collected dataset was processed and filtered out such that the only performance values that were recorded are the ones associated with the webpages loaded on (1) Android devices and (2) Google Chrome browsers. In order to remove any influence of Performance Enhancing Proxies (PEPs), in terms of Web content caching and TCP split connections in the dataset, the authors of [i.45] considered latency for only Hypertext Transfer Protocol Secure (HTTPS) sessions. In this way latency for HTTPS sessions enabled them to accurately estimate the latency between CDN servers and client devices and ensure that the estimated latency is not between servers and PEPs in cellular networks.

The conclusions derived from the RTT (Round Trip Time) of the communication between subscribers and CDN experiments, see Figures 4 and 5 in [i.45] are as follows:

- In case of *Operator in USA 1*, the RTT for sessions over IPv6 network is lower than the sessions running on an IPv4 network. In particular, for median and for 80 % of the sessions:
  - RTT over IPv6 network is 49 % faster than the RTT in scenario where the IPv6 clients are connected to IPv4 servers via NAT 64 middleboxes.
  - RTT over IPv6 network is 64 % faster than the RTT in scenario where the IPv4 clients are connected to the IPv4 servers, over the IPv4 network.
- In case of *Operator in USA 2* the RTT for sessions over IPv6 network is similar to the RTT in scenario that uses IPv4-IPv6 tunnels and DS Lite sessions. Moreover, the same experiments show that the RTT over IPv4 networks experiences a higher latency than the RTTs in the two other scenarios, which is mainly influenced by the use of Carrier Grade NATs and Large Scale NATs. In particular, for median and for 80 % of the sessions:
  - RTT over IPv6 network is 29 % faster than the RTT in scenario that uses IPv4-IPv6 tunnels and DS Lite sessions.
  - RTT over IPv6 network is 44 % faster than the RTT in scenario where the IPv4 clients are connected to the IPv4 servers, over the IPv4 network.

- In case of *Operator in USA 3* and *Operator in USA 4* the RTT for sessions over IPv6 network is lower than the sessions running on an IPv4 network. In particular, for median and for 80 % of the sessions:
  - RTT over IPv6 network is 17 % faster than the RTT in scenario that uses IPv6 clients that are connected to IPv4 servers, using Dual Stack implementations.
  - RTT over IPv6 network is 24 % faster than the RTT in scenario where the IPv4 clients are connected to the IPv4 servers, over the IPv4 network.

On the time to resolve domain names from cellular DNS experiments, see Figure 6 in [i.45] the following conclusions can be derived:

- The DNS Lookup Time needed to resolve names from cellular DNS for the *Operator in USA 1*, *Operator in USA 3* and *Operator in USA 4*, is higher for IPv6 clients than IPv4 clients. For the *Operator in USA 2,* the DNS Lookup Time is approximately equal for IPv6 and IPv4 clients.
- One of the reasons for these DNS Lookup Time differences for IPv6 and IPv4 clients mentioned in [i.45], is the different technique followed by IPv6 and IPv4 clients for resolving domain names via type A queries.

On the webpage PLT distribution for dual-stack in different cellular carriers in the USA, see Figure 7 in [i.45], the following conclusions can be derived:

- In case of *Operator in USA 1* the webpage PLT for median and for 80 % of the page loads:
  - Website PLTs over IPv6 network are 9 % faster than the website PLTs in the scenario where the IPv6 clients are connected to IPv4 servers via NAT 64 middleboxes.
  - Website PLTs over IPv6 network are 14 % faster than the website PLTs in the scenario where the IPv4 clients are connected to the IPv4 servers, over the IPv4 network.
- In case of *Operator in USA 2* the webpage PLTs for median and for 80 % of the page loads:
  - Website PLTs over IPv6 network are 48 % faster than the website PLTs in scenario that uses IPv4-IPv6 tunnels and DS Lite sessions.
  - PLTs over IPv6 network are 64 % faster than the website PLTs in scenario where the IPv4 clients are connected to the IPv4 servers, over the IPv4 network.
- In case of *Operator in USA 3* and *Operator in USA 4* the website PLTs over IPv6 network are lower than the website PLTs over IPv4 networks

In general it can be observed that for all four USA mobile network operators, the PLTs of pages loaded by IPv6 clients over IPv6 networks are lower than PLTs of the same pages loaded by IPv4 clients over the respective carrier's IPv4 networks. Interesting to observe that despite DNS lookup times are being higher for IPv6 clients, the PLTs are lower for IPv6 clients loading pages over IPv6 network. Moreover, [i.45] argues that the actual benefits of using the faster IPv6 network can be observed when several round trips are needed to load multiple Web objects.

The main conclusions driven by [i.45] are as follows:

- RTT, DNS lookup and Webpage 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.
- CDN RTT performance for mobile content can be improved when IPv6 networks are used, due to the fact that in-path middleboxes for IPv6 address translation deployed by cellular carriers are not anymore needed.
- Cellular mobile network operators are advised to upgrade their network and support IPv6 instead of continuing deploying IPv4 technologies in their cellular mobile network.

4.4 5G and Internet of Things (IoT)

The current and previous generations of mobile networks enabled voice, data, video, and other life-changing services. It is expected that the 5th Generation (5G) mobile networks will change our society by opening up the telecom ecosystem to vertical industries. 5G will help vertical industries to achieve the "Internet of Things" (IoT) vision of ubiquitously connected, highly reliable, ultra-low latency services for massive number of devices. Moreover, the 5G networks are not only envisioned as a support for IoT, but also as means to give rise to an unprecedented scale of emerging industries, instilling an infinite vitality in future telecommunications. Extensive studies have shown that IoT requires support for a diverse range of service types, such as eHealth, Internet of Vehicles (IoV), smart households, industrial control, environment monitoring, and so on. It is expected that these services will drive the rapid growth of IoT and facilitate hundreds of billions of devices to connect to the network, which also conceives the IoT vision especially from vertical industries. In particular, IPv6 can be seen as one of the main drivers for the rapid growth realization and deployment of IoT.

Therefore, the conclusions and recommendations derived in ETSI GR IP6 008 [i.46], apply also in the context of 5G.

5 Possible IPv6 Transition Strategies in 5G

The IPv6 transition strategies in 5G mobile networks are similar to the ones described in ETSI GR IP6 006 [i.3]. In particular, due to:

1) the performance improvements seen in IPv6 deployments;

2) support of multi layered secure networking, see e.g. ETSI GR IP6 008 [i.46]; and

3) the deployment of IPv6 by large content provider, mobile operators are being stimulated to deploy IPv6 in their 4G mobile networks. This trend is expected to be continued for 5G mobile networks.

However, due to the fact that only a few applications or services are available only in IPv6, it is expected that it will take a long time until all IPv4-only services will be transitioned to IPv6. Therefore, it is expected that IPv4 and IPv6 will co-exist for a long time, and thus, even in the presence of IPv6-deployment, IPv4 provisioning needs to be taken into account.

It is important to notice that many operators are reluctant to share their IPv6 transition strategy in 4G mobile networks, since it is considered to be a trade secret. It is expected that this holds also for the IPv6 Transition Strategies that will be followed by mobile operators in 5G mobile networks.

Some of the applied IPv4 - IPv6 transition strategies by mobile operators in their 4G mobile networks are, see also clause 4.3 of the present document:

- *Operator in Europe 1*: Incrementally planned and deployed IPv6, where already in 2013 the entire core network has been IPv6 enabled.
- *Operator in Europe 2*: 464XLAT.
- *Operator in Europe 3*: IPv6 dual-stack, expected to deploy in the future: IPv6 only with NAT64/DNS64.
- *Operator in Europe 4*: In IPv6 only + NAT64.
- *Operator in China 1*: IPv6 dual-stack, DS-Lite and NAT444.
- *Operator in China 2*: IPv6 dual-stack.
- Operator in USA 1: use of 464XLAT and IPv6-only solutions, since 2014. Currently, deploying only IPv6-only solutions.
- Operator in USA 2: routes packets from IPv6 devices:
  - via IPv6 network with no stateful middleboxes; and
  - via IPv4-in-IPv6 tunnels using Gateway Initiated Dual-Stack Lite (DS Lite) [i.35] software on the phone.

6 Lessons Learned

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 validated. In overall, this will enable the fast deployment and success of 5G. This section uses the information provided in the previous sections and derives the lessons learned:

- According to press releases coming from law enforcement units, e.g. Europol, the carrier grade NAT technology is creating a serious online capability gap in law enforcement efforts to investigate and attribute crime and recommendations are being done towards ISPs and mobile operators to stop using this technology. This can be experienced as an important stimulus by mobile operators to start deploying IPv6 in their future 5G networks.
- Mobile operators are currently being stimulated to deploy IPv6 in their 4G mobile networks due to:
    - the performance improvements seen in IPv6 deployments;
    - support of multi layered secure networking, see e.g. ETSI GR IP6 008 [i.46]; and
    - the deployment of IPv6 by large content provider. This trend is expected to be continued for 5G mobile networks. However, it is expected that IPv4 and IPv6 will co-exist also in 5G deployments due to the fact that only a few applications or services are currently available only in IPv6. This means that even in the presence of IPv6-deployments, IPv4 provisioning needs to be taken into account.
- 5G will help vertical industries to achieve the "Internet of Things" (IoT) vision of ubiquitously connected, highly reliable, ultra-low latency services for massive number of devices. In particular, IPv6 can be seen as one of the main drivers for the rapid growth realization and deployment of IoT.

7 Conclusions

IPv6 can support the 5G infrastructure deployments with performance improvements and more secure multi-layered secure networking compared to IPv4 based infrastructures. Moreover, since it is expected that 5G will help vertical industries to achieve the "Internet of Things" (IoT) vision, IPv6 can enables the scalability required by the IoT and can provide enhancement from IPv4 in the field of for example, mobility support, stateless address auto-configuration, support of constraint devices and security.

It is important to be as well noted that one of the operators in USA announced that in new 5G deployments only the IPv6-only solution will be applied.

It is however, expected that IPv4 and IPv6 will co-exist also in 5G deployments due to the fact that only a few applications or services are currently available only in IPv6. This means that even in the presence [i.46] of IPv6-deployments, IPv4 provisioning needs to be taken into account.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Georgios Karagiannis, Huawei, Germany

Other contributors:
Latif Ladid, Former Chair, ETSI IP6 ISG, University of Luxembourg

Annex B (informative): Change History

Date	Version	Information about changes
June 2015	V0.0.1	Document creation Latif Ladid E-mail: mailto:latif@ladid.lu
October 2015	V0.0.2	Sent before October f2f meeting, but not yet uploaded as Draft. Created new table of contents
January 2016	V0.0.3	Updated clauses 4.2 and 4.4
June 2016	V0.0.4	Updated clause 4.4
November 2016	V0.0.5	Removed clause 4.4.2 and included clause 4.4.6
February 2017	V0.0.6	Added clauses 4.4.6, 4.4.7, 4.4.8, 4.4.9 and 4.4.10
March 2017	V0.0.7	Changed template from GS to GR and renamed titles of clauses in order to avoid names of companies
June 2017	V0.0.8	• Updated clause 4.2.2: 3GPP (3rd Generation Partnership Project) • Updated clause 4.5: 5G and Internet of Things (IoT) • Renamed the company used in the text (associated with the trademark disclaimer)
August 2017	V0.0.9	• Work out comments by Mrs. Christine Mera: (1) introduced trademark disclaimer related paragraph. (2) removed hanging text (3) accepted editorial corrections, (4) changed title of GR from: IPv6-Based 5G Mobile Wireless Internet INTO: IPv6-Based 5G Mobile Internet, (5) removed Executive Summary • Added text to clause 5: Possible IPv6 Transition Strategies in 5G
December 2017	V0.0.10	• Incorporates version that has been discussed and approved during the ETSI ISG IP6 nr. 6 • Included cross-references that are complying to the ETSI guidelines [i.47] ... [i.1], etc. • Clause 4.3 5: G Use cases and Key Requirements has been deleted, due to lack of contributions
January 2018	V0.0.11	• Finalized clause 6 (lessons learned) and clause 7 (conclusions). Moreover, the abbreviation clause is completed
February 2018	V0.0.12	• UK spell check and matching title with approved WI form
October 2018	V1.1.1	• Worked out the comment provided by Edit Help

History

Document history		
V1.1.1	October 2018	Publication