ETSI GR IP6 030 V1.1.1 (2020-10)

IPv6-based Vehicular Networking (V2X)

Disclaimer

The present document has been produced and approved by the IPv6 Integration (IP6) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/IP6-0030

Keywords
IPv6, V2X

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] ETSI GR IP6 011 (V1.1.1): "IPv6-Based 5G Mobile Wireless Internet; Deployment of IPv6-Based 5G Mobile Wireless Internet".

[i.2] Alcatel-Lucent Strategic White Paper (April 2015): "464XLAT in mobile networks IPv6 migration strategies for mobile networks".

[i.3] IETF RFC 6342 (December 2011): "Mobile Networks Considerations for IPv6 Deployment".

[i.4] ETSI GR IP6 006: "Generic migration steps from IPv4 to IPv6".

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.5] 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.6] IETF RFC 3633 (December 2003): "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".

[i.7] IETF RFC 3769 (June 2004): "Requirements for IPv6 Prefix Delegation".

[i.8] IETF RFC 7755 (February 2016): "SIIT-DC: Stateless IP/ICMP Translation for IPv6 Data Center Environments".

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.9] 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.10] ETSI GR IP6 008: "IPv6-based Internet of Things Deployment of IPv6-based Internet of Things".

[i.11] 5G Automotive Association (5GAA): "MNO Network Expansion Mechanisms to Fulfil Connected Vehicle Requirements", White Paper, 23 June 2020.

[i.12] ISO 21217:2014 "Intelligent transport systems -- Communications access for land mobiles (CALM) - Architecture", April 2014.

[i.13] ETSI EN 302 665 (V1.1.1): "Intelligent Transport Systems (ITS); Communications Architecture".

[i.14] ISO 21210:2012: "Intelligent transport systems -- Communications access for land mobiles (CALM) -- IPv6 Networking", June 2012.

[i.15] ISO 29281-1:2018: "Intelligent transport systems -- Localized communications -- Part 1: Fast networking & transport layer protocol (FNTP)", June 2018.

[i.16] IETF RFC 3963 (January 2005): "Network Mobility (NEMO) Basic Support Protocol".

[i.17] ETSI EN 302 636-5-1 (V2.1.1): "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol".

[i.18] ETSI EN 302 636-6-1 (V1.2.1): "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols".

[i.19] IETF RFC 5648 (October 2009): "Multiple Care-of Addresses Registration".

[i.20] ETSI EN 302 636-4-1 (V1.2.1): "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[i.21] IETF RFC 8200 (July 2017): "Internet Protocol, Version 6 (IPv6) Specification".

[i.22] IETF RFC 2663 (August 1999): "IP Network Address Translation (NAT) Terminology and Considerations".

[i.23] IETF RFC 4241 (December 2005): "A Model of IPv6/IPv4 Dual Stack Internet Access Service".

[i.24] IETF RFC 6275 (July 2011): "Mobility Support in IPv6".

[i.25] José Santa, Pedro J. Fernández, Fernando Pereñíguez, Fernando Bernal, Antonio Moragón, Antonio F. Skarmeta, "IPv6 Communication Stack for Deploying Cooperative Vehicular Services", International Journal of ITS Research, Vol. 12, May 2013.

NOTE: Available at https://www.researchgate.net/publication/261718503_IPv6_Communication_Stack_for_Deploying_Cooperative_Vehicular_Services.

[i.26] Pedro Javier Fernández Ruiz, Fernando Bernal Hidalgo, José Santa Lozano and Antonio F. Skarmeta, "Deploying ITS Scenarios Providing Security and Mobility Services Based on IEEE 802.11p™ Technology". (Published: February 13th, 2013).

NOTE: Available at https://www.intechopen.com/books/vehicular-technologies-deployment-and-applications/deploying-its-scenarios-providing-security-and-mobility-services-based-on-ieee-802-11p-technology.

[i.27] IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".

[i.28] Pedro J. Fernandez, José Santa, Fernando Bernal and Antonio F. Skarmeta,"Securing Vehicular IPv6 Communications" (2015).

[i.29] Donenfeld, J.A.: "WireGuard®: Next generation kernel network tunnel", In: 24th Annual Network and Distributed System Security Symposium, NDSS 2017.

[i.30] Perrin, T.: "The Noise protocol framework" (2018).

NOTE: Available at https://noiseprotocol.org/noise.html.

[i.31] Jacob Appelbaum, Chloe Martindale, Peter Wu, "Tiny WireGuard Tweak". Department of Mathematics and Computer Science Eindhoven University of Technology, Eindhoven, Netherlands.

[i.32] 5G Automotive Association (5GAA): "5GAA Efficient Security Provisioning System", White Paper, 18 May 2020.

NOTE: Available at https://eprint.iacr.org/2019/482.pdf.

[i.33] IETF RFC 4861 (September 2007): "Neighbor Discovery for IP version 6 (IPv6)".

[i.34] IETF RFC 4862 (September 2007): "IPv6 Stateless Address Autoconfiguration".

[i.35] IETF RFC 6550 (March 2012): "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks".

[i.36] IETF RFC 4291 (February 2006): "IP Version 6 Addressing Architecture".

[i.37] IETF RFC 8273 (December 2017): "Unique IPv6 Prefix per Host".

[i.38] IETF RFC 8505 (November 2018): "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery".

[i.39] IETF RFC 6775 (November 2012): "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)".

[i.40] IETF draft draft-ietf-6lo-backbone-router: "IPv6 Backbone Router".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-6lo-backbone-router/.

[i.41] IETF draft draft-ietf-6lo-ap-nd: "Address Protected Neighbor Discovery for Low-power and Lossy Networks".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-6lo-ap-nd/.

[i.42] IETF RFC 4191 (November 2005): "Default Router Preferences and More-Specific Routes".

[i.43] IETF RFC 8691 (December 2019): "Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11™".

[i.44] IETF Distributed Mobility Management WG.

NOTE: Available at https://datatracker.ietf.org/wg/dmm/about/.

[i.45] ETSI EN 302 663 (V1.3.1): "Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band".

[i.46] ETSI TS 122 185 (V14.3.0): "Service requirements for V2X services (3GPP TS 22.185 Release 14)".

[i.47] AIOTI WG03 - loT Standardisation, "IoT Relation and Impact on 5G", April 2020.

NOTE: Available at https://aioti.eu/wp-content/uploads/2020/05/AIOTI-IoT-relation-and-impact-on-5G-R3-Published.pdf.

[i.48] IETF Draft: "draft-thubert-roll-unaware-leaves".

[i.49] IETF Draft: "draft-thubert-6man-ipv6-over-wireless".

[i.50] IETF Draft: "draft-pthubert-raw-architecture".

[i.51] IEEE Std 802.11™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.52] IEEE Std. 802.3™: "IEEE Standard for Ethernet".

[i.53] IEEE Std. 802.1™: "IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control".

[i.54] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501)".

[i.55] IETF RFC 4903 (June 2007): "Multi-Link Subnet Issues".

[i.56] IETF RFC 7668 (October 2015): "IPv6 over BLUETOOTH(R) Low Energy".

[i.57] IETF RFC 6830 (January 2013): "The Locator/ID Separation Protocol (LISP)".

[i.58] IETF RFC 7401 (April 2015): "Host Identity Protocol Version 2 (HIPv2)".

[i.59] IETF RFC 7181 (April 2014): "The Optimized Link State Routing Protocol Version 2".

[i.60] IETF RFC 3561 (July 2003): "Ad hoc On-Demand Distance Vector (AODV) Routing".

[i.61] ETSI TS 123 285: "Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for V2X services (3GPP TS 23.285)".

[i.62] IETF RFC 5614 (August 2009): "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding".

[i.63] IETF RFC 5820 (March 2010): "Extensions to OSPF to Support Mobile Ad Hoc Networking".

[i.64] IETF RFC 7137 (February 2014): "Use of the OSPF-MANET Interface in Single-Hop Broadcast Networks".

[i.65] IETF RFC 3775 (June 2004): "Mobility Support in IPv6".

[i.66] IETF RFC 4889 (July 2007): "Network Mobility Route Optimization Solution Space Analysis".

[i.67] IETF RFC 8655 (October 2019): "Deterministic Networking Architecture".

[i.68] AUTOPILOT EU LSP Project.

NOTE 1: Available at https://autopilot-project.eu/.

NOTE 2: Versailles Project available at https://autopilot-project.eu/wp-content/uploads/sites/16/2018/09/Versailles.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	Third Generation Partnership Project
5G	5th Generation
5G NR	5G New Radio
5G-DRIVE	5G HarmoniseD Research and TrIals for serVice Evolution
AD	Autonomous Driving
ADAS	Advanced Driver Assistance System

AEAD	Authentication Encryption with Additional Data
AF	Application Function
AH	Authentication Header
AI	Artifical Intelligence
AIOTI	Alliance for Internet of Things Innovation
AMF	Access and Mobility Function
AODV	Ad hoc On-Demand Distance Vector routing
AP	Access Point
APN	Access Point Names
APNIC	Asia Pacific Network Information Centre
AR	Address Resolution
AR/VR	Augmented Reality/Virtual Reality
ASL	Adaptation Sub-Layer
ATM	Asynchronous Transfer Mode
BA	Binding Acknowledge
BID	Binding Identification Number
BLE	Bluetooth Low Energy
BS	Base Station
BSM	Basic Safety Message
BSS	Basic Service Set
BTP	Basic Transport Protocol
BU	Binding Update
C-ADAS	Cooperative Advanced Driving Assistance Systems
CAM	Cooperative Awareness Message
CCAM	Cooperative, Connected and Automated Mobility
CCSA	China Communication Standards Association
CDN	Content Delivery Network
CGN	Carrier Grade NAT
CG-NAT	Carrier-Grade NAT
CLAT	Customer-side transLATor
CN	Correspondent Node
CoA	Care of Address
CORE	Core Network
CPM	Collective Perception Message
CSAE	China Society of Automotive Engineers
CSFB	Circuit Switched FallBack
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuation Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DMM	Distributed Mobility Management
DNS	Domain Name System
DS	Dual-Stack
DSRC	Dedicated Short Range Communication
EARO	Extended Address Registration Option
EDCA	Enhanced Distributed Channel Access
EDM	Edge Dynamic Map
EIID	Extended Interface Identifier
EPS	Evolved Packet System
ESP	Encapsulation Security Payload
ES-PT	Spain-Portugal
ESS	Extended Service Set
EUI	End-system Unique Identifier
FN	Foreign Network
FOT	Field Operational Tests
GLOSA	Green Light Optimal Speed Advisory
GN	Geo Networking
GPRS	General Packet Radio Service
GR	Group Report
GR-TR	Greece-Turkey
GUA	Global Unique Address
GVL	Geographical Virtual Link
HA	Home Agent

HD	High Definition
HIP	Host Identity Protocol
HMI	Human Machine Interface
HN	Home Network
HoA	Home of Address
HR	Home Router
HSS	Home Subscriber server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAB	Internet Architecture Board
ICT	Information and Communications Technology
IDC	Internet Data Centre
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IID	Interface Identifier
IKEv2	Internet Key Exchange version 2
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
IPWAVE	IP Wireless Access in Vehicular Environments
ISP	Internet Service Provider
ITS	Intelligent Transport System
ITS-G	5,9 GHz Cooperative ITS system
ITU-R	International Telecommunication Union - Radiocommunication Sector
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN	Local Area Network
LISP	Locator/ID Separation Protocol
LLA	Link Local Address
MAC	MAC Medium Access Control layer
MANET	Mobile Ad-hoc NETworks
MCoA	Mobile Care of Address
MIIT	Ministry of Industry and Information Technology (China)
MIPv6	Mobile IPv6
MLSN	Multi-Link Subnet
MME	Mobile Management Entity
MN	Mobile Node
MNN	Mobile Network Node
MNO	Mobile Networks Operator
MNP	Mobile Network Prefix
MR	Mobile Router
NA/RA	Neighbor Advertisement/ Router Advertisement
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
NCC	Network Control Center
ND	Neighbour Discovery
NDP	Neighbour Discovery Protocol
NEMO BS	NEtwork MObility Basic Support
NEMO	Network Mobility
NGMN	Next Generation Mobile Network
NR	5G New Radio interface
NS	Neighbor Solicitation
NS/NA	Neighbour Solicitation/Neighbour Advertisement
OCB	Outside the Context of a BSS
OFDM	Orthogonal Frequency Division Multiple Access
OLSR	Optimised Link State Routing
OS	Operating System
OSI	Open Systems Interconnection
PDN	Packet Data Network
PDP	Packet Data Protocol

PGW	Packet data network GateWay
PHY	Physical Layer (protocol layer)
PIO	Prefix Information Option
PLMN	Public Landline Mobile Network
PLT	Page Load Time
PS	Pilot Site
RA	Router Advertisement
RAT	Radio Access Technologies
RAW	Reliable and Available Wireless
RFC	Request For Comments
RIPE	Reseaux IP Europeens
RPL	Routing Protocol for Low-Power and Lossy Networks
RS	Router Solicitation
RSU	Road Side Unit
RTT	Round Trip Time
RUM	Real User Monitoring
SA	Security Association
SAD	Security Association Database
SC-FDMA	Single Carrier-Frequency Division Multiple Access
SCMS	Security Credential Management Systems
SLLAO	Source Link-Layer Address Option
SMF	Session Management Function
SNMA	Solicited-Node Multicast Address
SPD	Security Policy Database
SSH	Secure Shell
SSL	Secure Socket Layer
STA	Station
STD	STandarD
TC	(ETSI) Technical Committee
TCP	Transmission Control Protocol
TD	Temporary Document
TLS	Transport Layer Security
UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
ULA	Unique Local Address
UMTS	Universal Mobil Telecommunications System
UP	User Plane
V2X	Vehicle to everything
VoIP	Voice over IP
VoLTE	Voice over Long Term Evolution
VRU	Vulnerable Road User
WI	Work Item
WiMAX™	Worldwide interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

4 IPv6-based Vehicular Networking (V2X)

4.1 Introduction

Internet protocol version 6 (IPv6) is a new version of the Internet protocol (IP) defined in IETF RFC 8200 [i.21] and designed to replace Internet protocol version 4 (IPv4). IPv6 provides several advantages that cover important needs in cooperative vehicular communication, such as the large space of addressing due to the exhaustion of IPv4 address space, which impacts the growing of internet continuity. In fact, most mobile terminals will not be able to connect to IPv4 Internet without the intermediate technology called Network Address Translation (NAT) [i.22], which allows one or more public addresses to serve many private IP addresses in order to conserve addresses, hence the importance of using IPv6 which goes from 32-bit addressing to 128-bit addressing. Dual stack [i.23] is considered as one of the most used mechanisms that applies migration from IPv4 to IPv6. It allows the implementation of IPv4 and IPv6 in terminals in order to use IPv4 access services that have not yet been migrated to IPv6.

In addition to all the advantages already mentioned, IPv6 protocol also brought other numerous benefits such as the improvement of mobility and security services and mainly the addition of node auto-configuration mechanisms to facilitate the configuration of connected equipment. In fact, one of the main functions of an IPv6 node based on its ability to be configured automatically when its connected to a network using router discovery message ICMPv6 (Internet Control Message Protocol version 6). During this mechanism, an address named (Link-Local) is created by IPv6 node in order to search for the routers present on its network segment using the Neighbour Discovery Protocol (NDP) [i.33] and connect to other nodes connected to the same communication channel.

In order to obtain an IPv6 global address, the IPv6 node sends a router solicitation message using as destination the multicast address (FF01 :: 2). After receiving this message, the routers respond with a Router advertisement (RA) message, which is often transmitted periodically by routers and contain IPv6 prefix to all nodes located on their network. When receiving the RA messages, the node creates its IPv6 address by adding its network identifier extracted from its Mac address, to the received IPv6 prefix. Finally, to avoid double assignment of IPv6 addresses, the IPv6 node performs Duplicate Address Detection (DAD) for the newly generated IPv6 address.

This mechanism of auto-configuration is called stateless, because nodes can be configured without using manual configuration or a help of a server such as DHCPv6 (Dynamic Host Configuration Protocol version 6), and it is very important in the vehicular network, because it offers fast connectivity with other ITS station and reduce latency.

4.2 IPv6 Transition Strategies

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] and [i.2], are listed below. More details on mobile networks considerations for IPv6 deployment are described in [i.3].

- **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 an 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 an 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.4].

4.3 World Wide V2X Standardisation Initiatives

4.3.1 Applying IPv6 to Extra-Vehicular Communication

The emergence of automotive Ethernet for in-vehicle communications and variations of Wi-Fi® designed to operate outside of the context of a BSS (IEEE Std 802.11™ [i.51] OCB and new work from TG 802.11bd) naturally brings in the need for IP communications. IP enables to leverage:

i) ICT technologies such as Internet access;

ii) AI and big data for applications such as video, LiDAR, and traffic-sign recognition inside the car;

iii) Connectivity-based services such as remote diagnostics, location based services, autonomous vehicles and Cooperative-Advanced Driving Assistance Systems (C-ADAS).

While it seems simple to design a model for IP subnets inside the vehicle that connects and isolates functions and ECUs as required, the connectivity to the outside appears a lot more problematic:

- IP addresses are normally assigned to fixed locations around an abstract link where a subnet resides. Subnets are then aggregated by routers in larger and larger aggregations that are finally advertised in the Internet default-free zone. This is what routable addresses mean. But the vehicle and the prefixes within are mobile, and a technology such as Network Mobility (NEMO) is required to maintain IP connectivity and session continuity from the inside to the outside of the vehicle at all times.

- Cars may be moving together and may need to maintain connectivity within the platoon whether connectivity to the larger internet is available or not. Depending of the type of swarming (relative movement inside the platoon) and the size of the platoon (average number of relays), one of the possible Mobile Ad-hoc Network (MANET) technologies may be more appropriate than another.

- IPv4 addresses are running out; RIPE NCC ran out on November 25th, 2019. With millions of cars produced each year and several subnets inside each car, it makes sense to leverage IPv6 and IPv6-specific types of addresses such as unique-local addresses (ULA) to design the networks inside the cars and define their interconnectivity at Layer-3. While it is possible to tunnel the traffic to the outside in IPv4 tunnels or to apply NAT64 techniques, vehicle communication will hugely benefit from a pervasive native IPv6 access.

- As the vehicle moves, it may be connected to the Internet, other vehicles or the infrastructure with one or more of 3GPP networks (LTE, 5G), Wi-Fi® hotspot (e.g. with openroaming), and specialized V2X communication such as OCB. Each of these communication methods has its own challenges in terms of geographical availability and bandwidth. Selecting a technology or a set of technologies at every point of time and deciding whether to leverage redundant transmissions is now being discussed in the context of Reliable and Available Wireless (RAW) networking.

- Wireless LANs in particular present unique challenges for IP communications, that are not fully resolved at the IETF. As unrelated cars move in and out an access location, which ones are members of a local subnet and for how long? When should a vehicle form an address and for how long should it retain that state? Should that address be preserved for that vehicle and for how long? Indeed, what is the Link model for IPv6 in that case?

4.3.2 Modelling IPv6 Links and Subnets over a Wireless LAN

At the physical (PHY) Layer, a broadcast domain is the set of nodes that may receive a datagram that one sends over an interface, i.e. the set of nodes in range of radio transmission. On WLAN and WPAN radios, the physical broadcast domain is defined by a particular transmitter, as the set of nodes that can receive what this transmitter is sending. Literally every datagram defines its own broadcast domain since the chances of reception of a given datagram are statistical. In average and in stable conditions, the broadcast domain of a particular node can still be seen as mostly constant and can be used to define a closure of nodes on which an upper-layer abstraction can be built.

A PHY-layer communication can be established between 2 nodes if their physical broadcast domains overlap. On WLAN and WPAN radios, this property is usually symmetrical, meaning that if B can receive a datagram from A, then A can receive a datagram from B. But there can be asymmetries due to power levels, interferers near one of the receivers, or differences in the quality of the hardware (e.g. crystals, Power Amps and antennas) that may affect the balance to the point that the connectivity becomes mostly uni-directional, e.g. A to B but practically not B to A.

It takes a particular effort to place a set of devices in a fashion that all their physical broadcast domains fully overlap, and it cannot be assumed in the general case. In other words, the property of radio connectivity is generally not transitive, meaning that A may be in range with B and B may be in range with C does not necessarily imply that A is in range with C.

With IEEE Std 802.11™ OCB, the broadcast domain that is usable at the MAC layer is the same as the physical broadcast domain. This contrasts with the MAC-layer Broadcast Emulation schemes that Wi-Fi® provides with the IEEE Std 802.11™ [i.51] Infrastructure Basic Service Set (BSS).

A BSS provides a closure of nodes as defined by the broadcast domain of a central Access Point (AP). The AP relays both unicast and broadcast packets and ensures a symmetrical and transitive emulation of the shared wire between the associated nodes, with the capability to signal link-up/link-down to the upper layer. Within an Infrastructure BSS, the physical broadcast domain of the AP serves as emulated broadcast domain for all the nodes that are associated to the AP. Broadcast packets are relayed by the AP and are not acknowledged. To ensure that all nodes in the BSS receive the broadcast transmission, AP transmits at the slowest PHY speed. This translates into maximum co-channel interferences for others and longest occupancy of the medium, for a duration that can be 100 times that of a unicast. For that reason, upper layer protocols should avoid the use of broadcast when operating over Wi-Fi®.

IPv6 defines the (physical) concept of an IP Link, a Link Scope and Link-Local Addresses (LLA), an LLA being unique and usable only within the Scope of a Link. On wired media, the Link is often confused with the physical broadcast domain because both are determined by the serial cable or the Ethernet shared wire. Ethernet Bridging reinforces that illusion by providing a MAC-Layer broadcast domain that emulates a physical broadcast domain over the mesh of wires. But the difference shows on legacy Non-Broadcast Multi-Access (NBMA) such as ATM and Frame-Relay, on shared links and on newer types of NBMA networks such as radio and composite radio-wires networks. It also shows when private VLANs or Layer-2 cryptography restrict the capability to read a frame to a subset of the connected nodes.

In Infrastructure BSS, the IP Link extends beyond the physical broadcast domain to the emulated MAC-Layer broadcast domain. But with OCB radios, IP Links between peers come and go as the individual physical broadcast domains of the transmitters meet and overlap. The nodes may need to form new LLAs to talk to one another and the scope where LLA uniqueness can be dynamically checked is that pair of nodes. As long as there is no conflict a node may use the same LLA with multiple peers, but it has to recheck for address duplication with every new peer node. In practice, each pair of nodes defines a temporary P2P link, which can be modelled as a sub-interface of the radio interface.

IPv6 also defines the (logical) concept of Subnet for Global and Unique Local Addresses. Addresses in the same Subnet share the same prefix and, by extension, a node belongs to a Subnet if it has an interface with an address on that Subnet. A Subnet prefix is Globally Unique, so it is sufficient to validate that an address that is formed from a Subnet prefix is unique within that Subnet to guarantee that it is globally unique. IPv6 aggregation relies on the property that a packet from the outside of a Subnet can be routed to any router that belongs to the Subnet, and that this router will be able to either resolve the destination MAC address and deliver the packet, or route the packet to the destination within the Subnet. If the Subnet is known as on-link, then any node may also resolve the destination MAC address and deliver the packet directly, but if the Subnet is not on-link, then a host will need to pass the packet to a router for forwarding.

On IEEE Std. 802.3™ [i.52], a Subnet is often congruent with an IP Link because both are determined by the physical attachment to an Ethernet shared wire or an IEEE Std. 802.1™ [i.53] bridged broadcast domain. In that case, the connectivity over the Link is transitive, the Subnet can appear as on-link, and any node can resolve a destination MAC address of any other node directly using the IPv6 Neighbour Discovery (IETF RFC 4861 [i.33] and IETF RFC 4862 [i.34]) Protocol (IPv6 ND).

But an IP Link and an IP Subnet are not always congruent. In a shared Link situation, a Subnet may encompass only a subset of the nodes connected to the Link. In Route-Over Multi-Link Subnets (MLSN) (see IETF RFC 4903 [i.55]), routers federate the Links between nodes that belong to the Subnet, the Subnet is not on-link and it extends beyond any of the federated Links. The routing service can be a simple reflexion in a Hub-and-Spoke Subnet that emulates an IEEE Std 802.11™ [i.51] Infrastructure BSS at Layer-3. It can also be a full-fledge routing protocol such as RPL (IETF RFC 6550 [i.35]). RPL was designed to adapt to various LLNs such as WLAN and WPAN radio MLSNs. Finally, the routing service can also be an ND proxy function that emulates an IEEE Std 802.11™ [i.51] Infrastructure ESS at Layer 3.

The basic procedures of IPv6 ND expect that a node in a Subnet is reachable within the broadcast domain of any other node in the Subnet when that other node attempts to form an address that would be a duplicate or attempts to resolve the MAC address of this node. This is why ND is only applicable for P2P and transit links and requires extensions for other topologies.

4.3.3 Applying IPv6 ND to Wireless Links

IEEE STD. 802.1™ [i.53] Ethernet Bridging provides an efficient and reliable broadcast service for wired networks; many applications and protocols that heavily depend on this feature for their core operation have been built. Local wireless networks generally do not provide the broadcast capabilities of Ethernet Bridging in an economical fashion.

As a result, protocols designed for bridged networks that rely on multicast and broadcast often exhibit disappointing behaviours when employed unmodified on a local wireless medium. Wi-Fi® Access Points (APs) deployed in an Extended Service Set (ESS) act as Ethernet Bridges, with the property that the bridging state is established at the time of association. This ensures connectivity to the node (STA) and protects the wireless medium against broadcast-intensive Transparent Bridging reactive Lookups. In other words, the association process is used to register the MAC Address of the STA to the AP. The AP subsequently proxies the bridging operation and does not need to forward the broadcast Lookups over the radio. Like Transparent Bridging, IPv6 ND is a reactive protocol, based on multicast transmissions to locate an on-link correspondent and ensure the uniqueness of an IPv6 address.

The IPv6 ND mechanism for Duplicate Address Detection (DAD) (IETF RFC 4862 [i.34]) was designed for the efficient broadcast operation of Ethernet Bridging, which enable Subnet-wide broadcast domains at reasonable cost. Since broadcast can be unreliable over wireless media, DAD often fails to discover a duplication. In practice, IPv6 addresses very rarely conflict because of the entropy of the 64-bit Interface IDs, not because address duplications are detected and resolved.

The IPv6 ND Neighbour Solicitation (NS) (IETF RFC 4861 [i.33]) message is used for DAD and Address Resolution (AR) when a node moves, or wakes up and reconnects to the wireless network. The NS message is targeted to a Solicited-Node Multicast Address (SNMA) (IETF RFC 4291 [i.36]) and should in theory only reach a very small group of nodes. To be noted that in the case of Ethernet LANs, as well as most WLANs and LPWANs, the Layer-3 multicast operation becomes a Layer-2 broadcast for the lack of a Layer-2 multicast operation that could handle a possibly very large number of groups in order to make the unicast efficient.

The overuse of Layer-2 broadcast can be alleviated by reducing the IPv6 ND broadcasts over wireless access links. This has been done by splitting the broadcast domains and by routing between subnets, at the extreme by assigning a /64 prefix to each wireless node (see IETF RFC 8273 [i.37]). Wireless ND (WiND) introduces a new approach to IPv6 ND that is designed to apply to the WLANs and WPANs types of networks. On the one hand, WiND avoids the use of broadcast operation for DAD and AR, and on the other hand, WiND supports use cases where Subnet and MAC-level domains are not congruent, which is common in those types of networks unless a specific MAC-Level emulation is provided.

WiND leverages Route-Over Multi-Link Subnets and enables mobility within the subnet, e.g. vehicle-to-vehicle links relaying packets in a parking lot towards a common access point, the whole parking lot forming a single subnet. Nodes register their addresses to their serving routers with IETF RFC 8505 [i.38]. With the registration, routers have a complete knowledge of the nodes they serve, and, in return, nodes obtain routing services for their registered addresses and may in turn act as routers. The registration is abstract to the routing protocol, and it can be protected to prevent impersonation attacks.

WiND allows P2P, P2MP hub-and spoke applicable to V2I, MAC-level broadcast domain emulation such as mesh-under and Wi-Fi® BSS, and Route-Over meshes applicable to V2V in a platoon or a parking lot. There is an intersection where Link and Subnet are congruent and where both ND and WiND could apply. This includes P2P, the MAC emulation of a PHY broadcast domain, and the particular case of always on, fully overlapping physical radio broadcast domain. But even in those cases where both are possible, WiND is preferable vs. ND because it reduces the need of broadcast.

There are also numerous practical use cases in the wireless world where Links and Subnets are not P2P and not congruent, and where IPv6 ND is not applicable:

- Bluetooth® (see IETF RFC 7668 [i.56], IEEE std 802.15.1™) provides a Hub-and-Spoke access technology at the MAC layer. BLE may be used within a vehicle to connect HMI comodos to the control system. It would make little sense to configure a different subnet between the central and each individual peripheral node. Rather, (see IETF RFC 7668 [i.56]) allocates a prefix to the central node acting as router, and each peripheral host (acting as a host) forms one or more address(es) from that same prefix and registers it using WiND.

- A large network such as a smartgrid mesh that puts together Route-Over MLSNs comprising thousands of IPv6 nodes. Peerings that are actually used come and go with the dynamics of radio signal propagation. Allocating prefixes to all the possible P2P Links and maintain as many addresses in all nodes is not even considered. This model is applicable to a large parking lot with cars relaying packets for one another for the duration of their stay. A vehicle may leave and come back later with the expectation to reuse the same IPv6 address. As opposed to IPv6 ND, WiND can protect the ownership of an address as long as it is persisted in its central registrar.

4.3.4 Deeper dive on IPv6 Wireless ND

Wireless Neighbour Discovery (WiND) comprises IETF RFC 6775 [i.39], IETF RFC 8505 [i.38], draft-ietf-6lo-backbone-router [i.40], and draft-ietf-6lo-ap-nd [i.41]. WiND defines a new ND operation that is based on two major paradigm changes:

i) proactive address registration by hosts to their attachment routers; and

ii) routing to host routes (/128) within the subnet.

This allows WiND to avoid the classical ND expectations of transit links and Subnet-wide broadcast domains. WiND does not change IPv6 addressing IETF RFC 4291 [i.36] or the current practices of assigning prefixes to subnets. It is still typical to assign a /64 to a subnet and to use interface IDs of 64 bits.

The proactive address registration is performed with a new option in NS/NA messages, the Extended Address Registration Option (EARO) defined in IETF RFC 8505 [i.38]. This method allows to prepare and maintain host routes in the routers and avoids the reactive (multicast) NS Lookup found in IPv6 ND. For Global Unique Address (GUA) and Unique Local Addresses (ULA), DAD is validated at the Subnet Level, using a central registrar. For Link-Local Addresses, DAD is performed between communicating pairs of nodes.

In the Hub-and-Spoke case, each Hub-Spoke pair is a distinct IP Link, and a Subnet can be mapped on a collection of Links that are connected to the Hub. The Subnet prefix is associated to the Hub. Acting as a router, the Hub advertises the prefix as not-on-link to the spokes in RA messages Prefix Information Options (PIO). Acting as hosts, the Spokes autoconfigure addresses from that prefix and register them to the Hub with a corresponding lifetime. Acting as a central registrar, the Hub maintains a binding table of all the registered IPv6 addresses and rejects duplicate registrations, thus ensuring a DAD protection for a registered address even if the registering node is sleeping or temporarily too far away. Acting as a router, the Hub also maintains a neighbour cache for the registered addresses and can deliver a packet to any of them for their respective lifetimes. It can be observed that this design builds a form of Layer-3 Infrastructure BSS.

A Route-Over MLSN is considered as a collection of Hub-and-Spoke where the Hubs form a connected dominating set of the member nodes of the Subnet, and IPv6 routing takes place between the Hubs within the Subnet. A single logical registrar is deployed to serve the whole mesh. The registration in IETF RFC 8505 [i.38] is abstract to the routing protocol and provides enough information to feed a routing protocol such as RPL as specified in [i.49]. In a degraded mode, all the Hubs are connected to a same high-speed backbone such as an Ethernet bridging domain where IPv6 ND is operated. In that case, it is possible to federate the Hub, Spoke and Backbone nodes as a single Subnet, operating IPv6 ND proxy operations [i.40] at the Hubs, acting as 6BBRs. It can be observed that this latter design builds a form of Layer-3 Infrastructure ESS.

4.3.5 Connecting to the infrastructure with IPv6 Over Wi-Fi®

An IEEE std 802.11 Infrastructure BSS provides a Layer-2 emulation of an Ethernet Link, whereas the ESS extends that over a bridged domain with multiple APs. This emulation allows to apply IPv6 ND over the whole ESS. But as the network grows larger and the churn of association and dissociation augments, the amount of IPv6 multicast becomes detrimental to the network operation and the lifetime of battery-operated devices.

IEEE std 802.11 [i.51] recommends using an IPv6 ND proxy to coexist with Ethernet connected nodes. In order to proxy IPv6 ND, the proxy needs to learn the addresses that are reachable over the wireless medium. Learning IPv4 addresses that are obtained via DHCP is relatively easy at the DHCP server.

In contrast to IPv4, IPv6 enables a node to form multiple addresses, some of them temporary to elusive, and with a particular attention paid to privacy. Addresses may be formed and deprecated asynchronously to the association. Even if the knowledge of IPv6 addresses used by a wireless station (STA) can be obtained by snooping protocols such as IPv6 ND and DHCPv6, or by observing data traffic sourced at the STA, such methods provide only an imperfect knowledge of the state of the STA at the AP. This may result in a loss of connectivity for some IPv6 addresses, in particular for addresses rarely used and in a situation of mobility. This may also result in undesirable remanent state in the AP when a STA ceases to use an IPv6 address. It results that snooping protocols is not a recommended technique and that it should only be used as last resort.

The recommended alternate is to use the WiND IPv6 Registration method. By that method, the AP exposes its capability to proxy ND to the STA in Router Advertisement messages. In turn, the STA may request proxy ND services from the AP for one or more IPv6 addresses, using an Address Registration Option. The Registration state has a lifetime that limits unwanted state remanence in the network. The registration is optionally secured using [i.41] to prevent address theft and impersonation. The registration carries a sequence number, which enables a fast mobility without a loss of connectivity.

A Wi-Fi® mesh provides a broadcast domain emulation with reflexive and Transitive properties and defines a transit Link for IPv6 operations. It results that the model for IPv6 operation is similar to that of a BSS, with the root of the mesh operating an Access Point does in a BSS/ESS. While it is still possible to operate IPv6 ND, the inefficiencies of the flooding operation make the IPv6 ND operations even less desirable than in a BSS, and the use of WiND is highly recommended.

4.3.6 Connecting to the infrastructure with IPv6 Over OCB

IEEE Std. 802.11 OCB uses IEEE Std. 802.11 MAC/PHYs but without the BSS functions, thus OCB does not provide MAC level broadcast emulation. OCB-compliant networks are used for vehicular communications as vehicular Wi-Fi® Access. IEEE Std 802.11 [i.51] OCB mode allows all nodes in a wireless range (frequency band) to directly communicate with each other without authentication/association procedures.

The 802.11 OCB links are specified to be compatible as much as possible with the behaviour of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11 OCB MAC layer offers practically the same interface to IP as the Wi-Fi® and Ethernet layers do (802.11a/b/g/n and 802.3).

Regarding IPv6 deployment over IEEE Std 802.11 [i.51] OCB networks, some considerations have to be taken into account:

- **Operation Outside the Context of a BSS (OCB):** the 802.11p links are operated without a Basic Service Set (BSS). This means that the messages Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used.

- **Frequency range:** In the case of 802.11 OCB, systems are working within the band "5,9 GHz". This band is different from the bands "2,4 GHz" or "5 GHz" used by Wireless LAN. As consequence, technical conditions are different. On one hand, the allowed power levels, and implicitly the maximum allowed distance between vehicles, is of 33 dBm for 802.11p (in Europe), compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to a maximum distance of approximately 1 km, compared to approximately 50 m. On the other hand, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in US) and on the use of frequencies for Intelligent Transportation Systems (in EU), compared to Wireless LAN (802.11a/b/g/n).

- **Prohibition of IPv6:** on some channels relevant for the PHY of IEEE 802.11-OCB IPv6 is prohibited, as opposed to IPv6 not being prohibited on any channel on which 802.11a/b/g/n runs;

- '**Half-rate' encoding:** as the frequency range, this parameter is related to PHY, and thus has not much impact on the interface between the IP layer and the MAC layer.

- **Privacy concerns:**

The IETF IPWAVE WG - IPWAVE stands for Wireless Access in Vehicular Environments - defines in particular the operation of IPv6 over OCB. The initial product of the WG, the "Basic Support for IPv6 over IEEE Std 802.11 [i.51] Networks Operating Outside the Context of a Basic Service Set", focuses on applying a legacy IPv6 stack to connect the vehicle to the infrastructure over OCB.

In that mode, P2P Links can be formed and maintained when a pair of radios transmitters are in range from one another. It is possible to operate IPv6 ND over those Links with Link Local addresses. DAD should be performed for all addresses on all P2P IP Links. If special deployment care is taken so that the physical broadcast domains of a collection of the nodes fully overlap, then it is also possible to build an IP Subnet within that collection of nodes and operate IPv6 ND. The model can be stretched beyond the scope of IPv6 ND if an external mechanism avoids duplicate addresses and if the deployment ensures the connectivity between peers. This can be achieved for instance in a Hub-and-Spoke deployment if the Hub is the only router in the Subnet and the Prefix is advertised as not on-link.

IPWAVE showed that a legacy IPv6 stack can be made to work under controlled conditions but yields a number of pitfalls that limit the possibilities to use is for the generic consumer use cases.

WiND is the recommended approach since it uses more unicast communications which are more reliable and less impacting for other users of the medium. Router and Hosts respectively send a compressed NA/RA with a SLLAO at a regular period. The period can be indicated in a RA as in an RA-Interval Option (see IETF RFC 6275 [i.24]). If available, the message can be transported in a compressed form in a beacon, e.g. in OCB Basic Safety Messages (BSM) that are nominally sent every 100 ms. An active beaconing mode is possible whereby the Host sends broadcast RS messages to which a router can answer with a unicast RA.

A router that has Internet connectivity and is willing to serve as an Internet Access may advertise itself as a default router (see IETF RFC 4191 [i.42]) in its RA. The NA/RA is sent over an Unspecified Link where it does not conflict to anyone, so DAD is not necessary at that stage. The receiver instantiates a Link where the sender's address is not a duplicate. To achieve this, it forms an LLA that does not conflict with that of the sender and registers to the sender using IETF RFC 8505 [i.38]. If the sender sent an RA (PIO) the receiver can also autoconfigure an address from the advertised prefix and register it.

The lifetime in the registration should start with a small value and exponentially grow with each re-registration to a larger value. The IP Link is considered down when a number of expected messages are not received in a row. To be noted that the Link flapping does not affect the state of the registration and when a Link comes back up, the active registrations are still usable. Packets should be held or destroyed when the Link is down.

An example Hub-and-Spoke is an OCB Road Side Unit (RSU) that owns a prefix, provides Internet connectivity using that prefix to On-Board Units (OBUs) within its physical broadcast domain. P2P Links may be federated in Hub-and-Spoke and then in Route-Over MLSNs as described above. An example of Route-Over MLSN is a collection of cars in a parking lot operating RPL to extend the connectivity provided by the RSU beyond its physical broadcast domain. Cars may then operate NEMO (IETF RFC 3963 [i.16]) for their own prefix using their address derived from the prefix of the RSU as CareOf Address.

4.3.7 Enabling network mobility

A number of protocols enable the separation of the locator (e.g. an IP address that indicates where the vehicle is) from the identifier (an IP address that is attached to the vehicle regardless of its location). For individual addresses, Mobile IPv6 (MIPv6) [i.24], LISP (see IETF RFC 6830 [i.57]) and the HIP (see IETF RFC 7401 [i.58]) are notable examples of such protocols. In contrast, NEMO [i.16], which stands for network mobility, was defined as an extension to MIPv6 to enable the mobility of not only a single address but a full prefix.

Mobile IPv6 (MIPv6)

The Mobile IPv6 protocol was defined by IETF mip6 working group in IETF RFC 6275 [i.24] to solve some problems related to continuity of service while changing networks or access technologies. It allows a node to use a fixed IPv6 address, called Home of Address (HoA), regardless of its movement by separating the identification and location functions through providing nodes with different IP addresses, called Care of Address (CoA), where each one belongs to the network it crosses. Therefore, mobile nodes can receive communications messages while roaming to Foreign Network (FN).

As described in [i.25], the vehicle is considered as Mobile Node (MN) that changes place from its Home Network (HN) to another point of attachment. The MIPv6 protocol allows other nodes to connect with MN without realizing that it has moved from its HN. This mechanism is achieved through an entity called Home Agent (HA) which is responsible for Binding the HoA and the CoA acquired by Foreign network and then intercept the packets addressed to the MN and transfer them using an IPv6-IPv6 tunnel. During this process, when a MN changes a network, it sends a Binding update message (BU) in order to inform its HA of the CoA modification and update the binding cache (HoA-CoA). This message will be acknowledged by HA.

Network Mobility Basic Support (NEMO BS)

Network Mobility Basic Support (NEMO BS) [i.16] is an advanced extension of the MIPv6 protocol. Contrary to MIPv6 protocol, NEMO BS allows the vehicle to become a mobile router (MR) for a mobile network in order to maintain internet connectivity in C-ITS between all nodes in an in-vehicle (MR) and infrastructure. It also allows these nodes to be reachable at a permanent address. To accomplish this functionality, Mobility exchanges take place between MR and Home Agent (HA) located in the Home Network. In the C-ITS environment the ITS Central Station is considered as a Home Agent. During the mobility process, the transmission of traffic will not be stopped, because no change of address will be necessary while roaming from one network to another. In addition, Network Mobile Nodes (MNN) located behind the MR will not be aware of movement changes.

Figure 1 illustrates the mobility mechanism provided by NEMO in vehicular networks. MR performs mobility management by broadcasting periodically its mobile network prefix (MNP) acquired from its HA and used by MR to assign addresses to MNNs in order to join the network. When the mobile router moves outside its home network (Central ITS-S), it receives Router Advertisement (RA) from an access router located in the Foreign network (Roadside ITS-S). Therefore, the MR acquires a new operational address called Care of Address (CoA) valid in the visited network. Thanks to Binding Update (BU) messages, the new CoA is immediately notified to HA which replies by a Binding Acknowledge message (BA) in order to establish the CoA-HoA connection. At least, that one will be stored in the Binding cache of HA, which is responsible for delivering packets sent by a Correspondent node (CN) to MR or a subnetwork behind MR (MNP) through an IP-IP tunnel established between the HA and the CoA of the MR. As well for MR which will redirect all the traffic it receives from these nodes (MNN) to the HA by establishing another tunnel.

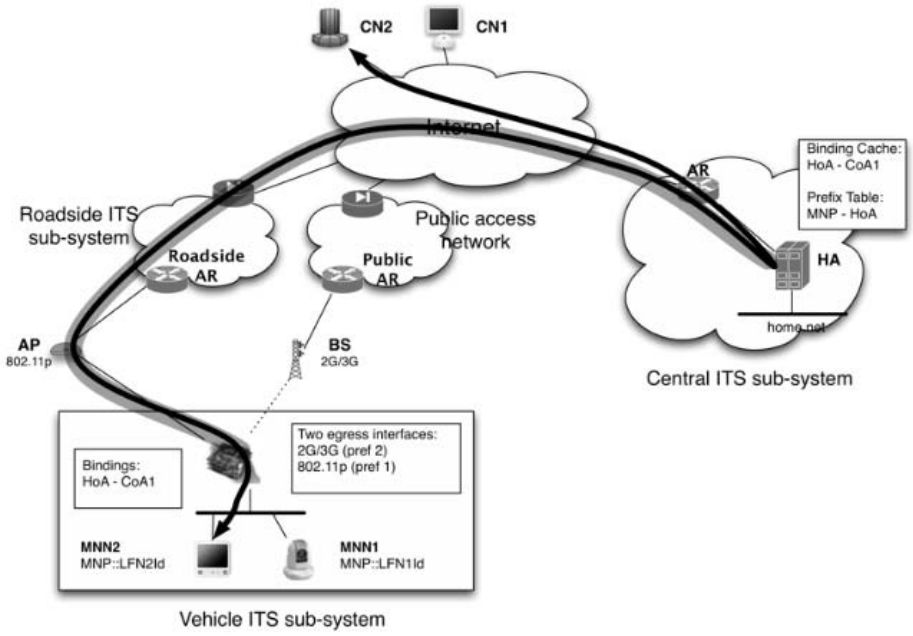

Figure 1: Application of NEMO in C-ITS scenario

NEMO combines a local routing protocol such as a MANET with NEMO to enable a global reachability for the prefix(es) inside the vehicle over multiple other cars.

Multiple Care of Address (MCoA)

Multiple Care of address (MCoA) defined in IETF RFC 5648 [i.19], designate a new advanced extension of the two mobility protocol MIPv6 and NEMO BS. In fact, the application of MCoA mechanism in the C-ITS environment is very useful, where vehicle (MR) can use simultaneously multiple interface such as IEEE 802.11p™ [i.26], WiMAX™, GPRS/UMTS, etc. According to the NEMO mobility protocol, a MR can have several CoA, but only one called primary CoA will be saved in the binding cache of the HA in order to send traffic, while rejecting the other interfaces. Contrary to NEMO, MCoA has been deployed to allow to MR to bind several CoA with HoA and therefore establish several IPv6-IPv6 Tunnels between the MR and the HR. Each tunnel will be identified by an identifier called Binding Identification Number (BID). This identifier is used to mark the packet in order to determine the traffic to be sent on each interface.

The above-mentioned network mobility solutions are focusing on wireless network deployments and rely on hierarchical schemes that lead to centralized deployment models, where a small number of mobility anchors are able to manage both mobility and reachability for a mobile node.

Currently, the IETF is developing a distributed model for mobility management in which traffic does not need to traverse centrally deployed mobility anchors far from the optimal route. This work is done in the IETF Distributed Mobility Management WG, see [i.44].

4.3.8 Vehicle-to-Vehicle connectivity with MANET Technologies

MANET covers a broad set of routing protocols for ad hoc wireless networks. It divides in proactive protocols that set up the routes before they are needed such as OLSR (see IETF RFC 7181 [i.59]) and reactive protocols that set them on demand such as AODV (see IETF RFC 3561 [i.60]). Compared to classical routing protocols, MANET brings in awareness of radios, in particular in terms of metrics and link fuzziness.

The Routing Protocol for Low-Power and Lossy Networks (RPL) [i.35], though not a product of the MANET WG at the IETF, inherits those concepts. RPL was optimized for the IoT space with a minimum control plane, no need for a global convergence and no topological awareness. RPL builds a rooted mesh topology that provides connectivity back and forth to a shared internet access. This applies in particular to the ever-changing topology formed by cars that relay packets for one another to extend the connectivity provided by a Road side unit.

RPL can be combined with NEMO as follows: The RSU provides a prefix and connectivity to the internet. It is also the Root of an RPL network. RPL distributes the prefix and forms a MultiLink Subnet of cars. Each vehicle forms an IPv6 address from the RSU prefix and injects it in RPL to obtain reachability. Then the vehicle uses that address as CareOf Address for NEMO, which provides reachback to the prefix inside the vehicle from the global Internet. This scenario is illustrated in Figure 2.

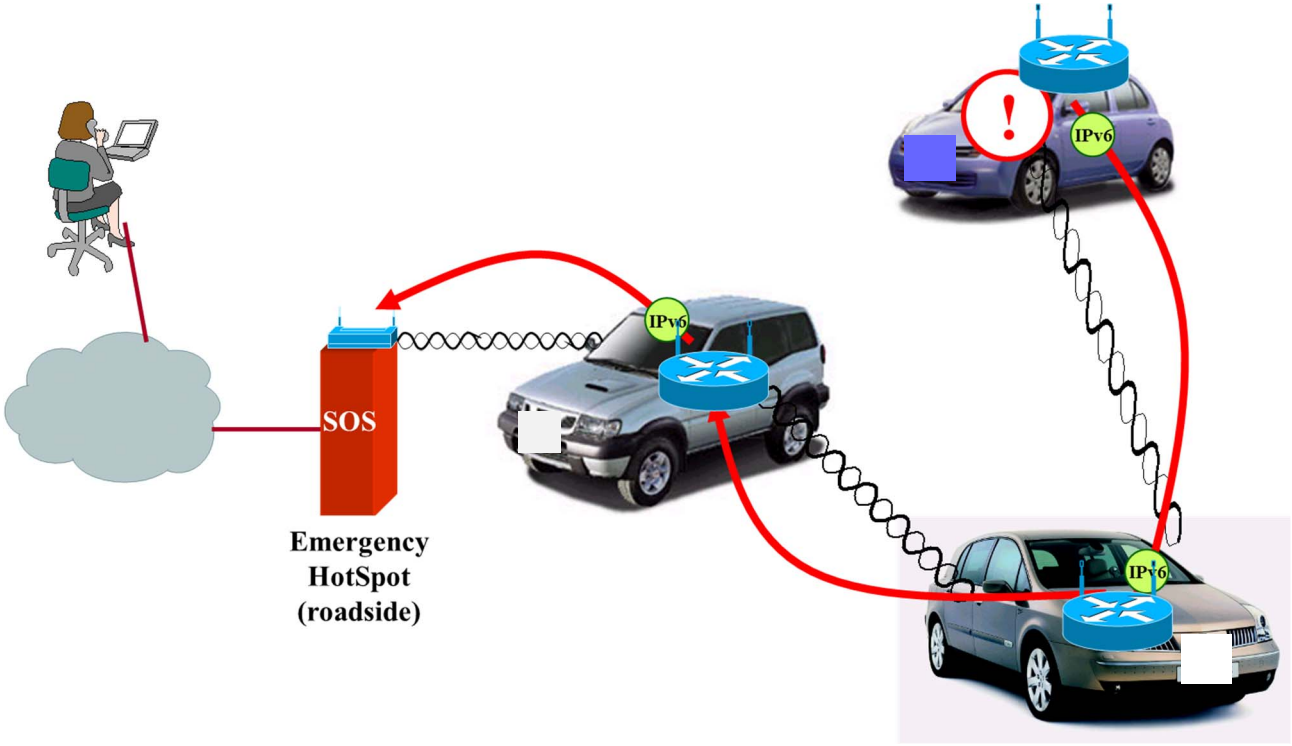

Figure 2: Example of RPL operation with NEMO

4.3.9 Security

IPv6 Security based IPsec

The IP Security Protocol (IPsec) defined by IETF in IETF RFC 4301 [i.27], is a set of mechanisms intended to protect IP traffic between two endpoints. Contrary to other security protocol such as Secure Socket Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), the IPsec services are provided at IP layer level. Therefore, the protection is offered for IP and all higher-level protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

The security services offered by IPsec protocol are integrity, authentication of data, protection against replay attacks and confidentiality which provides protection against traffic analysis. In fact, these services are provided through two security protocol used by IPsec called Authentication Header (AH) and Encapsulation Security Payload (ESP). These protocols can be operated in two different operations mode. The first one is transport mode, where the security services are applied only to the next layer protocols and the second one is Tunnel mode, where the protection is applied to the whole IP packets which is sent via a tunnel.

The application of IPsec protocol consists of establishing a secure connection called Security Association (SA) stored in a Database called Security Association Database (SAD), for selecting the traffic to be protected exists the concept of Policy. These policies are stored in a database called Security Policy Database (SPD) which is defined by the administrator. Every policy should be linked with a SA that determines the protocol (AH or ESP), the cryptographic algorithms and key materials to be used in order to encrypt the information transmitted. This IPsec SAs can be configured manually or by using Internet Key Exchange version 2 which is been specially deployed to provide such functionality. In vehicular domain all the all the traffic tunnelled by NEMO is encapsulated using this IPsec procedure. More details on the application of IPsec and IKEv2 protocols to secure IPv6 network mobility NEMO in the vehicular domain are provided by the authors of this article [i.28].

Security based WireGuard® protocol

WireGuard® [i.29] is a new, secure network tunnelling protocol operating at layer 3 and uses modern cryptography. It aims to replace the existing technologies such as IPsec and OpenVPN offering high performance and secure protocol design that rejects the cryptography agility, which means no form of negotiation over cryptographic parameter is needed. It is purposely implemented in a few lines of code (~4 000 lines) in order to be easily auditable for security vulnerabilities and less complexity than other traditional solution.

WireGuard® provides a secure network Tunnel between two-endpoints using UDP as a transport protocol for transmitting IP packets. Therefore, each message is encapsulated entirely inside UDP packets, which are further encapsulated in IP packets. WireGuard® does not have state for any IP Packets that it transmits, and it does not re-transmit packets if they are dropped by the network. The cryptographic handshake of WireGuard® is based in Noise protocol framework [i.30] that implies the application of Authentication Encryption with Additional Data (AEAD) in order to encrypt the IP packets transmitted through a tunnel. Contrary to other tunnelling protocols, either endpoint has the ability to react as server or client role. In fact, the endpoint that wishes to initiate the handshake is called Initiator while the peer that it tries to communicate with is referred as a Responder. These two endpoints are identified by a static 32-byte Curve25519 public key and will never respond to messages unless the sender proves knowledge of this public key. The authors of [i.31] give a detailed description of different handshake mechanisms between two endpoints.

4.3.10 3rd Generation Partnership Project (3GPP)

In Release 14 of ETSI TS 123 285 [i.61], 3GPP has announced a set of new technical specifications, such as which proposes an architecture enhancement for V2X services using the modified sidelink interface that originally is designed for the LTE-Device-to-Device (D2D) communications. 3GPP-R14 specifies that the V2X services only support IPv6 implementation. 3GPP is also investigating and discussing the evolved V2X services in the next generation cellular networks, i.e. 5G new radio (5G-NR), for advanced V2X communications and automated vehicles' applications.

Based on the key 5GC network elements introduced in ETSI TS 123 501 [i.54], Figure 3 illustrates the typical V2X architecture evolution.

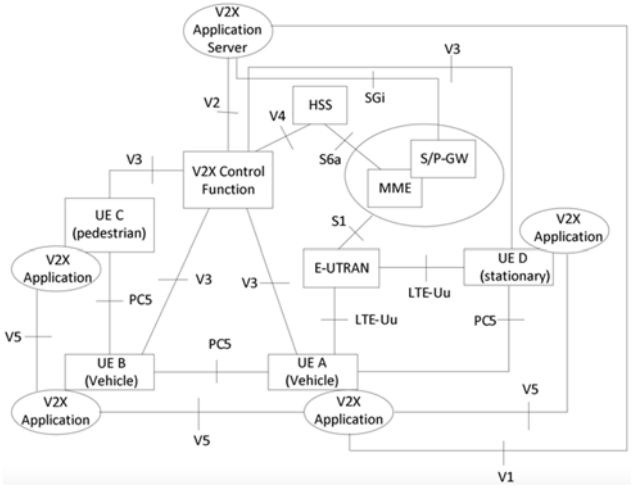

Figure 3: 3GPP reference architecture for V2X

Typically, the V2X control function is used to provision the subscriber vehicle device with necessary parameters in order to use V2X communication: Public Land Mobile Network (PLMN) specific parameters that allow the device to use V2X in this specific PLMN, or parameters that are needed when the device is not served by the cellular network. The V2X application server is an application server dedicated to V2X applications.

Some of the 4G functions, for example, Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access (E-UTRAN), Mobility Management Entity (MME), Serving/PDN Gateway (S/PGW), Home Subscriber Server (HSS), would evolve naturally to the 5G architecture with 5G New Radio (NR), Access and Mobility Function (AMF), Session Management Function - User Plane Function (SMF-UPF) and Unified Data Management (UDM), while a V2X application server becomes an Application Function (AF) in the 5G architecture terminology. This function can be part of the operator network or be in the domain of a third party. Similarly, as 5G core network design is progressing, the V2X control function of Release 14 will have to be integrated into the architecture.

4.3.11 International Organization for Standardization (ISO)

4.3.11.1 IPv6 in ITS Station Architecture

The International Organization for Standardization (ISO) Technical Committee 204 Working Group 16 (TC204 WG16) (also known as Communications Architecture for Land Mobile (CALM)) is in charge of standardizing a communication architecture for cooperative ITS. ISO TC204 WG16 is specially working on a communication architecture supporting all type of access to media and applications. In Europe, ETSI TC ITS is working on building blocks of the same architecture in harmonization with ISO TC204 WG16. Both ISO TC204 WG16 and ETSI TC ITS defined the ITS Station reference architecture [i.12] and [i.13].

Figure 4 shows the ITS Station architecture specified in ISO and ETSI. The graphical representations partly follow the ISO's OSI principle of separation of layers. The ITS architecture consists of six main parts. In the data plane (middle of the figure), the ITS Station architecture has four layers that perform different tasks. From the bottom to the top, Access, Network & transport, Facilities, and Application layers are stacked.

The Networking & Transport layer contains the different networking and transport protocol blocks needed for fully functional communication in an ITS communication mode. As a network protocol block, it contains ITS Network, geographic routing, IPv6, and other protocol blocks. IPv6 networking and non-IP networking are specified as standard in [i.14] and [i.15], respectively. To support mobility to a number of IPv6 nodes in the vehicle, NEMO [i.16] and multiple care-of address registration [i.19] is used. UDP and TCP is employed as the transport layer for IPv6.

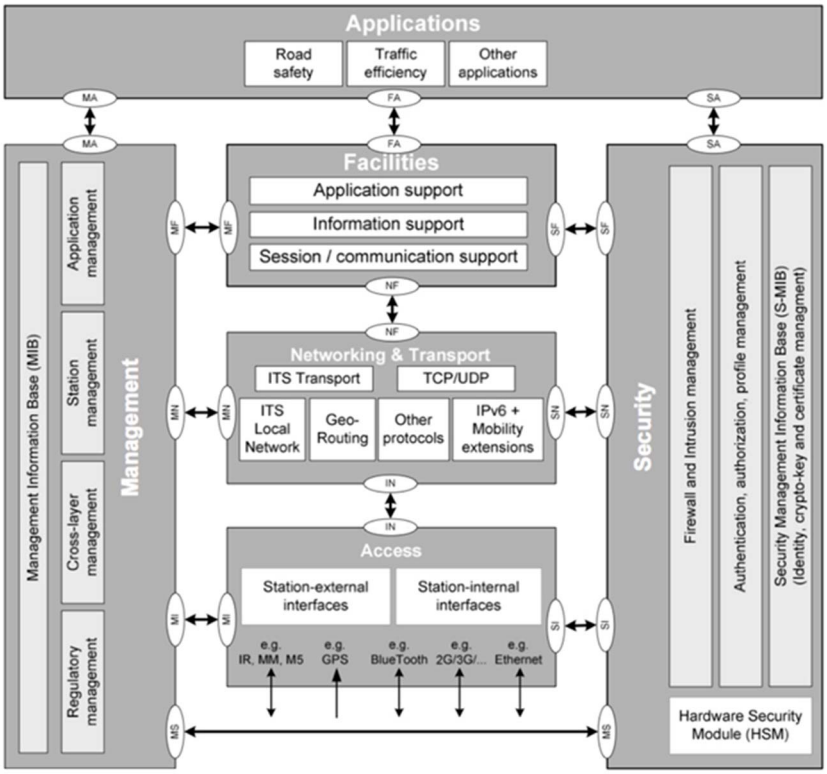

Figure 4: ITS station architecture

4.3.11.2 IPv6 GeoNetworking in ITS Station Architecture

The GeoNetworking (GN) architecture is defined in [i.15], and the GN protocol is specified in [i.20]. The GN protocol is a network layer protocol that provides packet routing in an ad hoc network. It makes use of geographical positions for packet transport. GN supports four types of communication modes: GeoUnicast, GeoBroadcast, GeoAnycast, and TopoBroadcast. First three modes employ a geographic routing, and the other uses topological routing. GeoUnicast routes data from a source node to a destination node for which the exact geographical location is known. GeoBroadcast delivers data from a source node to all nodes located within a specific geographic area. GeoAnycast routes data from a source node to any node located within a particular geographical area. TopoBroadcast routes data from a source node to all nodes situated up to a specific distance in terms of hops. As the forwarding, GN employs either greedy forwarding algorithm or contention-based forwarding algorithm.

As shown in Figure 5, the upper layer of GN can be Basic Transport Protocol (BTP) described in [i.17]. The other possibility of the upper layer can be IPv6. In this case, the adaptation layer to IPv6 is defined in [i.18] as IPv6 over GeoNetworking (GN6) adaptation sub-layer (ASL). In GN6, the GN header encapsulates IPv6 packet to tunnel the GN network. IPv6 Unicast packet is encapsulated in a GN GeoUnicast header to deliver the packet to a single ITS Station destination. IPv6 multicast is encapsulated in a GeoBroadcast header to disseminate the packets in a geographic scoped area.

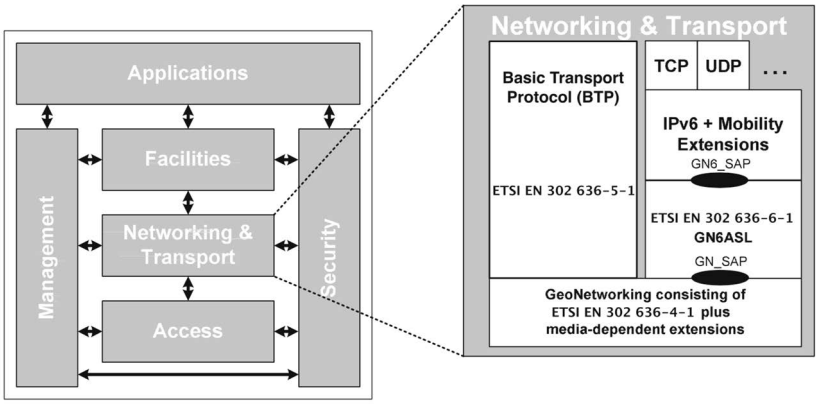

Figure 5: GN6ASL in the ITS station architecture [i.18]

To keep the interoperability with Neighbour Discovery (ND) protocol [i.33], GN6ASL introduces Geographical Virtual Link (GVL) which is a link-local multicast-capable virtual link spanning multiple physical links with geographically scoped boundaries. There are two types of GVL: static and dynamic. Static GVL provides symmetric reachability required in [i.33]. Dynamic GVL does not provide symmetric reachability but can be used when the dynamic definition of the broadcast domain is required. An IPv6 router issuing Router Advertisements have pre-configured values of the GVL Area for each Static GVL for which it is acting as a router. Upon the reception of a Router Advertisement, GN6ASL creates (if it does not exist yet) a new Static GVL and assigns a GVL Area equal to the destination area specified in the GeoBroadcast header. A network interface may have multiple GVLs. GN6ASL assigns an unique 12-bits ID to a GVL in order to distinguish the GVL from the IPv6 layer as shown in Figure 6.

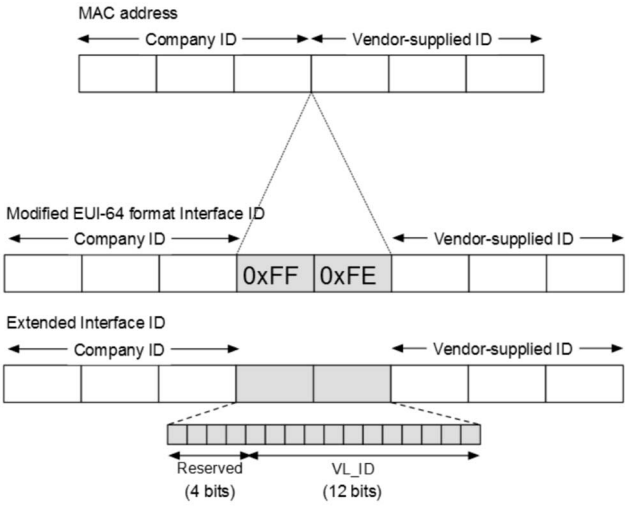

Figure 6: Creation of modified EUI-64 format IID and EIID from MAC address

4.3.12 ETSI ITS-G5 versus 3GPP C-V2X (AIOTI)

4.3.12.1 ITS-G5

ITS-G5 [i.45] and Cellular Vehicle-to-Everything (C-V2X) [i.46] are the two main technologies considered today for V2X communications [i.47]. While sharing many higher-layer protocols, these two technologies present totally different design principles, leading to fundamentally different radio interfaces. For example, ITS-G5, whose radio interface is based on the IEEE 802.11p™ [i.26] technology (also known as DSRC in the US), is specified by ETSI, whereas C-V2X is specified by 3GPP. Future realizations of both these technologies are envisioned, such as IEEE 802.11bd™ [i.51] for ITS-G5 and 5G New Radio V2X (5G NR-V2X), to meet more demanding V2X performance requirements.

ITS-G5 is designed for short-range radio communications between vehicles (V2V) and between vehicles and roadside infrastructure (V2I). This technology operates in a dedicated spectrum in the 5,9 GHz frequency band on 10 MHz channels using OFDM modulation. The PHY and MAC layers are based on the Wi-Fi®-like 802.11p specifications. The medium access paradigm is Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), which also comprises the Enhanced Distributed Channel Access (EDCA) mechanism to ensure the Quality of Service (QoS). The main differences with the "normal" 802.11 come from the session-based rules: while 802.11 standard operates in a Basic Service Set (BSS) context, meaning that the users who want to exchange information have to go first through a synchronization and/or setup procedure, 802.11p's operation mode is Outside the Context of a BSS (OCB). This is a set of lightweight procedures defined for highly dynamic vehicular environment, meaning that users do not have to belong to the same BSS to be able to communicate among each other. In particular, the OCB operation mode does not require authentication, association. and synchronization. The frames that are sent OCB have the Basic Service Set Identifier (BSSID) field set to all 1, which allows a receiver to ignore all other frames that are not sent OCB.

ITS-G5 supports short range communications (several hundred meters) with low latency (~2 ms under light traffic conditions) and high reliability and works in high vehicle speed mobility conditions. ITS-G5 operates independently of cellular network coverage.

4.3.12.2 C-V2X

LTE-V2X is today's realization of C-V2X and was standardized in 3GPP Release 14 in March 2017. LTE-V2X supports both short range and long-range communications.

LTE-V2X short range mode (PC5) supports communications between vehicles (V2V), between vehicles and roadside infrastructure (V2I), and between vehicles and pedestrians (V2P) or other vulnerable road users. The LTE-V2X short range mode (or sidelink) signal occupies a 10 MHz channel in the 5,9 GHz frequency band. The sidelink communication shares the same SC-FDMA technique as the LTE uplink. The minimum resource in the time domain is the TTI of 1 ms, while in the frequency domain is the 15 kHz subcarrier. The MAC layer is based on semi-persistent scheduling and allows deterministic sharing of the medium among multiple stations in a distributed manner. LTE-V2X short range mode operates independently of (and does not require the availability of) cellular networks (also known as Mode 4).

5G-V2X is the future realisation of C-V2X and will be enable more advanced safety services, such as those which might be required for autonomous vehicles. Standardisation of 5G-V2X is on-going in 3GPP with already a first step completed with Release 15 in June 2018, and a second step Release 16 expected to be finalized in December 2019.

4.3.13 IETF activity on vehicular communications

The first wave of IETF activity for vehicular communications happened in the first decade of 2000 with in parallel the development of MANET protocols for local mobility (e.g. V2V communication within a group of vehicles with no surrounding infrastructure) and the Mobile IPv6/NEMO protocols for global mobility over the Internet.

The MANET (e.g. OSPF-MANET IETF RFC 5614 [i.62], IETF RFC 5820 [i.63] and IETF RFC 7137 [i.64]) technologies found an application in the military, connecting convoys on the move, and enabling communication within a base camp. Mobile IPv6 (IETF RFC 3775 [i.65] and IETF RFC 6275 [i.24]) and NEMO (IETF RFC 3963 [i.16]) were demonstrated in vehicles but not deployed.

A MANEMO effort that would combine MANET and NEMO was envisioned to solve the nested NEMO problem (see IETF RFC 4889 [i.66]) and enable applications such as cars in a parking lot relying one another, but the project was abandoned.

The Mobile IPv6 effort moved towards proxy Mobile IP that is optionally used in 3GPP cores, and Distributed Mobility Management, but the focus on vehicular communications was lost.

The creation of the IPWAVE WG in 2016 marked the second wave came of IETF involvement in vehicular communications. IPWAVE has been operating to this day, and the currently chartered activity relates to use cases and problem statement.

IPWAVE produced one RFC, IETF RFC 8691 [i.43], that details how legacy IPv6 Neighbour Discovery can be used with special arrangements to form ad-hoc networks of cars in a common broadcast domain over IEEE Std 802.11™ [i.51] operating Outside the Context of a Basic Service Set (IOW in OCB mode). In very short, IPv6 ND was limited to P2P and transit networks, which can be guaranteed with wiring but difficult to automagically recreated between cars over radios.

The work triggered conceptual questions about IPv6 subnets that were brought to the attention of the IPv6 WG (6MAN) [i.49]. This work details the models that could be applied to extend the IPv6 Link and Subnet models, and how IETF RFC 8505 [i.38] can be used to enable a generic support of IPv6 over radios.

In parallel, common interests for reliable communication emerged between autonomous cars and aviation. Those interests coalesced with new industrial needs for wireless automation and lead to the formation of the RAW WG for Reliable and Available Wireless (see [i.50]).

The development of RAW technologies has been lagging behind deterministic networking efforts for wired systems both at the IEEE and the IETF (see the DetNet Architecture, IETF RFC 8655 [i.67]). But recent efforts at the IEEE (802.11ax and 802.11be) and 3GPP (5G URLLC) indicate that wireless is catching up at the lower layers and that it is now possible for the IETF to extend DetNet for wireless segments that are capable to provide delivery guarantees with scheduled transmissions.

Even open standards can be market-driven, and ultimately, it takes a developed market to generate striving standards efforts. The work that the IETF did in advance over the last 20 years did not result in a widespread deployment and a high perceived value for the users. It is unclear at this time how the vehicle communication will be distributed between Wi-Fi®, OCB and 5G, and what role IPv6 can play in integrating them. The work at HIP, NEMO and RAW indicates that it might be an overlay game, separating the location and the end point identities, and enabling a higher reliability for the users.

4.3.14 5G Automotive Association (5G-AA)

The 5G Automotive Association (5GAA) is a global, cross-industry organisation of companies from the automotive, technology, and telecommunications industries (ICT), that work together on developing and delivering concepts to improve the adoption of connected vehicles. The vision of a highly integrated vehicle-mobile network paradigm is embodied in the C-V2X technologies supporting advanced services, such as eCall, telematics, road safety related services, comfort services, and Internet access. 5GAA is currently supporting 3GPP in their efforts to specify the next evolutionary steps for C-V2X in order to enhance connected vehicle services, support higher level of autonomy, and provide additional environmental benefits via traffic optimisation.

In a recent white paper [i.11], 5GAA is advocating for a widespread, coordinated deployment of mobile network infrastructure providing strong radio coverage of roads to support the wide-area V2X communications mode alongside the short-range, direct mode for road safety critical services between vehicles and with the road infrastructure. Among the many reasons why such deployments are necessary and desirable are the continuity of telematics services for vehicle support systems, the ability for road operators to provide traffic safety, road monitoring and traffic control, and enabling mobile network operators to provide reliable Quality of Service (QoS), matching the specific requirements of connected vehicle applications. In this context, the cost-benefit considerations regarding the cellular road coverage represent a key driving factor towards the widespread deployment of this infrastructure. In particular, 5GAA identifies several socio-economic connected vehicle use cases that drive network requirements:

- **Road safety related**

  This category includes use cases that provide enhanced safety for the vehicle and the driver. Examples of use cases include emergency braking, intersection management assistance, collision warning or lane change.

- **Traffic efficiency and environmental friendliness**

  This category includes use cases that provide enhanced value to infrastructure, road or city providers, where the vehicles will be operating. As examples, green light optimal speed advisory (GLOSA), traffic jam information, maximum speed advice, curve speed warning and temporary restricted area information (also known as geofencing).

- **Society and community**

  This category includes use cases that are of value and interest to society and the public, e.g. Vulnerable Road User (VRU) protection, emergency vehicle approaching, traffic light priority, patient monitoring, crash report.

An overview of the key cellular network deployment aspects is provided in Figure 7. Clear synergies with road operator deployments are found for aspects such as access to ducts and power, simplified site permits and shared use of roadside infrastructure (lamp poles, traffic signs, etc.).

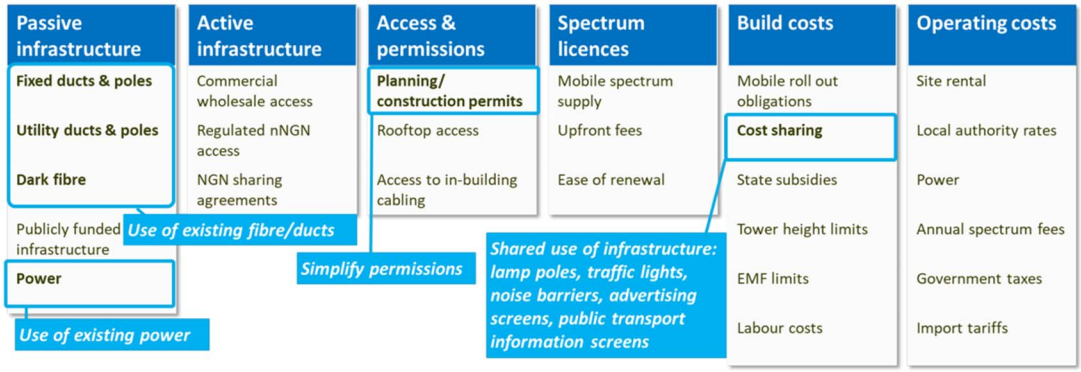

Figure 7: Key cellular network deployment aspects, including areas of road operator deployment synergies (figure provided courtesy of 5GAA [i.11])

Security plays an important role in building trust in V2X, protecting users' privacy, and enabling safety, efficiency and comfort. Efforts to reinforce trust in this ecosystem are driving global initiatives to develop, standardise and implement Security Credential Management Systems (SCMS). As a consequence, different stakeholders have put forward their requirements leading to differing, non-interoperable regional designs. 5GAA has evaluated existing system designs and their regulatory requirements, as well as identified some new 'advanced' features. The resulting recommendations for improved design fulfilling these security and privacy requirements in a large-scale system are outlined in [i.32]. Among these recommendations, 5GAA suggests removing the Location Obscurer Proxy (LOP) in order to simply the Efficient Security Credential Provisioning System (ESPS) design. Such simplifications are possible thanks to the benefits provided by the IPv6 privacy extension, which enhances privacy capabilities and reduces the exposed data in transport.

4.4 Best Cases on IPv6 Transition Strategies for Vehicular Networks

4.4.1 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.

[i.5] 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.7] and IETF RFC 3633 [i.6]), 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™ and Apple® iOS handsets 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.8], which specifies a stateless IP/ICMP Translation Algorithm in an IPv6 Internet Data Centre.
- 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.

4.4.2 The AUTOPILOT project

AUTOPILOT overall description

AUTOPILOT EU [i.68] project is a Large-Scale Pilot project dedicated to assessing how the Internet of Things (IoT) can enhance autonomous driving (AD) capabilities. It has five (5) permanent pilot sites (PS) acting as Field Operational Tests (FOT) and located in Italy (Livorno), Spain (Vigo), Finland (Tampere), The Netherlands (Brainport) and France (Versailles).

Platooning use case

The platooning use case demonstrates vehicular platoons consisting of a lead vehicle and one or more highly automated or driverless following vehicles which have automated steering and distance control to the vehicle ahead. The control is supported by V2V communication. Two variants of platooning have been evaluated in the project:

- A highway variant where one or more highly automated vehicles are going to follow a leading vehicle. The electronic allowance of the emergency lane (dedicated lane) was tested, as well as dynamic platoon forming (piloted in Brainport).

- An urban variant to enable vehicle rebalancing of a group of driverless vehicles involving only one driver in the lead vehicle (piloted in Versailles [i.68]).

In the Versailles PS, the focus was made on the platooning use case within an urban environment where autonomous driving vehicles have to deal with the coexistence with other non-connected and non-autonomous vehicles, Vulnerable Road Users (VRU) presence as well as traffic management infrastructures such as traffic lights and their controllers.

An "IPv6 over IEEE Std 802.11™ OCB"-based V2V communication approach has been implemented and tested within the context this context.

For IPv6 Neighbour Discovery, the experimentation was limited to IPv6 NDP (IETF RFC 4861) [i.33]. The IPv6 Neighbour Discovery Protocol is responsible for discovery of other network nodes on the local link, to determine the link layer addresses of the other nodes, to find available routers, and to maintain reachability information about the routes to other active neighbour nodes. The NDP RA Message (Router Advertisement) is used to exchange route and prefix information.

The implementation of such IPv6-based V2V communication for platooning system is done in two steps excluded the frequency step up which is out of the scope the present document.

Step1: Discover prefixes of direct neighbours

The aim of the prefix discovery is to be aware of the existence of other vehicles that are directly connected within the same frequency band, as represented in Figure 8.

Figure 8: Prefix discovery of direct neighbours

Step2: Propagate discovered prefixes

The aim of the propagation is to be aware of the existence of all the vehicles inside the platoon thanks to prefix propagation performed by each vehicle's device based on the prefixes discovered in Step1 as represented in Figure 9.

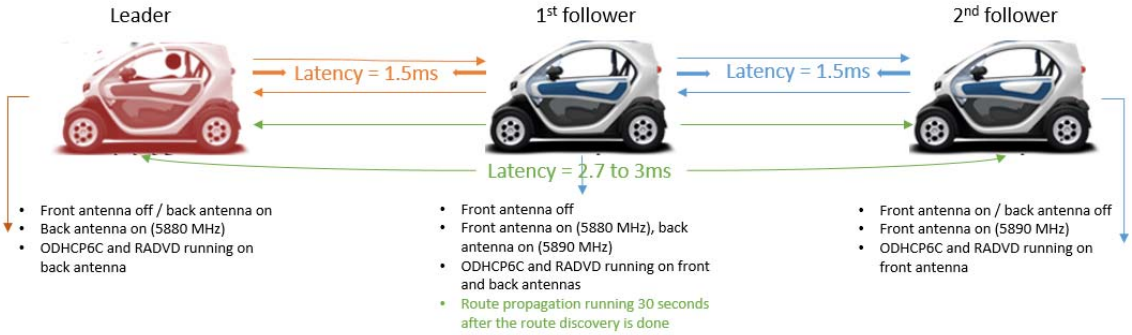

Figure 9: Prefix propagation

To complete the design of the platooning system, from a connectivity perspective, the cars can communicate through a cellular (LTE/4G) connexion to a cloud-based platform in order to send relevant platooning data and, as consequence, to be monitored remotely. This is schematized in Figure 10, where vehicles communicate with each other through IPv6 over IEEE Std 802.11™ [i.51]-OCB interfaces and with a cloud-based "Platooning supervision system".

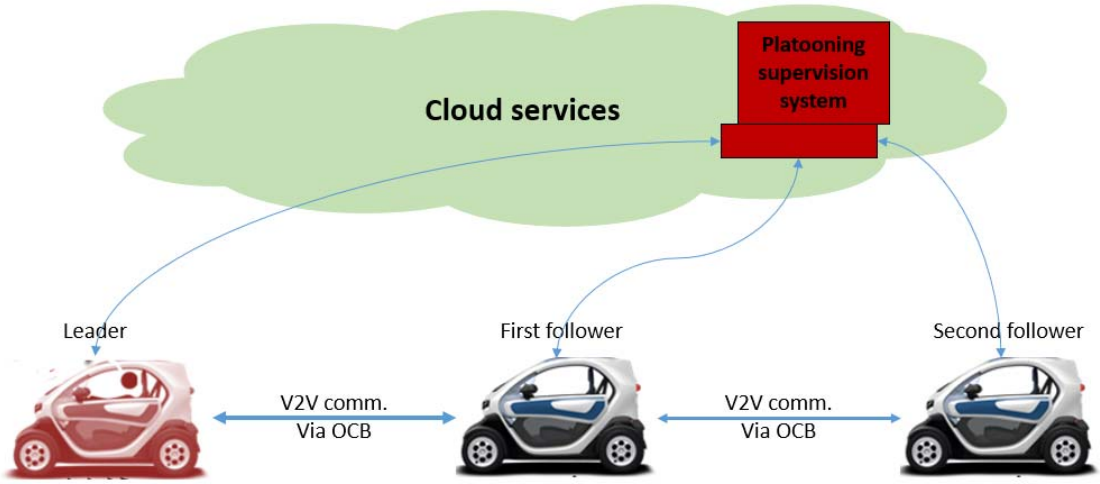

Figure 10: Complete platooning system design

However, the communication with cloud infrastructures does not rely on IPv6 communication.

4.4.3 Use Case in USA: Example of Web Performance Improvement in Vehicular Networks using IPv6

This clause is based on [i.1] and [i.9] 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.9] 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 (MNOs), and other Content Delivery Networks (CDNs).

The study in [i.9] 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.9]:

1) RTT (Round Trip Time) of the communication between clients and CDN (Content Delivery Networks), see Figures 4 and 5 in [i.9].

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.9].

3) Webpage Page Load Time (PLT) distribution for dual-stack in different cellular USA mobile network operators, see Figure 7 in [i.9].

For details on the scenarios used and the definition of the applied performance metrics, see [i.9].

Some highlights on the experimental setup are as follows. [i.9] 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.9] 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.9]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.9] 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.9]) 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.9], 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.9], 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.9], 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.9] 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.9] 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.

4.4.4 Use Case in Europe: 5G-MOBIX Project

5G-MOBIX is a project dedicated to showcasing the added value of 5G technology for advanced Cooperative, Connected and Automated Mobility (CCAM) use cases and validate the viability of the technology to bring automated driving to the next level of vehicle automation (SAE L4 and above). The project executes CCAM trials along two cross-border (x-border) corridors - Spain-Portugal (ES-PT) and Greece-Turkey (GR-TR) - using 5G core technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context. The use cases studied by the project fall into five main categories:

1) Advanced Driving:
   a) Complex manoeuvres in cross-border settings.
   b) Infrastructure-assisted advanced driving.
   c) Cooperative collision avoidance.
   d) Cloud-assisted advanced driving.
2) Platooning:
   a) Platooning with "see what I see" functionality in cross-border settings.
   b) eRSU-assisted platooning.
   c) Cloud-assisted platooning.
3) Extended Sensors:
   a) Extended sensors for assisted border-crossing.
   b) EDM-enabled extended sensors with surround view generation.
   c) Extended sensors with redundant edge processing.
   d) Extended sensors with CPM messages.

4) Remote Driving

   a) Automated shuttle remote driving across borders.

   b) Remote driving in a redundant network environment.

   c) Remote driving using 5G positioning.

   d) Remote driving with data ownership focus.

   e) Remote driving using mmWave communication.

5) Vehicle QoS Support

   a) Public transport with HD media services and video surveillance.

   b) QoS adaptation for security check in hybrid V2X environment.

   c) Tethering via vehicle using mmWave communication.

The 5G-MOBIX common architecture, which acts as the basis for the 5G network deployments in the ES-PT and GR-TR corridors, is illustrated in Figure 11. It is based on overlay dedicated networks where all signalling and user plane traffic are carried out via a direct interconnection link.

The project identifies a series of telecommunication cross-border issues that should be addressed by this common architecture, related to roaming, handover, networking, data protection & privacy. One example is the Inter-PLMN handover in higher layers, which can imply the change of network address with impact on running UDP/TCP communications and the disconnection of the data path for the services running on-board. Here, several IP-related issues have been identified, such as IP re-addressing, IPv4 to IPv6, and IPv6 to IPv4. From a confidentiality point of view, 5G-MOBIX proposes to exploit the benefits of IPv6 by, e.g. using Encapsulated Security Payload (ESP) at the network layer.

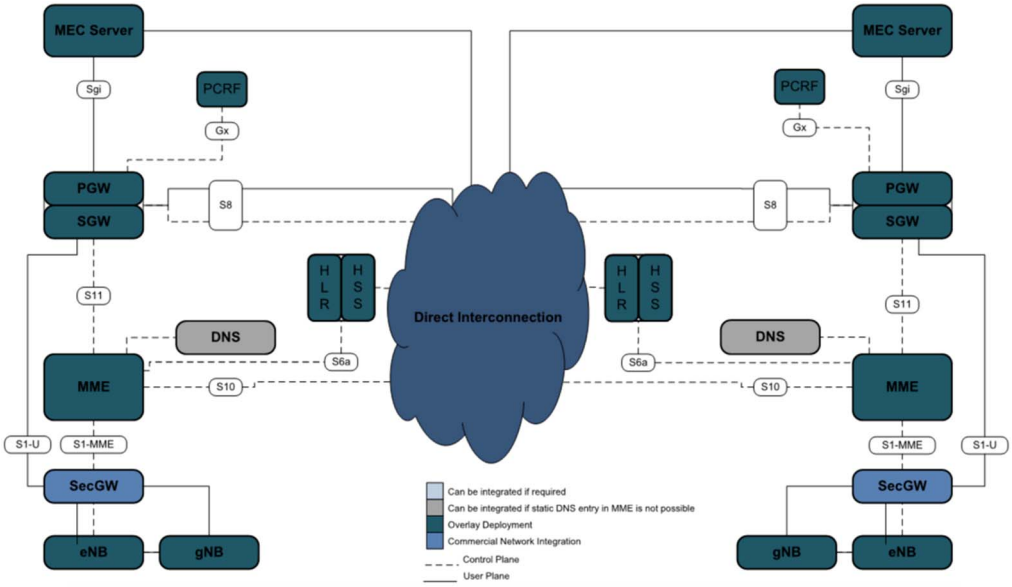

Figure 11: The 5G-MOBIX common architecture

4.4.5 Use Case in Europe: 5G-DRIVE Project

The 5G-DRIVE project aims at performing a close collaboration between EU and China to synchronise 5G technologies and spectrum issues before the final roll-out of 5G. The main scope is to conduct 5G trials addressing two specific scenarios, Enhanced Mobile Broadband (eMBB) and Internet of Vehicles (IoV), each being illustrated by use cases describing particular applications of the technologies and solutions defined in 5G-DRIVE to real-life situations.

Enhanced Mobile Broadband (eMBB)

The applications used to test and validate the use of eMBB in the 3,5 GHz band are typical mobile broadband services as well as Virtual and Augmented Reality (AR/VR). The project considers two main eMBB use cases:

1) Cloud-Assisted AR/VR:

   - As opposed to conventional gaming consoles or personal computers (which are highly dependent on the signal processing capabilities of the GPU), cloud-assisted AR enables users to stream video games or virtual contents from cloud servers like other streaming media. This new type of services offers an opportunity for more varied and interactive contents and makes user devices lighter and cheaper. eMBB is required to reach tens of Gbps to support the speed requirement of AR application, providing a more uniform experience for users of AR given the ultra-high data volume requirements that can be handled more effectively.

2) Indoor Positioning:

   - Indoor position information supports navigating within building premises. However, this location information is also a valuable asset for providing and maintaining high quality eMBB services to end user devices. Positioning offers means to utilize location information to improve network communication reliability, to reduce latency, and to balance data loads.

Internet of Vehicles (IoV)

This scenario is based on LTE-V2X using the 5,9 GHz band for V2V and V2I services, as well as the 3,5 GHz band for Vehicle-to-Network (V2N) communications. More specifically, the optimisation of the band usage in multiple scenarios with different coverage is a key target, so as the validation of the geographic interoperability of the 3,5 and 5,9 GHz bands for the following use cases:

1) Green Light Optimal Speed Advisory (GLOSA):

   - GLOSA is a day-1 C-ITS service aimed at informing end users about the speed that needs to be sustained (within legal limits) to reach an upcoming traffic light in green status. It provides end users with short-term information on upcoming traffic light status to optimise traffic flows, help prevent speed limits violations, improve fuel efficiency and reduce pollution.

2) Intelligent Intersection:

   - This use case deals with safety on intersections, focusing on infrastructure detection of situations that are difficult to perceive by vehicles themselves. A good example is the situation where a vehicle wants to make a right turn while parallel VRUs also have a green phase and right of way (permissive green for motorized traffic).

4.4.6 Use Case in China: Example 1

During the last two years, IPv6 has been widely deployed in China in various types of network, including Metro Area networks, IP backbones, EPC, IDC and clouds, etc. In particular, due to the mature support of IPv6 capability in smartphones, the quantity of IPv6 users in mobile network increases rapidly, and more than 90 % mobile users are IPv6-capable. Although IPv6 has been widely deployed, every handset still has been configured with at least one IPv4 address for the access of IPv4 services. Due to address shortage, the IPv4 addresses for most handsets are private. In some large provinces of China, even private addresses are not enough for the addressing of the terminals due the huge number of mobile users. For this reason, the 10.0.0.0/8 space is used more than once, which makes the network too complicated, so dual stack is not a long-term solution. In 2018, the largest mobile operator in China began to conduct IPv6-only field trial in LTE network of Jiangsu province, the scheme is shown in Figure 12.

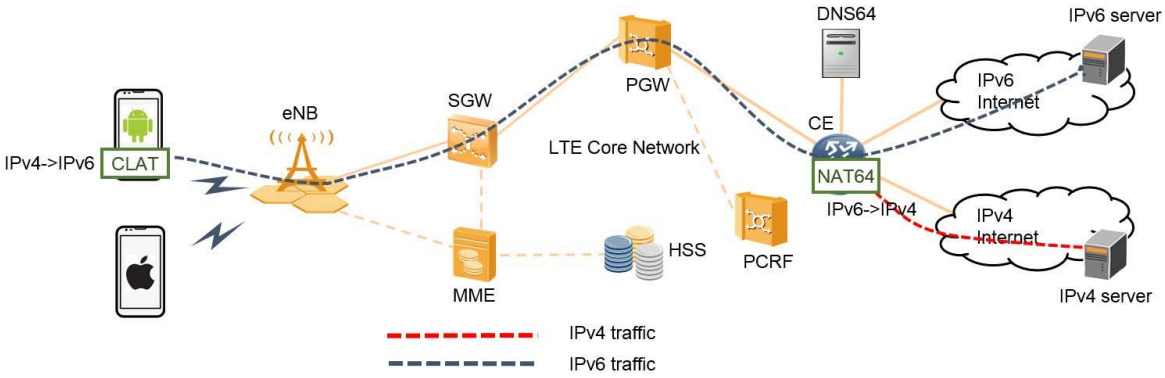

Figure 12: IPv6-only field trial in LTE

This scheme adopts NAT64/DNS64 standards defined in IETF, and IPv6-only is well supported in the handsets of Android and Apple iOS. In this approach, handsets with only IPv6 address can access legacy IPv4-only, IPv4/ IPv6 dual stack and IPv6-only services.

Since there is no IPv4 address allocation, each handset can be definitely identified by global unique IPv6 addresses, and the weaknesses caused by private addressing can be erased. For instance, there is no IPv4 address overlapping and no need to maintain two stacks in network operation. Up to now, most of the traffic in China is still IPv4-based, so NAT64 supports most of the traffic of IPv6-only users. With more and more content/service providers in China migrating to IPv6, it can be foreseen that IPv6-native traffic with increase gradually and become dominate ultimately.

This field trial is the start of IPv6-only in China, it will extend to more scenarios in the future, including V2X.V2X will need a secure, robust and scalable IP network, IPv6-only path will be right choice for V2X, where native-IPv6, instead of NAT44 or NAT64 will be the main communication model.

4.4.7 Use Case in China: 5G Large-scale Trial Project

The 5G Large-scale Trial project in China is funded in the Ministry of Industry and Information Technology (MIIT, see note) of the Chinese government and is vested in National Major Project program. The project consists of eight partners, with the largest mobile operator as the leader, and seven participants coming from the large network of vendors, industry, research institutes, and trial sites providers. As the name suggests, the scope of the project is large-scale trials covering 5 cities and more than 100 sites per city. 5G Large-scale Trial conducts 5G trials on two categories of scenarios: category 1 - eMBB and category 2 - V2X.

NOTE: In China, three ministries have defined the V2X test specification. The V2X development is regulated by the Ministry of Industry and Information Technology (MIIT), Ministry of Public Security (MPS), and Ministry of Transport (MOT). The MIIT specifies the spectrum for V2V and V2I operation, and coordinates the C-V2X trial activities in China. The MPS takes charge of the standard revision on traffic light and regulations on traffic information access. The MOT is responsible for regulating the road infrastructure for V2X services.

C-V2X trials in 5G Large-scale Trial is conducted on LTE-V2X to compliment the current industry development stage. So far, the LTE-V2X trials have been done in Wuxi, Shanghai, and other pilot areas. The V2X services defined match the Day-1 C-ITS services defined by Europe. However, in China some Day-1.5 services, like VRU protection have also been tested. The trials are expected to conclude in early 2020.

The project selects C-V2X (LTE-V2X) to trial because of China' philosophy of C-V2X technology with NR-V2X in the future. The IMT-2020 (5G) promotion group in China is major platform to promote 5G research, who organizes discussions together with China Communication Standards Association (CCSA), China ITS Industry Alliance (C-ITS), China Society of Automotive Engineers (CSAE), China Industry Innovation Alliance for the Intelligent and Connected Vehicles (CAICV), National Technical Committee of Auto Standardization (NTCAS).

C-V2X scenarios in 5G Large-scale Trial are categorized according to V2Vehicle (such as Emergent braking warning), V2Infrastructure (such as traffic light optimization) and V2Network (such as traffic info broadcasting). Two key use cases performed by the 5G Large-scale Trial V2X team are Intersection Warning (see Figure 13) and GLOSA (see Figure 14).

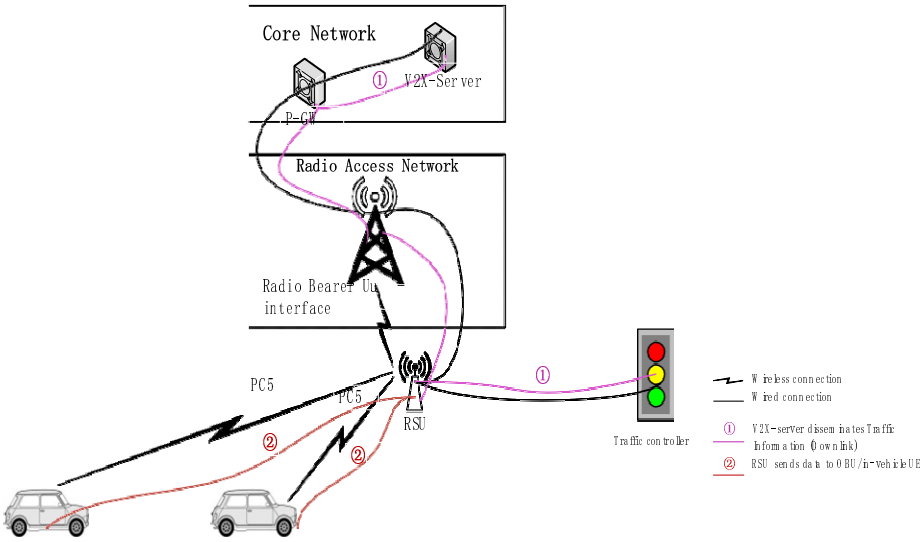

Figure 13: System architecture of Intersection Warning use case

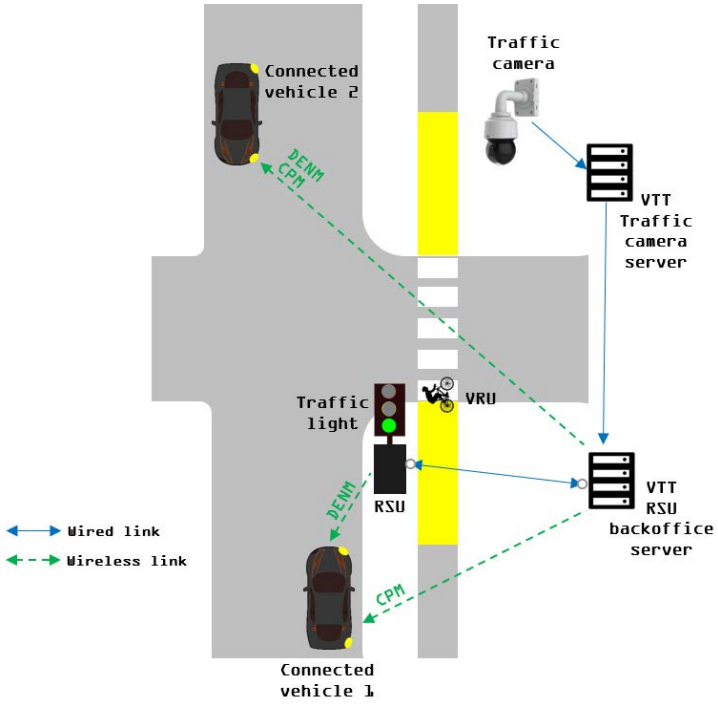

Figure 14: Architecture of the GLOSA use case

4.4.8 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.10], apply also in the context of 5G.

5 Lessons Learned

The following lessons have been learned on applying IPv6 in V2X:

- Several standardisation bodies and alliances are focusing on enabling IPv6 to be applied in V2X, such as IETF, ETSI, 3GPP, 5GAA, AIOTI.
- Various best cases show that IPv6 can be considered as an enabler for the deployment of V2X on a global scale.
- Challenges identified on applying IP in V2X can be alleviated by using IPv6 in such scenarios. Such IP-related challenges are:
  - IP addresses are normally assigned to fixed locations around an abstract link where a subnet resides. These subnets can be aggregated and finally advertised in the Internet default-free zone, i.e. to achieve routable addresses. However, in mobile networks it is required to maintain IP connectivity and session continuity from the inside to the outside of the vehicle at all times. Moreover, as the vehicle moves, it may be connected to the Internet, other vehicles or the infrastructure with one or more of 3GPP networks (LTE, 5G), Wi-Fi® hotspot (e.g. with open roaming), and specialized V2X communication such as OCB. In addition, IPv4 addresses are running out. These challenges can be solved by applying technologies supporting IPv6, such as IPWAVE, MIPv6, DMM, MANET, NEMO, WiND and RAW networking.

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.

6 Conclusions

The present document argued that IPv6 facilitates IP-enabled applications to be applied and used in vehicular communications. It also argued that IPv6 provides several advantages covering important needs in cooperative vehicular communication, such as (1) the large space of addressing due to the exhaustion of IPv4 address space, which impacts the growing of internet continuity and (2) other numerous benefits, such as the improvement of mobility and security services, and the addition of node auto-configuration mechanisms to facilitate the configuration of connected equipment. Furthermore, the present document showed that various standardization bodies and alliances are focusing on enabling IPv6 to be applied in V2X, such as IETF, ETSI, 3GPP, 5GAA, AIOTI. Moreover, it presented best cases where IPv6 is considered as an enabler for the deployment of V2X on a global scale.

Due to the fact that vehicular networks are considered to be a new network pattern in the global Internet, IPv6-only should be stimulated to be the main IP based approach for V2X, while other transition should be considered as auxiliary. This is due to the following reasons:

1) There are not enough IPv4 addresses for V2X. On 25 November 2019, RIPE NCC made final /22 IPv4 allocation from the last remaining addresses in their available pool. Since then, RIPE NCC have run out of IPv4 addresses, which also marks that all the regional registries run out of IPv4 address.

2) IPv6 has replaced IPv4 for new protocol compatibility and optimization. On 7 November 2016, The Internet Architecture Board (IAB) of IETF advised its partner Standards Development Organizations (SDOs) and organizations that networking standards need to fully support IPv6. The IAB expects that IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6.

3) New "CAR" should not be configured with old "WHEELS". Similarly, Vehicular Networks should not be configured with old protocol. As a new generation of IP protocols, IPv6 has been designed and polished by global Internet community, and it has gained technical advantages over IPv4 protocol, in terms of address space, forwarding efficiency and routing efficiency, etc.

4) Compared with dual-stack, IPv6 single stack approach will make V2X more concise and economically reasonable. The industry should be encouraged to use IPv6-only for V2X development, construction and operation.

History

Document history		
V1.1.1	October 2020	Publication