EuWireless

Project: H2020- INFRADEV-777517

Project Name:

Design of the European mobile network operator for research (EuWireless)

Deliverable D1.3

Enabling technologies

Date of delivery:	2018/10/31	Version:	1.1
Start date of Project:	2018/01/01	Duration:	24 months

Deliverable D1.3: Enabling technologies

Project Number:	INFRADEV-777517
Project Name:	Design of the European mobile network operator for research
Project Acronym	EuWireless
Document Number:	INFRADEV-777517-EuWireless/D1.3
Document Title:	Enabling technologies
Lead beneficiary:	UMA
Editor(s):	Pedro Merino (UMA)
Authors:	Pedro Merino (UMA), Laura Panizo (UMA), Álvaro Martín (UMA), Álvaro Ríos (UMA), Bárbara Valera (UMA), Almudena Díaz (UMA), Delia Rico (UMA), Iván González (UMA), Janie Baños (DEKRA), Óscar Castañeda (DEKRA), Carlos Cárdenas (DEKRA), Joaquin Torrecilla (DEKRA), Rosario Trapero (DEKRA), Adam Flizikowski (ISW), Maciej Soszka (ISW), Lukasz Kwiatkowski (ISW), Slawomir Pietrzyk (ISW), Jarno Pinola (VTT), Ilkka Harjula (VTT), Jerry Sobiesky (NORDU)
Reviewers:	Pedro Merino (UMA), Janie Baños (DEKRA), Oscar Castañeda (DEKRA), Adam Flizikowski (ISW), Jarno Pinola (VTT), Ilkka Harjula (VTT)
Dissemination Level:	PU
Contractual Date of Delivery:	2018/10/31
Work Package Leader:	UMA
Status:	Draft
Version:	1.1
File Name:	EuWireless_Deliverable_D1_3_v1.1

Abstract

This deliverable identifies the most promising technologies to be considered in the design of

the EuWireless research infrastructure. The document provides the context of the EuWireless project, the foundations of 5G networks, the sharing technologies for network resources and infrastructure, and an introduction to the GÉANT Testbed Service (GTS), as the main current experimental platform offered to the scientific community. The conclusions of the document provide a very early evaluation of how the presented technologies could cover the objectives defined for the project.

Keywords

Enabling technologies, 5G network, sharing network, GTS

EuWireless Consortium

Universidad de Málaga	UMA	
DEKRA Testing and Certification	DEKRA	
Teknologian tutkimuskeskus VTT Oy	VTT	
IS-Wireless	ISW	
time.lex	TL	
NORDUnet A/S	NORDU	

Executive Summary (Editor, Co-Editor)

EuWireless project is designing a pan-European network to support research activities that require access to large field deployments and to licensed spectrum. This deliverable identifies the most promising technologies to be considered in the design of the architecture of such infrastructure. The first sections provide the context of EuWireless, highlighting the motivation and the main objectives. The core of the document are the sections devoted to:

a) Fundamentals of 5G networks, as the state of the art in modern mobile networks. The main concept in 5G networks is the network slice, providing a kind of isolated network with specific configuration e.g. to fulfil the requirements to support one service. To this aim, 3GPP proposes a new architecture and solutions at the radio (5G NR) and core network (5G core). In addition, the role of software as a key part of the network is reinforced with the concepts of Software Defined Networks (SDN) and Network Function Virtualization (NFV).

b) Sharing network resources and infrastructure, as the potential tools for implementing EuWireless. Standards and recent research are designing methods to share spectrum, access nodes, transport network, core networks and other infrastructures in order to make several operators to coexist in a given area. These methods also include procedures to enable advanced connectivity of one operator's subscribers to other operators' networks beyond classic roaming.

c) GÉANT Testbed Service (GTS) is a research infrastructure on top of GÉANT pan-European communication network. GTS supports virtualization of network resources to create researcher specific temporal platforms, and it can be expanded to include the implementation of slices in the context of EuWireless.

The conclusions section provides a table summarizing a very early evaluation of how the presented technologies could cover the objectives defined for the project. This table is a reference for the following tasks in the project towards the design of the EuWireless architecture.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3GPP	3rd Generation Partnership Project
5GC	5G Core Network
AAA	Authentication, Authorization and Account
AE	Application Entities
AMF	Access Control and Mobility Management
APN	Access Point Name
ASA	Authorized Shared Access
BSS	Business Support Systems
BBU	Baseband Unit
CAPEX/ OPEX	Capital Expenditures and Operation Expenditures
CAPIF	Common API Framework for 3GPP Northbound API
CBRS	Citizens Broadband Radio Service
CN	Core Network
CoMP	Coordinated Multi-Point
COTS	Commercial Off-the-Shelf
CP	Control Plane
C-RAN	Cloud Radio Access Network
CRN	Cognitive Radio Networks
CSE	Common Service Entities
CU	Central Unit
DC	Dual Connectivity
DCN	Dedicated Core Network
DNS	Domain Name System
DSRC	Dedicated Short Range Communications
DU	Distributed Unit
EFS	Edge and Fog Computing System
eMBB	enhanced Mobile Broadband
EMS	Element Management System
eNB	Enhanced NodeB
EPC	Evolved Packet Core
eSIM	Electronic SIM
ETSI	European Telecommunication Standards Institute
EU	European Union
E-UTRAN	Evolved Universal Terrestrial Access Network
eV2X	Enhanced Vehicular to Everything
FCC	Federal Communications Commission
FCAPS	Fault, Configuration, Accounting, Performance, Security
GAL	General Authorized Access
gNB	5G NodeB
GSMA	Global System for Mobile Communications Association
GTS	GÉANT Testbed Service
GVM	Generic Virtualization Model
GWCN	Gateway Core Network
HLS	Higher Layer Split
HSS	Home Subscriber Server
IC	Infrastructure SDN controller
ICIC	Inter-Cell Interference Coordination
IFOM	IP Flow Mobility

IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunication
IoT	Internet of Things
ISG CIM	Industry Specification Group for cross-cutting Context Information Management
ITS	Intelligent Transportation System
LAA	License Assisted Access
LC	LSA Controller
LCM	Life Cycle Management
LLS	Lower Layer Split
LPWA	Low Power Wide Area
LR	LSA Repository
LSA	Licensed / authorized Shared Access
LSRAI	LSA Spectrum Resource Availability Information
LTE	Long Term Evolution
LTE-U	LTE unlicensed spectrum
LWA	LTE-WAN aggregation
LWIP	LTE-WLAN Radio Level Integration using IPsec Tunnel
M2M	Machine to Machine
MAC	Medium Access Control
MANO	Management and Orchestration
MAPCON	Multi Access Packet Data Network Connectivity
MCC	Mobile Country Code
MEC	Multi-access Edge Computing
MFCN	Mobile/fixed Communication Networks
MIMO	Multiple Input Multiple Output
MIoT	Massive Internet of Things
MME	Mobility Management Entity
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
MORAN	Mobile Operator Radio Access Network
MPQUIC	Multipath QUIC
MPTCP	Multipath TCP
MTC	Machine Type Communication
N3IWF	Non-3GPP InterWorking Function
NB-IoT	Narrowband IoT
NEF	Network Exposure Function
NF	Network Function
NFR	Network Function Repository
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NG	Next Generation
NG-RAN	Next Generation Radio Access Network
NGSI-LD	Next Generation Services Interface for Linked Data
NM	Network Management
NRA	National Regulatory Authority
NSI	Network Slice Instance
NSSI	Network Slice Subnet
OAM	Operation, Administration and Maintenance
OBU	On-board Units

OSM	Open Source Mano
OSS	Operational Support Services
OMA	Open Mobile Alliance
PAL	Priority Access License
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDU	Packet Data Unit
PGW	Packet Gateway
PHY	Physical Layer
PLMN	Public Land Mobile Network
PNF	Physical Network Functions
PoD	Point of Distribution
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RAT	Radio Access Technologies
RCA	Resource Control Agent
RLC	Radio Link Control
RRH	Remote Radio Head
RSU	Road Side Units
S1AP	S1 Application Protocol
SAS	Spectrum Access System
SBA	Service Based Architecture
SDN	Software Defined Network
SCEF	Service Capability Exposure Function
SFC	Service Function Chain
SGW	Serving Gateway
SIM	Subscriber Identity Module
SMF	Session Management Function
SMS	Short Message Service
S-NSSAI	Single Network Slice Selection Assistance Information
SST	Slice/Service Type
TC	Tenant SDN controller
TVWS	Television White Space
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UP	User Plane
UPF	User Plane Function
V2I	Vehicle to Infrastructure
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
VIM	Virtualized Infrastructure Manager
VNF	Virtual Network Function
VPLMN	Visited Public Land Mobile Network
VoIP	Voice over IP
WAN	Wireless Access Network
WBA	Wireless Broadband Alliance
WPA2	Wi-Fi Protected Access 2

1 Introduction

This deliverable contains an analysis of the technologies that could contribute to implement a network satisfying the objectives of the EuWireless project. EuWireless will produce a design of a European level infrastructure to support research in mobile networks in the next 10 years. The main idea behind the design is to propose technical and legal methods to share resources between commercial mobile operators (MNOs) and the research community. The specific requirements will be detailed in deliverable D1.1, while the architecture with the proposed solutions will be reported in deliverables D2.1 and D2.2. In this context, the current document focused on the most recent directions in the standardization and implementation of 5G networks, including key concepts like network slicing and virtualization technologies.

The document is organized as follows. Section 2 provides the context of EuWireless, with a summary of the objectives and the initial high-level architecture to be refined in deliverables D2.1 and D2.2.

Starting with this context, Section 3 provides more insight on the standardization of 5G networks trying to identify which technologies should be available in EuWireless because they should be exposed to researchers and/or because they are enabling technologies to implement EuWireless. For instance, slicing technologies to share the network for different uses fit the two objectives: researches expect to define and to configure slices, and it enables the support of many concurrent researches on top of the same infrastructure. The same applies to Multi-access Edge Technologies (MEC), which enables the deployment of services close to the final users. The details of these technologies are described in Section 4 when applicable.

Section 4 focuses on techniques to share the network components in different levels: spectrum, access nodes, transport and backhaul, core networks and platforms to deploy services. These are the main techniques to create slices and to share both MNOs and researchers' infrastructures. Two major technologies in this area are Software Define Networking (SDN) and Network Function Virtualization (NFV).

Section 5 provides a separate description of specific tools or frameworks that implement a combination of the sharing technologies. The most relevant one is GÉANT Testbed Service (GTS), a platform promoted by GÉANT and NORDUnet to create isolated experimental platforms for researchers in Europe. Nowadays, GTS does not support mobile networks; however, it is the main resource provided by NORDUnet to EuWireless and could play a key role in the final architecture.

Finally, Section 6 provides a summary of the role that all these enabling technologies and specific frameworks could play in the EuWireless architecture to be elaborated in the next months.

2 EuWireless motivation and objectives

2.1 Motivation

European citizens, like in other parts of the world, are shifting to wireless communications as the next step to high speed Internet access, with more subscribers now in wireless cellular networks than in the wired domain in many countries. According to CISCO [1] periodic report, 429 million new mobile devices were added to cellular networks in 2016 in the world. The report estimates **11.6 billion mobile-connected devices (including machine-to-machine) by 2021**, which means 1.5 devices per capita. Alongside, research in Information and Communication Technologies (ICT) is also shifting from fixed (wired) to wireless networks.

Due to the growing complexity of the mobile networks (5G and beyond), the scientific community needs more realistic experimental facilities with the purpose of validating new ideas on network or services against the expected behaviour. This need is especially critical to study aspects such as Quality of Service (QoS) or Quality of Experience (QoE). All over the world, powerful indoor research platforms built with private or public funding are appearing. For instance, around 60 experimentation platforms to support research in mobile technologies have been identified recently in Europe by the Networld2020 European Technology Platform [2]. However, current **small-scale testbeds are not enough** for realistic validation, and the **scientific community needs now large-scale field deployments** working with the same radio spectrum than the commercial networks and capable of supporting the new technologies and services. The evolution from lab testbeds to field deployments is required to increase the validation capabilities for complex systems such as connected cars, massive Internet of Things (IoT), or eHealth solutions. In that direction, Networld2020 recommends the European Commission to increase support for the aggregation of the experimental facilities, for example interconnecting the current testbeds and **field trials**. Similar needs are now being identified in other research and industrial initiatives; for instance, the Trials and Spectrum working groups in the 5G Infrastructure Public Private Partnership (5GPPP) [3].

In the case of Europe, field trials are currently hosted by commercial mobile network operators (MNOs), which often do not provide access neither to the results, nor to the infrastructure that they have deployed and own. The regulation is very heterogeneous, but in most cases, restricts the access of researchers to regulated spectrum. There might be additional conditions: for instance, in France and Spain, in order to use regulated spectrum, it is mandatory to be registered as an operator, even when having the permission from the owner of the license. The provision of feasible methods to share MNO resources with researchers will open **new research collaboration and business opportunities for MNOs** that will have access to novel research and technical advancement.

European research infrastructures around wired and wireless communication networks have been considered in the FP5, FP6, and FP7, and H2020 research programmes with relevant outputs like GÉANT and FIRE. GÉANT is the pan European e-infrastructure that interconnects Europe's national research and education networking (NREN) organisations. This e-infrastructure has been supporting and will be supporting the research and educational community for both standard connectivity and research activities, but offering a similar service focused on large scale mobile networks requires a major upgrade. The Future Internet Research and Experimentation (FIRE) objective in FP7 and H2020 has extended, federated, or even created new research infrastructures for ICT in Europe. Some of them support wireless cellular communication, but they are basically for indoor deployments, without connection to commercial operators.

The same problem has been partially addressed in USA with the network SciWinet [4] for universities. SciWinet works as an umbrella to make agreements easier between universities and MNOs to install new equipment for limited use under a master agreement to share the spectrum.

A pan-European legal entity registered as an operator in different European countries could partially solve the problems to deploy large scale research pilots using regulated spectrum. However, technical, legal and planning work should be done to design such operator, with the technical infrastructure, the regulatory aspects, and the business model as the first steps to the implementation with the collaboration of national and European agencies, such as ESFRI or the H2020 programme.

2.2 Project objectives

The global objective of EuWireless is to design the European operator for research on mobile networks. The following table describes more specific objectives of the proposal and how they are addressed by the consortium:

Table 1. EuWireless Objectives

Objective	How it is addressed by EuWireless
To identify requirements and barriers to support large scale research on mobile networks using regulated spectrum.	Analysis of real requirements for the scientific community and research industrial centres regarding the new research infrastructure. Study of national and European regulations that allow or prevent research in this area (spectrum, security, privacy, other). Identification of the candidate technologies that can contribute to the solution.
To design technical solutions for a shared pan-European research mobile network.	Theoretical and practical evaluation of technical solutions at all levels of the architecture, and provision of several design choices all of them compliant with current standards.
To design the implementation strategy and the governance model of the new infrastructure.	Work around the evaluation of the applicability of the approach to some uses cases followed by the evaluation of the implementation and operation cost, the funding opportunities, the business model and the governance rules of the new infrastructure.

In the context of the first objective, this deliverable has been produced in parallel with deliverables D1.1 and D1.2 related to requirements. The rest of sections in the document responds to the "identification of the candidate technologies that can contribute to the solution".

3 Fundamentals of 5G networks

In the last years, the mobile network industry has experimented a strong growth of the demand for higher broadband capacity, wider coverage availability and reliable and dramatically lower latency, amongst many other requirements set by the evolution of the market and the needs of the users. In order to meet such challenging goals, 5G mobile network technology is being developed.

This section aims to provide an insight into the 5G technology. First, it depicts the 5G network architecture, showing its main entities and functionalities. Second, it describes technologies with critical importance in the 5G environment, i.e. technologies that enable heterogeneous access to the network, multiple connectivity technologies at different layers, virtualization technologies and Multi-access Edge Computing (MEC) technologies. Then, the section reviews some relevant R&D projects in the 5G landscape. Finally, it depicts different APIs that provide network function exposure for third parties.

3.1 Architecture of a 5G network and main components

The fifth generation of mobile communication technology (5G) development process is experiencing a strong boost as several organizations from the public and the private sector are working hard to reach an overall consensus on architecture, involved technologies, uses cases, etc. From the beginning of its design, the 5G ecosystem aims to create a flexible platform in which a large number of different actors coexist, providing means to integrate easily new business cases and models.

The envisaged usage scenarios for 5G have been classified into three basic categories: Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low-Latency Communications (uRLLC) and Massive Machine Type Communications (mMTC).

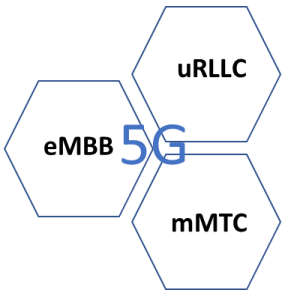


Figure 1. 5G categories of services

The performance requirements extracted from these scenarios come up with the necessity of composing a list of expected key performance indicators (KPIs) that 5G technology should fulfil [5] [6]:

Table 2. 5G KPIs

Parameter	Target value	Definition
Peak data rate	DL: 20Gbps UL: 10Gbps	Maximum achievable data rate under ideal conditions per user/ device
Peak Spectral efficiency	DL: 30bps/Hz UL: 15bps/Hz	Peak data rate normalised by bandwidth
User experienced data rate	DL: ≤ 1Gbps UL: ≤ 500Gbps	Achievable data rate that is available ubiquitously across the coverage area to a mobile user/device
Area traffic	DL: ≤15Tbps/km	Total traffic throughput served per geographic

capacity	UL: ≤ 7.5Tbps /km2	area
Connection density	≤ 100 000/km2	Total number of devices fulfilling a target QoS per unit area
Latency	0.5ms ~ 10s	The contribution by the radio network to the time from when the source sends a packet to when the destination receives it
Mobility	≤ 500km/h	Maximum speed at which a defined QoS and seamless transfer between radio nodes can be achieved
Mobility interruption time	≤ 100 000/km2	Shortest time during which a user terminal cannot exchange user packets with network
Reliability	99.9% ~ 99.9999%	The success probability of transmitting a packet

The 3rd Generation Partnership Project (3GPP) is the organization in charge of compiling all the knowledge produced by researchers on former mobile communication technologies and 5G and writing technical specifications to standardize them. 3GPP has numerous working groups which periodically produce studies on different topics to consolidate all the aspects of the different technologies.

When a new mobile communication technology is being developed, assuring a certain interconnectivity or coexistence with former technologies is a key factor. Following this idea, 3GPP defined a two steps deployment of 5G:

- The first set of specifications, Release 15, published in early 2018, defines the so-called Non-StandAlone (NSA) deployment. It depicts an interworking scenario between 4G and 5G at Radio Access Network (RAN) level in which 5G RAN (New Radio (NR)) can handle user traffic, taking advantage of 5G NR, but it is a 4G Core Network (Evolved Packet Core (EPC)) that performs control plane tasks. To do so, a 4G RAN acts as master RAN and the NR as secondary RAN in a Dual Connectivity (DC) relationship.
- The second phase, included in Release 16, defines the StandAlone (SA) variant. SA is fully 5G and includes both 5G NR and 5G Core Network (Next Generation core network (NG)).

5G System architecture is been built around the idea of dynamically running multiple instances of virtual networks to meet specific needs. In 5G, former 4G network entities are split in more fine-granular Network Functions (NF), as well as new ones are included, to add flexibility and scalability features. Figure 2 shows a simple representation of the 5G System architecture in its first phase of development, in which NFs are interconnected in a similar fashion to LTE architecture, i.e. via reference interfaces.

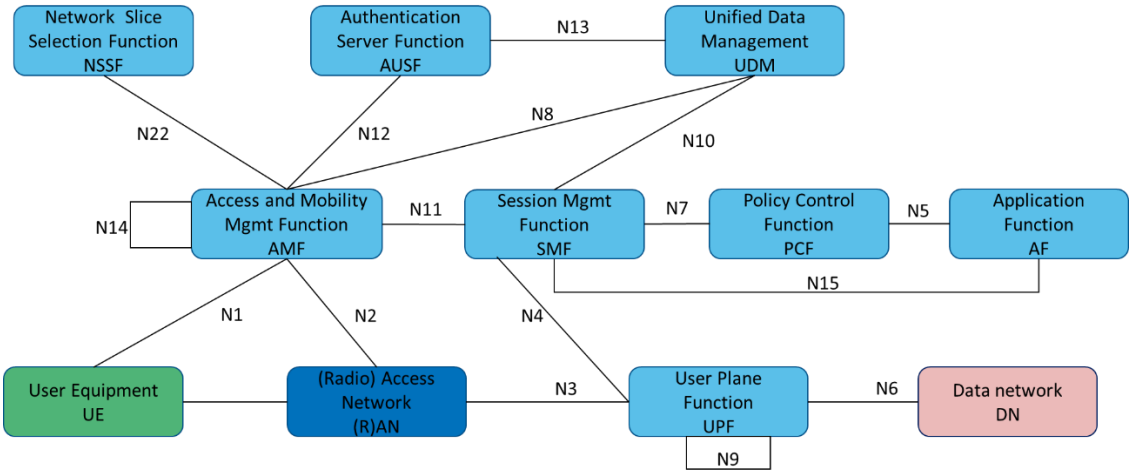


Figure 2. Non-Roaming 5G System Architecture in reference point representation [7]

The main NFs which compose the 5G System are listed below, along with some of their principal functionalities [7]:

- Access and Mobility Management Function (AMF): Former EMM, the EPS Mobility Management. AMF is in charge of the UE registration, connection, access authentication, access authorization and mobility management amongst other tasks.
- Session Management Function (SMF): Former ESM, EPS Session Management. In charge of session management (establishment, modification, release), UE IP address allocation.
- User Plane Function (UPF): Anchor point for Intra/Inter-RAT mobility, QoS handling for user plane, uplink traffic verification, downlink packet buffering and downlink data notification triggering.
- Policy Control Function (PCF): Former PCRF and also the network slicing policy framework: Supports unified policy framework to govern network behaviour, provides policy rules to Control Plane function(s) to enforce them.
- Authentication Server Function (AUSF) and Unified Data Management (UDM): Former HSS functionality. The AUSF supports authentication for 3GPP access and untrusted non-3GPP access. The UDM provides generation of 3GPP AKA authentication credentials, user identification handling, access authorization based on subscription data, subscription management.
- Application Function (AF): Interacts with the 3GPP Core Network to provide services such as application influence on traffic routing, accessing to Network Exposure Function (see section 3.7) and interacting with the Policy framework for policy control.
- Network Slice Selection Function (NSSF): Selecting the set of Network Slice instances serving the UE, determining the AMF set to be used to serve the UE.

In order to simplify the process of adding new NFs and reduce complexity, a second phase of development has been planned with a service-oriented architecture for control plane, as shown in Figure 3. NG core functions query a new NF, Network Repository Function (NRF), to discover and communicate with other entities. NFs offer events that other NFs can register to and consume.

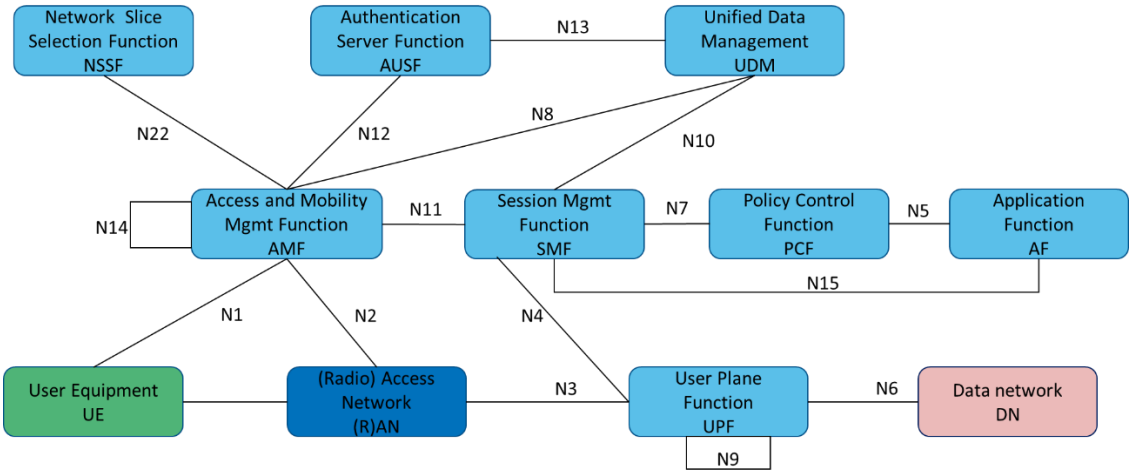


Figure 3. 5G System service-oriented architecture [7]

This way of communication between NFs facilitates the development of new functions since it does not require establishing specific end-to-end interfaces between them. In addition, it is better suited to deployment on the cloud infrastructure that leading operators pursue. In this cloud model, different NFs can be dynamically linked into an end-to-end service over standardized APIs on demand. With the SBA model, adding/modifying/removing NFs from already established service paths and creating new ones is simpler for operators.

3.2 Heterogeneous networks

Evolution of mobile networks has been always focused on increasing the network capacity. That is also true for 5G where new networks will need to fulfil the high traffic demand requirements, including extreme network capacity and very high data rates.

Heterogeneous Networks (HetNet) offer a way to handle this scenario through the deployment of macro cells together with small cells cooperating together to improve the performance of the network in terms of capacity dimensioning and access delay.

Approaches for HetNets where the macro and small cells cooperate to improve the performance of such methods are proven to be beneficial from both the access delay and a capacity dimensioning perspective.

Small cells can be deployed in places such as lampposts, traffic lights and inside buildings, making the deployment cheaper and simpler with less interference issues. Small cells have a short-range coverage but they may be located in hot-spot areas with heavy traffic demand, or in areas with poor coverage of the network, thus improving the coverage. Small cells are also suitable for offloading traffic from the macro cells.

5G networks will benefit from Heterogeneous Networks by combining the use of NR with other technologies, such as Wi-Fi, or IoT, devoted to match specific requirements of power consumption, cost, indoor coverage, etc.

Automotive is going to be one of the first verticals using the Heterogeneous Network concept due to the traffic capacity and network coverage requirements, where cellular technologies will cooperate with other technologies (e.g., DSRC).

3.2.1 Wi-Fi

Wi-Fi® is a WLAN (Wireless Local Area Network) technology based on the standards produced by the IEEE 802.11™ group. Wi-Fi is a trademark of the Wi-Fi Alliance®, allowing

the use of the 'Wi-Fi Certified' term only to products that have successfully completed the certification program.

According to the last Cisco update [8], by 2021 63% of global mobile data traffic (cellular) will be offloaded to Wi-Fi or small cell networks, up from 60% in 2016. From these figures it becomes clear that Wi-Fi must be an essential part of 5G networks and will be the non-3GPP radio most extensively used in 5G networks. Wi-Fi remains mostly in the spectrum below 6 GHz, except for WiGig® products that use the uncongested 60 GHz frequency band.

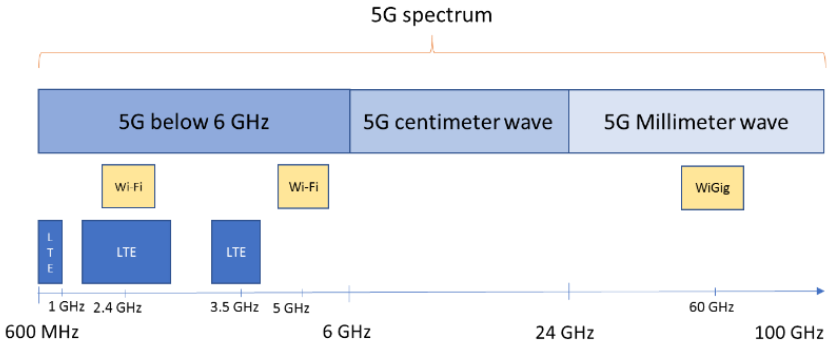


Figure 4. 5G spectrum

Table 3 lists the different Wi-Fi technologies (today called generations), the frequency band of operation as well as theoretical and expected real-world top speeds for each technology.

Table 3. Wi-Fi generations

Generation	IEEE Standard	Frequency band (GHz)		Max Speed (Approx.)		Year of Introduction
		2.4	5	Theoretical	Real-world[1]	
	802.11a	No	Yes	54 Mbps	25 Mbps	1999
	802.11b	Yes	No	11 Mbps	6.5 Mbps	1999
	802.11g	Yes	No	54 Mbps	25 Mbps	2003
Wi-Fi 4	802.11n	Yes	Yes	450 Mbps (1)	100 Mbps	2009
Wi-Fi 5	802.11ac	No	Yes	1300 Mbps (2)	350 Mbps	2014
Wi-Fi 6	802.11ax	Yes	Yes	14 Gbps	4.8 Gbps[2]	2019

IEEE 802.11a and 802.11b/g were the first standards introduced and for which the Wi-Fi Alliance developed a certification program. These standards are broadly extended in the market, can achieve real top speeds of 25 Mbps, and work at 2.4 GHz or at 5 GHz. Any Wi-Fi product today is compatible with these technologies.

[1] Several sources:
- MCS index 23, 64QAM, 3 spatial streams, coding rate 5/6, 40 MHz BW, 400 ns GI
- 802.11ac Wave 1

[2] This technology has not been widely introduced yet, so real speed is not available at the moment.

Wi-Fi 4 generation, based on the IEEE 802.11n standard, was designed to improve the throughput by utilizing MIMO (Multiple Input Multiple Output). It also extends the radio coverage thanks to its increased signal intensity.

Wi-Fi 5 generation, based on the IEEE 802.11ac standard, is the latest available generation of Wi-Fi, uses dual band technology supporting simultaneous connection in 2.4 GHz and 5 GHz, enabling devices to handle higher bandwidth demanding applications such as multimedia streaming and Ultra HD and 4K video.

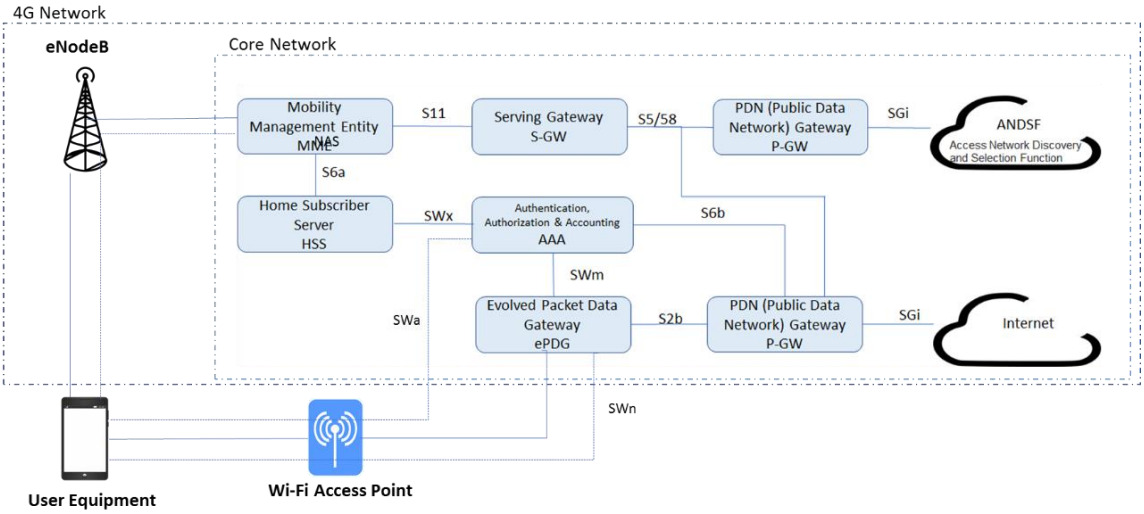
Wi-Fi 6 generation, based on the IEEE 802.11ax standard, is expected to be in the market in 2019 and will not only improve the throughput per user, it will also provide it in dense user environments. This standard implements several mechanisms offering better interference mitigation and a better scheduler among other solutions to serve a consistent and reliable data throughput to many users in crowded environments.

The Wi-Fi Alliance certification scheme has evolved with the IEEE standards, and today includes a large set of programs, such as Wi-Fi Direct®, Miracast® or Passpoint®. Passpoint is especially relevant for 5G networks as it eases the roaming between Wi-Fi and cellular technologies. Passpoint is a program that provides WPA2™ (Wi-Fi Protected Access 2) hotspot network access and online sign up. It enables mobile devices to discover, select and connect to Wi-Fi networks in a secure way without human intervention. Mobile devices may include or not SIM modules. Passpoint follows Hotspot 2.0 Technical Specification, specified by the GSMA association and the Wireless Broadband Alliance (WBA).

First release of the Hotspot technical specification included network selection and security. The second release of the specification added online signup and policy provisioning. Passpoint provides network operators a way to use Wi-Fi® technology to offload data from cellular networks, for example to lower the traffic load in busy locations such as football stadiums or city centres.

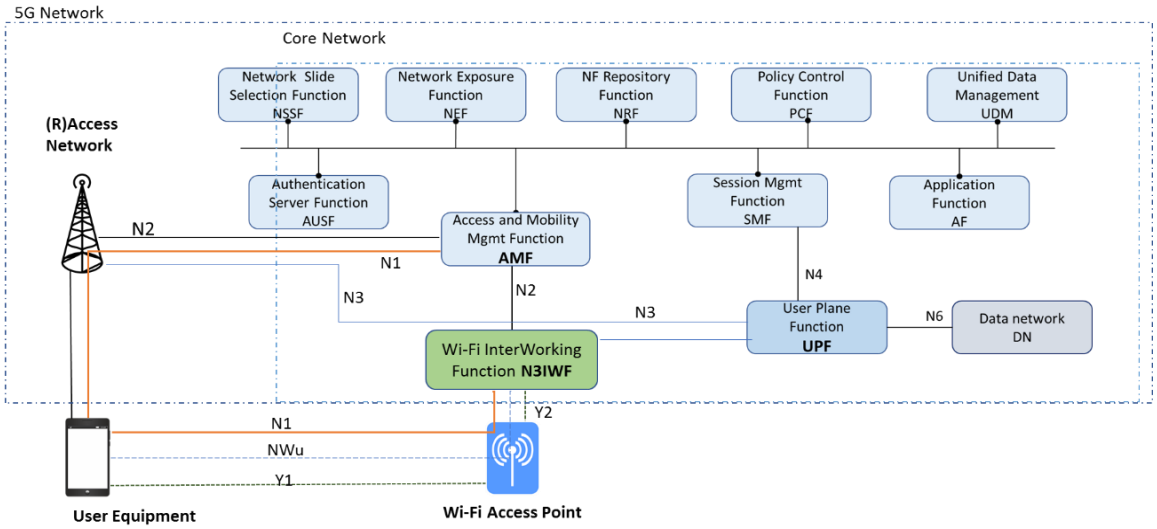
It is expected that Wi-Fi will have a significant role supporting mobile broadband end-users and new applications such as Smart cities.

Figure 5 and Figure 6 show the architecture of a 4G network and a 5G network, respectively, including cellular and Wi-Fi access in a non-roaming case.



SWa: Ref. point between the Untrusted non-3GPP IP Access and the 3GPP AAA
SWn: Ref. Point between the Untrusted Non-3GPP IP Access and the ePDG

Figure 5. Non-roaming architecture for a 4G Core Network with Wi- Fi access



Y1: Ref. Point between the UE and the Non-3GPP access
Y2: Ref. Point between the untrusted non-3GPP access and the N3IWF for the transport of NWu traffic .
Nwu: Ref. point between the UE and N3IWF for establishing secure tunnel(s) between the UE and N3IWF
N1: Ref. point between the UE and the AMF

Figure 6. Non-roaming architecture for a 5G Core Network with Wi- Fi access

The reference point between the UE and the Access control and Mobility and Management function (AMF), in the 5G network core, is performed through the Access Network (RAN) in the cellular network and through the Wi-Fi access by using the interworking function (N3IWF).

In [9], the WBA (Wireless Broadband Alliance) defines different categories of integration where all can be used to support what they refer as "switched-mode" (only one single access is used at a time) and "split-mode" (a device may have simultaneous access to multiple accesses over prolonged period). The three approaches are:

- Access Centric Integration: these approaches were first introduced in Release 13 for LTE based access, with LTE WLAN Aggregation (LWA) for integrating trusted Wi-Fi with LTE and LWIP for integrating untrusted Wi-Fi. These approaches are described in greater detail in section 3.3.1.
- Core-Centric Integration: these approaches were initially standardised in Release 8 for the integration of un-trusted Wi-Fi via an ePDG and in Release 11 for integrating trusted Wi-Fi into LTE's Evolved Packet Core, as described in 3.3.2.
- Above-the-Core integration: using techniques such as Multi-Path TCP and Multi-Path Quick UDP Internet Connection (QUIC). More recently these new protocols have been proposed to enable integration between Wi-Fi and cellular networks. These protocols are described in greater detail in section 3.3.3.

Figure 7 and Figure 8 show the architecture of access centric integration and core centric integration architecture.

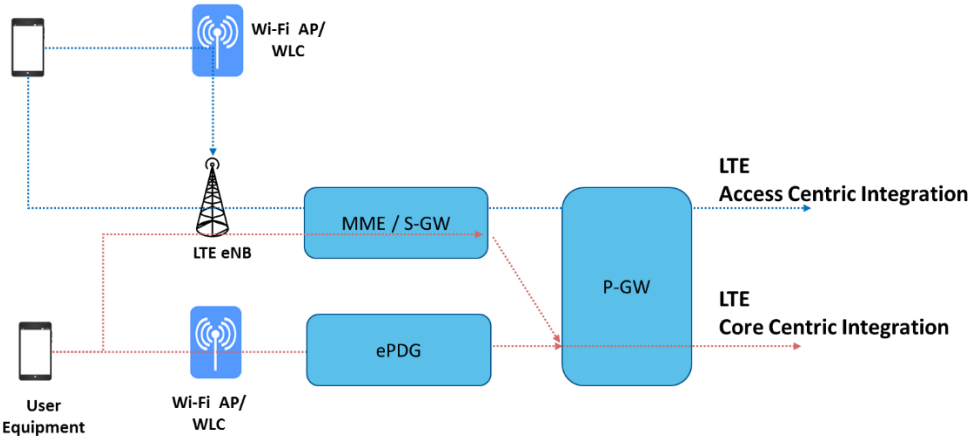


Figure 7. Access Centric integration and Core centric integration in an LTE network

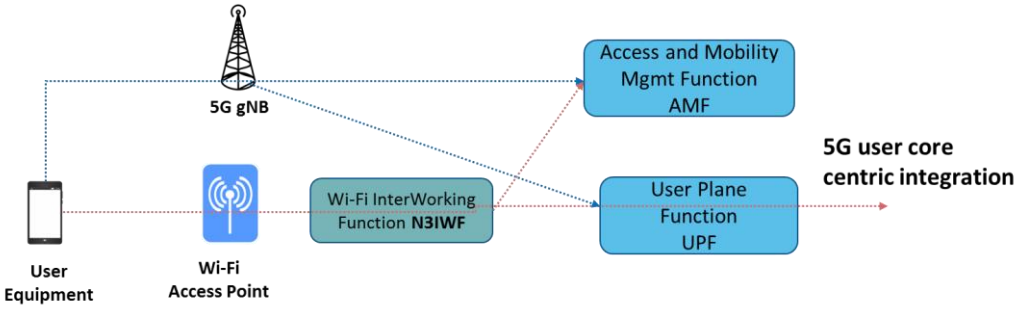


Figure 8. 5G user ore centric integration

The WBA envisions that this variety of integration approaches can lead to fragmentation of the market and/or delays in deployment as alternative approaches are evaluated. However, at to the date, only one Access Centric deployment has been reported compared to multiple Core-Centric (e.g., VoWiFi) and Above-the-Core (e.g., multi-path enabling specific applications). Accordingly, WBA proposes to focus on those solutions where Wi-Fi is treated as a peer of the cellular network.

3.2.2 Internet of Things (IoT)

M2M (Machine to Machine) is a known concept referring to any technology that enables wired and wireless devices connected through a network to exchange information and perform actions with other devices of the same type without the need for human intervention.

Internet of Things (IoT) goes a step further interconnecting ‘things’ (physical devices) within the existing Internet infrastructure. Each device has its own unique identifier. IoT supports a large number of different applications covering a wide array of vertical industries and disciplines, that are not all part of the ICT domain.

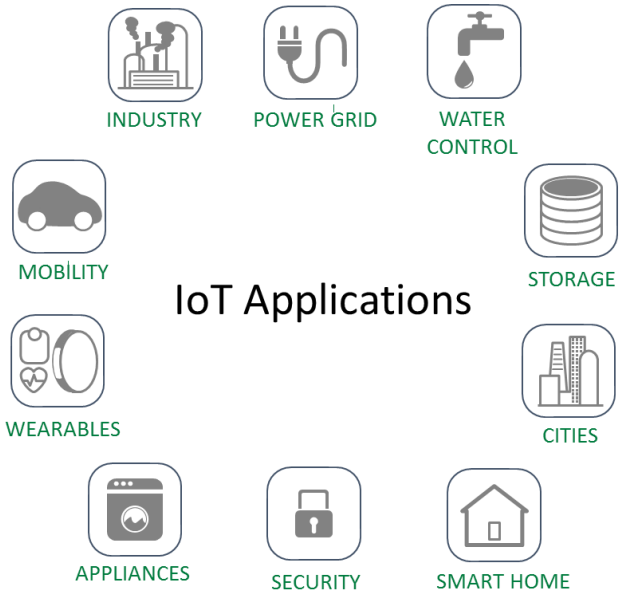


Figure 9. IoT applications in vertical industries

GSMA is very active in the promotion of the cellular IoT technologies NB-IoT and LTE-M with a focus on highlighting the advantages of using licensed spectrum solutions. GSMA initiatives include: a) Development of specifications and test plans expanding the scope of 3GPP standards; and b) Promotion of a worldwide network of IoT Open Labs, established by carrier infrastructure vendors and/or technical consortiums and open to device and solution developers willing to test their interoperability with commercial network equipment.

GSMA Intelligence predicts that by 2025, the figure of 3.1 billion IoT connections will be reached. Other sources provide similar or higher estimations. It is clear that with these numbers IoT is going to be an important niche in the connected world, and thus is part of 5G targets.

Most of the IoT devices will rely on wireless connection technologies, with only a few of them connecting through wired connections.

There is a plethora of IoT initiatives aiming to cover the IoT world requirements. Some of these initiatives offer a complete end-to-end service, working on top of the lower-layers of existing protocols such as WLAN, Bluetooth, Z-wave, etc. Some of the most relevant organizations active in the development of IoT standards are:

- AIOTI: Alliance for Internet of Things innovation
- ETSI: European Telecommunications Standards Institute
- IoT-GSI: Global Standards Initiative on Internet of Things
- HyperCat Consortium
- IEEE (Internet of Things (IoT) Architecture Working Group)
- IETF: Internet Engineering Task Force.
- IIC: Industrial Internet Consortium
- IoT-Ready Alliance
- ITU-T: Joint Coordination Activity on IoT – UIT
- LITU: Linaro IoT and Embedded Group
- OCF: Open Connectivity Foundation (merger of the Open Interconnect Consortium (OIC), AllSeen Alliance and UPnP Forum)
- OMA SpecWorks (merger of the Open Mobile Alliance (OMA) and the IPSO Alliance.
- OMG: Object Management Group

- oneM2M: global standards initiative for Machine to Machine Communications and the Internet of Things
- OpenFog Consortium: Drives industry and academic leadership in fog technology
- Thread Group: Responsible of IoT Thread technology.
- TIA (Telecommunications Industry Association) TR-50 M2M: Smart device communications.
- ULE Alliance: Responsible of the low-power wireless ULE technology
- W3C Semantic Sensor Network Incubator Group
- W3C Web of Things Community Group
- Weightless: Responsible for the low power, wide area networks (LPWAN) Weightless technology.
- Wize Alliance: Responsible of Wize standard for industrial IoT.
- Z-Wave Alliance: Responsible of Z-Wave IoT technology.
- ZigBee Alliance: Responsible of ZigBee IoT technology.

Devices have different connection requirements depending on the IoT solution into which they are integrated, such as high bandwidth, low bandwidth just to transmit a few bytes a few times per year, highly reliable connections, highly secure connections, low power consumption, etc. IoT technologies can also be classified according to the IoT devices requirements they target.

A relevant group inside IoT are the low power-wide area technologies. The main target of Low Power Wide Area (LPWA) technologies is long range and low power consumption communication among objects (devices), thus enabling devices to operate for many years with a single battery. Other requisites of these technologies are the low cost of devices, a secure connectivity, and intermittent transmission of little amount of data. Due to the diversity of IoT application requirements, a single technology is not capable of addressing all of the LPWA use cases. LPWA technologies can be broadly classified into 3GPP-based and non-3GPP-based technologies.

Mobile Internet of Things is the GSMA term that refers to the 3GPP standardised LPWA technologies using licenced spectrum bands (aka LTE-M, NB-IoT and EC-GSM-IoT).

- EC-GSM-IoT: Extended coverage GSM IoT is a standard-based LPWA technology. It is based on eGPRS and designed as a high capacity, long range, low energy and low complexity cellular system for IoT communications.
- LTE-M: Stands for "Long Term Evolution for Machines". It is the simplified industry term for the LTE-MTC (Long Term Evolution Machine Type Communications) LPWA technology standard published by 3GPP in the Release 13 specification. It specifically refers to LTE Cat M1, suitable for the IoT. It is also known as eMTC (enhanced machine-type communication). It is a cellular technology that uses licensed spectrum and can deliver up to 1 Mbps of throughput utilizing 1.4 MHz of bandwidth. The deployment of LTE-M networks started in March 2017. LTE-M has various ways to set up a connection to and from the device: a) VoLTE (optional) for voice call, b) packet data in the user plane, after setting the appropriate APN (Access Point Name), and c) SMS for small amount of data. The communication can be opened either from or to the device. LTE-M supports two coverage enhancements modes (Mode A (moderate) and Mode B (deep)), both are based on repetition techniques for both data and control channels. LTE-M supports two power classes (class 3 (23 dBm) and class 5 (20 dBm)). LTE-M supports full-duplex or half-duplex operation modes. It can be used 'in-band' with normal LTE carriers or using its own spectrum as standalone and can coexist with 2G, 3G and 4G. The technology provides improved both indoor and outdoor coverage, supports massive numbers of low data throughput devices, low delay sensitivity, ultra-low device cost, low device power consumption and optimised network architecture. In 2017 the LTE-M logo was developed for the GSMA LTE-M Task Force to enable

members and other technology users to clearly label products and services using LTE-M [10]. 3GPP defined in Release 13 [11] a set of frequencies to be used for LTE-M, bands: 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 18, 19, 20, 26, 27, 28, 31, 39, and 41. In Release 14, bands 25 and 40 were added. To achieve global roaming support in America, Europe and parts of Asia the following bands need to be covered: 1, 2, 3, 4, 5, 12, 13, 20, 25, 26 and 28.

- NB-IoT (Narrowband IoT), defined in 3GPP TS36.300 [12], is a 3GPP cellular radio technology standard that addresses the IoT requirements for LPWA networks. It uses licensed spectrum. NB-IoT, introduced in Release 13, uses new physical layer signals and channels and can be deployed in-band with the cellular carrier, standalone, or in a cellular carrier guard-band. While LTE-M supports any LPWA application, NB-IoT, also known as NB-IoT Cat-NB-1, is designed for simple static sensor type applications. NB-IoT enables data rate of just 10's of kbps occupying 200 kHz of bandwidth. Because the underlying technology is very simple, its costs are expected to decrease rapidly. NB-IoT can coexist with 2G, 3G, and 4G mobile networks. 3GPP has defined a set of frequency bands where NB-IoT can be used. 3GPP TS 36.101 [13] from Release 13 provides the list of the supported bands: 1, 2, 3, 5, 8, 12, 13, 17, 18, 19, 20, 26, 28, 66. Release 14 added bands: 11, 25, 31 and 70 and Release 15 added bands: 4, 14 and 71. In Europe, according to GSMA, deployments have been using bands: B3 (1800), B8 (900) and B20 (800).

Figure 10 provides the architecture for NB-IoT and LTE-M in the roaming case, showing the connection of the MTC App in the UE through the RAN (Random Access Network to the MSC (Mobile Switching Center), MME (Mobile Management Entity), SGSN (Serving GPRS Support Node) and the S-GW (Serving Gateway) in the Visitor PLMN (Public Land Mobile Network) and then to the Home PLMN.

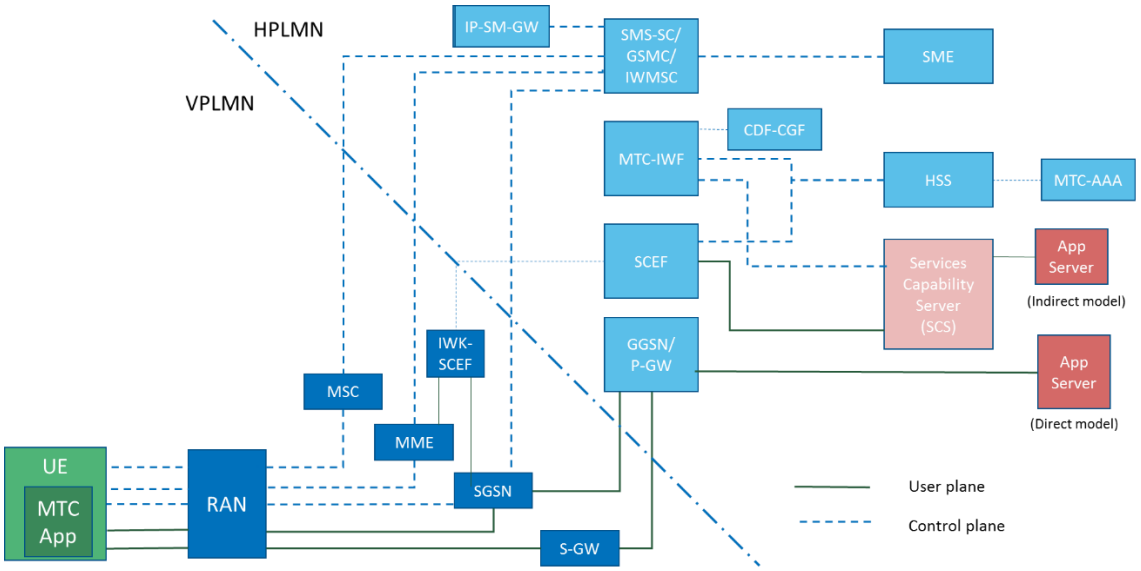


Figure 10. NB-IoT and LTE-M architecture (roaming case)

Although NB-IoT and LTE-M technologies are based on LTE, GSMA considers them to be an integral part of 5G, as they will cover LPWA 5G use cases and will coexist with other 5G components. Major operators such as Telefónica also consider NB-IoT and LTE-M as integral part of 5G.

Furthermore, the MulteFire Alliance is adapting LTE IoT to operate in the unlicensed spectrum. This will in turn bring new opportunities for private LTE networks and enable use cases, leveraging narrowband LTE IoT technology. MulteFire Alliance is supported by Tier 1

companies around the world, including chipset and device vendors, infrastructure manufacturers and other companies related with LTE private network deployment. MulteFire is developing a proprietary technical specification based on 3GPP but intended to design a technology similar to LTE operating only in unlicensed spectrum. Version 1.0 of MulteFire specification focuses on mobile broadband, while version 1.1 will expand support of IoT by adapting NB-IoT and LTE-M (eMTC) technologies to the unlicensed domain.

In terms of non-3GPP LPWA technologies, the most relevant emerging standards are:

- LoRaWAN [14] open networking protocol specification developed and maintained by the LoRa Alliance, a non-profit association with more than 500 member companies. LoRaWAN™ defines the communication protocol and system architecture for the network while the LoRa® is the physical layer or modulation and is based on chirp spread spectrum modulation which enables the long-range communication. LoRaWAN uses a simple star topology, where devices connect through a base station (gateway) to the central server. In a LoRaWAN™ network nodes are not associated with a specific gateway. Instead, data transmitted by a node is typically received by multiple gateways. The gateways are connected to the network server via standard IP connections and act as a transparent bridge, simply converting RF packets to IP packets and vice-versa. LoRaWAN networks are deployed in unlicensed spectrum below 1 GHz, at different frequencies depending on the region. LoRa Alliance has a certification scheme in place for LoRaWAN devices.

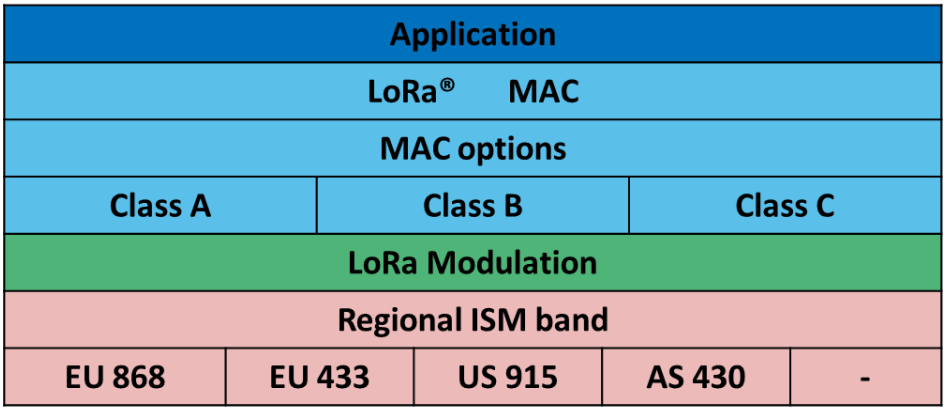


Figure 11. LoRaWAN protocol stack [14]

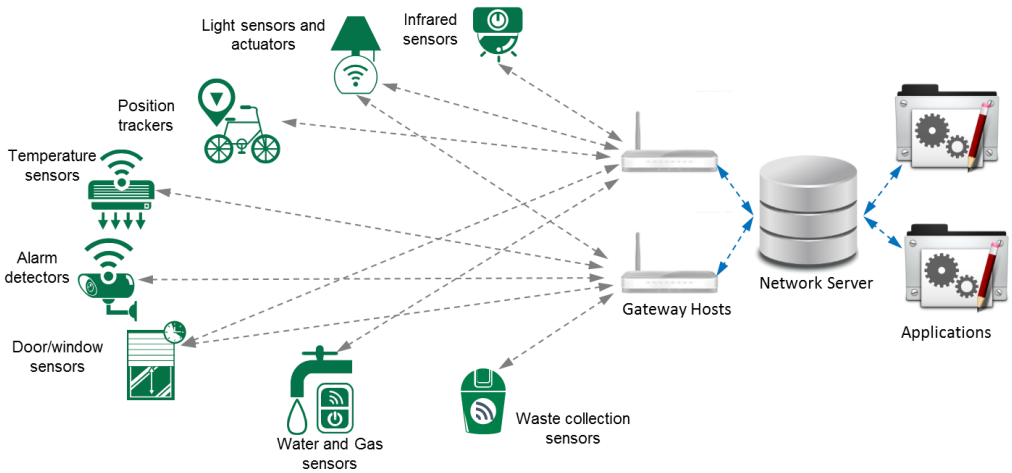


Figure 12. LoRaWAN architecture [14]

- SigFox is also a LPWA network, using unlicensed spectrum. It only provides uplink connection (a restricted downlink option is also possible). SigFox devices broadcast data that is received by any base station in the range, without the requirement of establishing and maintaining a network connection. The network and computing complexity is handled in the cloud, reducing devices consumption, complexity and costs. SigFox modules are cheaper compared to other technologies. SigFox operates in the 868 MHz frequency in Europe and in the 902 MHz frequency in North America.

The coverage for LTE-M and NB-IoT is very good as they rely on 4G coverage and they provide a better quality of service than LoRa and Sigfox. LoRa connections costs are cheaper compared to cellular ones, and the devices battery life is longer. Additionally, LoRa works better with moving devices than NB-IoT or SigFox.

There are other IoT Low Power technologies aiming to shorter ranges (Wireless Local Area Networks). These include Wi-Fi, Bluetooth, Zigbee, Thread, etc.

- One of these technologies is 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) supporting personal area networks. One of the most successful 6LoWPAN technologies is THREAD. Thread [15] is a mesh network designed to connect hundreds of products around the home. Thread is based on the IEEE 802.15.4 standard providing a low-power, low-bandwidth way to reliably connect devices together in a mesh network. Thread is not a standards group but one aiming to create market awareness".

As a summary, all these technologies have their specific advantages and drawbacks, meaning that they all may have their space in 5G networks as they fit different devices requirements in the IoT ecosystem.

Because IoT has evolved from efficiently transporting sensor (or actuator) data, it is possible to move further and have global IoT services and make information accessible for automatic knowledge processing agents. To achieve this, locally available IoT resources (sensors and actuators) must be combined with cloud-based services. In order to achieve interoperability, semantic processing to enable data mediation is essential.

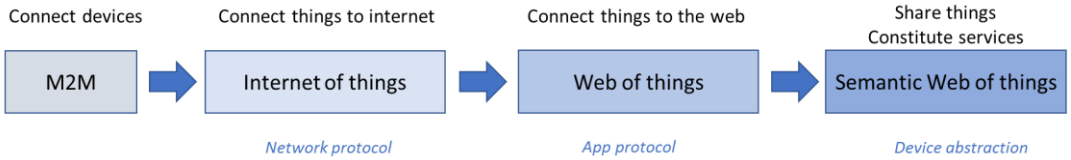


Figure 13. Evolution of devices connection

Various standardization organizations are working in this area.

- FIWARE [16]: The FIWARE Community is an independent open community whose members are committed to materialise the FIWARE mission: "to build an open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that will ease the development of new Smart Applications in multiple sectors". It is based on the work developed within the context of various EU funded projects. FIWARE is providing a set of cloud enablers that can be used for receiving, processing, contextualizing and publishing IoT data. FIWARE is built on the concept of configuring a service platform from a library of existing enablers. Various companies are already offering commercial solutions using FIWARE.

- oneM2M. The fragmented nature of the M2M and IoT markets have led to the creation of oneM2M, an alliance of standardization organisations, such as ETSI, aiming to develop a single horizontal platform for the exchange and sharing of data among all applications. oneM2M [17] is defining an international standard for IoT data exchange focusing on the communication aspects. oneM2M develops technical specifications, which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software elements. In the oneM2M functional architecture two types of entities are defined. Application Entities (AE) and Common Services Entities (CSE). CSEs expose services though defined reference points (Mca and Mcc) and AEs. OneM2M defines a Common Services Layer, which is a software layer that sits between the network and applications, be it in the wide area network domain or in the field domain (where devices and gateways are generally deployed). The functions in the Common Services Layer include: device management, data collection, protocol conversion and interworking, group management, security, etc. Those functions are exposed to applications (in the cloud, gateway or devices) via Restful APIs. Figure 14 depicts the oneM2M architecture. oneM2M, already in release 2, has matured and there is even a certification scheme in place, being backed by GCF.

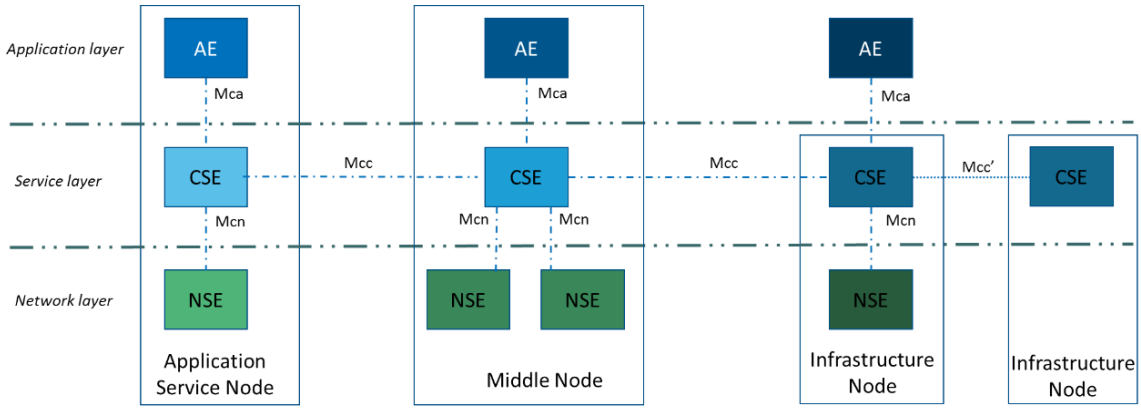


Figure 14. oneM2M architecture [18]

- Another initiative, the ETSI Industry Specification Group for cross-cutting Context Information Management, ETSI ISG CIM, identifies a need for an API (called by the group NGSI-LD) to exchange the definitions/metadata/context. This API needs to be agnostic to the kind of data architecture used. ETSI ISG CIM will specify protocols running on top of IoT platforms and enable exchange of data together with its context. This includes what is described by the data, what was measured, when, where, by what, the time of validity, ownership, and others. That will dramatically extend the interoperability of applications. ETSI ISG CIM will focus on developing specifications for a common context information management API, data publication platforms and standard data models.
- "Linked Data" is other initiative dealing with sharing data on the web based on its 5-star model for measuring the maturity of open data. It was introduced by Sir Tim-Berners Lee [19] and it is based on the following principles: 1. be available on the Web under an open licence; 2. be in the form of structured data; 3. be in a non-proprietary file format; 4. use URIs as its identifiers; 5. Include links to other data sources.

3.2.3 Connected Car based on Wi-Fi technologies

ITS stands for Intelligent Transportation System. This term is used to refer to the systems that use information and communication technologies to improve several aspects of the transport systems in general, including any transport method. Nowadays, the most frequent use for this

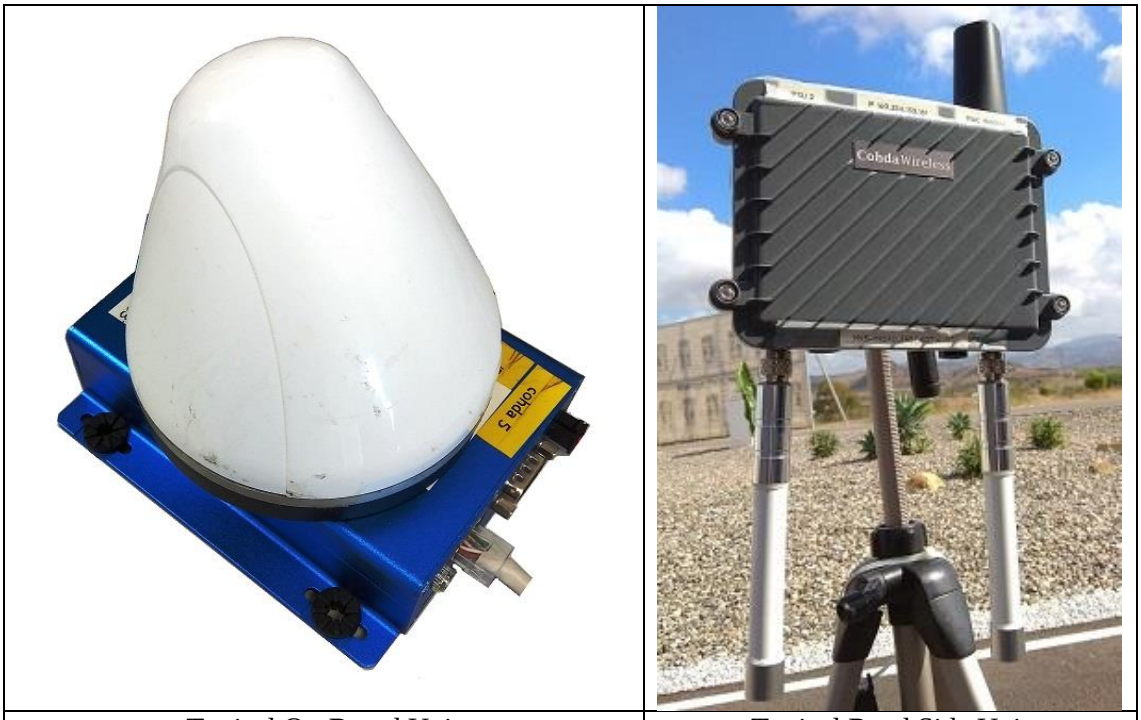
term is related to the road transportation methods, and it focuses on aspects such as safety, traffic management, electronic tolling, energy consumption, traveller information, CO_2 emissions, etc.

For the initial deployment of vehicular communication, consistent sets of standards have been created, commonly named C-ITS in Europe and DSRC/WAVE in the U.S.A., both relying on the Wi-Fi standard IEEE 802.11. Specifically, the IEEE 802.11p standard enables ad hoc communication and the direct exchange of information among vehicles in their vicinity, including the communication between vehicles and the roadside infrastructure. Vehicle to anything (V2X) is the general term used to refer to vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrians (V2P), etc., communications.

DSRC/WAVE relies on IEEE 802.11 standards which define the physical transmission (PHY) and medium access control (MAC). The Internet protocol (IP), the default networking protocol for many todays' networks, in combination with the transport protocols UDP and TCP, is used in DSRC. However, many V2X applications apply direct communication among vehicles and between vehicles and roadside units. For this purpose, the IEEE 1609 series of standards has been developed. The Wave Short Message Protocol (WSMP) defined in IEEE 1609.3 is at the core of the protocol stack a single hop network protocol with minimum header of few bytes. Overall, the U.S.A. version (a combination of IEEE 802.11p and IEEE P1609) is referred to as DSRC/WAVE, where WAVE stands for wireless access in vehicular environments.

There are two classes of devices in a WAVE system: on-board units (OBU) and roadside units (RSU). OBU will repetitively broadcast their own position coordinates and speed vector as a beacon, so other vehicles around can use this information to calculate potentially dangerous situations. These calculations are performed by each vehicle's OBU, and actions can be taken if necessary. The message repetition rate is 100 ms (i.e. 10 messages per second). A vehicle at 180 km/h travels 5 m in that period of time. This has been considered a good enough solution, since higher repetition rates would imply higher processing requirements and higher RF channel load.

RSU can be used to inform drivers of any events happening on their way, such as accidents, road conditions, weather, traffic light status, and so on. They can also be used to collect useful traffic statistical information. Even pedestrians or cyclist could use portable devices to improve their safety. Figure 15 shows some example devices.



Typical On-Board Unit	Typical Road Side Unit

Figure 15. Example of On-Board Unit and Road Side Unit

The parallel development of V2X communication has led to a different protocol stack in the USA. and Europe. The V2X version of the standard in Europe is termed ITS-G5. The PHY and MAC are also based on IEEE 801.11p. The upper layers also rely on the IP protocol for non-safety applications, but a major difference is at the automotive specific protocols: The usage of TCP/UDP and IP version 6 is similar to the U.S.A. version, whereas C-ITS specifies an ad hoc routing protocol for multi-hop communication, termed GeoNetworking which is specified in the ETSI EN 302 636 standard series. A key feature of this protocol is the usage of geographical coordinates for addressing and forwarding. IPv6 packets can also be transmitted over GeoNetworking, for which the adaptation sub-layer GN6 (IPv6 over GeoNetworking) has been designed and standardized. Compared to the WSMP in the DSRC protocol stack, GeoNetworking is optimized for multihop communication with geo-addressing, which provides more technical features in application support, but comes with an increased protocol complexity and overhead.

V2X technologies are being promoted by several countries, mainly in USA and Europe, by means of DoT Strategic Plans in the U.S.A., or European Directives in Europe. Japan has its own set of standards. Other countries are developing their standards too.

As already mentioned, V2X technologies specified in Europe and U.S.A. use IEEE-802.11p specification for the physical layer. From this viewpoint, it is similar to Wi-Fi, but the layers on top of it are different, and they also differ from U.S.A. to Europe. This means that V2X devices in U.S.A. and Europe can use the same hardware, but the firmware should be different. Figure 16 shows both protocol stacks.

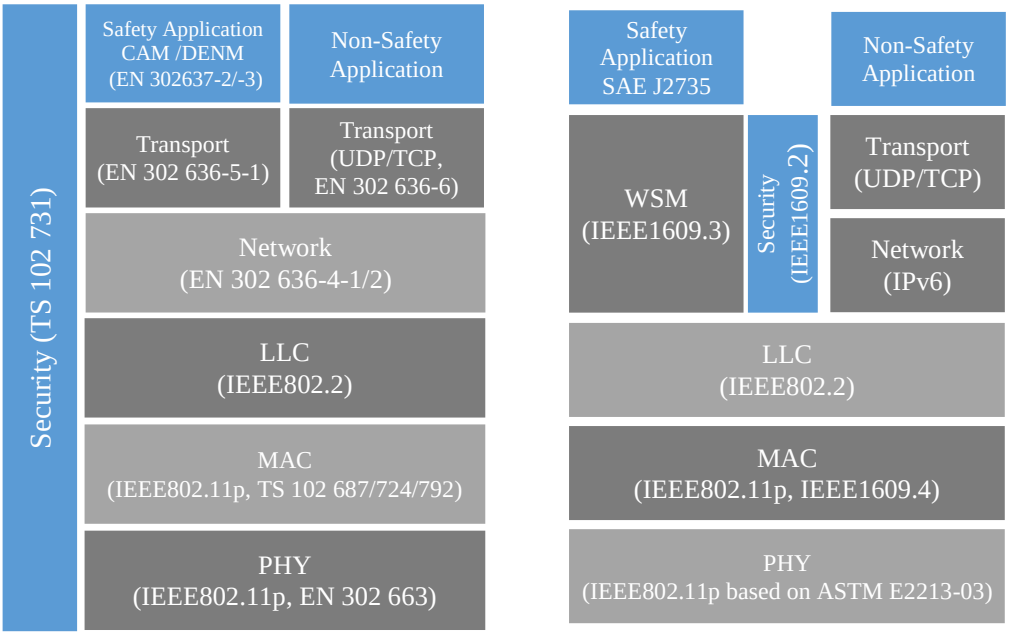


Figure 16. DSRC ITS-G5 and DSR/WAVE protocol stacks

Figure 17 and Figure 18 show the channels allocation for V2X in Europe and USA. 10MHz channels have been defined in the 5.9GHz frequency band, ranging from 5845 MHz to 5925 MHz. For some purposes, two adjacent 10 MHz channels can be combined in one single 20 MHz channel.

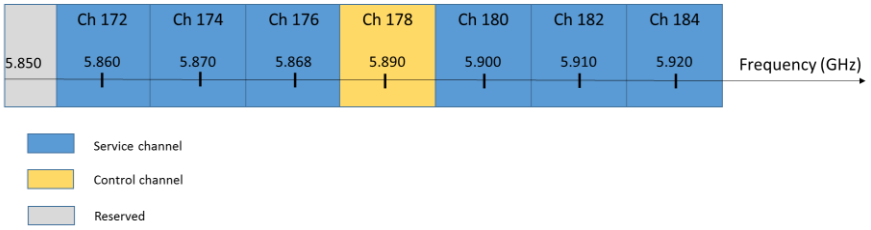


Figure 17. DSRC Channels and frequencies used in USA

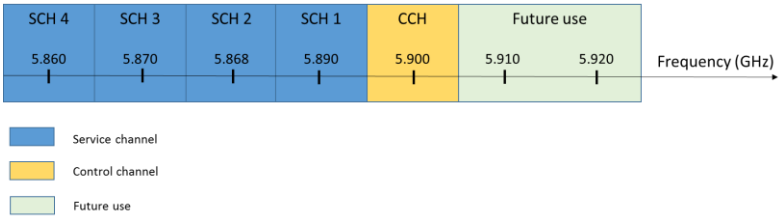


Figure 18 DSRC Channels and frequencies used in Europe

The use of the channels is specified by the standards. Different types of messages have been defined, depending on the use case. Some examples of these messages are BSM and WSA for the American "WAVE" protocol, or CAM and DENM for the European "ITS-G5" protocol.

Depending on the applications running on top the physical and network layers, V2X devices can perform many different tasks. Since safety and security are the main concerns, safety applications have been the first ones to be specified by standardization organizations from USA

(Omniair [20]) and Europe (ETSI). The following is a list of the main safety applications taken into consideration:

- Forward Collision Warning (FCW)
- Emergency Electronic Brake Lights (EEBL)
- Intersection Movement Assist (IMA)
- Vehicle Turning Right in Front of a Transit Vehicle (VTRFTV)
- Blind Spot Warning (BSW)
- Lane Change Warning/Assist (LCA)
- Work Zone Warnings (WZW)
- Spot Weather Impact Warning (SWIW)
- Speed & Curve Compliance
- Railroad Crossing Violation Warning
- Green Light Optimal Speed Advisory (GLOSA) / Time To Green (TTG)
- Red Light Violation Warning
- Distress Notification (DN)
- Intersection Movement Assist

3.2.4 Connected Car based on cellular technologies

C-V2X is a recent term introduced for cellular technologies optimized for connected vehicles. In particular, the C refers to the 3GPP technologies 4G LTE and 5G NR (new radio), whereas X refers to multiple things' vehicles may connect with. C-V2X includes both network-based communications that have been in use for decades, like vehicle-to-network (V2N), as well as a new complementary mode of operation first defined in the 3GPP Release 14 specifications and approved in June 2017, which allows direct communications between vehicles (V2V), as well as between vehicle and road side infrastructure (V2I and I2V) without requiring any cellular network coverage or subscription.

The first incarnation of C-V2X technologies was defined in 3GPP Rel.14, mostly to provide a data transport service for basic road safety messages such as CAM, DENM, BSM and so on. This release is based on a new interface (PC5) as an evolution of the existing Rel.12 sidelink for D2D communications; with appropriate changes to adapt to the specific requirements of moving vehicles.

Rel. 14 introduces two communication modes (modes 3 and 4) specifically designed for V2V communications. In mode 3, the cellular network selects and manages the radio resources used by vehicles for their direct V2V communications. In mode 4, on the other hand, vehicles autonomously select the radio resources for their direct V2V communications. Mode 4 can then operate without cellular coverage, and is therefore considered the baseline V2V mode since safety applications cannot depend on the availability of cellular coverage. Mode 4 includes a distributed scheduling scheme for vehicles to select their radio resources and includes the support for distributed congestion control.

On top of the work done in Rel.14, 3GPP Rel. 15 defines new features to cover additional scenarios, including:

- Vehicle Platooning: enables the vehicles to dynamically form a group travelling together. All the vehicles in the platoon receive periodic data from the leading vehicle, in order to carry on platoon operations. This information allows the distance between vehicles to become extremely small, i.e., the gap distance translated to time can be very low (sub second). Platooning applications may allow the vehicles following to be autonomously driven.

- Advanced Driving: Advanced Driving enables semi-automated or fully-automated driving. Longer inter-vehicle distance is assumed. Each vehicle and/or RSU shares data obtained from its local sensors with vehicles in proximity, thus allowing vehicles to coordinate their trajectories or manoeuvres. In addition, each vehicle shares its driving intention with vehicles in proximity. The benefits of this use case group are safer travelling, collision avoidance, and improved traffic efficiency.
- Extended Sensors: Extended Sensors enables the exchange of raw or processed data gathered through local sensors or live video data among vehicles, RSUs, devices of pedestrians and V2X application servers. The vehicles can enhance the perception of their environment beyond what their own sensors can detect and have a more holistic view of the local situation.
- Remote Driving: Remote Driving enables a remote driver or a V2X application to operate a remote vehicle for those passengers who cannot drive themselves or a remote vehicle located in dangerous environments. For a case where variation is limited and routes are predictable, such as public transportation, driving based on cloud computing can be used. In addition, access to cloud-based back-end service platform can be considered for this use case group.

For Rel.16, it is expected that a new direct communication mode is included, based on the NR air interface, increasing bandwidth and reducing latency. This 3GPP release is currently in an early stage, being end of 2019 the expected target for completion of the specification.

It is important to note that PC5 (and its successors for direct communication) is one important part of the C-V2X ecosystem, but not the only one. The existing LTE Uu interface (and its NR successors) is also part of the C-V2X offering, providing wide bandwidth in very extensive geographical areas; being a very good candidate for certain types of applications, like RWW, signage, etc.

3.3 Multiple Connectivity

Multiple connectivity is a technology that consists in having different connections at the same time, whereas aggregation includes the combination of multiple network connections. Both technologies grant benefits such as improving reliability, throughput, etc.

Multiple connectivity and traffic aggregation can be classified according to the layer in which they act: link, network, transport or application layer.

3.3.1 Data Link Layer

Multiple connectivity and aggregation at the link layer include technologies such as CA (Carrier Aggregation), DC (Dual Connectivity), LTE-U (LTE in Unlicensed spectrum), LAA (License Assisted Access) and LWA (LTE-WLAN Aggregation).

- CA was introduced in 3GPP TR 36.808 [21] to enable a UE to simultaneous transmit and receive data on multiple component carriers from a single eNB.
- DC was introduced in 3GPP TR 36.842 [22] to enable a UE to simultaneously transmit and receive data on multiple component carriers from two cell groups via a master (MeNB) and a secondary (SeNB) eNB.
- LTE-U is a proposal, originally developed by Qualcomm [23], for the use of the 4G LTE radio communications technology in unlicensed spectrum, such as the 5 GHz band. LTE-U is intended to let cell networks boost data speeds over short distances, without requiring the user to use a separate Wi-Fi network as they normally would. A control channel remains using LTE, but all data flows over the unlicensed 5 GHz band, instead of the carrier's frequencies.
- LAA approach, studied in 3GPP TR 36.889 [24], uses unlicensed spectrum alongside the licensed bands, evolving LTE-U. It uses carrier aggregation in the downlink to

combine LTE in unlicensed spectrum (5 GHz) with LTE in the licensed band. One of the main features of 3GPP Rel-14 is the introduction of Enhanced-Licensed Assisted Access (eLAA), which includes uplink operation for LAA.

- LWA, defined in 3GPP TS 36.300 [25] and TS 36.360 [26], performs aggregation at the PDCP layer of eNB, and therefore it belongs to link layer aggregation. LWA architecture follows LTE DC design, but allowing connection to WLAN instead of LTE Secondary eNB. A LWA data bearer may be routed via both eNB and WLAN access whereas the control plane connection remains on LTE.

3.3.2 Network Layer

In network layer, multiple connectivity can be found in technologies such as IFOM (IP Flow Mobility) and MAPCON (Multi Access PDN Connectivity), and aggregation in LWIP (LTE-WLAN Radio Level Integration Using IPsec Tunnel).

- IFOM [27] mobility method connects 3GPP and non-3GPP networks to the same PDN (Packet Data Network) and maintains the connection while managing the mobility data in different flows. IFOM allows to select particular flows per UE and bind them to one of the two different access networks, LTE and WLAN. This strategy belongs to Host Based Mobility mechanisms.
- MAPCON [28] is a method for managing mobility by handling multiple PDN connections when the UE itself has multiple IP addresses. The UE achieves simultaneous connections to LTE and WLAN networks, which allows dividing data for communications. As opposed to IFOM, MAPCON belongs to Network Based Mobility mechanisms.
- LWIP aggregation technology was firstly introduced in 3GPP Release 13 in TS 36.300 [29] and 36.361 [30]. In LWIP, a data bearer may be configured to use LWIP aggregation, and packets belonging to that bearer can be routed over LTE or WLAN on a per-packet basis, whereas the control plane stays in LTE. This technology is very similar to LWA, except for the aggregation which takes place at IP layer, thus enabling the use of legacy WLAN without the need of changes.

3.3.3 Transport Layer

In transport layer, the aggregation is performed using different IP addresses, grouping subflows of traditional transport protocols, such as TCP or UDP, to create a unified enhanced data flow as shown in Figure 19.

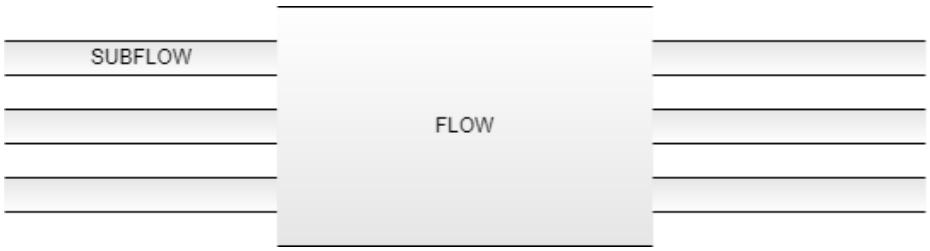


Figure 19. Aggregation in transport layer

Some of the most important multiple connectivity protocols are:

- Multipath TCP (MPTCP): Multipath TCP is a protocol standardized as experimental in January 2013 (IETF RFC 6824 [31]). MPTCP creates and manages different TCP subflows performing similar TCP handshakes to initiate the connection and add different subflows. This extension maintains TCP benefits like reliability, flow control, congestion control, etc., while offering improvements such as better QoS, load balancing or resilience.

- Multipath QUIC (MPQUIC): Multipath QUIC is an extension of the QUIC protocol presented in an IETF Internet draft [32] in 2017. MPQUIC is analogous to MPTCP, as it works creating and managing different QUIC subflows. The main difference is that MPQUIC is based on UDP instead of TCP (see Figure 20). QUIC uses UDP in order to reduce latency and improve the performance of web applications, but fails in terms of reliability. MPQUIC intention is to enhance QUIC protocol reliability and resilience using the benefits of multi-connectivity.

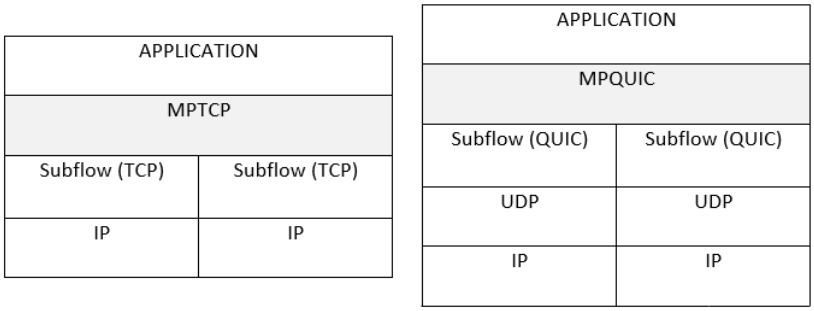


Figure 20. MPTCP stack vs MPQUIC stack

3.3.4 Application Layer

If aggregation takes place in the application layer, the application itself must be aware of the existence of multiple interfaces and manage the aggregation.

Another possibility is for the aggregation to take place at a lower layer but having the application layer being aware and controlling it. This is achieved using enhanced APIs.

There are a variety of solutions in the application layer under investigation. For example, Tesema et al. [33] show the importance of context-awareness in improving robustness. The work of Nielsen et al. [34] takes advantage of network monitoring to improve diversity, Schmidt et al. [35] present the idea of Socket Intents to select different interfaces according to user activity and requirements, etc.

3.4 Virtualization technologies

In recent years, mobile data services have become essential for the majority of users, which means an increase of traffic in wireless networks. Thus, new network designs and architectures are proposed in order to satisfy the demands of suppliers, companies and users. Network virtualization arises in response to this need. Virtualization is the abstraction process used to simulate a hardware platform, such as a server, storage device or network resource, in software as a virtual instance. Virtualization is a well-known technique that has been used for years, especially in computing systems, e.g., use of virtual memory and virtual operating systems. Nevertheless, the idea of using virtualization to create complete virtual networks is rather new and emerges as the solution to diversify the network into multiple coexisting architectures, each one isolated and customized to fit the specific requirements of a particular service. By using network virtualization, organizations could centrally provision the network on-demand, in order to scale and adjust the resources available to their evolving needs without physically modifying the underlying infrastructure. By merit of its abstraction and dis-association with specific hardware, the virtual service objects can be easily tailored to user requirements and isolated from one another when they are “instantiated” in the physical infrastructure. In a rigorously virtualized services environment, the user is unable to distinguish a virtualized service object from the “real thing” – they are virtually the same.

Network virtualization has recently become more of a focus, with the growth of Software Defined Networking (SDN) and Network Function Virtualization (NFV) and the resulting

decoupling of application, control, and data planes. In the near future, mobile communications will require large amounts of wireless resources to deal with the heterogeneity of the networks and the high data rates expected. Hence, virtualizing mobile networks will result in more efficient utilization of the shared wireless resources. Furthermore, it can reduce the number of base station equipment required and thus, the energy and overall investment to set up and run the infrastructure.

In [36], a Network Service is defined as "a composition of NFs and defined by its functional and behavioural specification" and a NF is "a functional building block within a network infrastructure, which has well-defined external interfaces and a well-defined functional behaviour". The network service contributes to the behaviour of the higher layer service, which is characterized by at least performance, dependability, and security specifications. The end-to-end network service behaviour is the result of the combination of the individual network function behaviours as well as the behaviours of the network infrastructure composition mechanism. Network services are typically provided by a server, which can be running one or more services such as Domain Name System (DNS), Voice over IP (VoIP), directory services, file sharing, etc. There are diverse NFV use cases addressing both the short and long term, in addition to 5G networks, IoT and hybrid clouds. Many of these use cases focus on providing Layer 4 through 7 services, such as networking security services, session border controllers, load balancers and application delivery controllers, firewalls, intrusion detection devices, policy enforcement managers, DNS platforms, and WAN accelerators.

3.4.1 Software Defined Networking

Software Defined Networking (SDN) is transforming networking architecture. Many traditional networks have a static architecture, which makes them ill-suited to meet the requirements of today's dynamic environments. The architecture of SDN decouples network control from forwarding. The migration of the control, which formerly was tightly bound in individual network devices, into accessible computing devices enables the underlying infrastructure to be abstracted for applications and network services, which can then treat the network as a logical or virtual entity [37].

The Open Data Center Alliance (ODCA) details in [38] a list of requirements for SDN including adaptability, automation, maintainability, model management, mobility, integrated security, and on-demand scaling. The SDN paradigm is directly programmable and centralizes network intelligence and state in software-based controllers, which keep a global view of the network, in such a way that appears as a single, logical switch to the applications. Thus, network design and operation is simplified, and its control becomes vendor-independent. As a result, enterprises and carriers gain unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs.

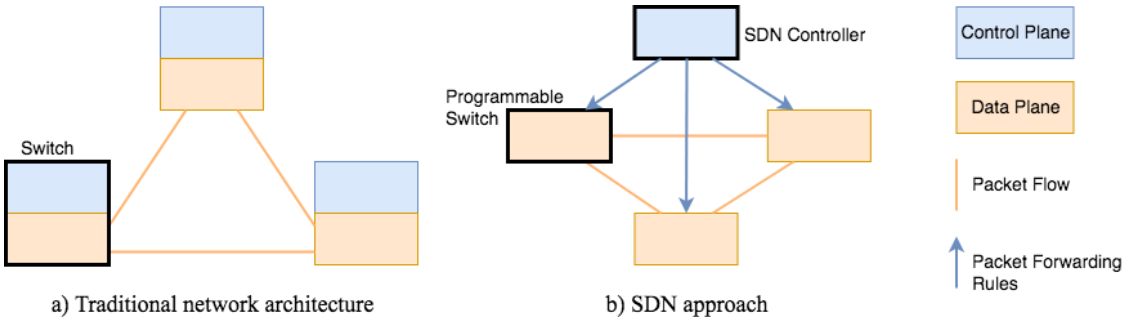


Figure 21. Control and data planes

As shown in Figure 21, the data plane in both approaches is responsible for forwarding packets. In the SDN approach, the control plane provides the intelligence via packet forwarding rules in

order to design routes, setting priority and routing policy parameters to meet the QoE (Quality of Experience) and QoS requirements, and dealing with the shifting traffic patterns that characterize today's networks. Open interfaces are defined to communicate SDN controllers with networking applications and switching hardware.

The data plane consists of network forwarding devices responsible for the transport and processing of data according to decisions made by the SDN control plane. It is a simple forwarding function since these devices are not able to make autonomous decisions. The forwarding rules are included in forwarding tables designating the next hop in the route for given categories of packets. The use of pipelined, multiple tables enables the nesting of flows, increasing the efficiency of network operations since it provides granular and real-time control at the application, user and session levels. The network device is also able to modify the packet header before forwarding or discarding the packet.

OpenFlow [39] is one of the many protocols available for the interface between the SDN control layer ant the resource layer, so-called southbound interface. It is widely accepted in the SDN community as the specification of the interface communicating SDN controllers and network devices [40]. The OpenFlow protocol enables the controller to perform add, update, and delete actions to the flow entries in the flow tables [41]. The control plane provides information about the network devices that form the data plane to applications and maps the requests received from the application plane into specific rules for the data plane. The application plane interacts with the control plane through the northbound interface and encloses applications and services that define, control and monitor network behaviour and components. Thus, the high-level architecture of SDN consists of three layers (see Figure 22), as defined in [42].

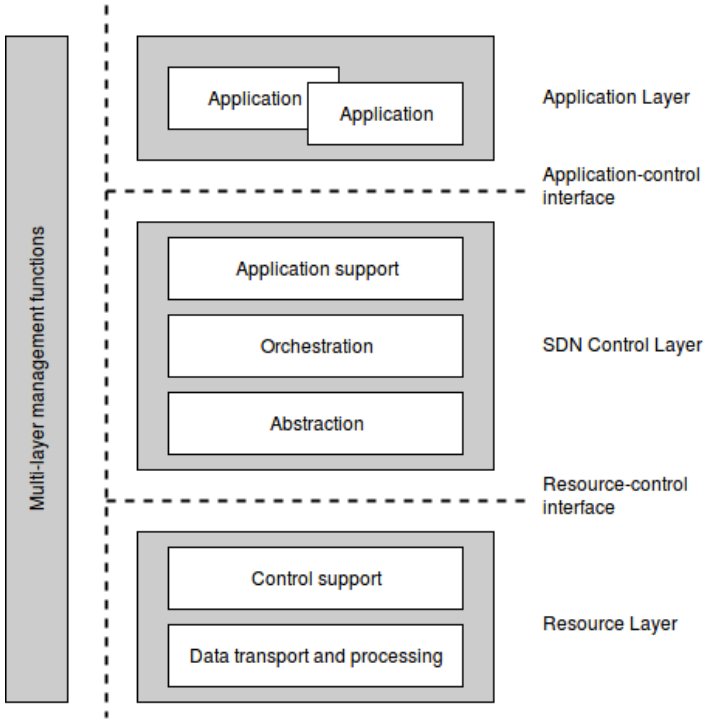


Figure 22. High-level architecture of SDN

Due to this centralized intelligence, network behaviour is altered in real-time, and new applications and network services can be rapidly deployed. Network resources are configured, managed and optimized by SDN programs. SDN architectures support a set of southbound and northbound APIs to implement common network services, custom tailored to meet business needs. These services include routing, multicast, security, access control, bandwidth management, traffic engineering, quality of service, processor and storage optimization, energy

usage, and all forms of policy management. Thus, applications operate through APIs on an abstraction of the network, optimizing computing, storage, and network resources as a result.

3.4.2 Network Function Virtualization technologies (network vs. services)

Network Functions Virtualization (NFV) is highly complementary to SDN. In [43], NFV is defined as the implementation of network functions in software that can run on a range of industry-standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need for installation of new equipment. NFV can rely on the mechanisms available in many data centres, but the separation of planes proposed by SDN can enhance performance, increase compatibility and simplify operation and maintenance procedures. Furthermore, NFV provides an infrastructure upon which the SDN software can be run.

In traditional networks, the elements might be seen as black boxes, proprietary platforms in which hardware cannot be shared. Thus, each element requires hardware to reach its maximum capacity that remains idle when system is not working at its maximum capacity. Network resources in NFV deployments are independent applications on a unified platform. Hence, software decouples form hardware and the capacity dedicated to each application is modified by adjusting the virtual resources on-demand. In this context, MNOs could determine which network applications and nodes include each service, and allocate the resources according to the system needs.

The Virtual Network Functions (VNF) are the blocks used to create end-to-end network services. These network services are created according to three key principles:

- Service chaining: one VNF offers limited functionality by itself, yet VNFs are modular and can be combined to achieve a more complex network functionality.
- Management and Orchestration (MANO): MANO manages the NFV infrastructure elements and involves deploying and managing the lifecycle of its instances.
- Distributed architecture: A VNF might comprise one or more VNF components. Each component might be deployed in one or multiple instances that could be deployed on the same or different hosts.

The reference architecture framework proposed to achieve these principles consists of four blocks, as shown in Figure 23, inspired in the framework reference from [44].

- NFV Infrastructure (NFVI): NFVI contains the software and hardware resources to deploy the VNFs and places the virtualized resources into pools.
- VNF/EMS: This block comprises the implemented VNFs and the Element Management System (EMS) used to manage those functions.
- NFV-MANO: This is the framework for the management and orchestration of all the available resources in the NFV environment. The NFV-MANO consists of three blocks: the NFV orchestrator to install and configure the network services and VNF, to manage the network services lifecycle and global resources, and to validate and authorize NFVI resource requests; the VNF manager to supervise the lifecycle management of VNF instances; and the virtualized infrastructure manager (VIM), to control and manage the interaction between its resources and the VNF. The NFV-MANO is responsible for the management and orchestration of the NFV environment. Additionally, it interoperates with the OSS/BSS aiming the management functionality for Support Systems' customers.
- Operational and Business Support Systems (OSS/BSS): The OSS/BSS implemented by the VNF service provider.

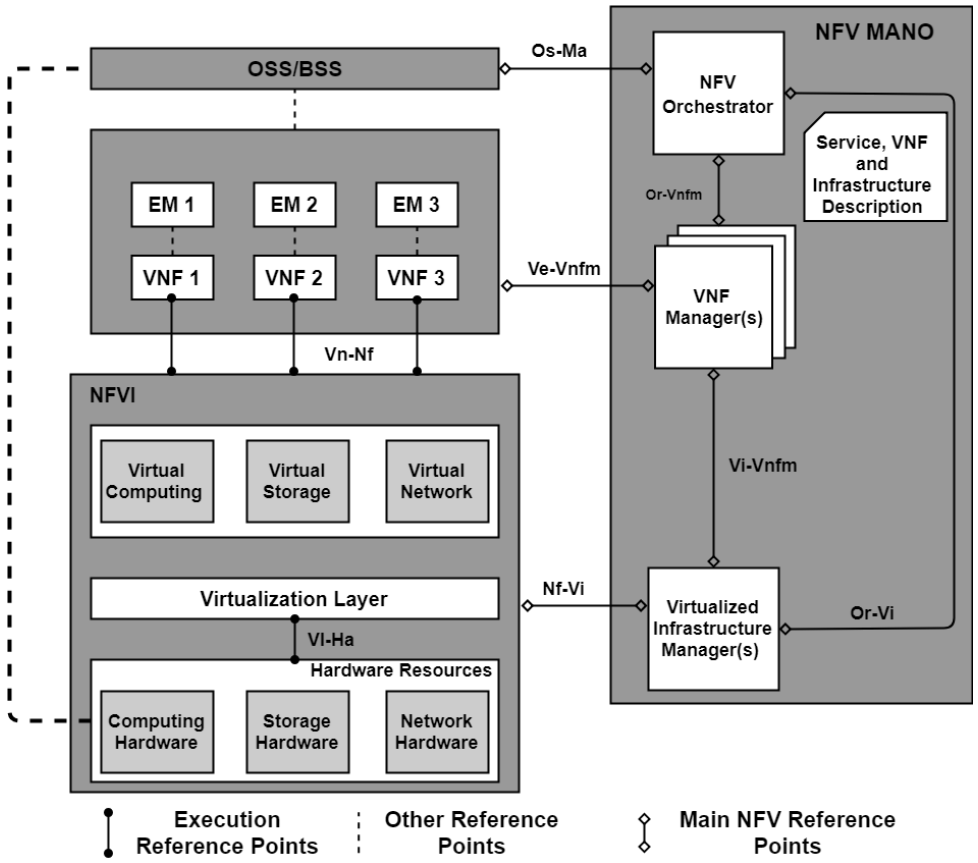


Figure 23. NFV reference architectural framework. Inspired in [44]

The NFV orchestrator coordinates and manages the NFVI resources among different VIMs by communicating with the VIMs directly through their northbound APIs. It might coordinate with the VNF Manager in order to create end-to-end services between different VNFs. It is capable of instantiating VNF Managers, if necessary, and is responsible for the topology management of the network services instances [45].

Considering the benefits of using open-source software, Open Source Mano (OSM) and OpenBaton are proposed as NFV orchestrators for this project, since both have received ample support from the NFV community.

The project Open Source MANO [46] is hosted by ETSI aiming at the development of software responsible for the Management and Orchestration according to ETSI NFV architecture. OSM is implemented generically, using VNF-specific code plug-ins called proxy charms, which makes it able to employ any interface of a VNF and/or its EM. These charms are ready to run in a container in the VNF Configuration Agent. Thus, OSM acknowledges the existence of multiple configuration methods available in NFV and cloud environments, and is prepared to consume any of the interfaces presented by commercial VNFs. Hence, an isolated execution environment is provided for each VNF.

Regarding the interoperability, OSM consumes south APIs from SDN controllers, VNFs, and Virtual Infrastructure Managers, and provides north APIs for on-boarding and control of network services, VNFs, and their lifecycles. The NFV descriptors define the blueprint used by OSM to instantiate and manage the lifecycle of a network service or VNF. NFV must be able to configure and control some specific resource parameters from the NFVI related to the throughput. This specification capability is required because the bottleneck for VNF capacity might be different to many cloud applications. However, the degree of specificity considered in

the modelling of resources should allow a limited degree of optimization to avoid over-specification of infrastructure requirements.

OpenVIM is a NFV specific VIM provided by OSM. OpenVIM supplies a reference for controlling the specific features of NFVIs that differ from general cloud controllers such as OpenStack, acknowledging the reusability of the infrastructure. Nevertheless, OSM aims no vertical integration but incorporating gradually its features to OpenStack and VIMs, such as VMware and even public cloud services [47].

OpenBaton [48] is an open source implementation of the ETSI NFV MANO specification. OpenBaton pursues the orchestration of network services across heterogeneous NFV Infrastructures. The management of VNFs is possible through a generic VNF Manager and a generic EMS, which use the descriptors of those VNFs to compose them runtime in the network services. OpenBaton provides a driver mechanism supporting different VIM types besides OpenStack, and it offers a network slicing engine supporting multi-tenancy. To ensure isolation between the slices, OpenBaton employs SDN technologies. It also integrates external OSS components to fulfil at runtime the needs of the Fault, Configuration, Accounting, Performance, Security (FCAPS) model. The integration with existing VNF Managers is made by a plug-and-play model, exposing Advanced Message Queuing Protocol and RESTful APIs, as well as SDKs in different programming languages (Java, Python, Go).

3.4.3 SDN-NFV Integration

The use of SDN and NFV should be coordinated to offer a unified software-based networking approach. SDN allows users and operators to configure the network dynamically. ETSI proposes in [49] a tentative framework to integrate SDN within the NFV reference architecture, since SDN itself lacks capabilities to manage the infrastructure resources and orchestrate their allocation. The proposed framework includes two SDN controllers that should be coordinated and synchronized, centralizing the control plane functionalities, as shown in Figure 24:

- Infrastructure SDN controller (IC): It is managed by the VIM and modifies the infrastructure behaviour on demand according to the specifications requested by the VIM. The IC manages the underlying networking resources to allow the deployment and connectivity of VNFs by using southbound interfaces. This controller enables functionalities such as provisioning, the configuration of network connectivity, bandwidth allocation, automation of operations, monitoring security, and policy control.
- Tenant SDN controller (TC): It might be instantiated as one VNF or as part of the network management system to manage the underlying VNFs according to the requests made by the tenant through the OSS to define the network services. This controller might be part of a service chain including other VNFs.

Additionally, the physical network resources should include enabled switch/NEs such as physical switches, hypervisor virtual switches, and embedded switches on the network interface cards. SDN applications might be VNF themselves. SDN-enabled VNF refers to VNFs controlled by the TC. The Network Functions (NFs) conforming the Core Network might be virtualized and deployed on top of the virtual network infrastructure as VNFs. Each VNF is composed by one or more NF.

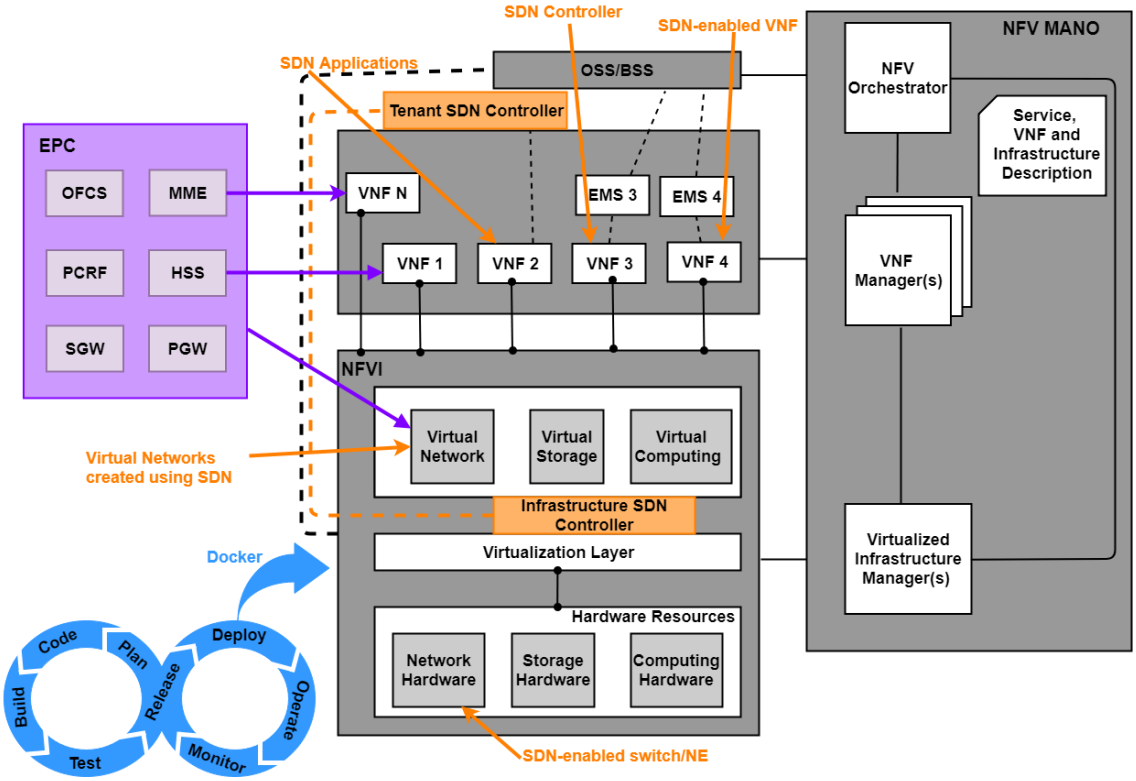


Figure 24 Integration of SDN controllers within the NFV reference architectural framework

3.4.4 Network reliability and security

Ensuring the correct behaviour of a network is an important task for network managers independently of the type of network. Network reliability addresses a wide range of issues, such as the analysis of the network in order to ensure the correct application of security policies, or determine the presence of unwanted loops, or black holes. Besides, network reliability issues can be studied in the design phase (pre-deployment), or during the deployment phase, in this case they combine the analysis with monitoring techniques and remote attestation techniques, to catch the current network status.

In the last years, networks are evolving to be hardware independent (and vendor agnostic) and easier to configure and manage. This transformation is achieved thanks to SDN, which proposes the separation of the control and data plane, using software-programmable forwarding equipment, and NFV that proposes the use of virtualization technology for the deployment of the network functions, allowing a cloud-based deployment.

These new trends in networking open the possibility for new tools to ensure network reliability.

Network managers can benefit from SDN and NFV paradigms to improve the reliability (and security) of the network, for instance developing and deploying SDN apps that deal with security policy enforcement or monitoring. However, the new networking paradigms also introduce new risks regarding network reliability and security, which requires the adoption of software engineering or cloud computing techniques to ensure/validate the network reliability. For example, some of the existing and proposed new open interfaces enabling network slicing and programmability can lead to new potential ways to attack software-based networks relying on both SDN and NVF. Securing the communication between VNFs [50] will enhance network reliability and benefit the implementation of the EuWireless concept.

In the last FP7 and H2020 funded ICT projects, a recurrent research topic is to ensure reliability in virtualised networks and data centres, or future 5G networks. For instance, the SHIELD [51]

project focuses on stablishing and deploying virtual security infrastructures into ISP and corporate networks using NFV technologies and concepts, effectively monitoring and filtering network traffic in a distributed manner. Other example is the 5GTango [52] project that addresses the flexible programmability of 5G networks combining DevOps and NFV as enabling technologies. DevOps is an approach that defines the lifecycle of the software development to achieve high quality and rapid time to market. To this end, testing and validation are performed repeatedly, at the early stages of the development cycle to eliminate errors and improve quality, and at the deployment stage, with monitoring and fault detection tools. DevOps has also been used in the UNIFY [53] project, which proposes a platform for users and services providers to develop and operate telecommunication services.

Panda et al. [54] proposes a method to verify isolation properties in networks that contains middleboxes. In particular, the authors are interested in networks with middleboxes (virtual network functions or physical network elements) whose behaviour depends on previously observed traffic, such as stateful firewalls or caches. The authors consider isolation at different levels, from network node isolation to flow or data isolation. To this end, the authors use symbolic model checking, in particular the Z3 SMT solver [62], to determine if the model of the middleboxes behaviour and the network topology satisfy the isolation properties. Finally, since the models are not automatically extracted from the middlebox implementation, the authors provide a runtime enforcement process that detects whether the middlebox instance behaviour deviates from the model.

Spinoso et al. [63] presents, in the framework of the UNIFY project, an approach to formally verify virtual network function (VNF) chains modelled as network function forwarding graphs. The verification is based on [54], and the verification is also carried out by the Z3 SMT solver in the pre-deployment phase. The authors have developed a catalogue of VNF models, including VNFs that can modify the packet content (e.g., NATs), which were not considered in [1]. These models can be chained to model complex network services. As of today, the prototype implementation analyses reachability properties in network function forwarding graphs, but they propose to extend the technique to deal with network reachability properties. This approach has been integrated in the Service Provider DevOps framework [64] designed in the UNIFY project, which combines on-the-fly verification, software-defined monitoring and automated troubleshooting of services.

More recently, in the framework of SHIELD project, Basile et al. [65] presented a method to assess network authorization policies based on reachability analysis. The objective is to detect permitted or unwanted connections between network hosts using the equivalent firewall model, which describes the network behaviour between peer hosts. The model is based on a geometric model capable of describing stateful network elements and also the transformation of packets. The policies are described in a SQL-like language called SRQL [66]. The method performs two types of reachability analysis, one based on the static routing information and other based on the dynamic routing information.

Also in the SHIELD project, Valenza et al. [67] proposes a formal approach to validate network policy enforcement in virtualized environments. This approach is based on monitoring and remote attestation techniques to perform online policy enforcement. To define the policies, the authors define a High Level Security Language (HLSL). The approach periodically checks the enforced HSPL rules. If a policy is wrongly enforced, an offline failure detection task is fired to determine the cause of the anomaly. Finally, the approach also includes remote attestation techniques to verify the trustworthiness of the VNFs and other components.

In [68], the authors present a methodology and a prototype to verify NFV-SDN networks. The proposal can verify different types or properties, such as inconsistencies due to delays during the update of the flow tables, or load balancing between VNF instances. The behaviour of the VNFs, the switches flow tables, and properties are described with a special process algebra

called pACSR [69] that are analysed with symbolic verification algorithms presented in previous works [70]. The prototype tool is placed between the SDN (OpenFlow) controller (or VNF orchestrator) and the NFV infrastructure, and is able to automatically extract the pACSR model from the NFV descriptions, including the SDN and NFV operations, the flow tables, the network topology and the resources states.

ChainGuard [71] is a tool developed in the SENDATE [177] project to verify Service Function Chains (SFC) independently of the cloud management platform. To this end, ChainGuard checks that the SFC rules stored in the switches' flow tables, conforms to the implemented/real SFC overlay and traffic steering using static verification. In order to deal with service migration, ChainGuard reruns the verification after detecting changes in the switches' flow tables, but performs an incremental verification; that is, it verifies just the parts affected by the flow table changes.

There are other research works dealing with SFC verification. For example, in [72] the authors propose a formal model of SFC base on functions, which can be used to verify the correct enforcement of security policies. The model is able to describe only a single SFC, and how network/service functions transform packets, and the policies that must be enforced. The authors also propose an algorithm to perform the analysis of the model against the policies, but no implementation has been presented.

SFC-Checker [73] is a prototype tool that performs static analysis of stateful SFC forwarding behaviour. To this end, the authors propose a new abstract model of the network function (NF) that combines the NF flow tables and a state machine describing the different possible states of the NF. In addition, the OpenFlow rules are extended in order to include information of the NF state. For instance, to match a rule, the NF must be in a particular state, or when applying a rule, it can trigger a state transition. SFC-Checker transform the flow tables and the state machines into a Stateful Forwarding Graph. The authors have designed several graph traversal algorithms to answer state-dependent reachability questions. Initially, the tools perform pre-deployment verification, but the authors planned to extend the prototype to real-time verification, by pulling states directly from network functions.

Testing has also been used to ensure the correct behaviour of network functions and network. Buzz [74] is a model-based testing framework, which produces network test cases in order to test the correct implementation of policies and uncover errors in stateful network functions. Given the network operator policies, BUZZ explores a model of the data plane to find abstract test traffic; that is, abstract data packets that trigger the states of the model related to the policy. The abstract test traffic is later translated into concrete data packets that are injected in the actual data plane, and finally, it is possible to report if the policy under test is enforced or not. The data plane model is based on the composition of finite state machines, where each network function is modelled as a single state machine. The model is explored with a symbolic execution algorithm that integrates domain-specific optimizations in order to tackle the state space explosion problem.

In [75], the 5GTango project presents a NFV architecture that supports the DevOps methodology. The architecture integrates a verification and validation platform that allows pre-deployment testing of network and service functions. The tests are described in TTCN-3 language and can be executed in different testing infrastructures. The 5GTango project proposes the use of NFV catalogue where the network functions, and the results of the different test passed, are published.

The complete isolation of slices allows for simpler and more efficient design of each slice with the goal of meeting the requirements of the applications and services offered to the end users by the slice tenant. In addition, network failure, overload, or security attacks in one slice will not affect the operation of other slices in the network. The capability of dynamically creating a new

sub-slice as a security enabler, e.g. to isolate malicious behaviour [60], is one promising method studied in the 5G-ENSURE project to enhance the security capabilities in end-to-end platforms. Such micro-segmentation capability can be an important enabler for scenarios, where both network performance and security are required. In addition, multi-level isolation is expected to be needed as infrastructure sharing by multiple virtual network operators will require strict isolation at multiple levels to ensure absolute security.

3.5 Multi-Access Edge Computing (MEC)

The Multi-Access Edge Computing (MEC) technology allows moving application hosting from centralized data centres down to the network edge. It provides network, computing and storage resources at the edge of mobile networks, enabling the use of applications with tight resource requirements such as very low latency or high bandwidth.

MEC is a universal access technology targeting to applications with locality or low latency requirements. Examples of this are V2X applications. MEC is key for meeting the demanding KPIs of 5G.

MEC is considered a 5G technology since it provides specific 5G functionalities including: local routing and traffic steering; session and service continuity (SSC) modes for different user equipment and application mobility scenarios; the ability of an Application Function to influence user Plane Function selection and traffic routing (either directly through the Policy Control Function or indirectly through the Network Exposure Function); and support of a Local Area Data Network by the 5G core, by connecting to the Local Area Data Network (LADN) in a certain area where local applications are deployed.

However, it can also be used in 4G and, in fact, industry is moving to use MEC in existing 4G networks.

MEC enables the implementation of applications as software-only entities running on a virtualization infrastructure located at the network edge. According to ETSI GS MEC 003 [144], MEC entities can be grouped into system level, host level and network level entities (see overview in Figure 25 and detailed view in Figure 26)

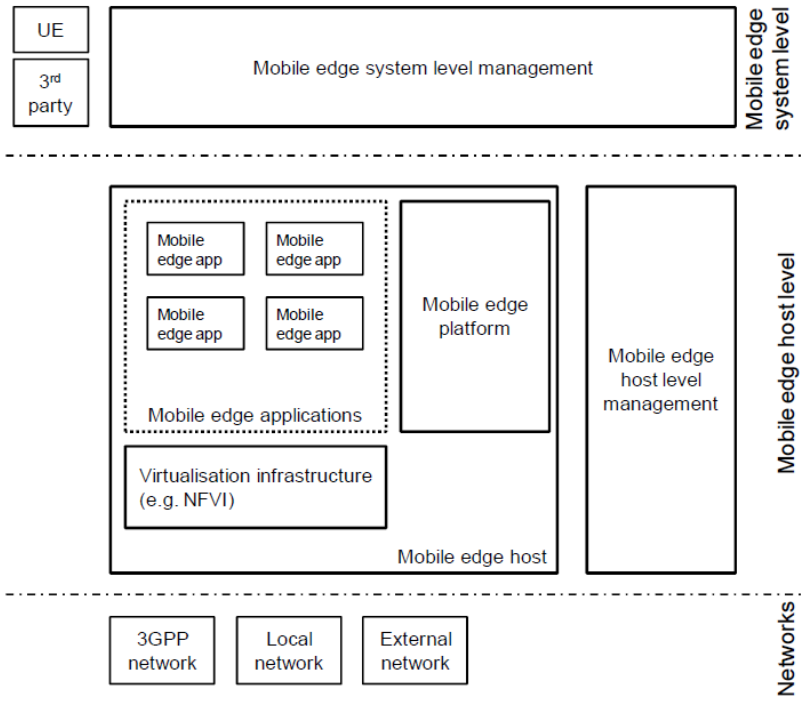


Figure 25. Grouping of MEC entities according to ETSI [144]

The mobile edge host contains a mobile edge platform, a virtualization infrastructure, where ME applications (Mobile Edge applications) can be instantiated, and the ME applications.

- The mobile edge platform provides the required functionality to run ME applications on a particular virtualization infrastructure and to provide and consume ME services.
- Virtualization infrastructure provides compute, storage, and network resources for running mobile edge applications (see Figure 23).
- Mobile edge applications are instantiated on the virtualization infrastructure of the mobile edge host, as detailed in Section 3.4.2.

The management of the MEC is performed at two different levels:

- The mobile edge system level management: Its main component is the mobile edge orchestrator, which has an overview of the complete mobile edge system.
- The mobile edge host level management handles the management of the mobile edge specific functionality of a particular mobile edge host and the applications running on it. It includes:
    - The mobile edge platform manager
        - Manages the life cycle of applications including informing the mobile edge orchestrator of relevant application related events;
        - Provides element management functions to the mobile edge platform;
        - Manages the application rules and requirements including service authorizations, traffic rules, DNS, configuration and resolving conflicts.
    - The virtualisation infrastructure manager
        - Allocates, manages and releases resources of the virtualisation infrastructure;
        - Prepares the virtualisation infrastructure to run a software image;
        - Facilitates rapid provisioning of applications (if supported);
        - Collects and reports performance and fault information about the virtualised resources;

- Performs application relocation (if supported).

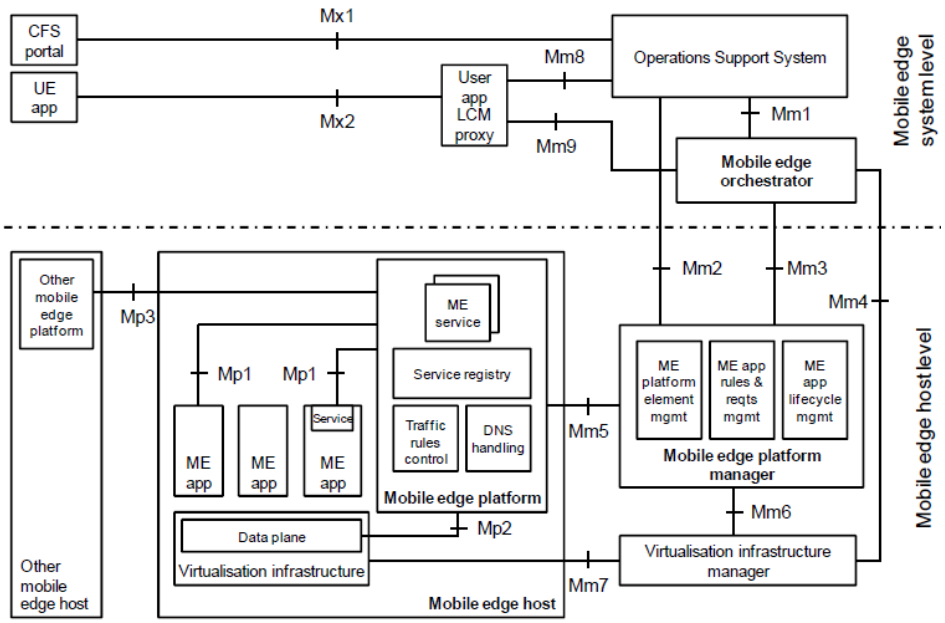


Figure 26. Details of MEC entities according to ETSI [144]

The ETSI standard defines all relevant reference points, between the Mobile edge host, and the rest of the MEC entities (see references points depicted in the overall architecture in Figure 27).

The Mobile edge platform reference points are:

Mp1: Mobile edge platform to mobile edge applications. This interface provides service registration, service discovery, communication support for services and other functionality such as application availability, session state relocation support procedures, traffic rules and DNS rules activation, access to persistent storage and time of day information, etc.

Mp2: Mobile edge platform to data plane of the virtualisation infrastructure. This reference point is used to instruct the data plane on how to route traffic among applications, networks, services, etc. However, ETSI does not specify this interface, as it is considering the Mp2 reference point to be based on vendor-specific solutions

Mp3: Interface between mobile edge platforms. It is used to control the communication between mobile edge platforms.

The Mobile edge management Reference points are:

Mm1: Triggers the instantiation and the termination of ME applications in the ME system.

Mm2: Used for the ME platform configuration, fault and performance management.

Mm3: Used for the management of the application lifecycle, application rules and requirements and keeping track of available ME services.

Mm4: Used to manage virtualised resources of the ME host, including keeping track of available resource capacity, and to manage application images.

Mm5: Used to perform platform configuration, configuration of the application rules and requirements, application lifecycle support procedures, management of application relocation, etc.

Mm6: Used to manage virtualised resources e.g. to realize the application lifecycle management.

Mm7: Used to manage the virtualisation infrastructure.

Mm8: Used to handle UE applications requests for running applications in the ME system.
Mm9: Used to manage ME applications requested by UE application.

The external entities Reference points are:

Mx1: Used by third-parties to request the ME system to run applications in the ME system.
Mx2: Used by a UE application to request the ME system to run an application in the ME system, or to move an application in or out of the ME system.

Moreover, it is worth noting that MEC and VNF mapping has been addressed by ETSI in [148]. It is assumed that the MEC app VNFs will be managed like individual VNFs, allowing that a MEC in NFV deployment can delegate certain orchestration and Life Cycle Management (LCM) tasks to the NFVO and VNFM functional blocks, as defined by ETSI NFV MANO.

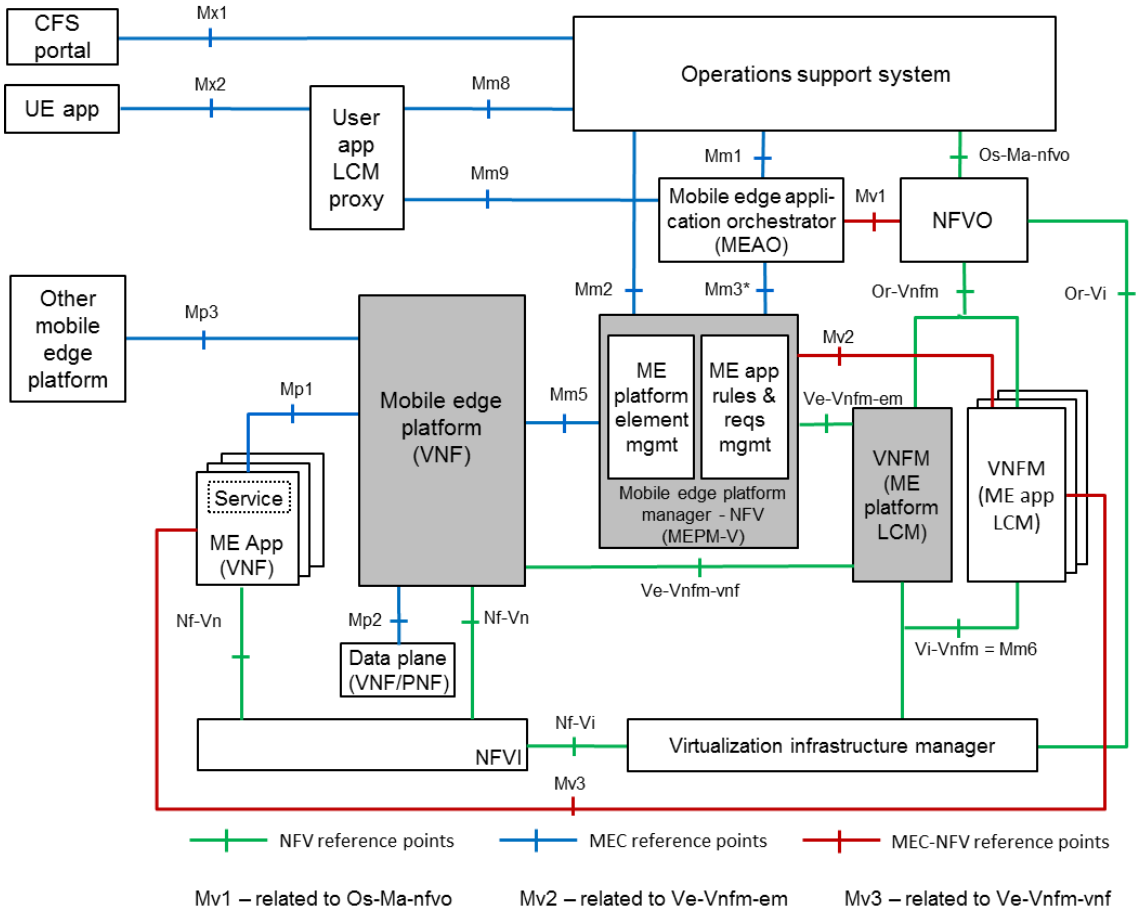


Figure 27 MEC reference architecture in a NFV environment

The following new reference points (Mv1, Mv2 and Mv3) are introduced between elements of the ETSI MEC architecture and the ETSI NFV architecture to support the management of ME app VNFs.

- Mv1: This reference point connects the MEAO and the NFVO. It is related to the Os-Ma-nfvo reference point, as defined in ETSI NFV.
- Mv2: This reference point connects the VNF Manager that performs the Life Cycle Management (LCM) of the ME app VNFs with the MEPM-V to allow LCM related notifications to be exchanged between these entities. It is related to the VeVnfm-em

reference point as defined in ETSI NFV, but will possibly include additions, and might not use all functionality offered by Ve-Vnfm-em.

- Mv3: This reference point connects the VNF Manager with the ME app VNF instance, to allow the exchange of messages e.g. related to the ME application LCM or initial deployment-specific configuration. It is related to the Ve-Vnfm-vnf reference point, as defined in ETSI NFV, but will possibly include additions, and might not use all functionality offered by Ve-Vnfm-vnf.

The management of MEC platform as a VNF is indicated in Figure 28.

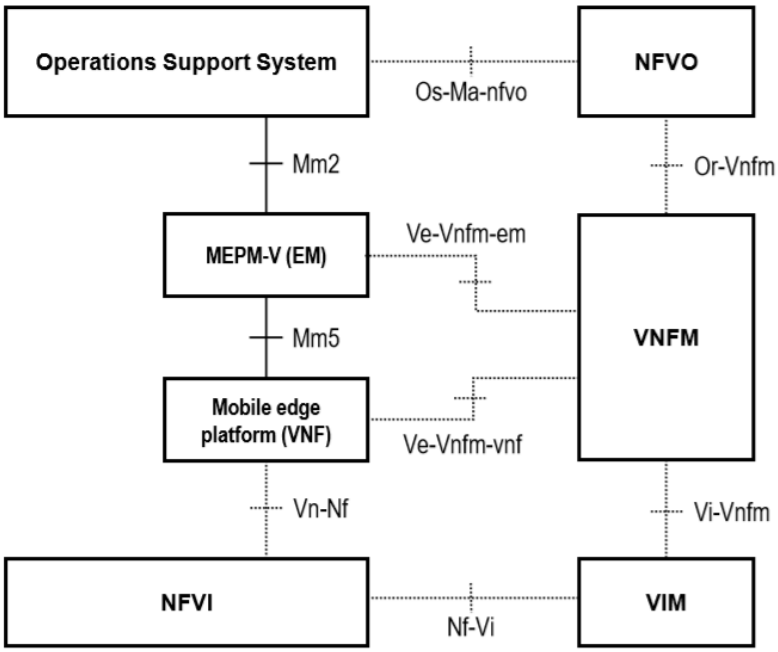


Figure 28. MEC deployed as VNF in the ETSI MANO framework [149]

When MEC is deployed in a NFV environment, there are two different possibilities to realize the Data Plane, both are valid and need to be supported:

- Realize the Data Plane as a Physical Network Function (PNF) or VNF or combination thereof, and connect it to the NS that contains the ME app VNFs
- Re-use the SFC functionality provided by the underlying NFVI for traffic routing. In such a deployment, the Data Plane as a dedicated component is not needed, and consequently, the Mp2 reference point does not exist. The SFC functionality in the NFVI will be configured by the NFVO in the VIM based on the NFP of the NFV NS, using the Or-Vi reference point

In the approach considered above, ME applications appear as VNFs so that ETSI NFV MANO functionality can be re-used. The MEC 017 specification [149] highlights that there is a need to analyse how MEC-specific files can be carried inside the VNF package without interfering with the existing package content, and how these can be identified by the MEC management and orchestration components. The document further analyses the similarities between VNF and App meta data and although a lot of similarities can be found, the AppD models much more detailed requirements to the infrastructure and service availability than the VNFD.

3.5.1 MEC ARCHITECTURE IN 5G

Figure 3 shows the basic 5G architecture (non-roaming case) as specified by 3GPP TS 23.501 [145], and Figure 29 illustrates a typical MEC implementation inside the 5G architecture.

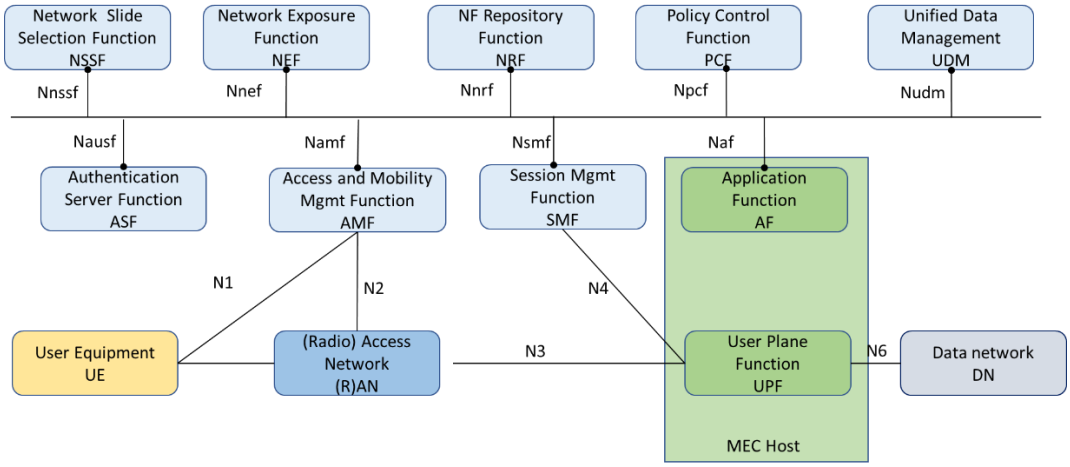


Figure 29. MEC Host in a 5G Architecture

The design approach taken by 3GPP allows the mapping of MEC onto Application Functions (AF) that can use the services and information offered by other 3GPP network functions based on the configured policies.

A number of enabling functionalities have been defined to provide support for different deployments of MEC and to support MEC in case of user mobility events.

In the 5G system specification, as aforementioned in section 3.1, there are two options for defining the architecture:

- Traditional, based on reference points and interfaces.
- Service Based Architecture (SBA), where the core network functions interact with each other.

In SBA, there are functions that consume services and others that produce services. The framework provides the necessary functionality to authenticate the consumer and to authorize its service requests. For simple service or information requests, a request-response model can be used. For any long-lived processes, the framework also supports a subscribe-notify model. Likewise ETSI [146], [146] defines an API framework for MEC (using the same SBA principles), specifying the use of the services such as registration, service discovery, availability notifications, de-registration and authentication and authorization.

A MEC application, i.e. an application hosted in the distributed cloud of a MEC system, can belong to one or more network slices that have been configured in the 5G core network.

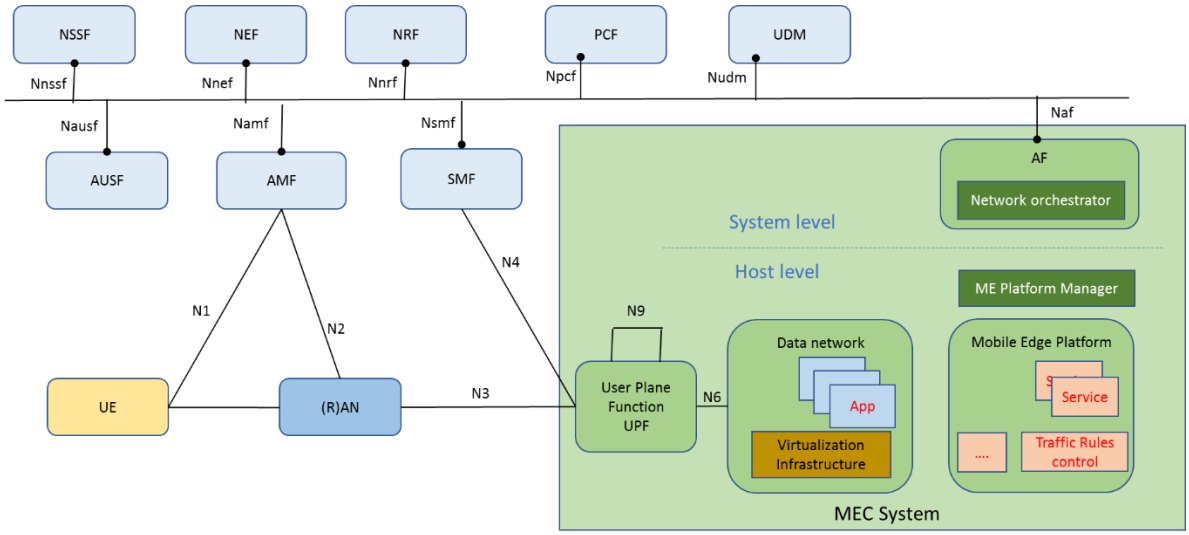


Figure 30. Integrated MEC deployment in a 5G network

UPFs can be seen as a distributed and configurable data plane from the MEC system perspective. The local UPF may even be part of the MEC implementation.

The MEC orchestrator is a MEC system level functional entity that, acting as an AF, can interact with the Network Exposure Function (NEF), or in some scenarios directly with the target 5G NFs. On the MEC host level it is the MEC platform that can interact with these 5G NFs, again in the role of an AF. An instance of NEF can also be deployed in the edge to allow low latency, high throughput service access from a MEC host. SMF exposes service operations to allow MEC, as a 5G AF, to manage the PDU sessions, control the policy settings and traffic rules as well as to subscribe to notifications on session management events.

MEC deployment

MEC hosts are deployed in the network edge or close to the edge. The User Plane Function (UPF) takes care of steering the user plane traffic towards the targeted MEC applications in the data network.

Network operators decide where to locate the data networks and the UPF depending on business and technical requirements. The MEC management system, orchestrating the operation of MEC hosts and applications, may decide dynamically where to deploy the MEC applications.

ETSI White Paper No. 28 “MEC in 5G networks” [147] shows some of the possibilities for physical location of MEC systems:

1. MEC and the local UPF collocated with the Base Station.
2. MEC collocated with a transmission node, possibly with a local UPF.
3. MEC and the local UPF collocated with a network aggregation point.
4. MC collocated with the Core Network functions (i.e. in the same data center).

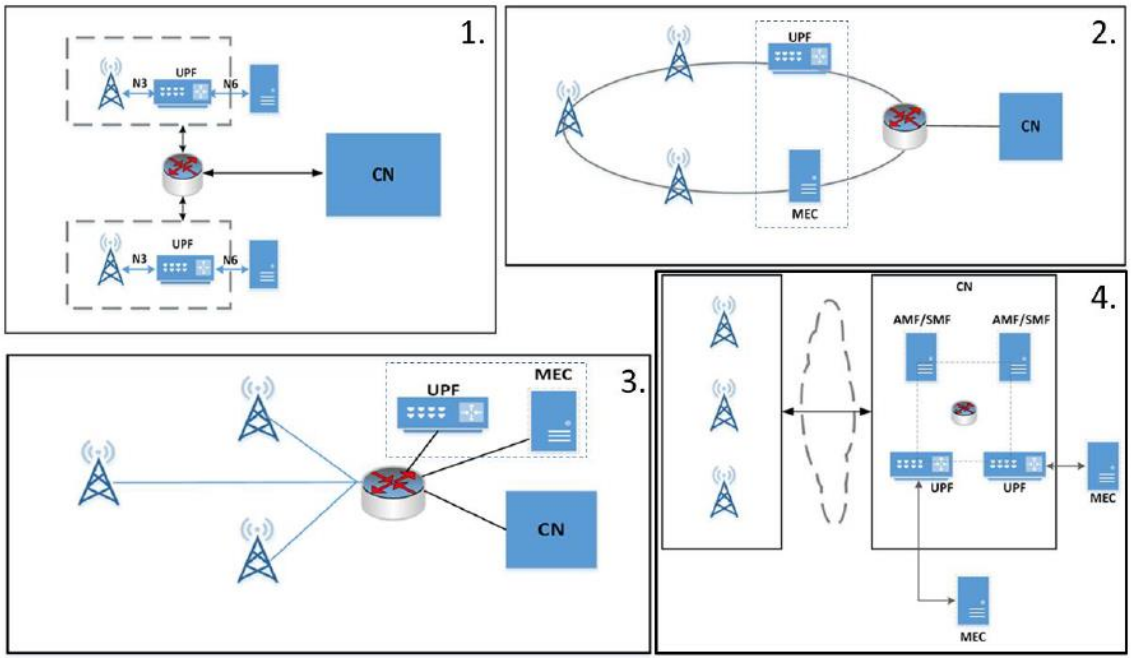


Figure 31. MEC locations in a 5G network [148]

3.5.2 MEC ARCHITECTURE IN 4G

There are several ways to deploy MEC hosts in 4G architectures. The most relevant ones are detailed below, i.e.:

- bump in the wire
- distributed EPC
- distributed SGW and PGW
- distributed SGW with Local Breakout.

All these scenarios can also be deployed according to the CUPS (Control-User Plane Separation) paradigm incorporating a new user plane in the MEC host.

3.5.2.1 Bump in the wire (LTE)

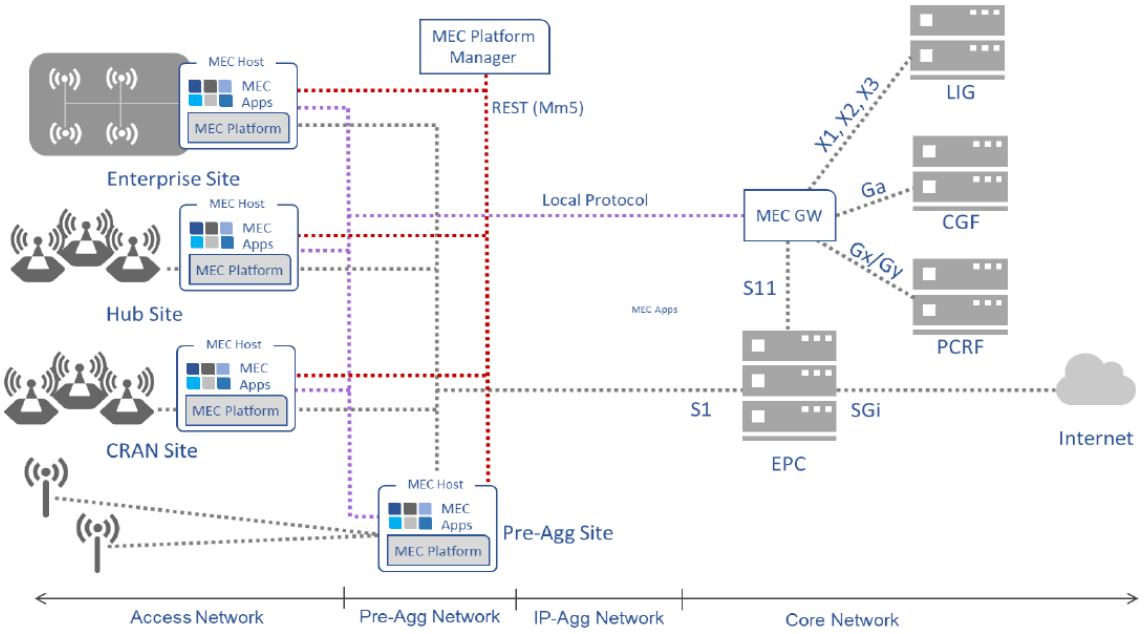


Figure 32. 4G MEC deployment using 'bump in the wire' approach (MEC between base station and CN) [169]

The architecture shown in Figure 32 is appropriate to facilitate intranet traffic to breakout to local services (the session connection is redirected to a MEC application, hosted typically on the MEC), and in architectures where MEC is co-located with C-RAN deployments.

3.5.2.2 Distributed EPC

The MEC deployment incorporates some or all the logical components of the LTE EPC (see Figure 33 and Figure 34). The MEC data plane is located on the SGi interface. In this scenario, the LTE network PGW assigns the user an IP address and local DNS information to resolve the MEC applications' IP address. In this deployment, the communication with the core network site is not mandatory. Accordingly, it is convenient for first responders, public safety, and mission critical industrial sites.

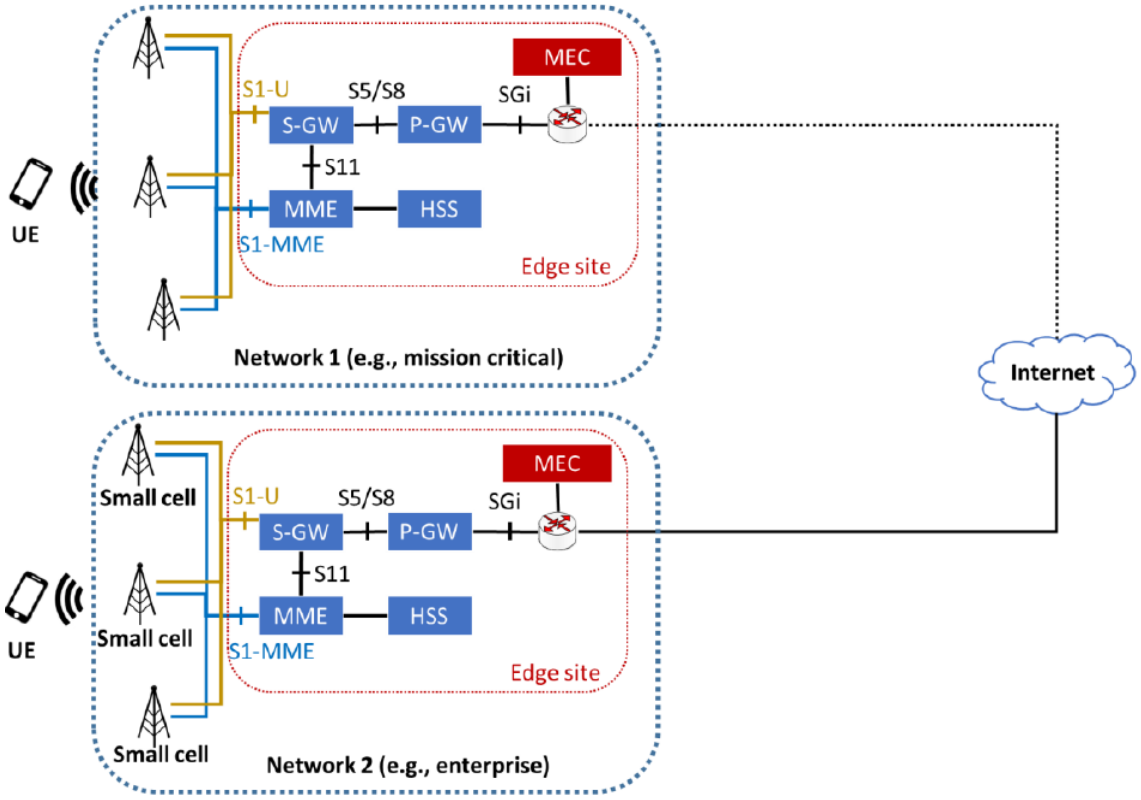


Figure 33. MEC deployment with distributed EPC [169]

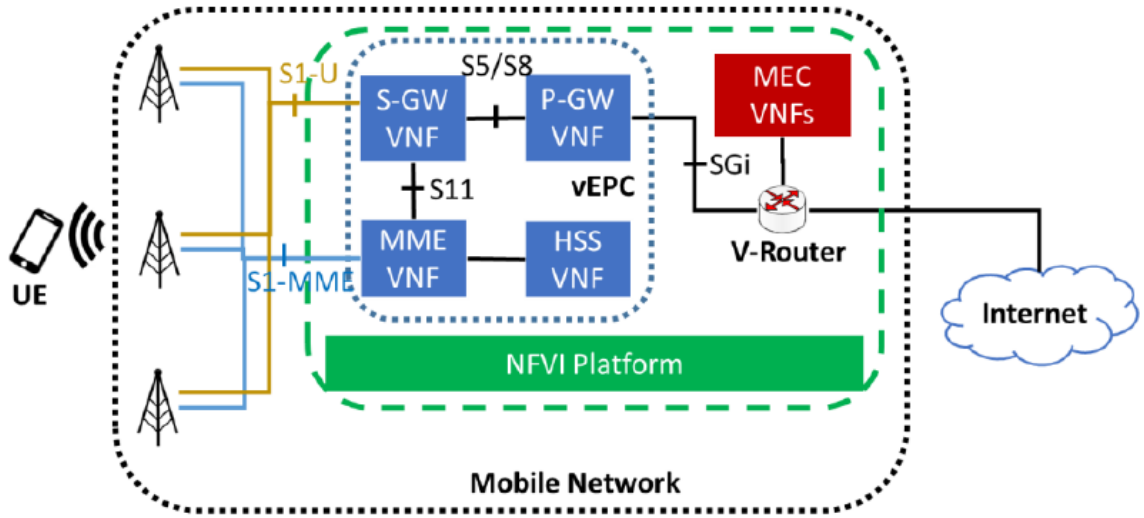


Figure 34. MEC deployment with EPC and MEC application on the same NFV platform (same MEC host) [169]

3.5.2.3 Distributed SGW and PGW

The MEC deployment incorporates the SGW and the PGW elements of the LTE EPC. The other EPC elements are located in the 4G core network site, including the control plane elements MME and HSS. The MEC data plane is also located on the SGi interface.

This architecture allows offloading the traffic based on the Access Point Name (APN).

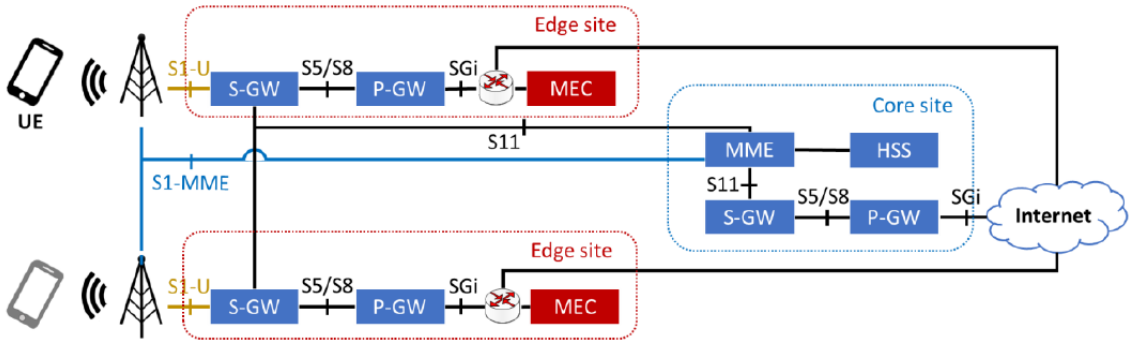


Figure 35. S-GW and P-GW MEC deployment [169]

3.5.2.4 Distributed SGW with Local Breakout

In the MEC deployment, the SGW is located in the MEC host. The session connection is redirected from the SGW to a MEC application running in the MEC host (typically on the same NFV platform than the local breakout-SGW.

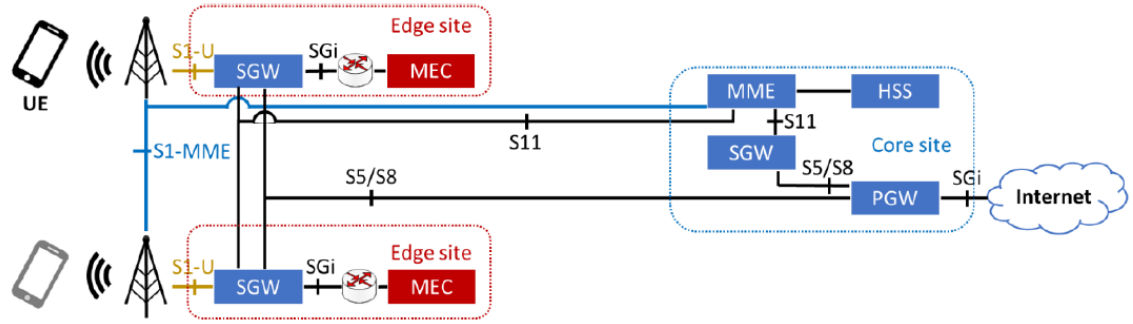


Figure 36. SGW-LBO MEC deployment [169]

3.6 Overview of most relevant MEC/FOG R&D projects

3.6.1 5G Coral

The 5G-CORAL system aims to address the ultra-low latency requirements of emerging 5G applications by leveraging the concept of "intelligent edge" to provide networking, computing, and storage capabilities closer to the end users. This is realized through an integrated and virtualised networking and computing solution where virtualised functions, user and third-party applications, and context-aware services are blended together to offer enhanced connectivity and better quality of experience. An integral part of the 5G-CORAL system is the distributed Edge and Fog Computing System (EFS) that offers a shared hosting environment for virtualised functions, services and applications [182].

The 5G-CORAL system constitutes two major building blocks, namely (i) the Edge and Fog Computing System (EFS), containing edge and fog computing substrates offered as a shared hosting environment for virtualised functions, services, and applications; and (ii) the Orchestration and Control System (OCS), responsible for managing and controlling the EFS, including its interworking with other (nonEFS) domains (e.g., transport and core networks, distant clouds, etc.).

This project defines number of use cases for demonstrations, one of them is interesting in the scope of EuWireless project, named "IoT multi-RAT Gateway". To implement this use case, technology-agnostic access points are deployed, offering IoT connectivity. The access point (AP) acts as a radio front-end, but signal modulation/demodulation as well as the rest of the communication stack is decoupled and running in the EFS. The AP collects low-level physical-

layer information (IQ samples as well as metadata) and makes it available through an EFS service. This is fed to the communication stack, performance enhancing functions, as well as to the localization function. Examples of performance enhancement functions include channel blacklisting and scheduling. Localization will exploit rich, low-level radio signals. This location data is used by the User Navigation and Object Localization applications.

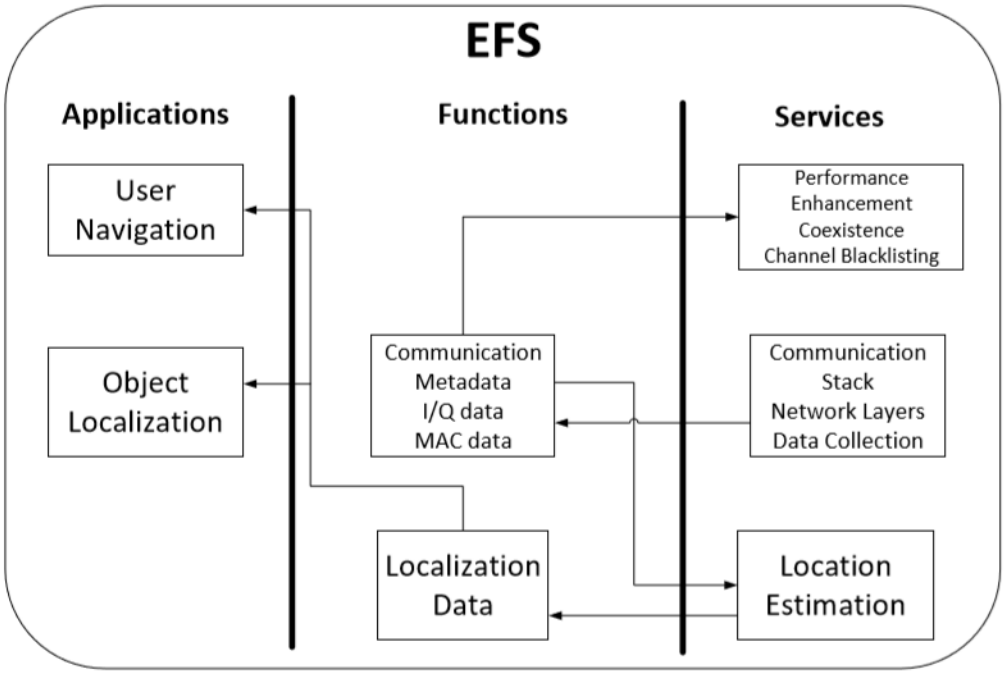


Figure 37. IoT multi-RAT gateway

The Multi-RAT communication stack implements the IoT communication layers (L1, L2, etc.) and related functions (e.g. management and control functions). Each of them acts as a virtualised modem for one IoT technology, same as the C-RAN concept (cloudifying the baseband functions). Examples of IoT technology under considerations are IEEE 802.15.4 (both nonbeacon-enabled and TSCH), NarrowBand-IoT, and Bluetooth LowEnergy (BLE), as well as LoRa [14]. It is interesting to note that in a "connected car" use case the edge cloud, in vehicle processing or RSU processing, is treated as fog nodes.

3.6.2 5G Norma and 5G Monarch

5G Norma is a finished 5GPPP (Phase1) project that was dealing with an architecture supporting slicing and intelligent RRM for the 5G systems. Currently the follow-up project 5G Monarch (5GPPP Phase2) is continuing the work undertaken by the NORMA consortium.

In [183], three options for RAN slicing considered by 5G NORMA. These three options differ by the degree of freedom offered for slice-individual customization, as well as the required complexity for implementation:

- Slice-specific RAN
- Slice-specific radio bearer
- Slice-aware shared RAN

It is worth noting that in comparison to the 3GPP specs, 5G NORMA has more extensive considerations on SDN/SDMC-enabled architectures and flexible multi-service and multi-tenancy supports via means of network slicing, resulting in a more centralized SDMC based architecture. The [184] describes the 5G Norma extensions to the ETSI MEC architecture in order to be able to integrate MEC with slice monitoring capabilities at the level of MEC

applications. The role of such modification is to be able to trigger network reconfigurations (e.g. slice updates) once predefined triggers apply.

3.6.3 MEC/FOG related standardization summary

Currently there are several COTS (Commercial off-the-shelf) solutions, as well as open-source frameworks, that already support MEC/Fog. As regards standardization, ETSI is clearly the source of MEC related specifications as described above. In the domain of Fog, the OpenFog alliance is the most active group that currently leads the fog standardization. The small footprint solution for the fog capable systems is provided by the Fog05 initiative, which is co-developed by organizations participating in the 5G Coral project. Fog05 implements part of MANO and enables deploying virtual programmes and life cycle management, but has no orchestration capability. Although the fog standardization is currently gaining its momentum, and activities in this domain are very active, it is still in its preliminary phase with strong standardization efforts promoted by OpenFog Alliance. Also, it seems that the MEC and fog approaches are not yet fully aligned. More time is needed to keep monitoring the situation related to both paradigms (as ETSI plans to release next phase of standards for the MEC). Some of the COTS MEC solutions, such as Advantech MEC, Saguna MEC, NOKIA MEC or Intel NEV, would require further analysis as regards their functionalities – still one has to remember that ETSI has also released reference implementation of the MEC APIs, which can be utilized for developments related to MEC.

3.7 APIs for Function Exposure

This section provides an overview of the standards APIs specified to interact with the network components of a mobile network.

3.7.1 Service Capability Exposure Function

SCEF (Service Capability Exposure Function) was introduced in the 3GPP technical report 23.708 “Architecture enhancements for service capability exposure”, Release 13 [165]. The SCEF provides a means to securely expose the services and capabilities provided by 3GPP network interfaces. It also provides a means for the discovery of the exposed service capabilities and access to network capabilities through homogenous network application programming interfaces (e.g. Network API) defined by OMA, GSMA, and possibly other standardisation bodies. The SCEF abstracts the services from the underlying 3GPP network interfaces and protocols.

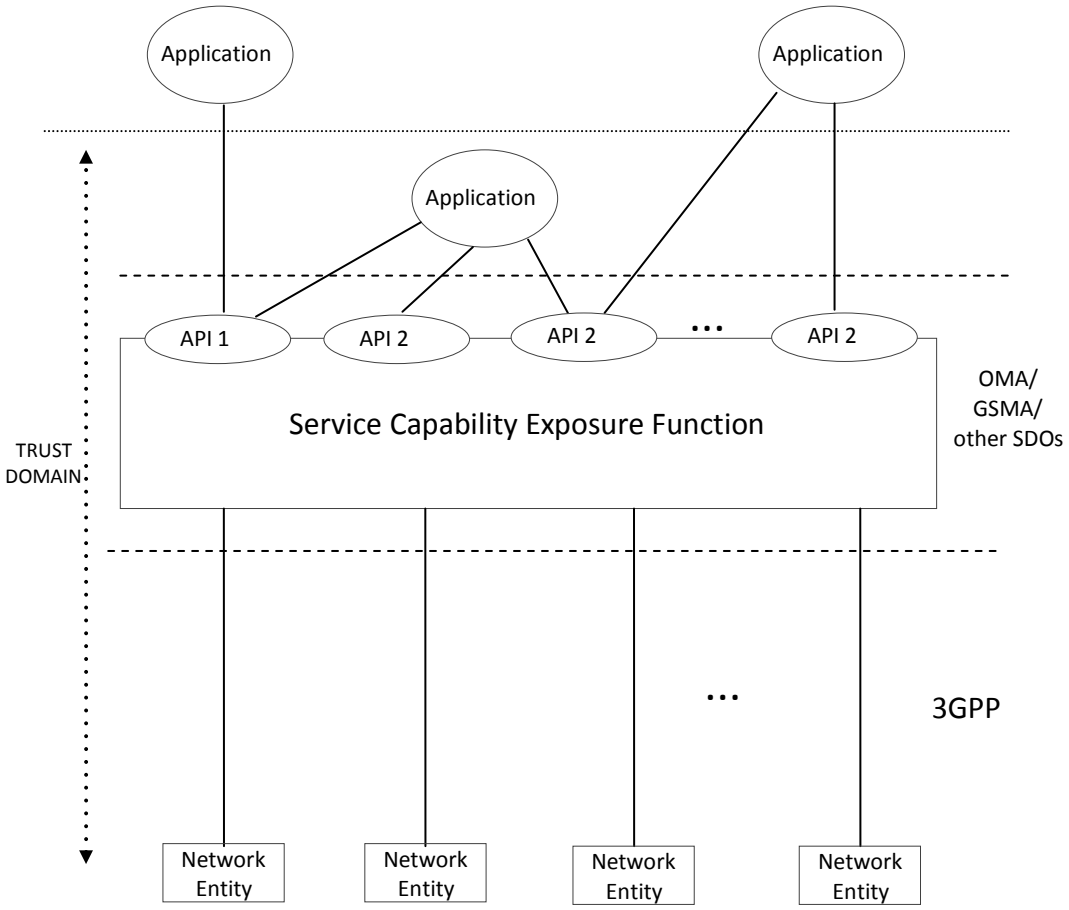


Figure 38. SCEF Architecture [165]

The APIs exposed through SCEF [165] to third parties are:

- Monitoring (e.g. loss of connectivity, IMSI-IMEI association, location, etc.)
- Non-IP Data Delivery
- Device Triggering
- Group Message Delivery
- Communication Pattern provisioning
- Packet Flow Description Management
- Setting-up QoS sessions
- Resource management of Background Data Transfer

3.7.2 Network exposure function

An important part of 5G is creating a network platform that is open to multiple industries for diverse services. This means these customers should be able to consume, and interact with, the network. This is addressed in 3GPP by the Network Exposure Function (NEF), that acts as an API gateway and allow external users the ability to monitor, provision and enforce application-level policies for users inside the operator network. NEF and the associated Nnef interfaces (Service-based interface exhibited by NEF), shown in Figure 39, are being specified in TS 23.501 in Release 15 [7].

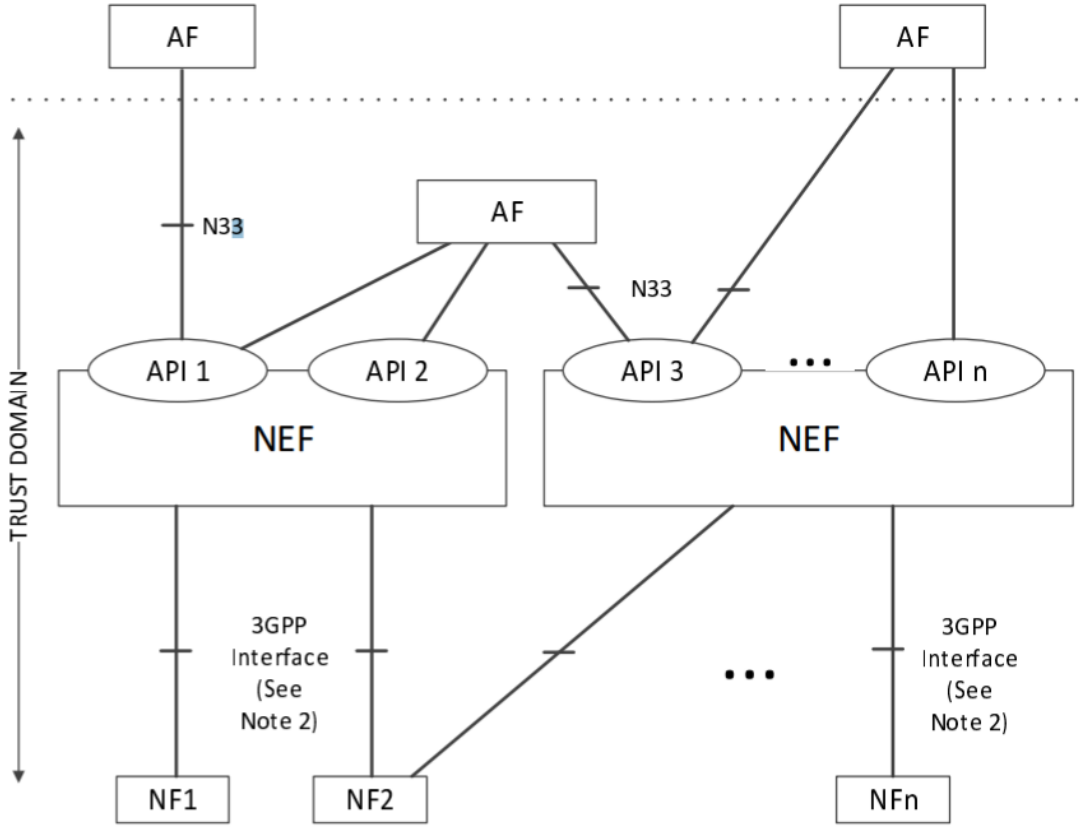


Figure 39. NEF in a reference point representation [7]

The APIs exposed through NEF are:

- Monitoring
- Device Triggering
- Communication Patterns provisioning
- Packet Flow Description Management
- Resource management of Background Data Transfer
- Procedures for Traffic Influence

3.7.3 CAPIF

The Common API Framework for 3GPP Northbound APIs (CAPIF) is being specified in 3GPP TR 23.722 in Release 15 [166]. In this specification, a Northbound API is an interface between an application Server (either in a mobile operator's network or external to it - operated by a third party) and the 3GPP system via specified Functions in a mobile operator's network. CAPIF considers the development of this Northbound APIs specifying common capabilities so that all Northbound APIs work similarly.
The relationship between the CAPIF and the 3GPP functionalities is the following [166]:

- CAPIF can be adopted by any 3GPP functionality providing service APIs;
- AEF represents an instance of service API exposure functions e.g. SCEF;
- CAPIF core functions are an evolution of some of the capabilities exposed by the northbound APIs (e.g. authentication, authorization, discovery, API management function); and

- Mapping specific APIs onto appropriate network interfaces is an internal implementation issue of the entity exposing the northbound APIs and is out of scope of the CAPIF.

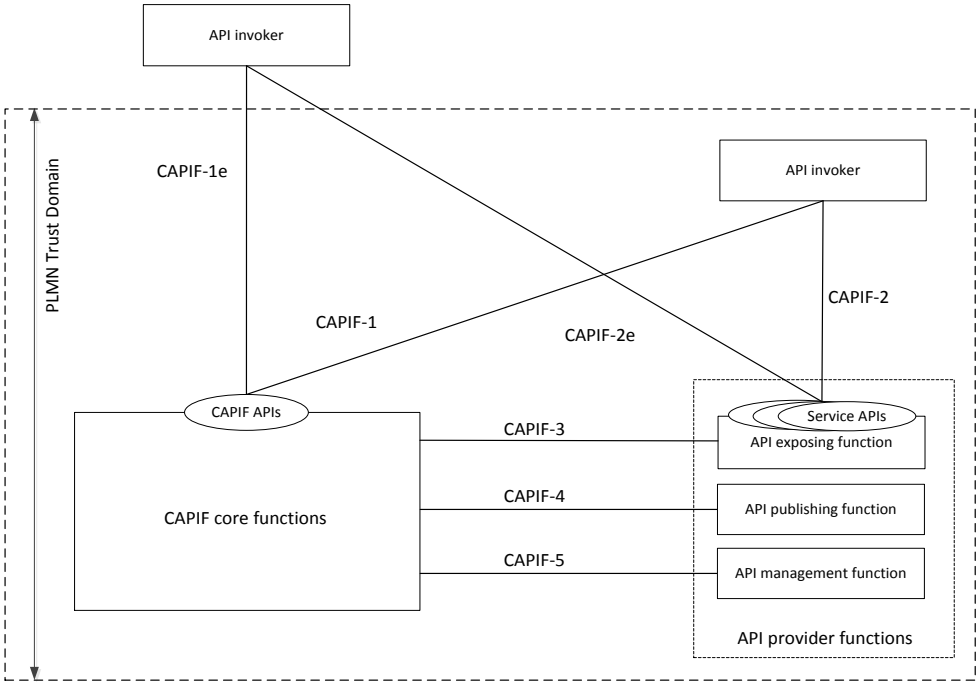


Figure 40. CAPIF Architecture

3.7.4 API Exchange GSMA

The API Exchange serves to bridge the gap between application providers' needs and operators' capabilities through cross-operator cooperation. It provides the required cross-operator capability while preserving the flexibility of individual operators to directly address its developer base, innovate on APIs in a fast and market-oriented manner, and differentiate in the market place.

The functions exposed through the GSMA APIs are:

- Federated User Profile
- Open ID connect
- Multi-factor
- Consent Management
- Context Charing
- Social Linking

3.7.5 OMA SpecWorks API

The OMA SpecWorks API program provides standardized interfaces to the service infrastructure residing within communication networks and on devices. Focused primarily between the service access layer and generic network capabilities, OMA SpecWorks API specifications allow operators and other service providers to expose device capabilities and network resources in an open and programmable way to any developer community independent of the development platform. By deploying APIs, fundamental capabilities such as SMS (Short Message Service), MMS (Multimedia Messaging Service), Location Services, Payment and other core network assets are now exposed in a standardized way. This reduces development

cost and time-to-market for new applications and services, as well as simplifies wider deployment of existing applications and services.

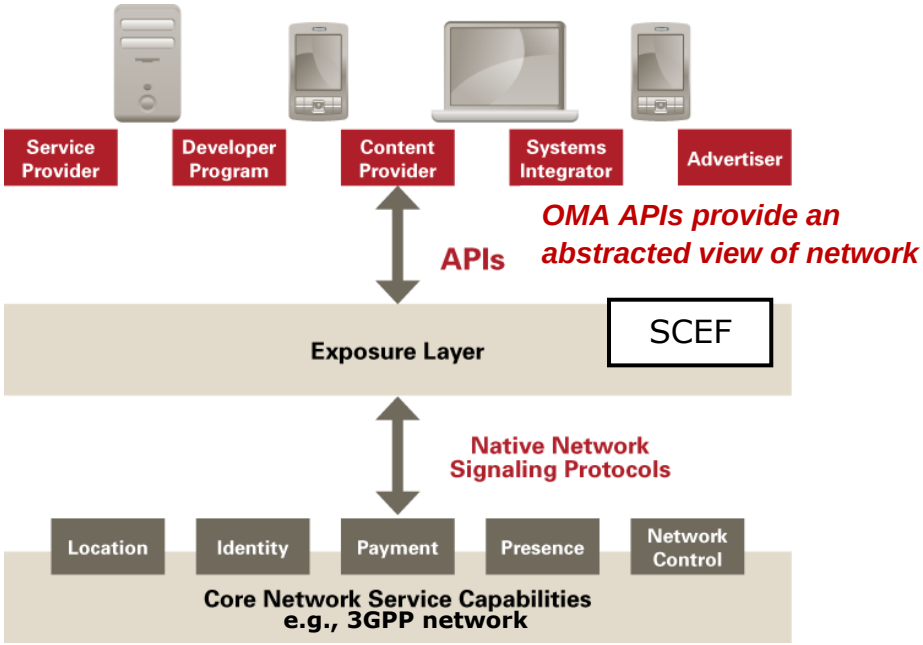


Figure 41. OMA APIs

OMA API landscape spreads across various dimensions ([166]):

- Abstract APIs: Focus on functional aspects and protocol independent aspects i.e., does not include a specific protocol binding for its operations;
- API binding technologies: SOAP/WSDL web services, HTTP protocol binding using REST architectural style; and
- Network API: exposed by a resource residing in the network.

The APIs exposed are:

- Terminal location
- Presence
- Payment
- Multimedia
- Messaging
- Device capabilities
- Call control APIs

4 Sharing the network resources and infrastructure

The resources in a mobile network include the spectrum and all the hardware and software components of the architecture. Following the idea of sharing the MNO network with the researchers, this section provides a detailed description of the sharing techniques from the lowest level, the spectrum, to the highest one, the applications. Most of them are methods to be effectively deployed in 5G networks.

4.1 Spectrum sharing

Dynamic spectrum access, in the form of spectrum sharing, could potentially open new opportunities for mobile operators to exploit spectrum bands whenever their owners underutilize them, and it has received considerable amount of attention form the academia, regulatory bodies and governments. The classification of the spectrum access methods can be done in different ways. This deliverable uses a taxonomy based on the licencing policy (authorization regimes) as presented in [93]. Thus, the spectrum access methods are classified into licensed access, light licensing, and license-exempt access.

4.1.1 Licensing and Authorization

Here, different licensing and authorization methods related to spectrum sharing are presented. First, the authorization methods based on individual authorization are given, then the light licensing methods are presented, and finally the general authorization methods are discussed.

4.1.1.1 Individual Authorization (a.k.a. Licensed Access)

In licensed access, the National Regulatory Authority (NRA) usually grants the right of access to a particular part (or parts) of the spectrum, referred to as licensed bands, to an MNO on exclusive basis. The licensed bands are usually granted to MNOs for a particular time through an auction.

Besides exclusive licensing to a MNO, which is the prevailing method to utilize licensed spectrum, different levels of shared access to the licensed bands can be granted. These frequency-sharing schemes can be classified into dedicated access, co-primary shared access, and licensed / authorized shared access (LSA). They are shortly presented below.

Dedicated access

As stated above, dedicated access is the prevailing method for utilizing the spectrum in mobile networks. In dedicated access, only the license holder, i.e. one MNO, can operate on the frequency band. Naturally, the spectrum resource is wasted if the license holder is not using the frequency band whilst other service providers might face capacity shortage. However, this access model is advantageous to the license holder, as there will be no other interfering systems operating in such bands. This assures that the QoS requirements can be met, and MNO's access to the spectrum is guaranteed.

Co-primary Shared Access

In co-primary shared access, the license holders use their licenced spectrum jointly in a shared manner through mutual agreements, subject to the permission of the respective NRA. In this access method, the MNOs have equal access rights to the spectrum, without priorities set by the regulation [94]. Co-primary shared access can be further divided into spectrum pooling and mutual renting [95].

In spectrum pooling, the NRA allocates licensed bands into a limited number of MNOs instead of dedicated allocation to a certain MNO. This allows the MNOs to acquire additional licensed bands on shared basis when needed, thereby improving the spectrum utilization efficiency. The spectrum access is coordinated via bi/multilateral agreements between MNOs to prevent

aggressive or un-coordinated access of the spectrum. However, it might be that the capacity requirements of the MNOs are not met in the case of multiple MNOs accessing the spectrum simultaneously. However, when used together with their own dedicated licensed spectrum, this access scheme can be seen as a complimentary opportunity to fulfil their capacity and QoS needs with considerably lower license fee compared to auction-based licenses.

In mutual renting, licensed bands, which have been allocated to an MNO on an exclusive basis, can be rented to another MNO subject to a permission of the respective NRA. By this arrangement, an MNO is provided with an opportunity to improve its revenue with the help of its temporarily unutilized spectrum. This scheme is also advantageous to the MNO that is facing a temporary capacity shortage and requires additional spectrum resources to accommodate high capacity or QoS needs. However, in this access method the spectrum owner has pre-emptive priority to its own spectrum at any time, in contrast to the spectrum pooling. Therefore, this access scheme can be seen more beneficial in the case where the spectrum is expected to remain unutilized for long periods of time by the license holder, or in the case of instantaneous spectrum opportunity detection taking advantage of the traffic diversity [96][97].

Licensed / Authorized Shared Access (Vertical Sharing)

This sharing scheme can be categorized as Authorized Shared Access (ASA), LSA and Spectrum Access System (SAS).

ASA is aimed for International Mobile Telecommunications (IMT) bands, initially 2.3 GHz in the U.K. and 3.8 GHz in the U.S. It is assumed to be used in shared and non-interference basis for mobile services [95] [98].

LSA is an extension of ASA concept, proposed by Conference of European Postal & Telecommunications, Electronic Communications Committee (CEPT ECC) [99]. It aims in facilitating the use of favourable licenced bands for mobile communications in a fully harmonized manner and under licensing regime, with the purpose of improving efficiency of spectrum usage efficiency. Compared to dedicated access, LSA also aims to provide the individual users with a lower spectrum license fee. According to this access scheme, a non-mobile communication license holder, referred to as incumbent, can share spectrum with one or more mobile communications systems under certain rules and in non-interfering basis. The details of such arrangements are subject to individual agreement between the incumbent and the MNOs and the permission is granted by the respective NRA [100][101].

In Europe, the current candidate channels for LSA are 2.3 - 2.4 GHz, but the future deployments of LSA are expected to go beyond IMT bands and will not be limited to mobile network use only [102]. Although ASA and LSA essentially refer to same paradigm, some differences between them can be found [99][100]. For example, ASA can be seen as a special case of LSA where the licensee is an MNO. Also, the requested level of authorization in ASA remains open without any specific clarification. In addition, the target bands in ASA are only suitable for mobile communications while LSA is targeted for as many bands as possible and it is supposed to support different types of spectrum users.

SAS is rather similar framework to LSA, but it is defined by Federal Communications Commission (FCC) and targets currently the 3.55 - 3.7 GHz bands to improve spectrum utilization efficiency. Unlike in LSA, however, three tiers are specified. Similar to LSA, the first tier is the incumbent system. Second tier is called Priority Access License (PAL), which can be an MNO. The third tier is referred to as General Authorized Access (GAL), which provides lower access guarantees than the PAL. The level of interference protections between the tiers is reduced top down, and similar to LSA, SAS offers lower license fee than exclusive access. For example, the Citizens Broadband Radio Service (CBRS) proposed for the 3.5 GHz band in the U.S., utilises SAS and spectrum sensors for spectrum management and incumbent protection.

Incumbent access users include authorized federal and grandfathered Fixed Satellite Service users currently operating in the 3.5 GHz band. These users will be protected from harmful interference from PAL and GAL users.

4.1.1.2 Light Licensing

The term light licensing refers to a simplified and more flexible regulatory framework of issuing spectrum authorizations compared to fully exclusive authorization, usually targeted to the frequency bands where the risk of interference is low [103]. However, some interference avoidance is expected to protect the already existing users. Example target bands considered to be reasonable for this access method are 60 GHz and 80 GHz bands, whose propagation characteristics facilitate the use with minimum risk of interference. In the U.K., the 5.8 GHz band has been also introduced as a candidate band for this access method [104]. In addition, the bands in 24 - 27 GHz and 64 - 66 GHz have been cleared for the use in backhaul and small cells in South Korea [105]. This type of access falls between the individual and general authorizations in a way that based on different sharing parties, it can lie in either individual or general authorization regimes.

4.1.1.3 General Authorisation (a.k.a. Unlicensed or License-Exempt Access and Opportunistic Access)

The term license-exempt access or unlicensed access is defined where a set of users co-exist and are able to utilize a specific frequency bands opportunistically with equal priority rights [103][106]. The bands can range from licensed to unlicensed bands such as narrowband licensed television white space (TVWS) and WiFi bands in 5GHz. However, the users operating on this licensing regime must comply with the general technical regulations defined for the bands, and be certified. Although the interference protection is minimal or non-existent, also the spectrum cost is very low or zero [103].

Cognitive Radio Networks (CRNs) fall under this authorization regime. For CRNs, many opportunistic spectrum access (OSA) and dynamic spectrum access (DSA) methods have been proposed based on prioritization of the users into primary and secondary hierarchies. Also, various enabling technologies have been studied for CRNs, such as spectrum sensing techniques [107], geo-location databases, beacon signalling, etc. [108]. The characterization of access methods in this authorization regime can be categorized into secondary horizontal shared access, unlicensed shared access, and unlicensed primary shared access.

Secondary Horizontal Shared Access

In secondary horizontal shared access, primary users among a diverse set of secondary users share the licensed bands in opportunistic and horizontal manner. This means that the access guarantees and interference guarantees are low. Currently, the associated bands comprise 2.4 GHz and 5GHz industrial, scientific, and medical bands.

Unlicensed Shared Access

In unlicensed shared access, license-exempt frequency bands have been authorized to be used by various types of users or services with equal access rights. The utilization of these bands are subject to specific transmission power constraints in order to protect the users from the interference, however, low or no other interference protection and access guarantees are offered. The idea of extending LTE-A to operate in license-exempt bands (see [109] and section 3.3.1 for more information) belongs to this access method category.

Unlicensed Primary Shared Access

In unlicensed primary shared access, bands are generally authorized so that all the valid technologies are permitted to them simultaneously. An example of this is access method is co-

existence of Digital European Cordless Telecommunications (DECT) in 1880 - 1900 MHz as primary user via mobile service allocations [110].

Use of 5G NR in unlicensed spectrum is being studied by 3GPP as part of Release 16 efforts. Results of this study are reflected in 3GPP document TR 38.889, which considers regulatory requirements (initially focused on 5 GHz band), spectrum considerations, deployment scenarios, design solutions (including the required adaptations in physical and higher layers) and performance evaluations. Coexistence with other technologies such as Wi-Fi are also considered.

Some of the proposed solutions have already been considered by other unlicensed spectrum technologies such as MulteFire, for example the use of Listen Before Talk (LBT) mechanism, which is a mandatory feature according to regulations applicable in some ITU regions.

Provided that use 5G NR in unlicensed spectrum is finally standardized by 3GPP, convergence of unlicensed technologies (MulteFire, CBRS) and cellular technologies (3GPP) could be a reality.

4.1.2 Centralized vs. Decentralized Coordination

Perhaps the biggest challenge from the technical point of view in the licensed shared access is interference control and mitigation. Failure to protect the QoS sensitive sharing players from the interference results in performance degradation of sharing schemes, and therefore there is less incentive for the sharing players to participate in spectrum sharing. Two types of coordination between the sharing players can be defined [94], namely centralized and decentralized coordination.

4.1.2.1 Centralized Coordination

In the centralized coordination techniques, the spectrum sharing players do not directly interact with each other but there is a central entity in between. This super resource scheduler, meta-operator, spectrum broker, or shared radio resource manager, manages the spectrum sharing process and takes care that the QoS requirements are met among the sharing players. This management process can be aided by a database that contains information about the spectrum usage. A geo-location database can be a simple database that holds information of the spectrum availability of a service provider, either MNO or incumbent. In a more complex approach, the interference between the users can be calculated based on offline theoretical propagation models allowing interference protection. This technique has been applied in TVWS and LSA reference system architecture.

The implementation of centralized coordination techniques requires some additional new hardware and media. For example, the management of the central entity as well as setting up the connectivity between the entity and sharing players requires additional investments. In the case of database-driven approach, also management of the database causes additional costs.

4.1.2.2 Decentralized Coordination

In decentralized coordination, the sharing players cooperate in a distributed manner without a central managing entity. Several techniques, such as spectrum sensing, game theory based approaches, and coordinated beamforming, have been applied to licensed spectrum.

By the aid of spectrum sensing techniques, the devices can detect the presence of other devices operating on shared bands. In the case where other devices are present, the device can abstain from transmitting in order to avoid interfering the other (incumbent) users. A wide range of sensing techniques have been presented in the literature [107], ranging from energy detection to feature detection of co-existence beacons, etc.

Game theory is a well-defined technique for studying decision-making in multi-user systems. The case of co-existence of multiple service providers in a shared licensed spectrum can also be studied from the game theoretical perspective. Depending on whether the players co-operate or not, the game can be cooperative or non-cooperative. Without coordination among the players, the existence of a stabile outcome can be analysed through Nash Equilibria [111].

Coordinated beamforming is an approach where the size and position of the cells is effectively adjusted by modifying the amplitude and phase of the signals to shape and steer the direction of the radiated signal. In the context of spectrum sharing, beamforming technologies facilitate co-existing multi-technology deployments. The main concern in real-life deployments in licenced spectrum sharing deployments is the requirement of sharing channel state information among the devices to avoid intersystem interference.

4.1.2.3 Hybrid Coordination

In the literature, hybrid methods based on joining centralized and decentralized coordination are also presented. For example, in [112] is proposed a framework for LSA networks that discourages licensee operator misbehaviour. The framework is built around three core functions: misbehaviour detection via the employment of a dedicated sensing network; a penalization function; and, a behaviour-driven resource allocation that is aided by LSA repository. A different approach is taken in [113], where the spectrum management is handled via spectrum manager, but utilizing a game-theoretic approach in the decision-making. The proposed model takes into consideration the competition among the LSA licensees to access the shared spectrum pool, while at the same time managing the interference through cooperation among the interfering players in the spectrum sharing game.

4.1.3 State of standards and potential implementation

Since spectrum sharing has become attainable solution, the standardisation entities have prepared new standards to enable usage of this technology. In this chapter, the current standardisation status of two licensed spectrum sharing approaches, i.e., LSA and SAS, is shown. As the LSA concept is mainly considered for the EU, this section discusses the LSA deployment in the mobile network. LSA in the context of Network Function Virtualisation (NFV), which is one of the key research fields also highlighted by authors [123], is also analysed. The NFV approach might support the spectrum sharing concept and enable the implementation of related enablers.

LSA was first introduced by ETSI with the general description of the LSA regime in 2013, and with the related requirements and architecture during the following years. Especially important may be to notice the LSA controller (LC) and its integration reference points described in number of specification documents (see Table 4). It is also worth mentioning that in 2017, 3GPP has released a specification that clearly places LC within the network management (NM) layer as one of the entities. The latter underlines the need to clearly align a LC component with proper interfaces between NMS, MANO and EMS elements. The table below summarizes the most relevant standards related with LSA.

Table 4. The list of standards that provide the LSA concept

Date	Standard
2013-07 (V1.1.1)	ETSI TR 103 113 System Reference Document on "Mobile broadband services in the 2300 MHz -2400 MHz frequency band under LSA regime"
2014-10 (V1.1.1)	ETSI TS 103 154 "System requirements for operation of Mobile Broadband Systems in the 2300 MHz -2400 MHz band under LSA" (STAGE 1)
2015-10 (V1.1.1)	ETSI TS 103 235 "System Architecture and High Level

	Procedures for operation of LSA in the 2300 MHz-2400 MHz band (STAGE 2)
21.03.2016 (Release 14)	3GPP TR 32.855 System Reference Document on "Study on OAM support for Licensed Shared Access"
2017-01 (V1.1.1)	ETSI TS 103 379 „Information elements and protocols for the interface between LSA Controller (LC) and LSA Repository (LR) for operation of Licensed Shared Access (LSA) in the 2300 MHz-2400 MHz band" (STAGE 3)
15.06.2017 (Release 14)	3GPP TS 28.301 "Telecommunication management; LSA controller (LC) Integration Reference Point (IRP); Requirements" (STAGE 1)
15.06.2017 (Release 14)	3GPP TS 28.302 "Telecommunication management; LSA controller (LC) Integration Reference Point (IRP); Information Service (IS)" (STAGE 2)
15.06.2017 (Release 14)	3GPP TS 28.303 "Telecommunication management; LSA controller (LC) Integration Reference Point (IRP); Solution Set (SS)" (STAGE 3)
21.09.2017 (Release 15)	3GPP TS 32.101 V15.0.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Principles and high level requirements (Release 15) as Network Management layer entity."

In the USA the alternative approach called SAS is considered. The approach is mostly discussed under the CBRS. In 2015 the Federal Communication Commission adopted "Report and Order and Second Further Notice of Proposed Rulemaking" which established the CBRS [124] that employs the SAS. The SAS is defined in the WinnForum reports [125] and with the new releases covered by [127].

Unlike LSA, SAS shares spectrum among two types of users (incumbents and LSA licensees). In addition, SAS is three-tier sharing scheme that allows three types of users to share the spectrum inside each administrative region: federal users, priority access licensed (PAL) users and General Authorized Access (GAA) users. The federal users take precedence over all other users and are protected against all types of interference. The PAL users will apply to geographic licenses through auctions. They are allowed to use spectrum exclusively when federal users don't use it. The GAA users spectrum opportunistically and are not protected against any interference [170].

The CBRS Alliance [117] suggests a detailed business environment and proposes some more general technical assumptions [128].

4.1.3.1 LSA deployment scenarios

The LSA concept is the approach considered for mobile networks within Europe. Two deployment scenarios within NM are considered in 3GPP TS 28.301. The first deployment scenario describes the LC as a relay for the LSA Spectrum Resource Availability Information (LSRAI) which is received from the LSA Repository (LR), and then, LSRAI is forwarded to the NM. In the latter one, the LC does not forward the LSRAI. It receives the LSRAI from the LR and radio planning parameters from the NM, and it computes the radio configuration constraints, which are sent to the NM. The LSA spectrum resource usage use cases in both scenarios are discussed in 3GPP TS 28.301.

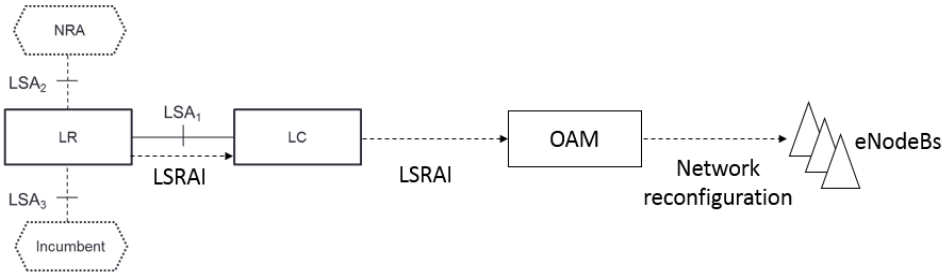


Figure 42. The overview of the alternative 1 [185]

In the first scenario, since the LC is registered within the system, it simply forwards the LSRAI information from the LR to the NM, and then, NM acknowledges the configuration changes in the mobile/fixed communication network (MFCN) to the LC. The LC sends the acknowledgement to the LR. The information is exchanged periodically until the LC deregisters from the LR and informs about this to the NM.

In the latter scenario, the LC starts the process when it receives the information about the resource usage by incumbents from the LR. The NM is asked by the LC to provide the cell parameters range which is available in the system. The constraints are defined by the LC and are based on LSRAI and NM responses. The LC sends the computed constraints to the NM, which in turn, applies the constraints and sends an acknowledgement to the LC. The process is finished.

In 3GPP TS 28.302 more details about the communication between the LC and the NM are described. 3GPP TS 28.303 provides more details about the Integration Reference Point (IRP) implementation in a CORBA/IDL and a SOAP/WSDL environment. However, in this consideration, the architectural aspects and the impact on the system are the main areas of interest. Hence, the communication and detailed implementation of IRP is not further discussed.

According to 3GPP TR 32.855, the allowed parameters and the list of allowed cells in operations are sent from Operation, Administration and Maintenance (OAM) to the eNodeBs in both alternatives (deployments). The difference is only as already aforementioned in sent content between LC and OAM. The alternatives are shown in Figure 42 and Figure 43.

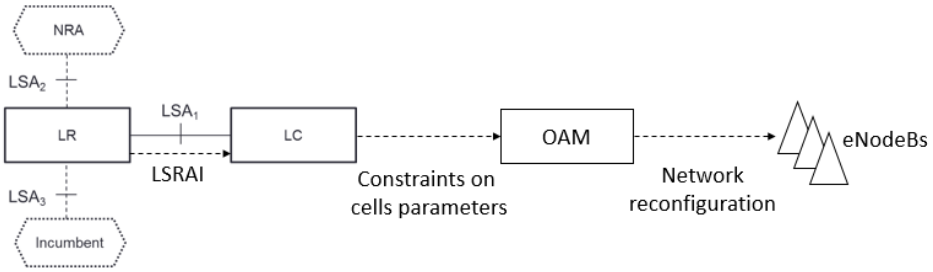


Figure 43. The overview of the alternative 2 [185]

The command is sent from Network Manager (NMr) to the Element Manager (EMr) via Itf-N interface which is the management interface identified by the 3GPP.

4.1.3.2 Network management interfaces vs LSA

Due to the fact that the LSA adjusts the network spectrum resources, the relevant and efficient network management shall be deeply analysed. In the NFV approach, Itf-N should also be

considered, as the 3GPP TR 28.500 states that the FCAPS (Fault, Configuration, Accounting, Performance, Security) exchange shall be provided via Itf-N.

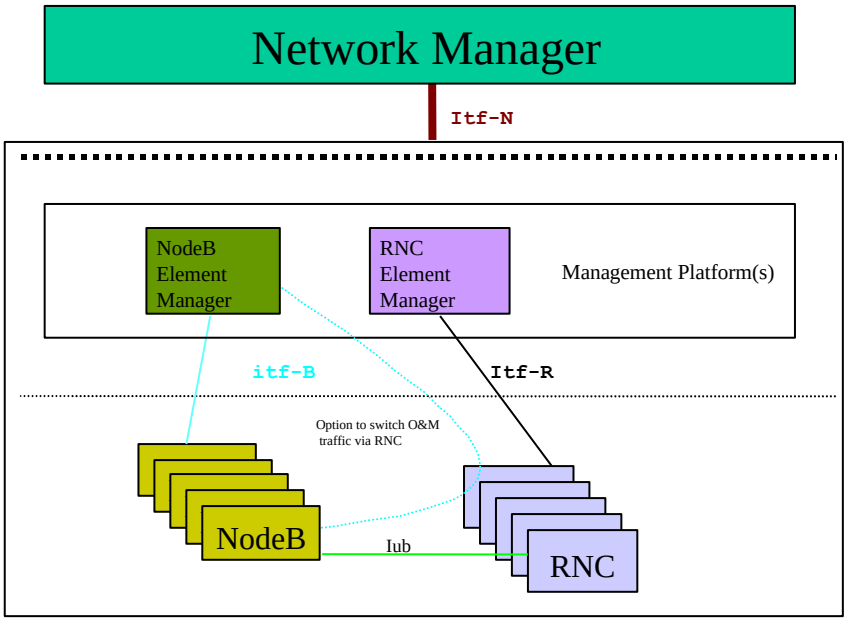


Figure 44. Radio Network management interfaces [186] (Fig 2)

It shall include both a VNF and a physical NF (PNF) FCAPS. The general NFV architecture is shown in Figure 45 with special focus on integration with 3GPP management system.

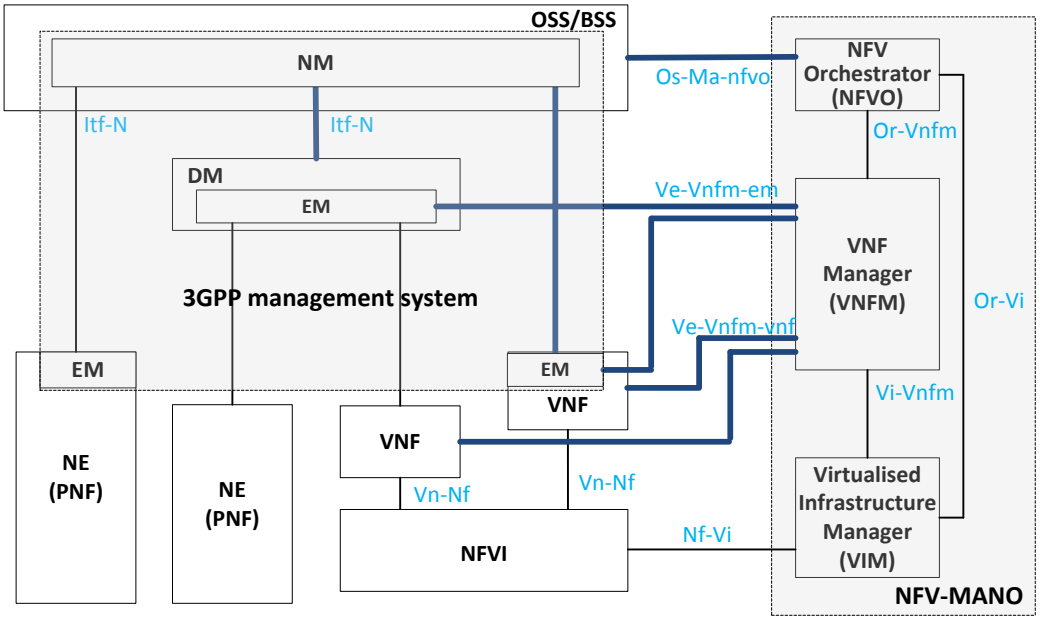


Figure 45. The NF network management [187] (Fig 6.1.1-1)

LSA entails the changes in the resource availability. This issue shall be considered in the NM and gives field for optimisation. When the new configuration is applied, and the fact is noted to

the NM, the NM shall send the confirmation to the LC. Finally, the notification shall be forwarded to the LR.

In 3GPP TR 22.830 and ETSI TR 103 588, the evolved LSA (eLSA) is already considered. The eLSA is expected to provide the locally-confined and temporarily-flexible access. The eLSA architecture is shown in Figure 46.

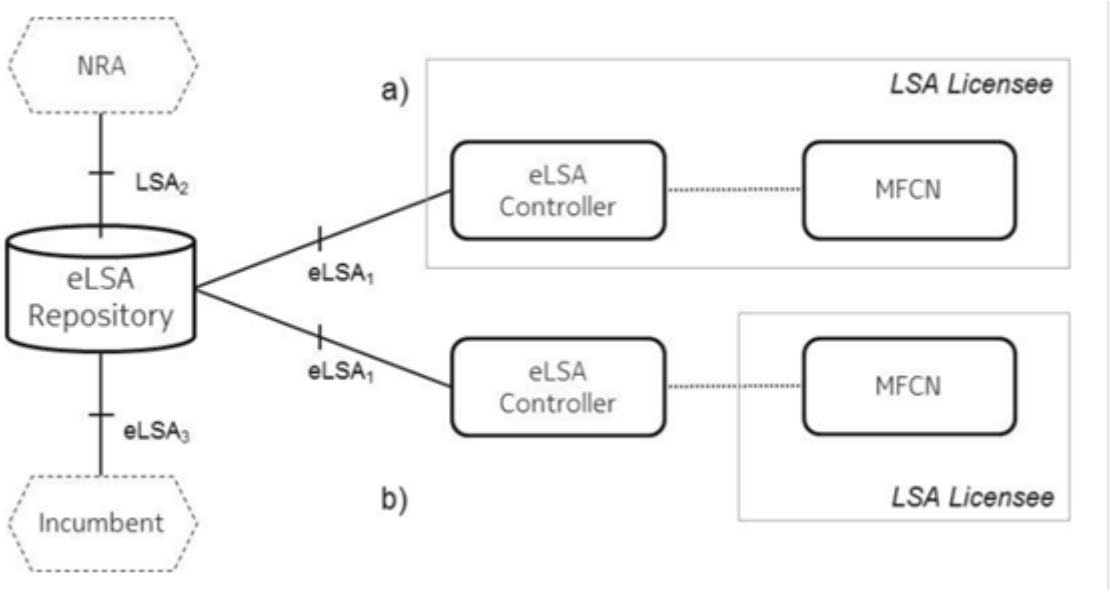


Figure 46. Evolved LSA Architecture [188]

The two potential deployments are considered within ETSI. In the first deployment, the licensee owns both the eLSA Controller (eLC) and the Mobile/Fixed Communication Network (MFCN). In the latter, the licensee is providing only the MFCN. However, eLSA still needs the eLC to be implemented in the NM layer and similar management features are required.

To conclude, EuWireless shall consider that the LSA is using the common 3GPP network management architecture and the only change is to provide the LSA Controller in the Network Management (NM) layer. To perform such adjustment, it would be needed to use the Integration Reference Points and the Network Manager modifications. However, the change in network spectrum resource shall be considered in both: the network planning and network management.

4.1.4 Research and implementation challenges and opportunities

To meet incumbents' demands and the technology objectives, the spectrum sharing approaches have to provide high performance with little requirements, i.e., the requirements that do not entail high investment in Licensee system. In order to provide it, some trade-offs shall be investigated. In this section, the existing research areas are presented and aligned with challenges and implementation opportunities which are recognised by the consortium. The analysis is done for the LSA system, however, most of the statements can be applied for SAS too. The potential research areas are shown in Figure 47.

Figure 47. The potential research areas for LSA systems

If the incumbent receives the granted permission to use LSA resources and the requested period starts, the licensee Network Manager (NM) shall rapidly leave the granted band. The time between incumbent request and the band release is considered as one of the major performance indicators [131] and is called evacuation time. In [131], the evacuation time is counted from the LSA Repository evacuation request to the moment that the base station that uses the requested band goes offline. Due to the incumbent right protection, the evacuation time shall be kept as short as possible. Furthermore, the short evacuation time yields another key benefit, as it improves the spectrum resource usage efficiency. The issue shall be strongly considered in dynamic spectrum sharing mode, i.e., the spectrum resource is allocated in real time for short periods of time. The real-time adjustment is also the key challenge for the use case with two network operators that share spectrum resources to improve their network capacities when the high throughput demand appears [132].

During the evacuation process, the traffic steering approach has to be employed. The challenge appears when the dynamic spectrum sharing is considered [94]. Since the UE shall be served within another frequency range, the handover procedure has to be applied and the quality of service for UE shall be held. Hence, the efficient traffic steering approaches are necessary.

The traffic steering is strongly related to the next research area that worth highlighting. Due to the necessity of keeping the EU connection, the optimum load balancing has to be considered within the licensee network [94]. The non-optimum algorithms could cause increased queuing and connection drop, which in turn, affect the quality of service. Hence, this issue shall be strongly considered within network managing (and planning).

The QoS requirements are widely referred, e.g., [133][94][134][135], as the approach shall be attractive for users and worth operators' investment. The taxonomy of types of shared access methods and authorisation regimes are employed [94]. The QoS depends on access method and regime. In [133], the author stated that some degree of exclusivity is necessary to provide the guarantee of QoS. An alternative is to simply share the spectrum by coexisting/cooperating but without any guarantee of QoS (e.g. 27 MHz citizens band radio).

Obviously, in the multiuser system, there is a need for single user rights protection. To protect the user right in the LSA, the LSA repository is employed [136]. The protection request might be described by protection distance, transmit power limit and the transmission setup.

Due to the user right protection and QoS requirement, the interferences shall be minimised, which in turn, requires strict power control. The maximum allowed power level shall be followed and the exclusion zones shall be protected [94]. This area also gives an opportunity for power control optimisation.

The spectrum sharing methods aim at improving the quantity of the spectral resources. In order to meet the objective, the efficient resource management approaches shall be employed and the performance indicators considered. The optimisation and automation of the LSA resources might be provided by employing LTE/LTE-Advanced network functionalities as, e.g., cell re-selection procedures [137]. The optimum and dynamic resource allocation at a short time scale is one of the key challenges for the LSA [98].

The very target of industry in the 21st century is the energy consumption reduction which applies also to the telecommunication industry and spectrum sharing approaches. The energy consumption reduction yields not only benefits for natural environment but also reduce the maintenance cost. The minimisation of energy expenditure is also considered as a key challenge in the LSA systems [98].

The spectrum management within LSA requires plenty of signalling between the LSA Controller and MNO network and the some signalling overhead might appear [94]. An efficient approach shall be employed to decrease the signalling and the coordination procedure execution time. The 3GPP TS 32.101 suggest placing the LSA controller in the MNO LTE network. The non-optimal placement of an LSA controller in the network might cause delays, in particular, in large-scale LSA deployment [94].

Since the LSA spectrum sharing method is expected not only to enable incumbent usage of the licensed spectrum but also to improve the MNO network capacity, it shall support the joint transmission on LSA band and exclusive MNO band. In particular, the support for non-contiguous bands Carrier Aggregation is necessary [94].

The Multi-RAT deployment is expected to be employed soon and the new techniques, as spectrum sharing methods, are expected to follow this trend. The Multi-RAT approach is limited by inter-RAT interferences [94] which shall be considered in the investigation of spectrum sharing.

The LSA approach is an appealing application to enhance the network capacity and enable new incumbents to use spectrum, however, the challenges even in its architecture appear. The systems entail the databases that store the spectrum availability. The LSA database architecture is an important area for further consideration. There are plenty of opportunities, but each entails some disadvantages. Further consideration is necessary, inter alia, in the following areas: the size of the region for one system and one database, the technique to exchange of information between databases, the advantages and disadvantages of a distributed system, the advantages and disadvantages of a centralized system.

The last but not least, it is worth highlighting the sensing aspect which is considered in some spectrum sharing approaches as, e.g., SAS. In the LSA approach the spectrum sensing could be used to improve the quality of the content (more realistic data) in the LSA Repository [94]. The mixed geolocation database and sensing technique (like in Cognitive Radio) might be the most efficient approach, and it might be the area for further investigation.

All in all, the potential research areas and implementation issues for licensed spectrum sharing systems are presented above to assist EuWireless research planned and suggest the different

challenges around LSA. The further research might require the tool that would enable research related with the influences the spectrum sharing will have on the overall network slice building on it. Such tool could be based on extensions provided to the 5G Toolset [123].

4.1.5 Spectrum Sharing in EU projects

Spectrum sharing is considered by 5GPPP and different EU projects. The ADEL project [139] challenges the three research problems in the LSA field [138]:

1. The allocation of spectral and power resources in the dynamic mode (seconds or even milliseconds).
2. The QoS guarantees.
3. The LSA network energy expenditure minimisation.

The LSA is also considered in the Coherent project [140] , which works on coordinated control and spectrum management. The spectrum is shared between incumbent and two network operators within the Coherent concept.

The spectrum sharing is also analysed by the 5GPPP phase 3 project - 5G Genesis [141] project as a part of a platform for IoT service. A similar approach to LSA is proposed by COGEU project [141]. The automatic spectrum-trading platform is provided for the Munich area by COGEU society. The participants propose the online booking tool to ask for resources. However, the main research area for the project is cognitive radio approaches. Most spectrum sharing initiatives are covered under the cognitive radio ideas. The spectrum sharing is considered in other projects as a part of the 5G environment, e.g., in METIS [142], METIS – II [143]. Currently, there are not many initiatives investigating directly LSA or SAS.

Regarding spectrum sharing testbeds, it is worth mentioning also the Fed4FIRE testbed facility in Ljubljana, it is named LOG-A-TEC [171]. This facility, under the open call programme, gives access to the spectrum sharing platform managed by the Josef Stefan Institute. In [58], the authors focus on how to introduce I/Q samples from multiple virtualized RAT technologies by multiplexing it within a single component carrier. The latter approach could be interesting solution for EuWireless proof-of-concept.

4.1.6 Gap analysis and research directions within EuWireless

Among others, the following topics will be considered for research in the WP2:

- Effective spectrum sensing to support spectrum management and monitoring.
- Strategies for distributed geolocation database implementation.
- Efficiency of spectrum management (acquire, release operations delays).
- Spectrum sharing enablers validation (e.g. Hydra RF multiplexing, existing spectrum sharing related testbed facilities).

The abovementioned topics will be the main plane for research for spectrum sharing, and they will be considered together with the research challenges already identified in the Section 4.1.4.

4.1.6.1 Spectrum sharing continuum

The spectrum sharing methods give the incumbent and the operator the opportunity to share resources under an agreed regime. Due to the fact that the resource is shared, the users might overuse the resource. The unfair resource sharing might affect both sides. To protect users, the NRA's role in LSA should be considered. The NRA shall control the resource usage and needs the tools to do their duties.

The supervision is necessary not only in Europe, but also in other countries that want to adopt the LSA approach. The spectrum sharing framework proposed for China is shown in Figure 48. The process starts with request for spectrum. Then, the Radio Access Optimization Center analyses the inquiry. If the spectrum is granted, the Spectrum Management Process is started

and the spectrum is assigned. Within the Spectrum Management Process one can see the Radio Monitoring block. This block could be supported by a dedicated probe/tool. When the Spectrum Management Process is finished the feedback is send to database. This process exemplifies the potential utilization of auxiliary tools that could be considered in the next phases of research in EuWireless.

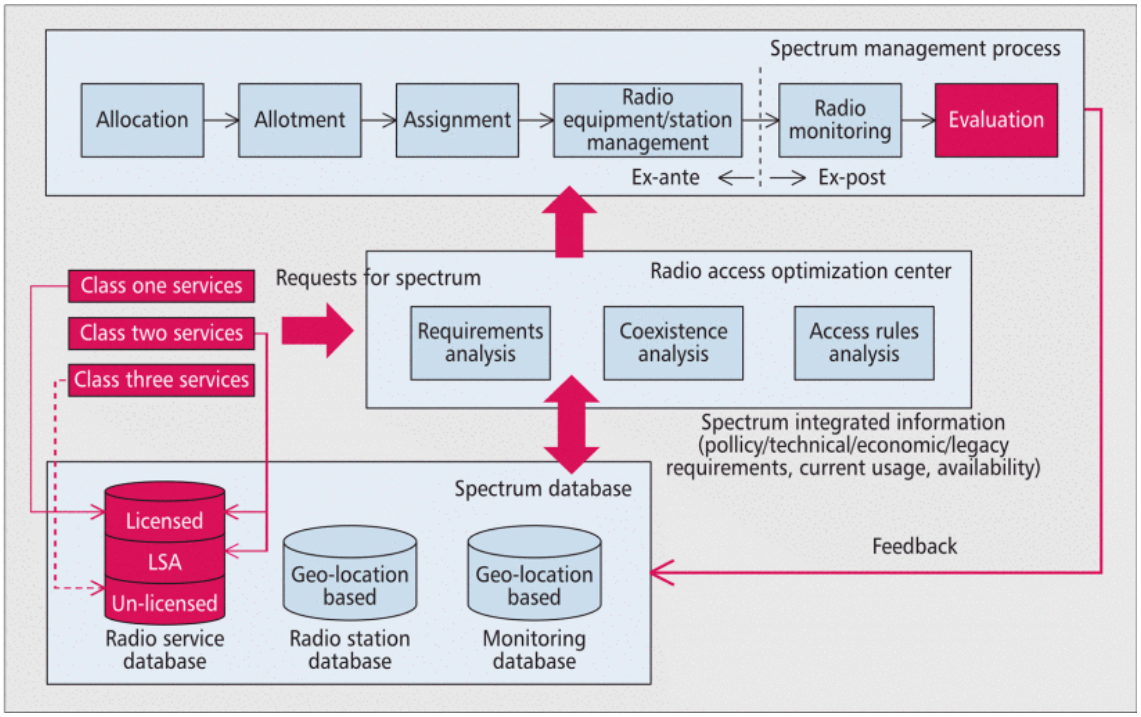


Figure 48. The spectrum management framework in China [116]

A probe which could be used by a NRA shall be available in order to support monitoring the effectiveness of LSA operating area. According to the EuWireless project assumptions, it will be analysed how to instrument a spectrum probe with features that support the investigation of the aforementioned LSA research topic.

4.2 RAN sharing

The 3GPP specification compliant RAN architectures have evolved from the traditional metro-site topologies, where all base station functionality is integrated into proprietary hardware at the cell site, towards more flexible deployments with the 3G and 4G networks. The first step has been the separation of radio and baseband processing units, which has made the installation of the base station equipment at different kinds of cell sites easier. The next step will be to virtualise and distribute the baseband processing functionality into the network based on the service needs. The virtualisation approach will realise a true Cloud RAN, making the RAN an integral part of the overall network as it allows key concepts of 5G networks, such as network slicing, to be better managed in end-to-end manner.

4.2.1 Centralized RAN

Centralized Radio Access Network (C-RAN), also known as Cloud RAN, Cooperative RAN and Clean RAN [85], is a cloud-computing-based architecture which takes advantage of the virtualization concept to cope with the challenge that massive access to mobile communications entails. In C-RAN, the base station functionality is divided into two Radio Access Network (RAN) elements, i.e. the Baseband Unit (BBU) and the Remote Radio Head (RRH). All functionality related to baseband processing and protocols on the Physical Layer (PHY) and above is provided by the BBU, and the RRH handles the radio functionalities. In a typical RAN

architecture used in the cellular network nowadays, the BBU is placed close to the cell tower where RRH is placed. BBUs are usually installed in a small equipment shelter, which involves leasing and site power costs amongst others. One or more RRHs is/are paired with one BBU with fixed allocations.

The C-RAN approach centralizes multiple BBUs in one location (i.e. Centralized RAN) and can further enhance the flexibility of the architecture by virtualising some functions of the BBUs in a common resource pool (i.e. Cloud-RAN) as shown in Figure 49. The additional step of virtualising and pooling of BBU resources enables the use of Commercial Off-the-Shelf (COTS) servers for processing the majority of the BBU routines and utilisation of data centres to host the equipment [86].

The C-RAN concept has several advantages when compared to a RAN architecture with fixed RRH-BBU pairs. First, in C-RAN, the use of virtualized BBU pools provides flexibility and better utilization rate in the access network, as the amount of allocated processing resources can be adapted per cell site according to the temporal changes in the local traffic loads. Sharing of BBU resources between cell sites means that less hardware and energy is needed to serve the same customers as before. Second, as the BBU processing is performed in the same data centre for several neighbouring cells, implementation of novel collaborative communication techniques requiring high data rates and low latency and jitter between base stations is facilitated. Even the 3GPP standard-based techniques, such as enhanced Inter Cell Interference Coordination (eICIC), Coordinated Multi-Point (CoMP) operation and soft handovers can benefit from C-RAN. Third, C-RAN allows easier network maintenance and RAN sharing between network operators. For example, one operator could rent RAN as a cloud service from another operator.

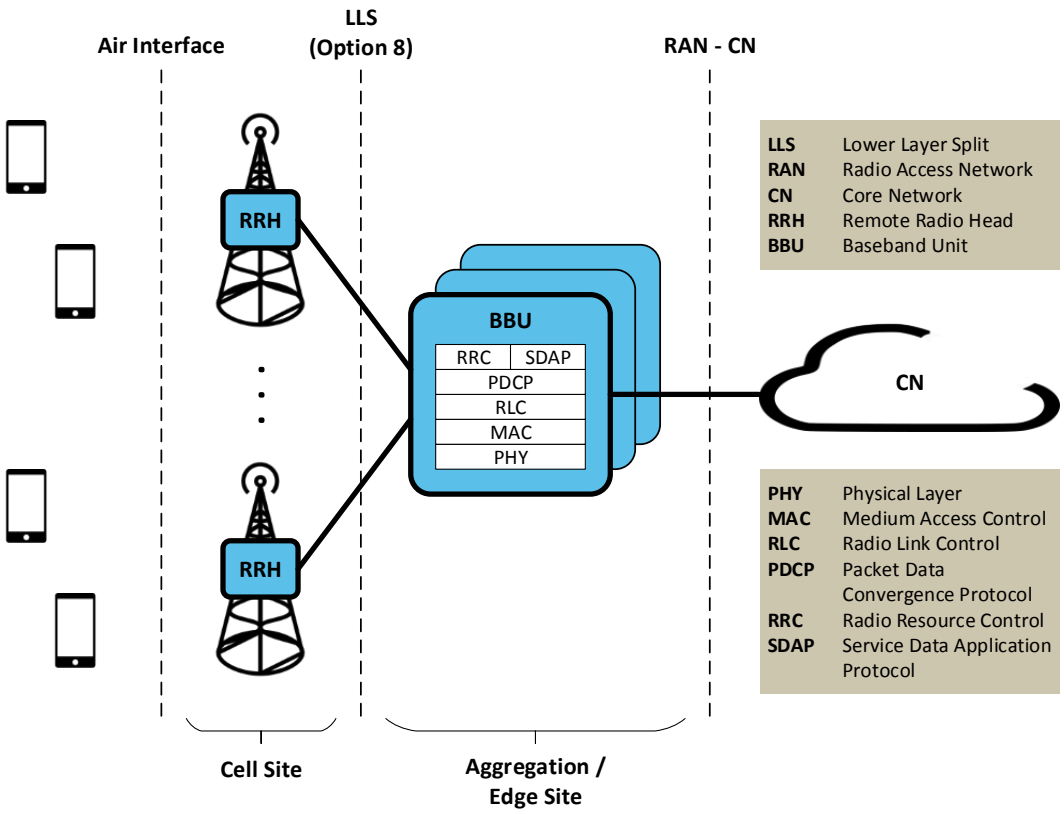


Figure 49. C-RAN architecture

C-RAN (known as the functional split Option 8 in 3GPP terminology [87]) also has some challenges when it comes to large-scale deployment in commercial network infrastructures. As the interface between the RRH and BBU is designed to transmit IQ data, the utilized protocols Common Public Radio Interface (CPRI) / enhanced CPRI (eCPRI), Open Base Station Architecture Initiative (OBSAI) or Open Radio Equipment Interface (ORI) protocols demand very high bandwidth as well as low latency and jitter in order to work. This means that the fronthaul connectivity must be implemented with fibre or microwave links. This increases the costs and decreases the flexibility of the fronthaul infrastructure. In addition to the high requirements for fronthaul links, additional measures to guarantee the security and resiliency of the centralised BBU pool are needed. Careful optimization of the shared resources between cells is needed in order to maintain network performance during peak hours and prevent overloads in the fronthaul and backhaul links. Virtualization can facilitate the optimization process. However, the strict and dynamically changing requirements of the RAN must also be met by the utilised virtualization techniques.

4.2.2 Next Generation RAN

In order to specify the Next Generation Radio Access Network (NG-RAN) architecture for 5G systems, 3GPP studied a variety of different options for a cloud-based RAN architecture and interfaces in its Release 14 study item on New Radio Access Technology [87]. In addition to the traditional fully integrated base station approach, different options to split the Evolved NodeB (eNB) and 5G NodeB (gNB) functionality were discussed.

Different options for the functional split between a Central Unit (CU) and a Distributed Unit (DU) are presented in the 3GPP specifications. In the Next Generation Mobile Network (NGMN) Alliance's technical documentation [88], Option 1 resents a fully distributed RAN, whereas Option 8 represents a fully centralized RAN. Options 2-7 in between are called flexible RAN and each of the options provide a different level of trade-off between performance, complexity, flexibility and transport requirements suitable for different usage scenarios. The Higher Layer Split (HLS) Options 1-5 provide additional deployment flexibility and new opportunities for RAN sharing when compared to a centralized RAN. The Lower Layer Split (LLS) Options 6-8 are in line with the traditional view of C-RAN architectures as described in the previous subsection with CU containing all of the BBU functionality and DU containing only the RRH functionality (see Figure 49).

After the assessment of the advantages and disadvantages of different HLS split options by 3GPP RAN3 Working Group, the flexible RAN Option 2 was chosen as the main CU-DU functional split for Release 15 NG-RAN [89]. In addition, the HLS Option 2 benefits from the already existing specifications on Long Term Evolution (LTE) Dual Connectivity (DC) functionality. The LLS Options 6 and 7 are study items for possible inclusion in the future releases and LLS Option 8 was considered to be sufficiently covered already by other technical specification and standardization activities and is not in the focus of 3GPP.

In HLS Option 2, the CU contains the Radio Resource Control (RRC), Packet Data Convergence Protocol (PDCP) and Service Data Application Protocol (SDAP) functionalities, whereas the DU contains the Radio Link Control (RLC), Medium Access Control (MAC) and PHY functionalities. In addition to the division of the eNB and gNB functionalities into the CU and the DU, the Control Plane (CP) and the User Plane (UP) functionalities are also separated in the NG-RAN architecture. The resulting basic NG-RAN architecture for the HSL Option 2 is presented in Figure 50. The different CP-UP and CU-DU configurations and the interfaces interconnecting the different logical entities can be found from the 3GPP Release 15 RAN specifications and from [88].

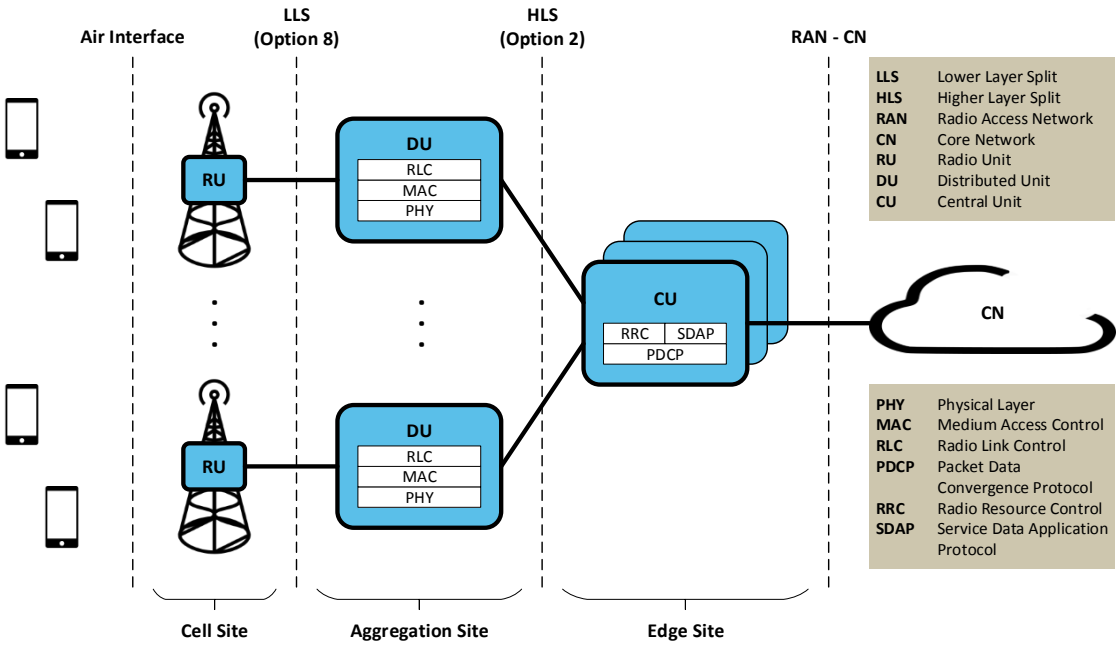


Figure 50. NG-RAN architecture

There are three main deployment scenarios defined for the Release 15 NG-RAN architecture. The first scenario represents a basic case where both the CP and the UP functionalities are centralized in the CU. This enables the installation of all CU functionality near the Core Network (CN) services and applications, e.g. into an operator's data centre, facilitating the cooperation and management of the overall network. However, if the data centre hosting the CUs is far away from the DUs, the transport latencies can cause RAN performance issues in very demanding use cases. In the second scenario, the CP functionality is distributed to the DUs and the UP functionality is centralized in the CU. This approach enables low latency control signalling between the network and the User Equipment (UE) and decreases the amount of CP traffic in the transport. In the third scenario, the CP functionality is centralized to the CU and the UP functionality is distributed to the DUs. This allows extremely low latency access to the user and application data, which is cached at the network edge.

The main advantage of the HLS Option 2 is the increased flexibility when it comes to the implementation and deployment of the hardware and software components in NG-RAN. Some of the key deployment challenges of C-RAN can be avoided in HLS where the bandwidth, latency and jitter requirements for the utilized transport technologies are considerably lower due to the use of non-real-time protocols in the F1 interface. Due to their better delay and jitter tolerance, the RAN architectures based on the HLS options are also better suited to network integration and cooperation scenarios in Network Functions Virtualization (NFV) / Software-Defined Networking (SDN) enabled telco cloud infrastructures. On the other hand, the downside of the HLS is that the excess latency between the CU and the DU can limit the performance of the RAN in some use cases. In addition, the added complexity in the DU can be a disadvantage in some deployment scenarios.

4.3 Core network oriented selection methods

The network sharing paradigm has evolved from previously deployed mobile network generations (e.g. LTE featured Multi-Operator Core Network (MOCN), Gateway Core Network (GWCN) or Roaming, which allowed Mobile Network Operators (MNOs) to statically share some entities of the network) to new technologies, such as the 5G Network Slicing feature.

Slicing enables dynamic allocation of network resources as per several criteria: type of traffic, status of the network, customer priority, etc.

4.3.1 S1-Flex, Multi-Operator Core Network and Gateway Core Network

S1-Flex functionality allows RAN entities to be concurrently connected to multiple CNs. In the case of LTE, the eNodeB entity should be connected to all the Mobility Management Entities (MMEs) belonging to the working pool area [149].

With Multi-Operator Core Network (MOCN) functionality, multiple network operators share the same RAN, while each one owns its Evolved Packet Core (EPC), as shown in Figure 51.

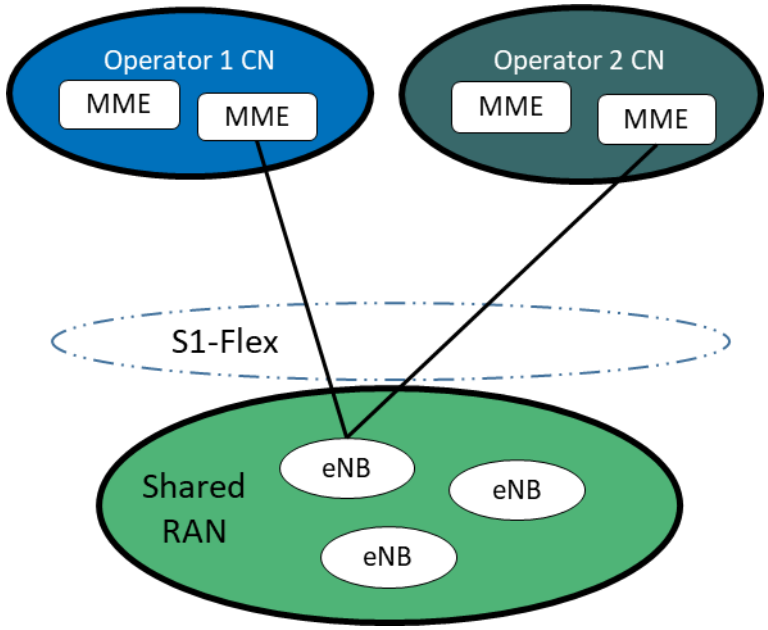


Figure 51. MOCN Architecture [151]

With Gateway Core Network (GWCN), multiple operators share the same RAN entities and also one of the entities of the CN, the MME, in charge of UE mobility functions and session management, as shown in Figure 52.

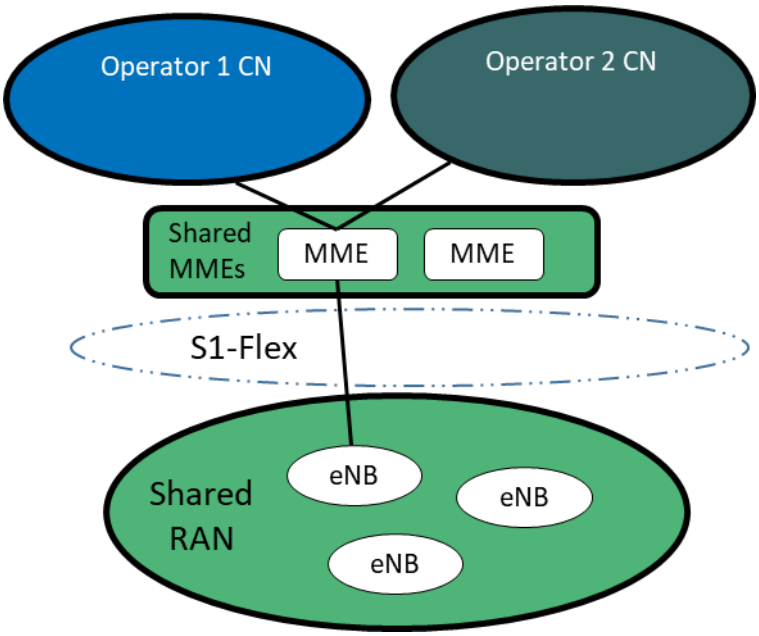


Figure 52. GWCN Architecture [151]

Regardless the specific sharing RAN technology, each cell within the shared RAN eNodeBs shall indicate the available CN operators to the UEs by broadcasting their CN operator identity, i.e. the Public Land Mobile Network (PLMN) id (a combination of the Mobile Country Code (MCC) and the Mobile Network Code (MNC)). The broadcasted set of PLMN-ids shall be the same for all the cells of a Tracking Area in a shared E-UTRAN network.

The 3GPP Technical Specification TS 23251 [151] provides further description of the RAN sharing features MOCN and GWCN.

4.3.2 Mobile Operator Radio Access Network

Mobile Operator Radio Access Network (MORAN) feature enables operators to share RAN equipment but not sharing spectrum. Thus, two or more operators could share a specific RAN node while each one has its own reserved spectrum.

Unfortunately, this configuration, in which a number of PLMN-id's corresponding to different frequency/cell coexist within an eNodeB, would imply multiple S1 connections between the eNodeB and one MME, adding extra complexity to the network. For this reason, MORAN has not been included into the standardized RAN sharing technologies by 3GPP.

4.3.3 Roaming Operator

The roaming feature enables subscribers to access to voice and data services connecting to other operator's networks (from now on Visited Networks) when the Home Network is not available (e.g. when travelling abroad). Actually, operators do not share any infrastructure but they let visitant subscribers to make use of their networks according to roaming agreements.

3GPP standards includes 2 types of roaming models for LTE ([152], section 4.2.2):

- Home Routed Roaming: In this configuration, a subscriber using a Visited Network (VPLMN) is served by the VPLMN MME and Serving Gateway (SGW) for signalling and data respectively. The MME contacts with the Home Subscriber Server (HSS) of the home operator to fetch the subscriber's profile whereas data traffic is routed from the visited SGW to the home Packet Gateway (PGW). This configuration is recommended when the relationship between operators is not completely trustworthy.

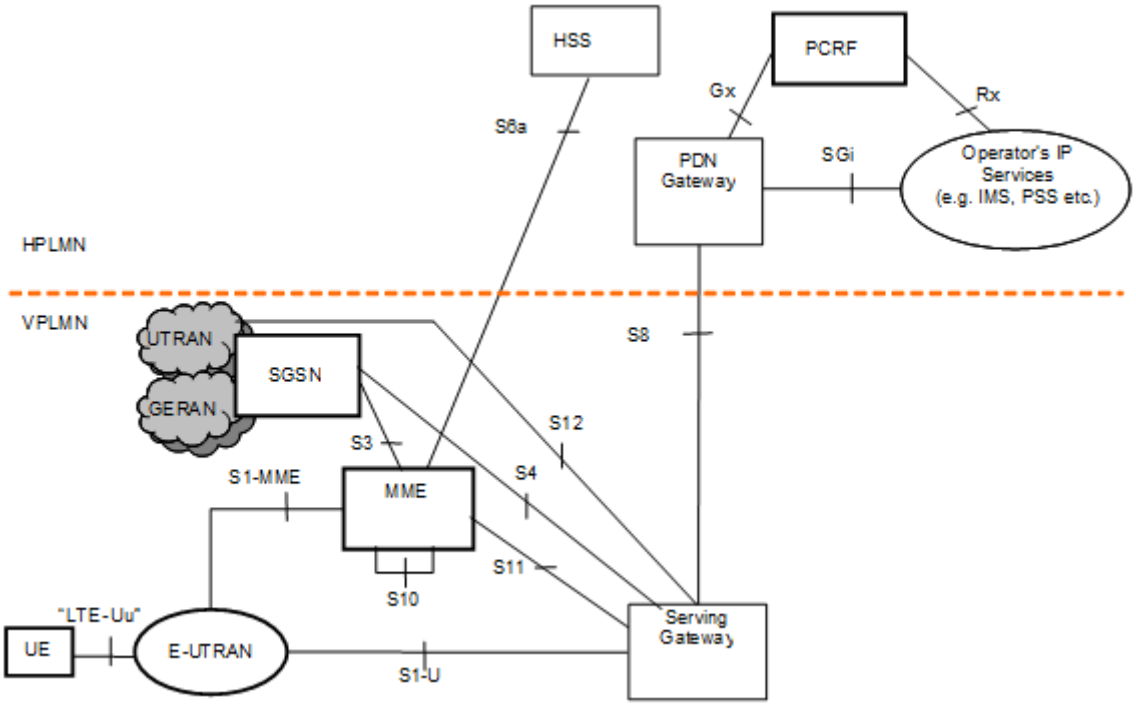


Figure 53. Home Routed Roaming Architecture [152]

- Local Breakout Roaming: In this configuration, the visitor subscriber is also serviced by the visited MME and SGW for signalling and data respectively. However, in this case data traffic is not handled by the home network but by the visited PGW. The visited Policy and Charging Rules Function (PCRF) communicates with home PCRF to be informed of the subscriber's allowed services.

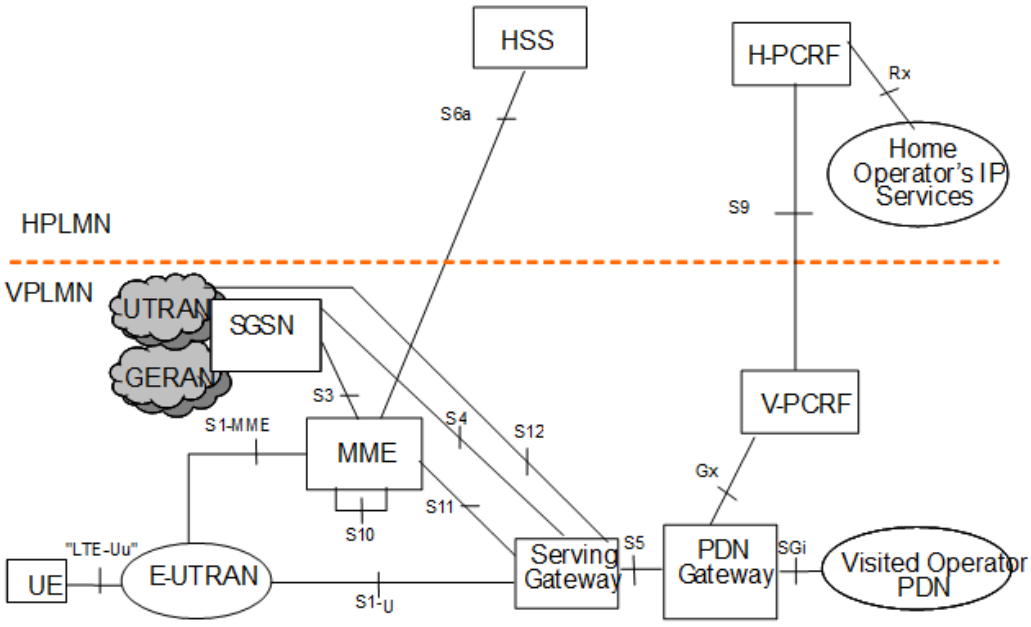


Figure 54. Local Breakout Roaming Architecture [152]

4.3.4 DECOR/eDECOR

DECOR feature allows operators to service subscribers with particular profiles with so called Dedicated Core Networks (DCNs), designed to handle user traffic according to the specific requirements of the communication. Every DCN may consist of one or multiple CN nodes. For instance, NBIoT devices would be assigned to NBIoT-DCNs, as depicts the following figure:

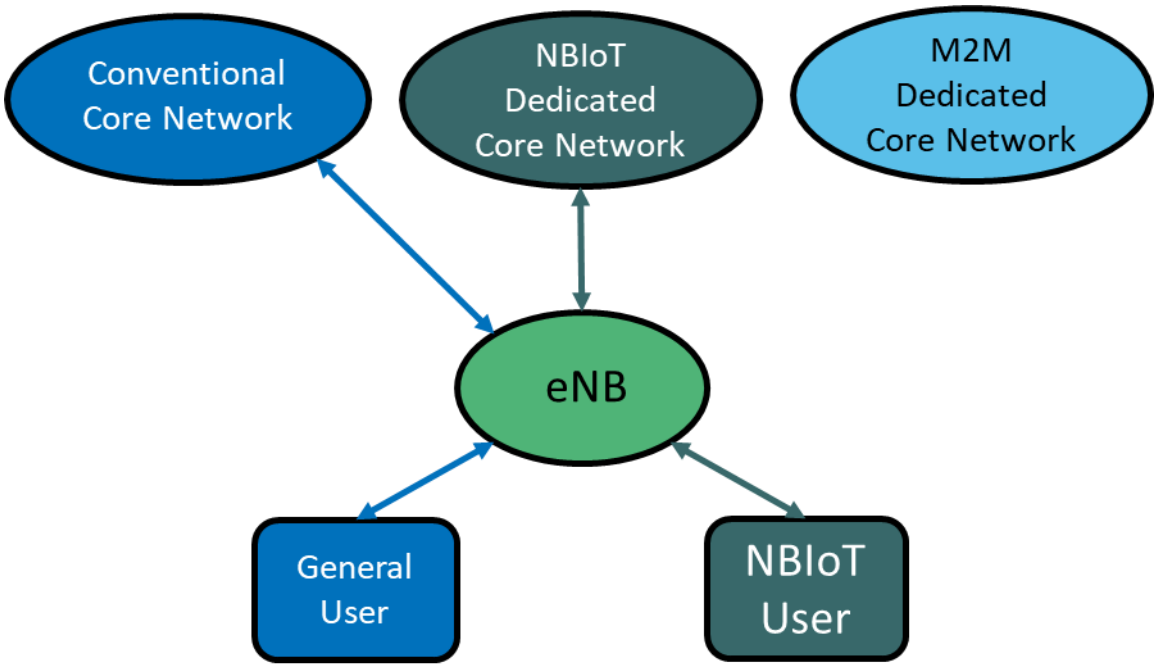


Figure 55. DECOR DCN Selection [152]

DECOR is included in 3GPP Release 13 technical specifications [152],[153]. This optional feature allows subscribers to be allocated to DCN based on subscription information ("UE Usage Type") stored in the HSS. DECOR does not require specific UE functionality. Thus, UEs compliant with former 3GPP releases are compatible with technology.

Since selection information is stored in the HSS, during the Attach procedure the eNodeB may allocate the UE into a "wrong" CN. After consulting the HSS, the allocated MME may request the eNodeB to resend the S1AP InitialUEMessage to the selected DCN MME by means of the Redirection procedure ([152], section 5.19.1):

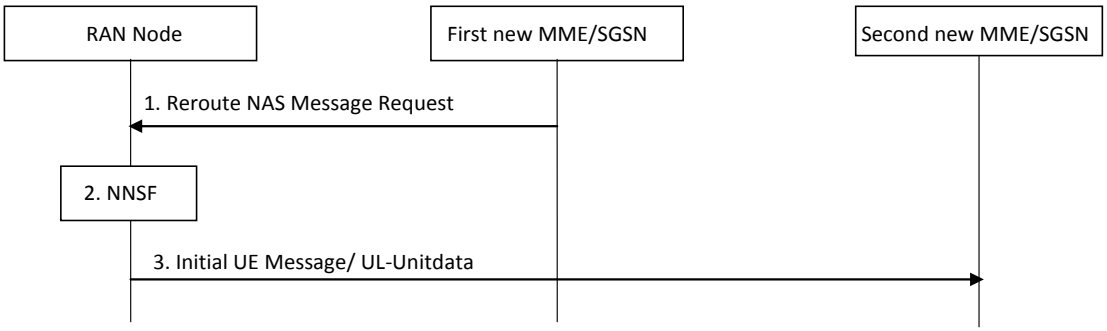


Figure 56. DECOR Redirection Procedure [152]

In Release 14, 3GPP introduced an improved version of DNC selection, Enhanced DECOR (eDECOR). This new version aims to reduce the need for DECOR rerouting by using an indication (DCN-ID) sent from the UE and used by the eNodeB to select the correct DCN. The DCN-ID is assigned to the UE by the specific DCN-ID whenever a PLMN specific DCN-ID is stored for the target PLMN. The eDECOR technology does require UEs compliant with Release 14 to operate.

4.4 5G Network Slicing

Network slicing feature enables the creation of multiple isolated virtual networks over a common shared physical infrastructure in an efficient way. These virtual networks can be created "on-demand" in order to meet specific needs of applications, devices, customers or operators.

A logical network, named Network Slice, could be comprised of multiple elements of the network (e.g. radio access, wire access, core, transport, and edge networks), and include shared and/or dedicated resources that could belong to one or multiple operators.

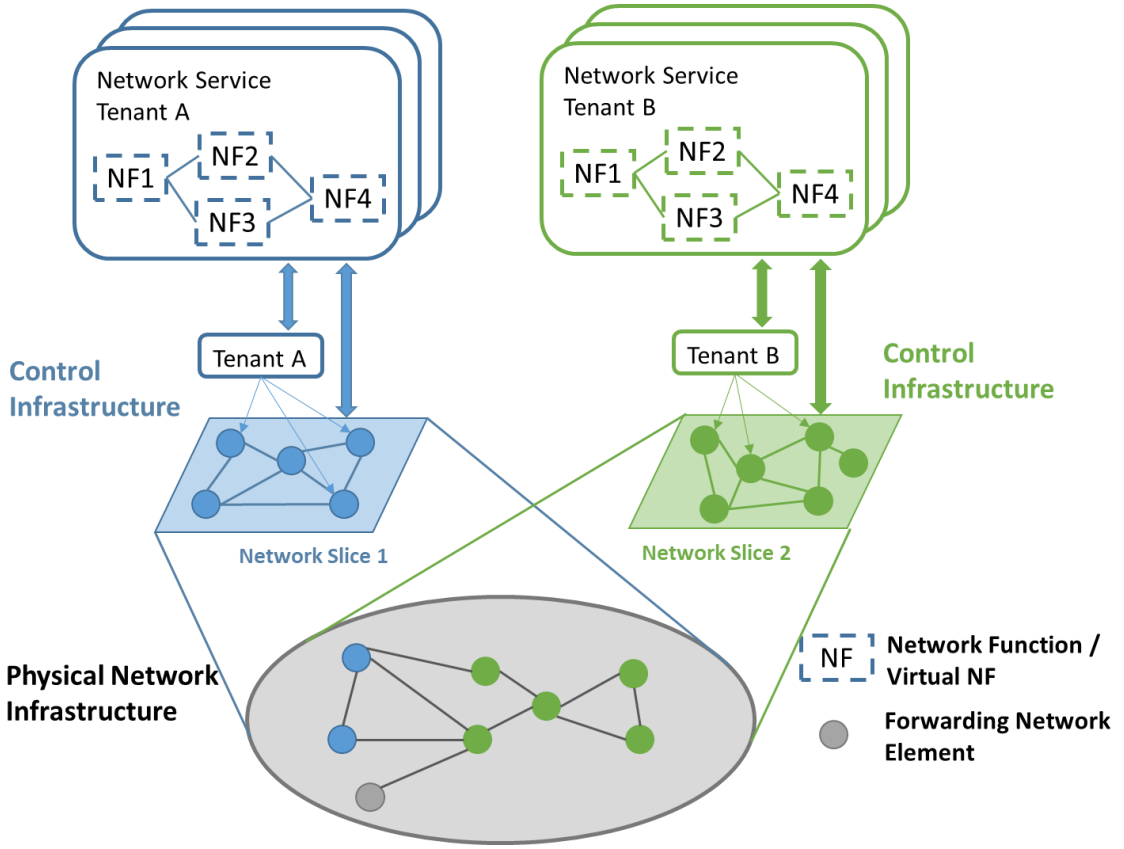


Figure 57. Network Slicing Representation [56]

Despite 3GPP and other groups have started the process of designing and standardizing Network Slicing feature within 5G context, plenty of investigation and development work is still pending. Researchers from academia and industry sectors are focusing their efforts on reaching consensus on different technical and business efficient approaches to get through the manifold challenges that Network Slicing paradigm entails. This section provides insight into the state of the art of 5G Network Slicing.

4.4.1 Use Cases

The possible use cases foreseen with regard to 5G slicing are manifold. 3GPP grouped these use cases into 5 main categories [154]:

- Enhanced Mobile Broadband (eMBB): eMBB requires greater data rates than LTE, including uplink, higher density, more coverage and improved user mobility.
- Critical Communications (CriC): These use cases require higher reliability, very low latency, higher network availability, improved accuracy positioning and mission critical services.
- Massive Internet of Things (MIoT): Use cases related to operational aspects, resources efficiency and connectivity aspects tailored to IoT devices.
- Enhanced Vehicular to Everything (eV2X): Ultra-high reliability, low latency, high bandwidth, improved seamless wide-area coverage and connected vehicles are some of the use cases included in this group.
- Network Operation (NEO): These use cases require system flexibility, scalability, mobility support, heterogeneous access support, efficient content delivery, security and interworking with earlier generations.

4.4.2 Management and Orchestration

Network Slicing feature entails a strong leverage of the complexity on managing network resources. In a context of virtualized networks hosted by multi-tenant infrastructures and the co-existence of different technologies, it is mandatory to design systems to efficiently manage and orchestrate all the elements and involved actors of the network in a dynamic fashion. Such a task requires a continuous process of both analysis of the network and allocation of resources. In [160], the authors address this process by defining two layers to control the network, each one with a set of functionalities:

- Service Management layer: Abstraction, negotiation, admission control and charging for verticals and 3rd parties. Service creation once a slice request is accepted.
- Network Slicing Control layer: Network abstraction for Service Management layer, network slice resource management and control plane operations. Slice performance monitoring and reconfiguration procedures.

Numerous network slicing orchestration architectures have been proposed in the last years. All of them imply an attempt, from different perspectives, of providing means to control the complex scenario in which Virtual Network Functions (VNFs), Physical Network Functions (PNFs), network and cloud resources, multiple tenants and multiple technologies coexist. The 5GPP "View on 5G Architecture" [56], Sonata [155], 5GEx [57], Necos [156], 5GNorma [157] and 5G-Transformer [158] are some examples.

In the document "Study on management and orchestration of network slicing for next generation network" [164] by 3GPP, Network Slice Instances (NSI) and service instance lifecycles untying is proposed. Thus, a service may use an existing NSI or one created on demand. Likewise, a NSI may be created to support one or multiple services with similar requirements and its lifecycle may last beyond the related services.

The Network Slice Subnet Instance (NSSI) concept appears in order to provide more granularity and facilitate NSI management. A NSI may contain multiple NSSIs. In turn, a NSSIs may contain one or multiple Network Functions (Physical Network Functions (PNF) and/or Virtual Network Functions (VNF), Core Network and/or Access Network functions) and also other NSSIs. In addition, a NSSIs may be shared by multiple NSIs. Figure 58 depicts the related information model of Network Slicing, in which it can be observed that service instances are handled by the Service Provider whereas NSIs are handled by Network operators:

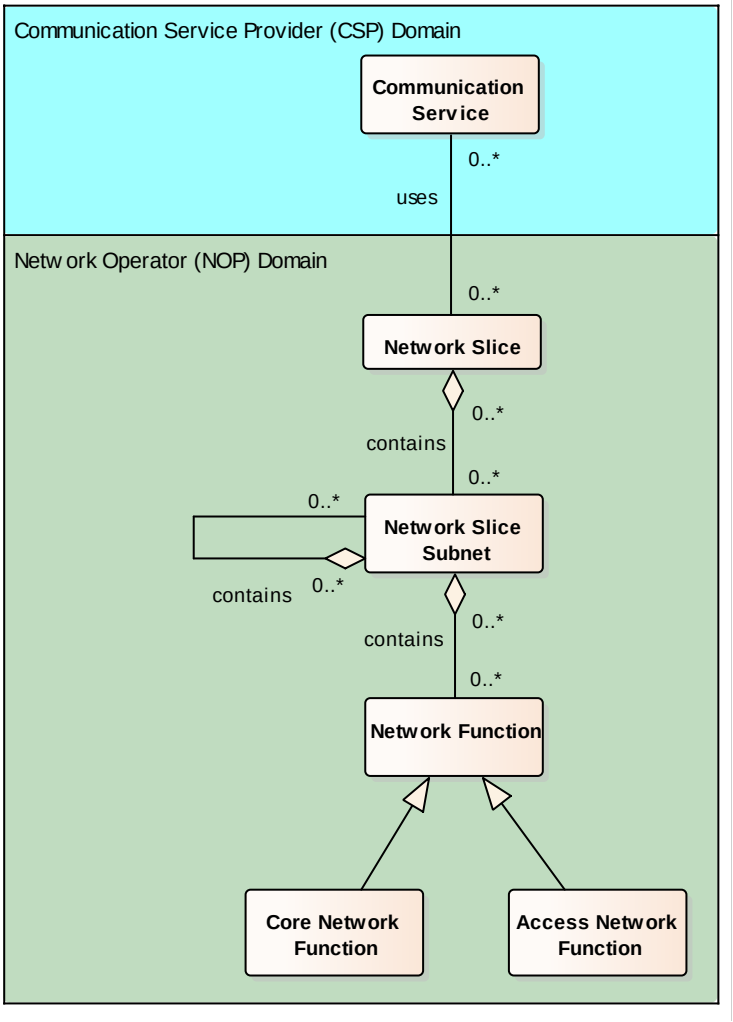


Figure 58. Network Slice related information model [164]

The same study [164] proposes a set of phases in the lifecycle of an NSI:

- Preparation phase: Needed network resources availability revision and preparation.
- Instantiation, Configuration and Activation phase: All resources are configured to a state where the NSI is ready for operation.
- Run-time phase: The NSI is able to handle traffic to support Service Instances. This phase also includes supervision, reporting and modification functions that may involve NSI topology changes, NSI scaling, association/disassociation of NFs, etc.
- Decommissioning phase: Deactivation or reclamation of shared resources and configuration of shared/dependent resources. NSI deletion.

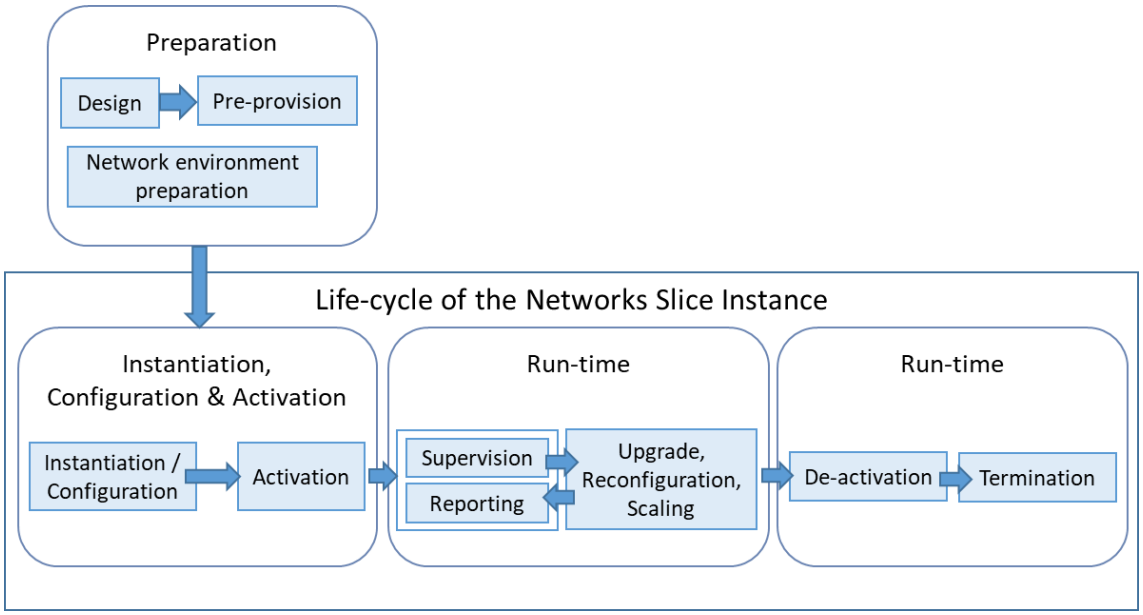


Figure 59. Lifecycle phases of an NSI [164]

4.4.3 RAN slicing

Network Slicing requires major changes in the design of Radio Access Network equipment. The dynamic nature of the slices requests more flexible and efficient procedures to manage the limited spectrum resources. New RAN must also provide means to guarantee isolation of slices for security and latency assurance reasons, but it may involve resources wasting. Thus, there is a trade-off that industry has to tackle.

In 3GPP networks, an end-to-end slice comprises of a RAN part and of a CN part. More specifically, 3GPP RAN slicing can be realized for an NG-RAN or for an Evolved Universal Terrestrial Access Network (E-UTRAN) connected to a 5G Core Network (5GC). An option to utilize non-3GPP 5G access networks as the RAN part of a network slices also exists. The following key principles and requirements have been defined in [90] for NG-RAN to support slicing:

- Support for the differentiated handling of traffic for different network slices.
- Support for the selection of the RAN part of an end-to-end network slice with the help of information provided by the UE and/or the 5GC.
- Support for policy enforcement between slices based on Service Level Agreements (SLA).
- Support for multiple slices per NG-RAN node.
- Support for Quality of Service (QoS) differentiation within a slice.
- Support for the selection of an Access Control and Mobility Management (AMF) entity for a network slice with the help of information provided by the UE and/or the 5GC.
- Support for resource isolation between slices.
- Support for slice access admission/rejection based on slice availability with the help of the 5GC.
- Support for a signalling connection per UE associated with multiple network slices.
- Support for slice awareness at a Packet Data Unit (PDU) session level.
- Support for initial validation of a UE's right to access a requested network slice.

Network slices in a 3GPP network are identified by using a Single Network Slice Selection Assistance Information (S-NSSAI) parameter, which is used as a unique slice ID in all control

signalling. The S-NSSAI parameter not only identifies a network slice, but it also contains information on the service type provided/supported by the slice in question. Currently, the 3GPP specifications lay down the high-level basic functionality required to enable slicing of NG-RAN resources. The authors in [91] analyse the impact of these high-level functional requirements from the RAN protocol architecture, network function and management framework design perspectives. The authors in [92] extend the analysis to the level of specific protocol functionalities, messages and parameters at RRM, RLC, MAC and PHY layers. They also propose a solution on how to implement slice configuration and management functionality into the 3GPP NG-RAN protocol stack, and present simulation results demonstrating the different levels of isolation achieved between RAN slices, depending on the configuration of shared and dedicated resources at different protocol layers of the RAN slices.

Regarding the different options to implement resource slicing in RAN, [93] analyses four different approaches from traffic (e.g. overload situations) and radio-electrical (e.g. mutual interference) isolation perspectives. The analysed four RAN slicing approaches are based on spectrum planning, Inter-Cell Interference Coordination (ICIC), packet scheduling and admission control functionalities. As the analysed RAN slicing approaches are hierarchical, in the sense that if resource slicing is performed at the highest spectrum planning level, the configuration of ICIC, packet scheduling and admission control functionalities can be customised for each slice. Similarly, if slicing is implemented utilising ICIC, the packet scheduling and admission control functionalities can be configured slice-by-slice, and so on. The higher in the hierarchy the slicing approach is, the larger is the area and the longer the time it covers, and the better is the traffic and radio-electrical isolation that can be achieved, i.e. spectrum planning offers the best isolation between RAN slices. On the other hand, the RAN slicing options lower down in the hierarchy, especially the ICIC and packet scheduling-based approaches, offer higher granularity for reconfigurations and, consequently, offer more flexibility and adaptability for dynamic slice management than RAN slicing implemented with spectrum planning.

For EuWireless, the first priority in RAN slicing should be to maximise the isolation between the experimental traffic and the traffic of the commercial MNO customers. Configuration, flexibility and adaptability of the RAN slices should be a secondary requirement, which can be pursued in order to facilitate the operations of the EuWireless operator, but should not do so at the expense of the achieved isolation.

Software Defined RAN (SD-RAN) concept pursues the abstraction of RAN by providing APIs to dynamically manage the resources assigned to network slices. In this line, several studies and approaches have been published:

- FlexRAN [161]: This is a programmable SD-RAN architecture that separates control from data plane through a custom-tailored southbound API. The control plane provides support for real-time RAN control applications and programmability to adapt as SDN/NFV technologies evolve. It is also able to dynamically modify the degree of coordination between base stations to run under centralized and distributed modes of operation.
- xRAN [162]: This initiative aims to decouple control and user planes and design standard interfaces to control the later one, abstracting the underlying network infrastructure. The key idea is to separate service definitions from hardware. The programmable control plane allows users to seamlessly adapt network behaviour to their needs. xRAN has three main components:
    - Decoupled Data/User Plane.
    - Software Defined Control Plane.
    - Slicing Plane.

xRAN Forum joined forces with C-RAN Alliance at the beginning of 2018 and formed the Open RAN (ORAN) Alliance, a consortium with the aim of evolving the RAN to 1) make it more open and smarter by using real-time analytics for machine learning systems and artificial intelligence and 2) provide virtualized elements of the network with open and standardized interfaces through ORAN Alliance reference designs (more details in section 5.3)

4.4.4 Network slicing with 5G CORE

In [163], the authors study different approaches to support network slicing in terms of various perspectives and requirements:

- Isolation between network slices.
- Allowed/required network sharing.
- Multiple slices serving an UE.
- Network slice creation/composition/modification/deletion.
- NFs to be included into specific network slice instances or to remain independent.
- Procedure for selection of network slices.
- Support for network slicing roaming scenarios.
- Support for 3rd parties to utilize network slicing.

As a result of this study, three groups of potential solutions were defined:

- Group A: Shared RAN NFs, dedicated core NFs. The UE obtains services from different network slices and different CN instances, aiming at logical separation/isolation between the CN instances, in a similar fashion to eDECOR. This option entails potential signalling increase in the network and over the air but facilitates isolation in the CN.
- Group B: Some NFs are common between slices and others dedicated.
- Group C: Control plane is composed of shared NFs whereas Data plane is composed of slice specific NFs.

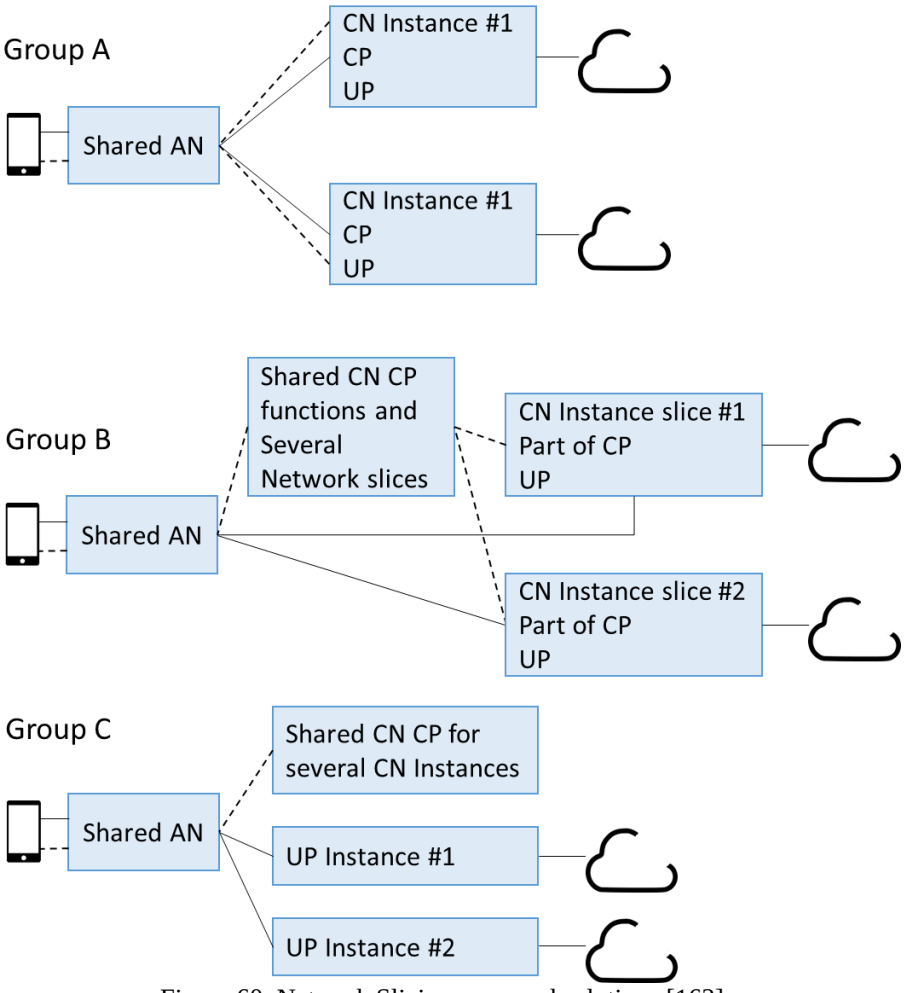


Figure 60. Network Slicing proposed solutions [163]

4.4.5 Slice Selection

According to 3GPP [7], a 5G network slice is defined within a PLMN and shall include:

- CN Control Plane and User Plane Network Functions.
- At least one of the following entities:
  - NG RAN.
  - N3IWF (Non-3GPP InterWorking Function)

Network Slices are identified by the parameter Single Network Slice Selection Assistance Information (S-NSSAI), which is comprised of:

- Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services. There are 3 standardised SST values so far: eMBB (1), URLCC (2) and MIoT (3).
- Slice Differentiator (SD), which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

During registration, based on the Requested NSSAI and the Subscription Information, the network shall select the Network Slice instance(s) to serve the UE, including the 5GC Control and User Plane Functions. The Requested NSSAI could also be used by the (R)AN to handle the UE Control Plane connection (in case of no 3G-GUTI (3G-Global Unique Temporary Identity)

provided). When the UE gets registered, the CN informs the (R)AN by providing the Allowed NSSAI [90].

Figure 61 depicts the selection process of the AMF during registration procedure:

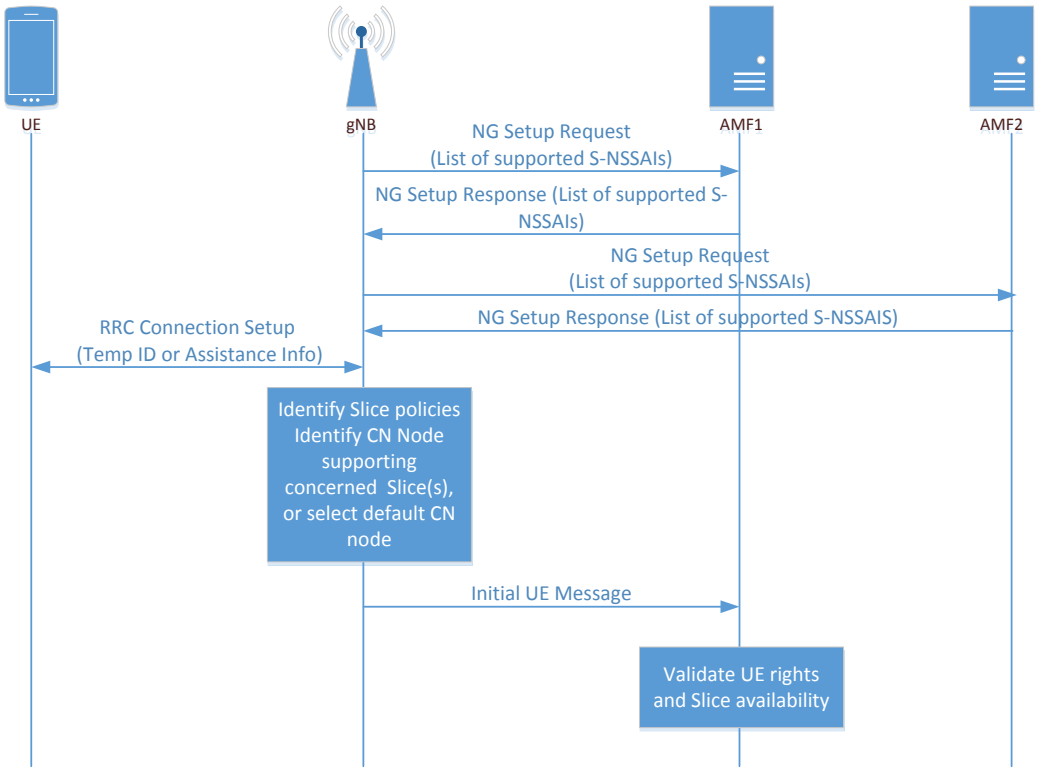


Figure 61. AMF instance selection [90]

The RAN entity (gBN) establishes connections with a set of AMFs and gathers the lists of supported S-NSSAIs from each one. Upon UE registration, if no former connection information available, the gBN uses the assistance parameters provided by the UE to select the appropriate AMF instance. If such information is also not available, a default AMF instance could be selected.

4.5 User access authorization and management

One of the main services provided by EuWireless is to offer researchers and other academic institutions access to the network to perform experiments that are not possible in a live commercial network. This access could include from aggregated data of bandwidth or QoS from the user perspective, to development and testing of new communication algorithms in any layer of the mobile stack. It is obvious that not everyone should have access to the internals of the network but only authorized researchers and, among them, only to the parts relevant to their experiments. It is necessary then to set up an architecture of Authentication, Authorization and Account (AAA) for researchers as well as for final users.

4.5.1 Computer networks user management

There are several architectures that perform AAA duties in a scale large enough to be useful to a network operator, such as Active Directory [176] or TACACS [175]. In computer network environments one of the most successful technologies is the RADIUS protocol, which is also the basis of the one used by mobile operators.

RADIUS [173][172] (Remote Authentication Dial-In User Service) is a standard protocol to authenticate and authorize users. Defined in 1998, it was quickly adopted for organizations to centralize the access from users to the resources of the network. However, while the definition of the third generation of mobile networks (3G or UMTS) was taking place, some limitations of the protocol became apparent:

- It was not extensible, meaning that services not in the protocol design were difficult to be widely adopted.
- It was designed to accommodate any number of users, but resource consumption and management becomes cumbersome when that number reach the millions of records traditional mobile operators have to allocate.
- The design did not include security aspects for the communication itself.

To overcome these limitations, the 3GPP consortium involved itself with the development of a successor to RADIUS, coming up with the DIAMETER [174] protocol with several enhancements compared to RADIUS:

- Protocol capabilities negotiation between parties.
- Error notification.
- Extensibility, through addition of new commands that can be negotiated during the communication setup.
- User sessions or accounting and session state maintenance provided to final applications.
- Accounting could be independent of the session management.

DIAMETER was clearly superior to RADIUS and was mandatory to use it by the 3GPP standard, so every operator adopted it. However, in the computer network world the RADIUS protocol was also evolving in parallel to the deployment of DIAMETER and its shortcomings were fixed, resulting in two equivalent but incompatible protocols.

4.5.2 Challenges in user management

The primary goal of EuWireless is to provide access to the network for the European academic community so, ideally, it could accommodate several millions of university students, researchers and experimenters across the continent. From the traditional perspective, every carrier maintains a database of its entire user base and every user is issued a SIM card that serves as authentication mechanism for the user to connect to the network. This approach will not work with a pan- European operator such as EuWireless for several reasons:

- Every institution (academic or otherwise) has different policies regarding its users. What is available from an operator in a country may not be in another, or even go against the local law.
- Need to maintain a 24x7 service only for authentication, plus coordinating the policies so that every institution can subscribe or unsubscribe its users at any given time.

The new European general data protection regulation imposes strict limitations of what can be done with the user data, including any information that can identify an individual user. Using a distributed approach regarding the authentication and authorization probably solves the previously noted problems. The vast majority of prospective users will be associated to a university or other academic or public institutions, so the authorization may be delegated to the existing infrastructure of the partner. For users not in that group, for example R&D done by a business entity who wants to use EuWireless infrastructure, having an in-house authentication method thanks to the more manageable size of this group would be feasible.

This approach is successfully used by large public organizations that manage millions of users such as Eduroam, the international academic consortium that provides Wi-Fi access to researchers and students in almost every university in Europe. However, even though Eduroam

has its roots in the computer network landscape, this organization relies in RADIUS protocol for authentication services.

4.5.3 Current mobile access methodology (SIM access)

Nowadays access to the mobile operator network is based on cryptographic keys distributed to the user by the operator in the form of a SIM card. In fact, the SIM card only stores these keys and a unique identifier for the card (the IMSI number) and it is the network who associate the card with a phone number or with a certain service.

Researchers could access the EuWireless network in two different ways: the first one assumes the researchers are directly connected using resources, such as spectrum and SIM cards, completely owned by EuWireless. In the second one, that would be the usual one, the EuWireless researchers use a commercial operator to access the network resources and services provided by EuWireless. From the point of view of that commercial operator, the user identification is indistinguishable from the standard roaming scenario between operators detailed in Section 4.3.3: once a user reaches the visited network, a request to identify the user is sent to the user's home network and, if it is authorized, the operator provides connectivity. Section 4.3.3 introduces the two standard approaches that are currently implementable: "Local BreakOut" and "in Home-Routed".

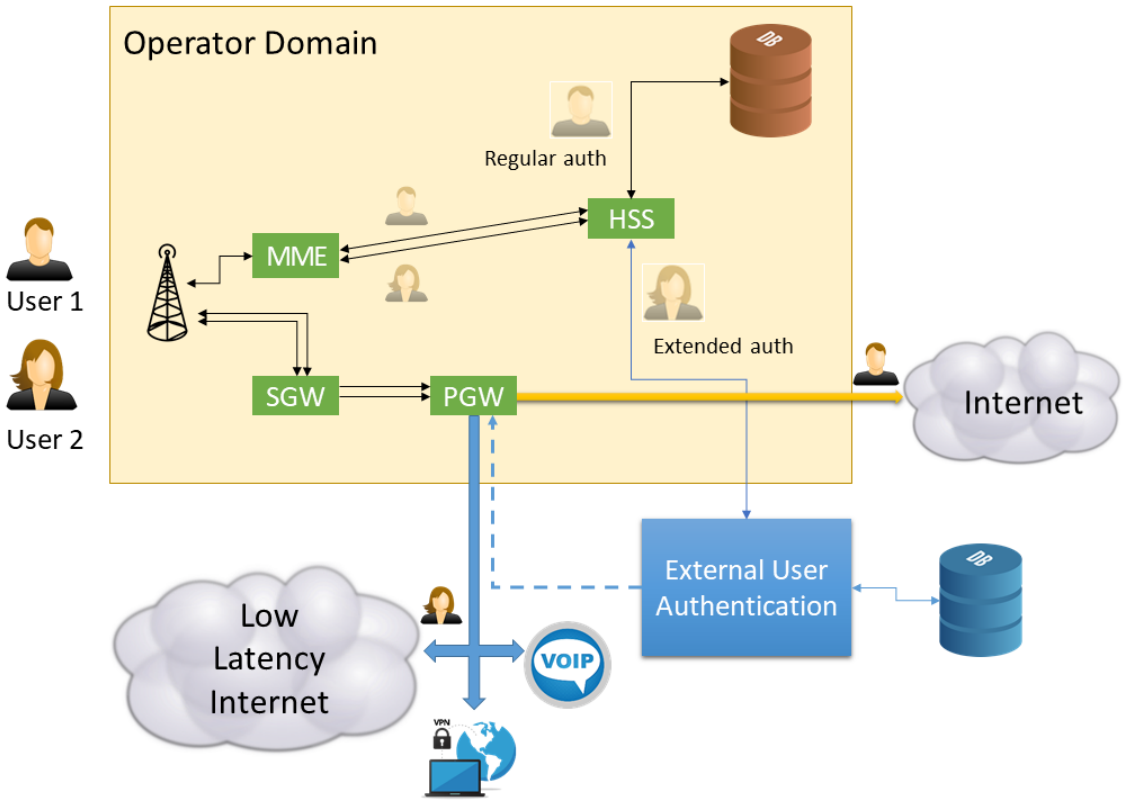


Figure 62: Architecture to provide enhanced services based on external authentication

4.5.4 Changes in future 5G deployments

The proposed 3GPP architecture for 5G changes completely the high-level landscape of the network. Some of the most radical changes that affects the communication between operators are:

- Network slicing: separation and possible isolation of the control plane and the user plane, offering flexible placement both for different services (e.g. to provide services closer to the RAN and hence closer to the user).
- Service Based Architecture (SBA): 5G networks are designed to allow abstract services with native support of the network, instead of the network oriented architecture on top of which services can be built. SDN and NFV are expected to be heavily used to provide the foundation of this kind of services.

In the context of user authentication and service provision, 5G standard introduces new use cases (i.e. IoT, privately owned networks, different access technologies) and thus, the authentication method is more fine-grained and with more optional steps. The primary authentication method, which will be mandatory, grants the user access to the 5G core network. In addition, other secondary authentication methods can be used to authorize the user in additional services, such as VPN access, different QoS, and so on. This scenario, in conjunction with the network slicing capabilities, greatly simplifies the operation of EuWireless when using another operator's network.

The security mechanisms are also expanded to more elements of the stack, so it is no more a binary yes-no situation for the entire connection. The standard specifies several security Termination Points that can be used to allow or restrict access to the RAN, security within the UE (e.g. eSIM credentials provided or updated securely by the operator), different Radio Access Technologies (RAT) or different network slices supported by the operator.

5 Artificial Intelligence

This section introduces fundamental concepts in AI, shows the relationship between AI and candidate features in 5G cellular networks, and provides some examples of how 5G networks can exploit AI to achieve intelligent networking.

5.1 Introduction

Artificial intelligence (AI) is a term for simulated intelligence in machines. These machines are programmed to "think" like a human and mimic the way a person acts. It was in the mid-1950s that McCarthy coined the term “Artificial Intelligence” which he would define as “the science and engineering of making intelligent machines”.

AI now consists of many fields. The most relevant are introduced below [189].

- Data Science: Data is increasing and growing at an unprecedented rate and it is very important to organize such data and understand it. The understanding of data will not only help in organizing it but it will also help in managing the work and making aware what impact data takes place. Data Science helps to manage the data, analyse it and create meaning for the data that companies have. All this is possible by applying data analytics to the data and then coming up with some meaning that is understandable by the end user.
- Machine Learning: Machine Learning is creating news every day with some new product launched by a company which makes use of ML techniques and algorithms in order to serve the consumer in a highly productive manner. Machine Learning performs tasks that can help to classify, categorize and predict data from a given dataset. Machine Learning models are made by complex math level skills, which are then coded in a language in order to build the entire system.
- Neural Networks and Cognitive Science: Neural Networks and Cognitive Science is a branch of Artificial Intelligence which makes use of neurology. Neurology means the branch of biology that deals with the nerves and the nervous system of the human body. Neural Networks and Cognitive Science deals with replicating or imitating the human brain by coding the it into a machine or system. By using a neural network and machine learning together, complex tasks can be easily performed and/or automated.
- Image Processing and Multimedia Analysis: Nowadays, there is not only text data but also multimedia data, in the form of images, audio, video, etc. To understand this multimedia data, using image processing and multimedia analysis is needed. The processing algorithms process the data internally and try to understand what the data may contain and what information it conveys. By using this and understanding what the multimedia data has to say, one can make it useful for many smart purposes where an image is scanned and an output associated with that image is shown directly based on understanding the content of the image.
- Robotic and Embedded Systems: This field involves the use of hardware and software components where both take part together to provide a system that helps the users to perform their tasks and work. Robots are used nowadays in manufacturing industries, where work is performed much faster, more accurately and more efficiently. This is possible with the use of robotics and embedded systems.

Data Science and Machine Learning are the fields that have more potential for enhancing mobile network development. There are four types of analytics that can be applied for mobile networks design, operation, and optimization. ML techniques and statistical models support the different types of analytics below:

- Descriptive Analytics examines and analyzes past performance by mining historical data to discover the reasons behind past successes and failures. Management reports such as sales, marketing, operations, and finance make use of this type of post-mortem analysis.
- Diagnostic Analytics focuses on determining what factors and events contribute to and explain the outcome. It is all about making 'why' statements.
- Predictive Analytics turns data into actionable information. Predictive analytics use data to determine the probable future outcomes or the likelihood of any particular event to occur. Predictive analytics employs statistical techniques that include ML, modelling, data mining, and game theory to assess current and historical facts to predict future events.
- Prescriptive Analytics automatically synthesizes Big Data, business rules, and ML to suggest decision/action options to take advantage of the predictions. Prescriptive analytics continually and automatically processes new data to improve prediction accuracy and provide better decision options.

Another technology which is now bringing a huge variety of applications is Deep Learning (DL). DL is a branch of ML based on algorithms that model high-level data abstractions using multiple processing layers, complex structures, and/or non-linear transformation. For instance, automatic anomaly detection systems are based on DL.

5.2 Uses Cases of AI in 5G

This section presents some examples of use cases where AI technologies will enable 5G advanced features.

5.2.1 Self-Learning and Adaptive Networks

A fundamental challenge in 5G networks design will be to manage and allocate resources to meet traffic demands under difficult constraints. Problems traditionally are resolved by applying sets of rules derived from system analysis and simulation with prior domain knowledge and experience. The level of intelligence is determined in the design phase, and the system behaves according to pre-programmed rules. However, this method faces increasing challenges due to today's dynamic and diverse traffic, and the complexity of network architectures and resource structures. In [190], the authors envision that 5G networks will be self-learning and adaptive to the needs of its user devices, radio conditions, and characteristics of the application-based traffic. Decision quality will continue to grow by learning from past behaviours and outputs, and also from similar entities in the same or other networks.

5.2.2 Proactive Network Monitoring and Root Cause Analysis

Network monitoring and maintenance are critical tasks in network operations. Today, network operators rely on alarms for monitoring. However, static alarm thresholds at the cell level lead to many missed alarms due to the dynamic nature of the cellular environment. For root cause analysis, network operators rely on knowledge-based engineering troubleshooting guides, although there are clear limitations to this approach. First, because engineers often propose one-size-fits-all guidelines, the rules may be inaccurate or need to be adapted to a different market. This is no longer acceptable. Second, and more importantly, these troubleshooting guidelines are limited by engineering knowledge and are useful only for 'known' issues. It is common knowledge that new issues occur for many reasons that require experienced engineers to investigate and formulate solutions. This can take a long time to resolve, making customers unhappy. This gap in time also can increase the cost of operation. In a world of instant gratification, this approach is insufficient. By applying diagnostic analytics, quick and accurate root cause analysis can be performed to detect network problems and resolve them, even before they occur.

5.2.3 Automated and Closed-Loop Optimization

Today, optimization relies on engineering knowledge and manual processing and analysis. However, the growing complexity of network technologies and cost-saving pressures call for more automated and scalable solutions. The key capabilities that enable automated and closed-loop optimization are the root cause and/or specific scenario incidents that trigger optimization engines or agents. The engine or agent combines domain knowledge and data-driven search settings.

5.2.4 User Experience-Driven Network Planning

Network planning is the first and most critical step for any network rollout. The quality of planning determines, to a large extent, user experiences and Return On Investment (ROI). Traditional network planning tools focus on the coverage capacity for voice services that is relatively simple to predict. Today, data traffic (including video) dominates the cellular traffic mix, while user experiences depend heavily on optimized parameters like data throughput and delay. ML and predictive modelling enhance network planning tools so that the network is more likely to meet not only the coverage target but also the user experience requirements of all customers.

In the past, for 4G networks, there has been work to explore ML technologies and their applications for pipe design and operation. For example, cell-level anomaly detection and root-cause analysis that have been tested in real network environments and have gained very positive feedback from operators.

5.2.5 Autonomous Driving

Another use case where 5G and AI fully merge is Autonomous Driving, where the car has to continuously collect millions of data points from its thousands of sensors, dozens of cameras and multitude of other monitors. This data is fed to highly sophisticated algorithms, the "intelligence" of the self-driving AI systems. In traditional 4G based solutions, the data collected from the vehicle will be sent to the cloud for processing, and instructions will be sent back to the vehicle [191]. However, for a moving vehicle in which decisions have to be made in milliseconds, this approach will not work.

The question for any effective AI system is where the intelligence should lie, in a centralized cloud or in a device. This dichotomy is applicable to many AI applications and use cases. For instance, extended reality (AR/VR), medical applications, robotics, industrial, consumer, etc. The obvious choice is to keep intelligence at the edge or as close as possible to it. However, devices typically have limited processing power and are battery powered and cannot replicate the performance of the cloud. Then, the solution is to move the intelligence that deals with immediacy toward the edge, keep processing-intensive functions in the cloud, and use 5G networking enablers to connect them intelligently.

5.2.6 Internet of Things

Finally, another use case which will rely on 5G and AI altogether is IoT. 5G and AI will enable large-scale internet of things applications and support blisteringly fast data processing across a diverse array of devices on a massive scale.

5.3 Industry and Research Community

In the Mobile World Congress (MWC) 2018, several major network operators announced the merging of the xRAN Forum with the C-RAN Alliance to form a world-wide, 'carrier-led' effort to push more openness into the radio access network of the next-generation wireless system, the ORAN Alliance. According to [192], ORAN will combine and extend the efforts of the C-RAN Alliance and the xRAN Forum into a single 'operator led' effort. There are two main ideas: evolving the radio access networks to make them more open and smarter than

previous generations by using real-time analytics for machine learning systems and artificial intelligence. Secondly, to equip virtualized network elements with open, standardized interfaces through ORAN Alliance reference designs.

In July 2018, Nokia and China Mobile agreed to jointly investigate the potential of artificial intelligence (AI) and machine learning in 5G networks. They want to "make joint effort in the O-RAN alliance which was kick offed recently to enhance the intelligence of 5G networks, reduce the complexity, and explore the new capabilities of the network" [193].

There are already many research studies which envision synergies between 5G and AI. The following are a few examples.

- In [194], the authors highlight the opportunities and challenges to exploit AI to achieve intelligent 5G networks and demonstrate the effectiveness of AI to manage and orchestrate cellular network resources. They envision that AI-empowered 5G cellular networks will make the acclaimed ICT enabler a reality.
- In [195], ZTE believes that AI can also greatly help telecom carriers optimize their investment, reduce costs and improve O&M efficiency, involving precision 5G network planning, capacity expansion forecast, coverage auto-optimization, smart MIMO, dynamic cloud network resource scheduling, and 5G smart slicing.
- In [196], Intel envisions that the ability to access additional information quicker through 5G networks will help AI-enabled devices understand their environment and the context in which they operate. This will supercharge AI-powered services, making them more reliable in a broad range of situations.

There are also more works in the pipeline. Table 5 shows the suggested in some relevant recent magazines topic which provides insight about what is coming in the near future as for 5G and AI.

Table 5. Applications of AI in 5G

Topics of Research: Applications of artificial intelligence in wireless communications [197]
Deep-learning and convolutional neural network approaches for wireless system applications and services
Machine-learning and pattern recognition algorithms for wireless communication technologies
Applications of AI for optimizing wireless communication systems, including channel models, channel state estimation, beamforming, code book design and signal processing
Applications of AI for 5G wireless transmission technologies, including coordinated multiple points transmission/reception, large-scale antenna array, and multi-hop relay
Applications of AI for 5G mobile management, including user association, handoff strategy, and backhaul technology
Applications of AI for 5G resource management, including spectrum resources, energy sources, cloud resources, computing resources, and communication infrastructure
The analysis and prediction of 5G network behaviour via AI technologies, including the multi-media traffic load, network overhead, and network collision
Evaluating the scope for and potential limitations of AI solutions in wireless communications

6 GÉANT Testbed Service

6.1 Overview of GTS

The GÉANT Testbeds Service (GTS) is a product of the GÉANT Network, a project funded by the European Commission and over 40 European national research and education networks (NRENs). The GÉANT project is missioned to provide networking infrastructure and services to enable collaborative science and education among the European NRENs and to/from international partner R&E networks globally. The GÉANT Network delivers high performance and transport and world class support services among these National R&E Networks (NRENs) who in turn deliver these capabilities to their constituents in each country. The EuWireless project sees this GÉANT infrastructure and collaboration as the backbone glue among regional, metro, and campus based MNOs and the applications and research activities they will address.

In 2013, the GÉANT [178] Project initiated the development of "Testbeds as a Service". The objective was to develop a service capability that would allow network researchers to deploy innovative concepts and run network experiments "at scale" across the GÉANT core backbone facilities. These experiments are able to coexist in parallel without interfering with one another and without interfering with other more mature applications or services using the same infrastructure. The service architecture drew upon and refined technologies and concepts explored in research projects in the EU FIRE [179] program and the US GENI [180] program. The service architecture evolved and is now based upon rigorous virtualization principles, extensive automation, and advanced orchestration and scheduling.

The service offers e-infrastructure resources such as virtualized compute platforms, SDN based switching/forwarding elements, transport circuits, and storage integrated with the core network footprint. These virtual resources can be tuned to user requirements and are under user control. They can be geographically located according to user topological and/or data flow requirements across the WAN infrastructure. The GTS service facilities are currently deployed in eight major European cities. This service has been re-named GÉANT Testbeds Service (GTS) [83] [84] and has been in pilot operation since 2014. GTS has matured and will be offered as a fully supported GÉANT production service beginning in 2018-Q4. The service offers researchers the possibility of defining, building and testing very agile virtual networks quickly, easily and cost-effectively.

The main advantage of this testbed environment is the full isolation of each experiment or testbed from other testbed domains, which offers to the researchers and experimenters resources within a real network to conduct their experiments with no effects of/on other testbeds or production services. The list of available resources includes mainly virtual machines, virtual circuits and instances of OpenFlow switches. This portfolio of resources can be expanded to include other virtualized facilities such as wireless or mobile resources. New resources classes need only develop a minimal set of resource control primitives to allow GTS to process them. To offer such a customized experimental network facility it is necessary to put in place two main components:

- Point of Distribution (PoD): the physical infrastructure that hosts the virtual resources available for the experimenters' use. PoDs are distributed in different geographical locations that can be referred to as the data plane of the testbed service. The GTS PoDs may vary in their inventory from one or two servers and a switch to a dozen or more servers with high performance SDN switching/forwarding hardware.
- Central Server Facility: the physical location of components and servers hosting the GTS control and management agents. The CSF also supports ancillary functions such as common access gateways that allow users to easily log into and reach their testbed components and persistent storage available for users to archive important data or results

of their projects. The CSF is nominally three or four servers depending on the number of users or projects.

The GTS service architecture evolved to one that is fully virtualized; i.e. all GTS user resources are implemented according to rigorous virtualization/abstraction rules that allow a common lifecycle service model to be applied to all such resources. This allows all resources to be managed and manipulated in a common manner in terms of reservation and scheduling, resource provisioning and performance verification, querying of state, and release of the resource when no longer needed. This architecture has been distilled into a Generic Virtualization Model (GVM) that abstracts the service objects into virtual resources that can be dynamically reserved and assigned to research projects and arranged into network topologies defined by the researcher. EuWireless proposes the use of this GVM to create a flexible and extensible facility for network research that can incorporate novel resource objects (such as eNodeB facilities, or spectrum assets, etc.) and extend emerging virtualized functional networking and network slicing to the mobile edge.

NORDUnet believes that GTS can define a spectrum resource that could be managed by GTS and shared amongst many potential wireless or mobile users. GTS does not develop the hardware, but develops the virtualization model and software virtualization functions by which the spectrum or associated physical facilities could be abstracted and manipulated by the research users to reserve/release spectrum as a resource, activate/deactivate the resource, or query the resource state. Once activated, the GTS software control plane does not intercept or act as intermediary between the researchers and the resource. The researcher is able to leverage that resource as needed to pursue their objectives. These functions define the lifecycle of the GTS virtual resource. While these virtual resources are intended to provide the researcher with facilities indistinguishable from dedicated physical facilities, the degree to which this can be accomplished is a function of the conceptual model for the virtual service object, the needs of the researchers, and is predicated upon proper secure and authorized access mechanisms to configure the underlying physical infrastructure facilities.

6.2 Experiment life cycle management

The GVM proposed by GÉANT defines resources as independent abstracted objects, each with specific attributes and data exchange capabilities. These objects are all manipulated through their lifecycle with a common set of very basic lifecycle primitives that Reserve (allocate and hold infrastructure facilities for a resource instance) and Release resources, Activate them (realize them in the infrastructure) or Deactivate them, and Query them (obtain their present state). These virtualized resources can be interconnected into user specified topologies or service graphs. These collections of interconnected virtual resources, known as testbeds or network slices, are under user control and function independently of other such virtual environments.

The GVM resources are defined using resource classes. Each class definition is a template that specifies a set of class attributes that characterize it and define its behavior. The attributes form the constraints used to find and reserve infrastructure suitable to instantiate objects of that class.

Within GVM, all resource classes must conform to a common object lifecycle model. This model consists of a Reservation phase where the necessary infrastructure is found and held in order to instantiate the desired resource, followed by an Active phase where the resource is realized in the infrastructure by configuring the hardware appropriately. The Active phase can be deactivated returning the resource to the Reserved state, or it can be deactivated and the reserved infrastructure released altogether; i.e. each virtual object is processed through its life cycle with a very basic set of lifecycle primitives consisting of a Reserve() primitive and complementary Release() primitive to perform scheduling and infrastructure allocation and

release, Activate() and complementary Deactivate() primitives to perform provisioning and configuration of underlying infrastructure to realize the resource object and place it in service, and a Query() primitive to retrieve resource state. The user interaction with the GTS service is through these primitives, even though the GTS GUI is implemented as a user agent that employs these primitives to communicate the user's slice configuration to the service.

Each resource class is implemented within the GVM software architecture via a Resource Control Agent (RCA). RCAs are software agents that implement the lifecycle primitives noted above. These are not "runtime" modules that do the actual hardware virtualization, but rather management and control entities that leverage the runtime capabilities implemented by/within other packages or technologies. For instance, RCA-OS implements the virtual machine class (Host). It converts the GVM lifecycle primitives to a southbound interface to OpenStack (OS) to acquire and spin up VMs of appropriate flavors. While the GVM lifecycle model and primitive set is the same for all virtual objects, the underlying implementations can be quite different depending upon the class. Thus, there are different RCAs for virtual machines, bare metal servers, virtual circuits, virtual (SDN) switches, etc. Hence, the GVM common lifecycle model and the virtualized object model form a "normalization layer" within the virtualized service architecture that allows almost any type of e-infrastructure component or logical network function to be conceived as a virtual object and specified as a GVM resource class.

This hierarchical modularity and extensible class specifications is key to creating an operationally supportable service model for production services. One of the key features of such a simple and generalized virtualization model is its extensibility, i.e., its ability to incorporate arbitrary new resource classes with the development of an appropriate virtual object model, and the RCA software to implement the lifecycle primitives. The EuWireless project leverages this extensibility by defining one (or several) virtual objects, and then to develop an appropriate RCA module. The GÉANT GTS Software Suite implements the GVM architecture and provides RCAs for a number of basic virtual resources. EuWireless will define additional resource classes appropriate to mobile wireless networks and expected experimental needs, and develop the associated RCAs to support those objects. These mobile resource RCAs can be plugged into the base virtualization software suite, and appropriate physical infrastructure can be placed under control of those RCAs, resulting in an integrated and comprehensive facility to create user defined and user controlled environments – network slices.

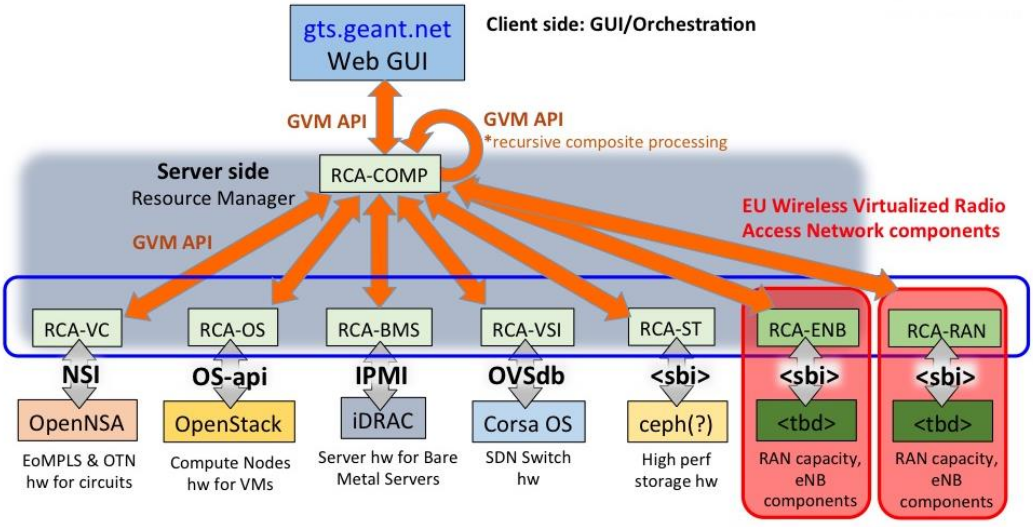


Figure 63. GVM incorporating EuWireless Resource Control Agent(s)

7 Conclusions

The current identification of enabling technologies will be revised in the design of the final EuWireless architecture in deliverable D2.2. However, from the current analysis the consortium concludes that such design and implementation is feasible. To justify this statement, the following table provides some arguments (not exhaustive nor complete).

Table 6. Enabling technologies justification

Enabling technologie	**Why is relevant to implement EuWireless**
Architecture of a 5G network and main components	5G System is going to be the most relevant mobile communication network in the world in the short and middle term. In Europe, they plan to deploy extensively 5G, a technology which, moreover, aims to integrate a wide range of consolidated as well as brand-new technologies under a unique platform. In such a context, analysing the architecture of 5G and comprehending its main components, functionalities and how they interact is mandatory to EuWireless project. For this purpose, this document provides relevant information on the architecture of 5G System, mentioning also the phases of the process of specification by 3GPP.
Heterogeneous networks	Nowadays a relevant part of existing traffic is performed in indoor environments, making heterogeneous network a necessary ally in 5G networks. Moreover, Wi-Fi has become ubiquitous and is called to play a key role in these future networks. Other technologies show their value for IoT applications, with optimized access and power consumption characteristics or for specific verticals applications, such as 'Connected car' technologies in the automotive case.
Multiple Connectivity	With the growth of multihomed devices and NATs, multiple connectivity is gaining importance, and proposals are being developed and standardized. It is interesting for EuWireless since it allows to adapt to scenarios with different requirements, such as those demanding high throughput or strong reliability and can offload network congestion, being beneficial to both users and network operators. Link layer technologies are widely used and implemented in commercial equipment, taking advantage of its performance improvement. Network layer offers the ability of managing mobility and adapt to specific traffic scenarios while transport layer multiple connectivity is easy to deploy as it is transparent to the network architecture. Finally, Application layer aggregation is the less interesting,

	since it does not exist any standardized or widely used protocol.
Virtualization technologies	Network virtualization has recently become more of a focus, with the growth of Software Defined Networking and Network Function Virtualization and the resulting decoupling of application, control, and data planes. In the near future, mobile communications will require large amounts of wireless resources to deal with the heterogeneity of the networks and the high data rates expected. Hence, virtualizing mobile networks will result in more efficient utilization of the shared wireless resources. By using network virtualization, organizations could centrally provision the network on-demand, in order to scale and adjust the resources available to their evolving needs without physically modifying the underlying infrastructure. All of this will allow EuWireless to deploy the Research Network as a Service, adapting the network to the specific needs of each user.
MEC	In EuWireless, the MEC/fog initiatives should be traced mainly from perspective of their relation to multi-tenancy, vRAN deployment and the support for potentially heavy computations related to the experimentation instrumentation and data processing. Still these functionalities should further be studied in the remaining deliverables of EuWireless. Both MEC/fog solutions as well as their implementations available e.g. inside European testbeds (e.g. Fed4FIRE, 5GinFire) will be considered when identifying means to further experiment with MEC/fog in the project.
APIs for Function Exposure	The identification of standard approaches for interacting with commercial mobile networks is key to attract and involve mobile operators in EuWireless deployments. At the same time, the usage of standards APIs for accessing to the network capabilities also reduces the complexity and the cost of the implementation. Finally, the standard APIs guarantee the interoperability and sustainability of the architecture proposed in the project as the new features developed in the new 3GPP releases will be also accessible through these APIs.
Spectrum sharing	LSA seems to be the most relevant option for implementing dynamic spectrum access in EuWireless. During the last few years, several LSA trials have been successfully carried out in Europe demonstrating the potential for improving the performance of the networks. In addition, regulation work is ongoing for supporting the LSA deployment in Europe. In EuWireless, the centralized

	coordination will be the natural coordination method as it is a prerequisite for implementing the LSA. However, hybrid coordination is a promising way to improve the performance of the networks, so in EuWireless it will be considered as a method for joining some decentralized coordination aspects with mainly centrally coordinated spectrum management. EuWireless will build upon the state-of-art solutions presented in section 4.1 and will focus on enablers that are crucial in order to progress beyond state of art towards cellular RAN infrastructure that effectively can be utilized in agreement between incumbent and operators.
RAN sharing	In C-RAN architectures, the centralized processing of RAN traffic in data centre based BBU pools enables better coordination of transmissions between neighbouring sites. If the BBU resources are fully virtualized, deployment of private RANs on top of the same physical infrastructure is also enabled and EuWireless could rent the RAN as a cloud service from an MNO. NG-RAN offers additional flexibility to RAN sharing by dividing the processing of the traffic in several logical entities in the RAN architecture, so the sharing can potentially be done for the whole RAN or for just parts of it. Extensive virtualization of the RAN functions enables the NG-RAN to be built using VNF service chaining and be modified e.g. according to the requirements of the targeted EuWireless end user group or use case.
Core network oriented selection methods	Network Sharing is a concept consolidated in LTE which allows MNOs to share same components of their networks, saving resources. EuWireless, as a pan-European operator, could take advantage of these technologies to make use of the infrastructure of MNOs. For instance, MOCN technology would allow the EuWireless Core Network to utilize MNO RAN to serve EuWireless users.
5G Network Slicing	Network Slicing is one of the most promising features of 5G. It allows MNOs and third parties to allocate resources of the network to match specific needs of users in a flexible fashion, including multitenancy and virtualization of network functions. For EuWireless, this feature may be key since it provides means to request ad-hoc end-to-end connections to MNOs on demand and even incorporate EuWireless Network Functions to the slice.
User access authorization and management	Fine-grained user authentication and authorization allow the creation of new services beyond those envisioned in the standard. By using these extended capabilities or delegating them to external entities,

	differentiated access to the network can be easily provided for certain types of users and/or traffic. This will allow EuWireless to provide specific services, like research access or internal networking, while still leveraging the existing infrastructure of commercial operators to provide standard connectivity.
GÉANT Testbed Service	GTS develops the virtualization model and software virtualization functions by which the spectrum or associated physical facilities could be abstracted and manipulated by the research users to reserve/release spectrum as a resource, activate/deactivate the resource, or query the resource state. Once activated, the researcher is able to leverage that resource as needed to pursue their objectives. The GÉANT GTS Software Suite implements the GVM architecture and provides RCAs for a number of basic virtual resources. EuWireless will define additional resource classes appropriate to mobile wireless networks and expected experimental needs, and develop the associated RCAs to support those objects, resulting in an integrated and comprehensive facility to create user-defined and user-controlled environments – network slices.
Artificial Intelligence	The potential of artificial intelligence (AI) and machine learning in 5G networks is well proven in multiple areas such as autonomous driving and IoT. EuWireless will explore the possibilities of AI in the different aspects involved in the development of a pan-European mobile network.

8 References

[1] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper.

[2] NetWorld 2020 ETP 5G Experimental Facilities in Europe White Paper. https://www.networld2020.eu/wp-content/uploads/2016/03/5G-experimentation-Whitepaper-v11.pdf

[3] 5G Infrastructure Public Private Partnership. https://5g-ppp.eu/5g-ppp-work-groups/

[4] Science Wireless Network (SciWiNet). http://sciwinet.org/

[5] 3GPP, "Study on Scenarios and Requirements for Next Generation Access Technologies", TR 38.913, June 2017, Available at http://www.3gpp.org

[6] Dr Ying Li, Multiple Access Communications Ltd, "5G KPI Targets and Enabling Technologies", August 2018

[7] 3GPP TS 23.501; System Architecture for the 5G System. Stage 2.

[8] Global Mobile Data Traffic Forecast, 2016–2021

[9] Wireless Broadband Alliance. "Unlicensed integration with 5G networks". October, 2018.

[10] GSMA London Forum. September 2011, www.gsma.com/iot/lon

[11] 3GPP TS 36.101. E-UTRA;User Equipment (UE) radio transmission and reception. Available at http://www.3gpp.org.

[12] 3GPP E-UTRA and EUTRAN. Overall description. Stage 2. TS 36.300, Release 13, TS 36.300. Available at http://www.3gpp.org.

[13] 3GPP, "E-UTRA; User Equipment radio transmission and reception", Release 13, TS 36.101. Available at http://www.3gpp.org

[14] A technical overview of LoRa and LoRaWAN. https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf

[15] Thread Group webpage. https://www.threadgroup.org

[16] FIWARE webpage. https://www.fiware.org

[17] oneM2M webpage. http://www.onem2m.org

[18] Taking a look inside oneM2M. Nicolas Damour. Available at www.oneM2M.org

[19] 5 starts Open Data webpage. https://5stardata.info

[20] OmniAir Consortium. https://omniair.org

[21] 3GPP, "E-UTRA; Carrier Aggregation; BS radio transmission and reception", TR 36.808, July 2013, Available at http://www.3gpp.org

[22] 3GPP, "Study on Small Cell enhancements for E-UTRA and E-UTRAN; Higher layer aspects", TR 36.842, November 2013, Available at http://www.3gpp.org

[23] Qualcomm, "LTE in Unlicensed Spectrum Research", https://www.qualcomm.com/invention/research/projects/lte-unlicensed

[24] 3GPP, "Feasibility Study on Licensed-Assisted Access to Unlicensed Spectrum", TR 36.889, Available at http://www.3gpp.org

[25] 3GPP, "LTE-WLAN Aggregation", in TS 36.300, section 22A.1, September 2017, Available at http://www.3gpp.org/

[26] 3GPP, "LTE-WLAN Aggregation Adaptation Protocol (LWAAP) specification, Release 14", TS 36.360, Available at http://www.3gpp.org

[27] 3GPP, IP Flow Mobility and Seamless Wireless Local Area Network (WLAN) Offload Stage 2, TS 23.261, Mar. 2012

[28] 3GPP, Multi Access PDN Connectivity and IP Flow Mobility TS 23.861,Febrery. 2010

[29] 3GPP, "LTE/WLAN Radio Level Integration with IPsec Tunnel", in TS 36.300, section 22A.3, Available at http://www.3gpp.org

[30] 3GPP, "LTE/WLAN Radio Level Integration Using IPsec Tunnel (LWIP) encapsulation; Protocol specification (Release 14)", in TS 36.361, Available at http://www.3gpp.org

[31] IETF, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, January 2013, Available at https://tools.ietf.org/html/rfc6824
[32] QUIC Working Group, "Multipath Extension for QUIC", Internet-Draft draft-deconinck-multipath-quic-00, October 2017, Available at https://tools.ietf.org/html/draft-deconinck-multipath-quic-00
[33] F. B. Tesema, A. Awada, I. Viering, M. Simsek, and G. Fettweis. Evaluation of context-aware mobility robustness optimization and multi-connectivity in intra-frequency 5g ultra dense networks. IEEE Wireless Communications Letters, 5(6):608–611, Dec 2016.
[34] J. J. Nielsen, R. Liu, and P. Popovski. Ultra-reliable low latency communication using interface diversity. IEEE Transactions on Communications, 66(3):1322–1334, March 2018.
[35] Philipp S. Schmidt, Theresa Enghardt, Ramin Khalili, and Anja Feldmann. Socket intents: Leveraging application awareness for multi-access connectivity. In Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, CoNEXT '13, pages 295–300, New York, NY, USA, 2013. ACM.
[36] ETSI GS NFV 003, "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV", V1.1.1, Oct. 2013.
[37] Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks", ONF White Paper, Apr. 13, 2012.
[38] Open Data Center Alliance, "Open Data Center Alliance Master Usage Model: Software-Defined Networking Rev. 2.0", White Paper, 2014.
[39] Open Networking Foundation (ONF) TS-025, "OpenFlow Switch Specification", V.1.5.1 (Protocol version 0x06), March 2015.
[40] Stallings, W., "Software-Defined Networks and OpenFlow", in The Internet Protocol Journal, Volume 16, No. 1, March 2013.
[41] Open Networking Foundation, "OpenFlow Switch Specification Version 1.3.0", June 2012.
[42] ITU-T Y.3300, "Global Information Infrastructure, Internet Protocol aspects and next-generations networks. Framework of Software Defined Networking", Jun. 2014.
[43] ETSI, "Network Functions Virtualisation. An introduction, benefits, enablers, challenges and call for action", Introductory White Paper, Oct. 2012 at the "SDN and OpenFlow World Congress", Darmstadt-Germany.
[44] ETSI GS NFV 002, "Network Functions Virtualisation; Architectural Framework", V1.2.1, Dec. 2014.
[45] Khan, F., "A beginner's guide to NFV Management & Orchestration (MANO)", Apr. 2015.
[46] OSM Project. https://osm.etsi.org/ Last accessed 25 Oct 2018
[47] ETSI, "Open Source MANO. Experience with NFV architecture, interfaces, and information models", White Paper, May 2018.
[48] OpenBaton http://openbaton.github.io/ Last accessed 25 Oct 2018
[49] ETSI GS NFV-EVE 005, "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework", V1.1.1, Dec. 2015.
[50] Shankar Lal, Aapo Kalliola, Ian Oliver, Kimmo Ahola, Tarik Taleb, "Securing VNF communication in NFVI," Standards for Communication and Networking (CSCN), Sept. 2017, Helsinki, Finland.
[51] SHIELD Project (H2020) https://torsec.github.io/shield-h2020/
[52] 5GTango Project (H2020) https://5gtango.eu/
[53] UNIFY (FP7)https://www.eict.de/en/projects/
[54] Panda, A., Lahav, O., Argyraki, K.J., Sagiv, M., Shenker, S. (2014) "Verifying isolation properties in the presence of middleboxes". CoRR abs/1409.7687
[55]
[56] 5GPPP, "View on 5G Architecture", 5GPPP Architecture Working Group, Dec. 2017.

[57] 5GEx Project, “Multi-Domain Network Service Orchestration” whitepaper, http://5gex.eu/
[58] M. Kist, J. Rochol, L. A. DaSilva and C. B. Both, "HyDRA: A hypervisor for software defined radios to enable radio virtualization in mobile networks," 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, 2017, pp. 960-961.
[59] GSMA, “NB-IoT DEPLOYMENT GUIDE to Basic Feature set Requiremets”, April 2018.
[60] Olli Mämmelä, Jouni Hiltunen, Jani Suomalainen, Janne Vehkaperä, “Towards Micro-Segmentation in 5G Network Security,” EuCNC 2016, June 2016, Athens, Greece.
[61] ETSI GS MEC 003; MEC, Framework and Reference Architecture.
[62] De Moura, L., Bjørner, N. (2008) “Z3: An efficient SMT solver. In Tools and Algorithms for the Construction and Analysis of Systems”. Springer
[63] Spinoso, S., Virgilio, M., John, W., Manzalini, A., Marchetto, G., Sisto, R. (2015) “Formal Verification of Virtual Network Function Graphs in an SP-DevOps Context”. In: Dustdar, S., Leymann, F., Villari, M. (eds) Service Oriented and Cloud Computing. ESOCC 2015. Lecture Notes in Computer Science, vol. 9306. Springer, Cham
[64] John, W. et al. (2017) “Service Provider DevOps”. In IEEE Communications Magazine, vol. 55, no. 1, pp. 204-211. doi: 10.1109/MCOM.2017.1500803CM
[65] Basile, C., Canavese, D., Pitscheider, C., Lioy, A., Valenza, F. (2017) “Assessing network authorization policies via reachability analysis”. In Comput. Electr. Eng. 64, C, pp. 110-131. doi: 10.1016/j.compeleceng.2017.02.019
[66] Liu, A., Khakpour, A. (2012) “Quantifying and verifying reachability for access controlled networks”. IEEE/ACM Trans Netw 2012;21 (2):551–65.
[67] Valenza, F., Su, T., Spinoso, S., Lioy, S., Sisto, R., Vallini, M. (2017). “A formal approach for network security policy validation”. In Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 8, no. 1, pp. 79-100.
[68] Shin, M.K., Choi, Y., Kwak, H.H., Pack, S., Kang, M., Choi, J. Y. (2015) “Verification for NFV-enabled network services”. In International Conference on Information and Communication Technology Convergence (ICTC), pp. 810-815. doi: 10.1109/ICTC.2015.7354672
[69] Lee, I., Philippou, A., Sokolsky, O. (2007) “Resources in process algebra”. In Journal of Logic and Algebraic Programming, vol. 72, no. 1, 2007, pp. 98-122, ISSN 1567-8326
[70] Kwak, H., Lee, I., Philippou, A., Choi, J. (1998) “Symbolic Schedulability Analysis of Real-time Systems”. In IEEE Real-Time Systems Symposium, December 1998.
[71] Flittner, M., Scheuermann, J.M., Bauer, R. (2017) “ChainGuard: Controller-independent verification of service function chaining in cloud computing” IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 1-7. doi: 10.1109/NFV-SDN.2017.8169846
[72] Durante, L., Seno, L., Valenza, F., Valenzano, A. (2017) “A model for the analysis of security policies in service function chains”. In IEEE Conference on Network Softwarization (NetSoft), pp. 1-6.
[73] Tschaen, B., Zhang, Y., Benson, T., Banerjee,S., Lee, J., Kang, J.M. (2016).”SFC-Checker: Checking the correct forwarding behaviour of Service Function chaining”. IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 134-140. doi: 10.1109/NFV-SDN.2016.7919488
[74] Fayaz, S.K., Yu, T., Tobioka, Y., Chaki, S., Sekar, V. (2016). “BUZZ: Testing Context-Dependent Policies in Stateful Networks”. The 13th Usenix Conference on Networked Systems Design and Implementation (NSDI’16), pp. 275-289. ISBN: 978-1-931971-29-4
[75] Zhao, M. et al. (2017) “Verification and validation framework for 5G network services and apps”. IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 321-326. doi: 10.1109/NFV-SDN.2017.8169878

[76] Yan, J., Zhang, H., Shuai, Q., Liu, B., Guo, X. (2015). "HiQoS: An SDN-based multipath QoS solution". IEEE China Communications vol. 12, issue 5, pp. 123-133. doi: 10.1109/CC.2015.7112035

[77] Govindarajan, K., Meng, K. C., Ong, H., Tat, W. M., Sivanand, S., Leong, L. S. (2014). "Realizing the Quality of Service (QoS) in Software-Defined Networking (SDN) based Cloud infrastructure". In 2nd International Conference on Information and Communication Technology (ICoICT), pp 505-510. doi: 10.1109/ICoICT.2014.6914113

[78] Egilmez, H. E. Dane, S. T., Bagci, K. T., Tekalp, A. M. (2012). "OpenQoS: An OpenFlow controller design for multimedia delivery with end-to-end Quality of Service over Software-Defined Networks". In Proceedings of The 2012 Asia Pacific Signal and Information Processing Association Annual Summit and Conference, pp. 1-8

[79] Carella, G., Pauls, M., Medhat, A., Grebe, L., Magedanz, T. (2017). "A Network Function Virtualization framework for Network Slicing of 5G Networks". In Mobilkommunikation – Technologien und Anwendungen, pp. 1-7.

[80] Dutra D., Bagaa, M., Taleb, T., Samdanis, K. (2017). "Ensuring End-to-End QoS Based on Multi-Paths Routing Using SDN Technology". In 2017 IEEE Global Communications Conference (GLOBECOM 2017), pp. 1-6. doi: 10.1109/GLOCOM.2017.8254076

[81] Karakus, M., Durresi, A. (2017). "Quality of Service (QoS) in Software Defined Networking (SDN): A survey". In Journal of Network and Computer Applications, vol. 80, pp. 200-218. doi: 10.1016/j.jnca.2016.12.019

[82] Bolivar, L. T., Tselios, C., Mellado Area D. and Tsolis G., "On the Deployment of an Open-Source, 5G-Aware Evaluation Testbed," 2018 6th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Bamberg, 2018, pp. 51-58. doi: 10.1109/MobileCloud.2018.00016

[83] GÉANT, "GTS v2.0 Architecture Guide", 2015.

[84] GÉANT, "GÉANT GTS Service Description", Nov. 2017.

[85] China Mobile Research Institute, "C-RAN: The Road Towards Green RAN," White Paper V2.5, 2011.

[86] A. Checko et al., "Cloud RAN for Mobile Networks - A Technology Overview," IEEE Commun. Surv. Tutorials, vol. 17, no. 1, pp. 405–426, 2015

[87] 3rd Generation Partnership Project, "Study on new radio access technology: Radio access architecture and interfaces," 3GPP TR 38.801 V14.0.0, 2017.

[88] Next Generation Mobile Networks Alliance, "NGMN Overview on 5G RAN Functional Decomposition," Technical Deliverable V1.0, 2018.

[89] 3rd Generation Partnership Project, "NG-RAN; Architecture description," 3GPP TS 38.401 V15.1.0, 2018.

[90] 3rd Generation Partnership Project, "NR; NR and NG-RAN Overall Description; Stage 2," 3GPP TS 38.300 V15.1.0, 2018.

[91] I. Da Silva et al., "Impact of network slicing on 5G Radio Access Networks," EUCNC 2016 - Eur. Conf. Networks Commun., pp. 153–157, 2016.

[92] R. Ferrús, O. Sallent, J. Pérez-Romero, and R. Agustí, "On 5G Radio Access Network Slicing: Radio Interface Protocol Features and Configuration," IEEE Commun. Mag., vol. 56, no. 5, pp. 184–192, 2018.

[93] O. Sallent, J. Pérez-Romero, R. Ferrús, and R. Agustí, "On Radio Access Network Slicing from a Radio Resource Management Perspective," IEEE Wirel. Commun. Netw. Conf. WCNC, vol. 24, no. 5, pp. 166–174, 2017.

[94] R. H. Tehrani, S. Vahid, D. Triantafyllopoulou, H. Lee and K. Moessner, "Licensed Spectrum Sharing Schemes for Mobile Operators: A Survey and Outlook," in IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2591-2623, Fourth quarter 2016.

[95] Y. Teng, Y. Wang, and K. Horneman, "Co-primary spectrum sharing for denser networks in local area," in Proc. 9th Int. Conf. Cogn. Radio Orient. Wireless Netw. Commun. (CROWNCOM), Oulu, Finland, 2014, pp. 120–124.

[96] "Licensed shared access (LSA)," ECC Rep. 205, Feb. 2014.

[97] A. Apostolidis et al., “Intermediate description of the spectrum needs and usage principles,” document ICT-317669-METIS/D5.1, Deliverable, METIS, Aug. 2013.

[98] T. Irnich, J. Kronander, Y. Selén, and G. Li, “Spectrum sharing scenarios and resulting technical requirements for 5G systems,” in Proc. IEEE 24th Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC Workshops), London, U.K., 2013, pp. 127–132.

[99] ASA Concept, ECC Report FM(12)084 Annex 47. (May 2011). [Online]. Available: http://www.cept.org

[100] M. Mustonen et al., “Considerations on the licensed shared access (LSA) architecture from the incumbent perspective,” in Proc. 9th Int. Conf. Cogn. Radio Orient. Wireless Netw. Commun. (CROWNCOM), Oulu, Finland, 2014, pp. 150–155.

[101] K. Buckwitz, J. Engelberg, and G. Rausch, “Licensed shared access (LSA)—Regulatory background and view of administrations, ” in Proc. 9th Int. Conf. Cogn. Radio Orient. Wireless Netw. Commun. (CROWNCOM), Oulu, Finland, 2014, pp. 413–416.

[102] P. Marques et al., “Spectrum sharing in the EU and the path towards standardization,” in Proc. Future Netw. Mobile Summit (FutureNetworkSummit), Lisbon, Portugal, 2013, pp. 1–9.

[103] “Novel spectrum usage paradigm for 5G,” White Paper, IEEE TCCN Special Interest Group Cogn. Radio in 5G, Nov. 2014.

[104] C. Dahlberg, Z. Liu, A. Pradini, and K. W. Sung, “A techno-economic framework of spectrum combining for indoor capacity provisioning,” in Proc. IEEE 24th Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), London, U.K., 2013, pp. 2759–2763.

[105] Broadband Wireless Access/Spectrum Access, Ofcom, London, U.K., Dec. 2013. [Online]. Available: http://licensing.ofcom.org.uk/ radiocommunicationlicences/mobile-wireless-broadband/cellularwireless-broadband/policy-and background/broadband-fixed-wireless

[106] K-ICT Free Band Strategy, Ministry Sci., ICT Future Plan., Gwacheon, South Korea, 2015. [Online]. Available: http://www.msip.go.kr

[107] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “A survey on spectrum management in cognitive radio networks,” IEEE Commun. Mag., vol. 46, no. 4, pp. 40–48, Apr. 2008.

[108] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” IEEE Commun. Surveys Tuts., vol. 11, no. 1, pp. 116–130, 1st Quart. 2009.

[109] F. Paisana, N. Marchetti, and L. A. DaSilva, “Radar, TV and cellular bands: Which spectrum access techniques for which bands?” IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1193–1220, 3rd Quart. 2014.

[110] “Extending LTE advanced to unlicensed spectrum,” White Paper, Qualcomm, San Diego, CA, USA, Dec. 2013.

[111] T. Rosowski et al., “Description of the spectrum needs and usage principles,” document ICT-317669-METIS/D5.3, Deliverable, METIS, Aug. 2014.

[112] M. Bennis, S. Lasaulce, and M. Debbah, “Inter-operator spectrum sharing from a game theoretical perspective,” EURASIP J. Adv. Signal Process., vol. 2009, Mar. 2009, Art. no. 4. [Online]. Available: http://asp.eurasipjournals.springeropen.com/articles/10.1155/2009/ 295739.

[113] C. Galiotto, G. K. Papageorgiou, K. Voulgaris, M. M. Butt, N. Marchetti and C. B. Papadias, "Unlocking the Deployment of Spectrum Sharing With a Policy Enforcement Framework," in IEEE Access, vol. 6, pp. 11793-11803, 2018

[114] R. Umar, A. U. H. Sheikh, M. Deriche, M. Shoaib and M. Hadi, "Multi-operator spectrum sharing in next generation wireless communications networks: A short review and roadmap to future," 2017 International Symposium on Wireless Systems and Networks (ISWSN), Lahore, 2017, pp. 1-5.

[115] The Impact of Licensed Shared Use of Spectrum, Deloitte, GSMA https://www.gsma.com/spectrum/wp-content/uploads/2014/02/The-Impacts-of-Licensed-Shared-Use-of-Spectrum.-Deloitte.-Feb-2014.pdf
[116] ECC Decision (14)/02
[117] Spectrum Analysis and Regulations for 5G, Tan Wang, Gen Li, Biao Huang, Qingyu Miao, Jian Fang, Pengpeng Li, Haifeng Tan, Wei Li, Jiaxin Ding, Jingchun Li, and Ying Wang
[118] "CBRS Alliance," [Online]. Available: https://www.cbrsalliance.org/.
[119] Promoting the shared use of Europe's radio spectrum, European Commission, https://ec.europa.eu/digital-single-market/en/promoting-shared-use-europes-radio-spectrum
[120] https://www.cept.org/ecc/topics/lsa-implementation#/4%20%20%20%20%20%20%20%20%20%20Relevant%20ECC%20deliverables%20and%20documentation
[121] (polish) UKE opublikował strategię do 2015 r., Rzeczpospolita, http://www.rp.pl/artykul/956074-UKE-opublikowal-strategie-do-2015-r-.html
[122] (polish) Ocena stopnia realizacji polityki telekomunikacyjnej w zakresie Strategii regulacyjnej do roku 2015, Paweł Kaczmarczyk, http://kolegia.sgh.waw.pl/pl/KES/czasopisma/kwartalnik_szpp/Documents/numer%202(6)%202015/SZPP%20nr%202_2015_P_Kaczmarczyk.pdf
[123] (polish) DZIENNIK USTAW RZECZYPOSPOLITEJ POLSKIEJ, Warszawa, dnia 11 maja 2017 r., Poz. 920, ROZPORZĄDENIE RADY MINISTRÓW z dnia 24 kwietnia 2017 r. zmieniające rozporządzenie w sprawie Krajowej Tablicy Przeznaczeń Częstotliwości, http://dziennikustaw.gov.pl/DU/2017/0920
[124] IS-Wireless, [Online]. Available: www.is-wireless.com.
[125] Federal Communications Commission, "3.5 GHz Band / Citizens Broadband Radio Service," [Online]. Available: https://www.fcc.gov/wireless/bureau-divisions/broadband-division/35-ghz-band/35-ghz-band-citizens-broadband-radio.
[126] Wireless Innovation Forum, "Interim SAS to CBSD Protocol Technical Report - A (WINNF-15-P-0023)," October 2015.
[127] Wireless Innovation Forum, "SAS to CBSD Protocol Technical Report-B (WINNF-15-P-0062)," March 2016.
[128] Wireless Innovation Forum , "Forum Historical Documents," [Online]. Available: https://www.wirelessinnovation.org/historical-documents.
[129] Kyung Mun, "OnGo White Paper: OnGo: New Shared Spectrum Enables Flexible Indoor and Outdoor Mobile Solutions and New Business Models," March 2017. [Online]. Available: https://www.cbrsalliance.org/wp-content/uploads/2018/04/Mobile-Experts-OnGo.pdf.
[130] CBRS Alliance, "CBRS Network Service Technical Specification (CBRSA-TS-1001) V1.0.0," 1 Februar 2018. [Online]. Available: https://www.cbrsalliance.org/wp-content/uploads/2018/06/CBRSA-TS-1001-V1.0.0.pdf.
[131] CBRS Alliance, "CBRS Network Service Technical Specifications (CBRSA-TS-1002) V1.0.0," 1 February 2018. [Online]. Available: https://www.cbrsalliance.org/wp-content/uploads/2018/06/CBRSA-TS-1002-V1.0.0.pdf.
[132] M. Palola, M. Matinmikko, J. Prokkola, M. Mustonen, M. Heikkilä, T. Kippola, S. Yrjölä, V. Hartikainen, L. Tudose, A. Kivinen, J. Paavola and K. Heiska, "Live field trial of Licensed Shared Access (LSA)," in IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN), McLean, VA, USA, 2014.
[133] T. Haustein, Fraunhofer HHi - Wireless Communications and Networks, "Spectrum Sharing," 05 11 2014. [Online]. Available: https://www.youtube.com/watch?v=LiCRRK8hJc0. [Accessed 07 08 2018].
[134] J. M. Peha, "Approaches to Spectrum Sharing," IEEE Communications Magazine, vol. 43, no. 2, pp. 10-12, 2005.

[135] J. Khun-Jush, P. Bender , B. Deschamps and M. Gundlach, "Licensed shared access as complementary approach to meet spectrum demands: Benefits for next generation cellular systems," in ETSI WORKSHOP ON RECONFIGURABLE RADIO SYSTEM, Cannes, France, 2012.
[136] SEVENTH FRAMEWORK PROGRAMME, EUROPEAN COMMISSION, "ADEL: Advanced Dynamic Spectrum 5G Mobile Networks Employing Licensed Shared Access," UE Project, 2013-2016. [Online]. Available: http://www.fp7-adel.eu/.
[137] M. Palola, T. Rautio, M. Matinmikko, J. Prokkola, M. Mustonen, M. Heikkilä, T. Kippola, S. Yrjola, L. Tudose, V. Hartikainen, J. Paavola, A. Kivinen, M. Mäkeläinen, J. Okkonen, H. Kokkinen and T. Hänninen, "Licensed Shared Access (LSA) trial demonstration using real LTE network," in CrownCom 2014, Oulu, Finland, 2014.
[138] M. Mustonen, M. Matinmikko, M. Palola, S. Yrjölä and K. Horneman, "An Evolution Toward Cognitive Cellular Systems: Licensed Shared Access for Network Optimization," IEEE Communications Magazine, vol. 53, no. 5, pp. 68 - 74, 2015.
[139] ADEL, EC FP7 Project http://www.fp7-adel.eu/ (Last accessed: 10/17/2018)
[140] Coherent, EC H2020 Project, http://www.ict-coherent.eu/ (Last accessed: 10/30/2018)
[141] "5GENESIS: 5th Generation End-to-end Network, Experimentation, System Integration, and Showcasing", http://5genesis.eu/ (Last accessed:10/17/2018)
[142] "Cognitive radio systems for efficient sharing of TV white spaces in European context", http://www.ict-cogeu.eu/ (last accessed: 10/17/2018)
[143] " Mobile and wireless communications Enablers for Twenty-twenty (2020) Information Society", https://www.metis2020.com/ (last accessed:10/17/2018)
[144] " Mobile and wireless communications Enablers for Twenty-twenty (2020) Information Society", https://metis-ii.5g-ppp.eu/ (last accessed:10/17/2018)
[145] ETSI GS NFV 002: NFV, Architectural Framework.
[146] ETSI GS MEC 009 General principles for Mobile Edge Service APIs.
[147] ETSI GS MEC 011 Mobile Edge Platform Application Enablement.
[148] ETSI White Paper No. 28. MEC in 5G networks.
[149] ETSI GR MEC 017; Deployment of Mobile Edge Computing in an NFV environment
[150] 3GPP, "E-UTRAN; Architecture Description", TS 36.401, Available at http://www.3gpp.org
[151] 3GPP, "Network Sharing; Architecture and functional description", TS 23.251, Available at http://www.3gpp.org
[152] 3GPP, " General Packet Radio Service (GPRS) enhancements for E-UTRAN access ", TS 23.401, Available at http://www.3gpp.org
[153] 3GPP, " S1 Application Protocol (S1AP)", TS 36.413, Available at http://www.3gpp.org
[154] 3GPP, "Study on new services and markets technology enablers", Release 14, TR 22.891, Sept. 2016. Available at http://www.3gpp.org
[155] Sonata NFV Project, Deliverable D2.2 "Architecture Design", http://www.sonata-nfv.eu/
[156] NECOS Project, Deliverable D3.1 "NECOS System Architecture and Platform Specification. V1", http://www.h2020-necos.eu/
[157] 5GNORMA Project, Deliverable D3.3 "5G NORMA Network Architecture – Final Report", http://www.it.uc3m.es/wnl/5gnorma/
[158] 5G-TRANSFORMER Project, Deliverable D3.1 "Definition of service orchestration and federation algorithms, service monitoring algorithms", http://5g-transformer.eu/
[159] GSMA, "LTE-M DEPLOYMENT GUIDE to Basic Feature set Requiremets", April 2018.
[160] "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions" Ibrahim Afolabi, Tarik Taleb , Konstantinos Samdanis, Adlen Ksentini, and Hannu Flinck
[161] X. Foukas, N. Nikaein, M. M. Kassem, and K. Kontovasilis, "FlexRAN: A flexible and programmable platform for software-defined

radio access networks," in *Proc. ACM CoNEXT*, Irvine, CA, USA, Dec. 2016
[162] Next Generation RAN Architecture (Extensible Radio Access Network (xRAN)). [Online]. Available: https://www.xran.org
[163] 3GPP, "Study on architecture for next generation system", Release 14, Sophia Antipolis, France, Rep. TR 23.799, Dec. 2016.
[164] 3GPP, "Study on management and orchestration of network slicing for next generation network", Release 15, TR 28.801. Available at http://www.3gpp.org
[165] 3GPP, "Architecture enhancements for service capability exposure", Release 13, TR 23.708. Available at http://www.3gpp.org
[166] 3GPP, "Study on Common API Framework for 3GPP Northbound APIs", Release 15, TR 23.722. Available at http://www.3gpp.org
[167] GSMA, "NB-IoT Deployment Guide to Basic Feature Set Requirements", April 2018.
[168] GSMA, ""LTE-M Deployment Guide to Basic Feature Set Requirements", April 2018
[169] ETSI White Paper No. 24. MEC Deployments in 4G and Evolution Towards 5G.
[170] Antonio Morgado, Kazi Mohammed Saidul Huq, Shahid Mumtaz, Jonathan Rodriguez, A survey of 5G technologies: regulatory, standardization and industrial perspectives, Digital Communications and Networks, Volume 4, Issue 2, 2018, Pages 87-97,
[171] LOG-a-TEC testbed facility, http://www.log-a-tec.eu/, last accessed: 17.X.2018
[172] RFC 2865 Remote Authentication Dial In User Service
[173] RFC 2866 RADIUS Accounting
[174] RFC 6733 Diameter Base Protocol
[175] RFC 1492 Terminal Access Controller Access Control System
[176] Active Directory Architecture https://technet.microsoft.com/en-us/library/bb727030.aspx
[177] SENDATE Project (CELTIC PLUS) http://www.sendate.eu
[178] GÉANT https://www.geant.org/ Last accessed 25 Oct 2018
[179] FED4FIRE+ Project https://www.fed4fire.eu/the-project/ Last accessed 25 Oct 2018
[180] GENI Project http://www.geni.net/ Last accessed 25 Oct 2018
[181] softFIRE Project (H2020): https://www.softfire.eu Last accessed 25 Oct 2018
[182] 5G-Coral Project (H2020) deliverable D2.1 "Initial design of 5G-CORAL edge and fog computing system", http://5g-coral.eu/?page_id=37, last accessed 25.X.2018
[183] 5G Norma project (H2020) deliverable D4.1 "RAN architecture components – preliminary concepts", http://www.it.uc3m.es/wnl/5gnorma/deliverables.html, last accessed
[184] 5G Norma project (H2020) deliverable D4.2 "RAN architecture components – final report", http://www.it.uc3m.es/wnl/5gnorma/deliverables.html, last accessed
[185] 3rd Generation Partnership Project, "Study on OAM support for Licensed Shared Access (LSA)" 3GPP TS 32.855 V14.0.0, 2018.
[186] 3rd Generation Partnership Project, "Telecommunication management; Principles and high level requirements" 3GPP TS 32.101 V15.0.0, 2018.
[187] 3rd Generation Partnership Project, " Telecommunication management; Management concept, architecture and requirements for mobile networks that include virtualized network functions" 3GPP TS 28.500 V15.0.0, 2018.
[188] ETSI TR 103.588, ETSI TR 103 588, Reconfigurable Radio Systems (RRS); Feasibility study on temporary spectrum access for local high-quality wireless networks Mobile Edge Platform Application Enablement, V1.1.1 (2018-02)
[189] "5 Artificial Intelligence fields that are Changing the way how Things Work". http://technoitworld.com/5-artificial-intelligence-fields-changing-way-things-work/
[190] New ICT. "AI-enabled Mobile Networks" Yang Jin, Director, Network Data Analytics Research, and Miguel Dajer, Vice President, Wireless Access Department, Huawei Technologies Co., Ltd.
[191] Forbes. "Living On The Wireless Edge With AI and 5G". Prakas Sangam. September 2018.

[192] XRAN Forum. "XRAN Forum merges with C-RAN Alliance to form ORAN Alliance". February, 2018.
[193] Port Technology. "Nokia and China Mobile explore AI for 5G". https://www.porttechnology.org/news/nokia_and_china_mobile_explore_ai_for_5g
[194] Li, Rongpeng & Zhifeng, Zhao & Zhou, Xuan & Ding, Guoru & Chen, Yan & Zhongyao, Wang & Zhang, Honggang. (2017). Intelligent 5G: When Cellular Networks Meet Artificial Intelligence. IEEE Wireless Communications. PP. 2-10. 10.1109/MWC.2017.1600304WC.
[195] ZTE. "AI enables Network Intelligence". ZTE White Paper, February 2018.
[196] Intel. "How 5G will make AI-powered devices smarter". February 2018.
[197] IEEE Communications Magazine. Call for papers. "Applications of AI in Wireless Communications".

Annex A. Copyright Licenses

This deliverable includes figures from ETSI, 3GPP document, 5G-Coral project, Coherent project, and CEPT-ECC decisions. The consortium has permission to reproduce the figures in this document. The following tables list the figures, the corresponding sources and the copyright license.

Figure in D1.3	Source
Figure 48	CEPT-ECC Decision (14)/02 Figure 14
Figure 37	5G CORAL project Deliverable 2.1 Figure 11
Permission to reproduce the figure	

Figure in D1.3	Source
Figure 38	3GPPTR 23.708 v13.0.0 (2015) Clause 6.1.1.2-1
© 2015. 3GPP™ TSs and TRs are property of ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided to you "as is" for information purposes only. Further use is strictly prohibited.	

Figure in D1.3	Source
Figure 42	3GPPTR 32.855 v14.0.0 (2016) Clause 6.2.1.1-1
Figure 43	3GPPTR 32.855 v14.0.0 (2016) Clause 6.2.2.1-1
© 2016. 3GPP™ TSs and TRs are property of ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided to you "as is" for information purposes only. Further use is strictly prohibited.	

Figure in D1.3	Source
Figure 44	3GPPTR 32.101 v15.0.0 (2017) Clause 2
© 2017. 3GPP™ TSs and TRs are property of ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided to you "as is" for information purposes only. Further use is strictly prohibited.	

Figure in D1.3	Source
Figure 41	3GPP TR 23.722 v15.1.0 (2018) Clause B1.1

Figure 40	3GPP TR 23.722 v15.1.0 (2018) Clause 7.1.1.1.2-1
Figure 58	3GPP TR 28.801 v15.1.0 (2018) Clause 4.2.2.1
Figure 39	3GPP TR 23.501 v15.3.0 (2018) Clause 4.2.3-5
Figure 53	3GPP TR 23.401 v15.5.0 (2018) Clause 4.2.2-1
Figure 54	3GPP TR 23.401 v15.5.0 (2018) Clause 4.2.2-2
Figure 56	3GPP TR 23.401 v15.5.0 (2018) Clause 5.19.1-1
Figure 61	3GPP TR 38.300 v15.3.1 (2018) Clause 16.3.4.2 -1
Figure 45	3GPP TR 28.500 v15.0.0 (2018) Clause 6.1.1-1

Figure in D1.3	Source
Figure 27	ETSI GR MEC 017 v1.1.1 (2018) Figure 5.2-1
Figure 28	ETSI GR MEC 017 v1.1.1 (2018) Figure 5.3-1

Figure in D1.3	Source
Figure 46	ETSI TR 103 588 v1.1.1 (2018) Figure 8

Figure in D1.3	Source
Figure 32Figure 46	ETSI White Paper 24 Figure 1
Figure 33	ETSI White Paper 24 Figure 2
Figure 34	ETSI White Paper 24 Figure 3
Figure 35	ETSI White Paper 24 Figure 4
Figure 36	ETSI White Paper 24 Figure 5
Figure 31	ETSI White Paper 28 Figure 3

Figure in D1.3	Source
Figure 25	ETSI GS MEC 003 v1.1.1 (2016) Figure 5-1
Figure 26	ETSI GS MEC 003 v1.1.1 (2016) Figure 6-1