



## Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access

Project no. 671704

Research and Innovation Action

Co-funded by the Horizon 2020 Framework Programme of the European Union



Call identifier: H2020-ICT-2014-1

Topic: ICT-14-2014 - Advanced 5G Network Infrastructure for the Future Internet

Start date of project: July 1st, 2015 (30 months duration)

### Deliverable D1.1

## CHARISMA intelligent, distributed low-latency security C-RAN/RRH architecture

Due date: 31/03/2016

Submission date: 06/06/2016

Deliverable leader: University of Essex

Editors list:

#### Dissemination Level

- 
- |                                     |   |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | PU: Public  |
| <input type="checkbox"/>            | PP: Restricted to other programme participants (including the Commission Services)        |
| <input type="checkbox"/>            | RE: Restricted to a group specified by the consortium (including the Commission Services) |
| <input type="checkbox"/>            | CO: Confidential, only for members of the consortium (including the Commission Services)  |
-

## List of Contributors

Participant	Short Name	Contributor
Fundació i2CAT	I2CAT	Eduard Escalona, Amaia Legarrea, Shuaib Siddiqui
Fraunhofer HHI	HHI	Kai Habel, Volker Jungnickel
Demokritos NCSR	NCSR	Eleni Trouva
APFutura	APFUT	Oriol Riba
Innoroute	INNO	Marian Ulbricht, Andreas Foglar
InCites	INCITES	Theodoros Rokkas, Ioannis Neokosmidis
JCP-Connect	JCP-C	Yaning Liu, Jean-Charles Point
University of Essex	UESSEX	Michael Parker, Geza Koczian, Terry Quinlan, Stuart Walker
Cosmote	COSMO	George Lyberopoulos, Eleni Theodoropoulou, Konstantinos Filis
Intracom Telecom	ICOM	Spiros Spirou, Konstantinos Katsaros, Dimitrios Kritharidis, Konstantinos Chatsias
Telekom Slovenije	TS	Blaž Peternel, Primož Jenko
PT Inovação e Sistemas	PTIN	Cláudio Rodrigues, Victor Marques
Ethernity	ETHER	Eugene Zetserov, David Levi
Ericsson	ERIC	Carolina Canales, Manuel Lorenzo

## Change history

Version	Date	Partners	Description/Comments
0.1	08/03/2016	UESSEX	ToC definition
0.2	12/03/2016	UESSEX	Initial Use Case descriptions and other contributions
0.3	21/03/2016	UESSEX	Additional section contributions and Use Case descriptions
0.4	4/04/2016	ALL	Additional section contributions and updated Use Case descriptions
0.5	11/04/2016	TS, PTIN, HHI	Final contributions before 1 <sup>st</sup> internal review
0.6	18/05/2016	ALL	Structural changes to chapter order, changes due to 1 <sup>st</sup> internal review
1.0	04/06/2016	UESSEX, I2CAT	Final revisions following 2 <sup>nd</sup> internal review

# Table of Contents

<b>Table of Contents .....</b>	<b>3</b>
<b>Figures Summary.....</b>	<b>5</b>
<b>Executive Summary.....</b>	<b>7</b>
<b>1. Introduction .....</b>	<b>8</b>
<i>1.1. Background.....</i>	<i>8</i>
1.1.1. State-of-the-art & gap analysis .....	8
<b>2. Architecture Definition .....</b>	<b>11</b>
<i>2.1. Layered Architecture Description.....</i>	<i>11</i>
2.1.1. CHARISMA Aggregation Levels (CALs) .....	12
<i>2.2. Data Plane .....</i>	<i>14</i>
2.2.1. TrustNode Design.....	14
2.2.2. Network Slicing and Traffic Model.....	17
2.2.3. Low latency hardware acceleration.....	18
2.2.4. D2D & D2I.....	18
2.2.5. Offloading and Caching.....	21
2.2.6. Mobile Cloud.....	28
2.2.7. Fronthaul Design.....	30
2.2.8. Ethernet fronthaul .....	31
2.2.9. NG-PON2.....	32
2.2.10. Backhaul.....	37
<i>2.3. Control and Management Plane.....</i>	<i>43</i>
<i>2.4. Summary.....</i>	<i>45</i>
<b>3. Workflows &amp; Service Life Cycle Design .....</b>	<b>46</b>
<i>3.1. Service Lifecycle Modelling .....</i>	<i>46</i>
<i>3.2. Actors and Stakeholders .....</i>	<i>48</i>
<i>3.3. Roles interaction .....</i>	<i>49</i>
<i>3.4. Service Workflows of CHARISMA.....</i>	<i>50</i>
3.4.1. NO and VNO interaction .....	50

- 3.4.2. VNO and AP interaction .....50
- 3.4.3. VNO and EU interaction .....51
- 3.5. Summary.....52
- 4. Use Case Scenarios .....53**
- 4.1. Introduction .....53
- 4.2. Use Case Comparative Tables.....54
- 4.2.1. Automotive - Trains .....54
- 4.2.2. Automotive – Platooning, Vehicle Collision Avoidance .....59
- 4.2.3. Automotive - Buses .....64
- 4.2.4. Big Event .....67
- 4.2.5. Emergency - Fire Fighters.....71
- 4.2.6. Factory of the Future (IoT).....75
- 4.2.7. Multi-tenant Access and Video Broadcasting Services .....79
- 4.2.8. Remote Surgery .....84
- 4.2.9. Smart Grid .....89
- 4.3. Requirements & Specifications .....91
- 4.4. Summary.....94
- 5. Conclusions .....95**
- References .....97**
- Acronyms.....101**

## Figures Summary

Figure 1: Generic multi-plane (S-, C-, D-planes) view of 5G networking architecture .....	12
Figure 2: Physical layer description of hierarchical CHARISMA aggregation levels (CALs) .....	13
Figure 3: Software-Defined Network Architecture as defined by ONF [1].....	14
Figure 4: TrustNode offloading Concept .....	15
Figure 5: TrustNode Architecture .....	16
Figure 6: OpenFlow Processing Pipeline.....	16
Figure 7: Physical and virtualized network.....	17
Figure 8: D2D & D2I example with 5 devices in a ring topology, and D <sub>1</sub> as a hub/gateway to reach RRH <sub>1</sub> ....	19
Figure 9: WLAN 3GPP IP access .....	23
Figure 10: IFOM scenario.....	24
Figure 11: MAPCON scenario .....	24
Figure 12: LIPA/SIPTO-Femto scenario.....	25
Figure 13: SIPTO-Macro scenario .....	26
Figure 14: Accessing a local cache with SIPTO architecture.....	28
Figure 15: Cloud-RAN architecture [21] .....	28
Figure 16: Cloud-RAN for 5G including functional split between BBU and RRH [22].....	29
Figure 17: New functional split [17] .....	30
Figure 18: PON Spectrum .....	33
Figure 19: NG-PON2 basic scenario.....	34
Figure 20: NG-PON2 wavelength tuning .....	34
Figure 21: Backhaul in 2G/3G/4G Networks .....	38
Figure 22: Wireless Backhaul Network with PtP and PtMP Configurations and CALs .....	39
Figure 23: Proposed architecture for SDN support at the backhaul .....	40
Figure 24: OFDM-PON architecture .....	41
Figure 25: OFDM spectrum .....	41
Figure 26: OFDM-PON layered architecture .....	42
Figure 27: The high-level CHARISMA control and management plane.....	44
Figure 28: CHARISMA Service Lifecycle Model.....	47

Figure 29: CHARISMA Service Lifecycle Model mapping to ITILv3 ..... 48

Figure 30: Interactions between 5G networking actors ..... 49

Figure 31: NO and VNO interaction workflow ..... 50

Figure 32: AP and VNO interaction workflow ..... 51

Figure 33: VNO and EU interaction workflow ..... 51

Figure 34: CHARISMA use cases within the 5G ecosystem ..... 54

Figure 35: Different channel characteristics for trains 5G networking ..... 55

Figure 36: Hierarchical CHARISMA architecture for trains ..... 56

Figure 37: Intelligent Transport Services / Collision Avoidance, Platooning ..... 60

Figure 38: Scenario of bus use cases ..... 65

Figure 39: Extended network capacity in Planica (March 2016) ..... 68

Figure 40: Schematic of access points in a big event (e.g. sports stadium) scenario ..... 69

Figure 41: End-user density variation in a big event context ..... 70

Figure 42: CHARISMA fire fighter use case – overview ..... 72

Figure 43: Factory of the Future ..... 76

Figure 44: Virtual Network Operators sharing the infrastructure of an access network (including an edge cloud). The inter-domain application on top is live video broadcasting ..... 80

Figure 45: Multi-tenancy in a video streaming application ..... 81

Figure 46: Remote surgery architecture ..... 86

Figure 47: Smartgrid (Sunseed FP7 project) use case ..... 90

## Executive Summary

This deliverable D1.1 “CHARISMA intelligent, distributed low latency security C-RAN/RRH architecture” provides an overview of the 5G CHARISMA architecture in its multi-layered control-, data-, and service-plane form. The CHARISMA architecture has been designed to achieve many of the 5G KPIs as defined by the 5G-PPP programme as well as other key technology drivers.

With particular regard to the technologies that underpin the low latency, open access, and virtualised security (v-security) performance of CHARISMA, the data plane architecture for CHARISMA is described. In addition, the CHARISMA architecture has been designed to be hierarchical and quasi-distributed in nature, via the use of four self-similar CHARISMA aggregation levels (CALs). Each CAL (from CAL0 to CAL3) is mapped onto one of the key physical and functional nodes of a 5G network, which are also explicitly identified for each use case (UC) scenario. Each active node (i.e. CAL) is designed to possess its own scalable intelligent management unit (IMU) performing data storage/caching, processing and routing functionalities. Data is routed, where possible, at the lowest common aggregation point, so as to assist in achieving low-latency networking. Distributing intelligence ever closer to the end-user also assists in reducing network latency, while allowing for more precise SDN and NFV control of the CHARISMA 5G network. The various technologies incorporated within the CHARISMA architecture to achieve these functionalities and key performance characteristics are all comprehensively described.

The expected service and workflow lifecycle that CHARISMA will have to support is defined; particularly with regard to the automation of the whole service delivery and operations process (i.e. dynamic provisioning and reconfiguration), since the UCs are highly dynamic in nature. As part of the service workflows, the most important actors in the CHARISMA network are defined, with particular regard to the virtualization of physical infrastructure, network operation, resources and network functions.

Finally, the 5G use cases that particularly exploit the CHARISMA architecture design are defined, with particular regard to exhibiting the CHARISMA features of low latency, open access, and security. Each UC is also described in terms of its own distinguishable requirements (in terms of functionality, performance, and its relative importance/criticality) and their associated KPIs, as well as the constraints, restrictions and technical challenges associated with each UC. An initial systematic categorization of the various requirements is performed to ascertain which requirements are of more general importance than other (more UC-specific) requirements.

# 1. Introduction

In this deliverable D1.1 of the CHARISMA project we are presenting the results of the work package WP1, which is providing the specifications and performance parameters associated with the CHARISMA architecture. In many senses this document is foundational to the CHARISMA project, and provides the required steer and guidance into the rest of the project. The first technical deliverable of the project was D3.1 (at month 6), which provided an overview of the control, management and orchestration (CMO) plane approach to CHARISMA (i.e. cognitive orchestration and virtualised security at the management plane). Since then, the architecture has continued to be designed in an incremental manner since the beginning of the project, but is now in a consolidated state subsequent to the technical discussions in WP2 and WP3 that have validated it. Now at month 9 of the project we present the initial definition and requirements of the CHARISMA architecture, as additionally based upon the relevant Use Case (UC) scenarios that have been identified during the first year of the project. In investigating the appropriate UC scenarios which best exploit the CHARISMA architecture, we have chosen those UCs where the three distinguishing features of the CHARISMA architecture are best exploited. In particular these three features, which CHARISMA has been specially designed to promote are: Low latency, security, and Open Access. As we shall see, these three features, which can be considered to be a subset of many of the key 5G KPIs, are not necessarily compatible (or consistent) with each other (i.e. they can be somewhat self-contradictory, e.g. the desire for Open Access can potentially compromise security, if the architecture does not appropriately take this into account, e.g. via appropriate tenant isolation measures) and so impose their own additional constraints on how the architecture is best designed. Conversely, these particular features can also act to reinforce and help each other, e.g. the desire for low latency can also act to assist in the secure operation of the network, e.g. by reducing the scope for interception or breakdown over long lengths of the topology, since low latency tends to require data to be processed (transmitted, etc.) as locally as possible to where it is required. In addition, in this deliverable rather than actually describing the CHARISMA security solution (which will be reported upon in later project deliverables arising from within workpackage WP3), we describe how the CHARISMA architecture will support a distributed security solution. In particular the support of distributed security is due to the CHARISMA architecture featuring distributed intelligence and processing capabilities, i.e. via the CHARISMA aggregation levels (CALs), which are described in this deliverable. The CALs are the key architectural step in order to be able to adopt a distributed end-to-end security solution.

## 1.1. Background

### 1.1.1. State-of-the-art & gap analysis

The design of a network architecture suitable for 5G deployment has become a complex undertaking. Where previously physical- and logical-layer topological descriptions of the network would provide an adequate explanation of the network architecture, such an approach is no longer sufficient. Earlier additional complexity to the description also required a distinction to be made between the data and control planes of the architecture; however such a dual layer approach is now also arguably too simple. On the one hand the

advent of virtualization in ICT technologies, e.g. through network functions virtualization (NFV) in next-generation networking, has required a much clearer understanding and distinction be made between the physical and virtualised environment of network equipment and associated functions; as a means to enable use of commoditised equipment and achieve cost savings (CapEx) through use of standardized commercial-off-the-shelf (COTS) solutions. Allied to this has been the development of software-defined networking (SDN), which allows network control to be separated from the forwarding elements (physical equipment) and manage network services through an abstraction of their functionalities. A suitable control plane description, which also describes the required management and network orchestration of the virtualised functions, is therefore required. The increased functionalisation of the CMO plane also enables a greater sophistication in the range and type of network services that can be offered. In addition to the network being composed of a range of different actors, e.g. physical infrastructure providers (PIPs), network providers (NPs), service providers (SPs), virtual network operators (VNOs), etc., and the different application programming interfaces (APIs), which is another aspect of the commoditisation of network equipment to achieve CapEx savings required. To interface between applications and services means that we also need to consider what is called the multi-service management layer. In addition to managing the different services and applications available to end-users and between network actors, is the importance of monitoring the quality of the performance of the various network functions and services. On the one hand, this is to ensure the appropriate quality of service (QoS) and quality of experience (QoE) as expected by end-users, in particular as set out by the service level agreements (SLAs) that will have been signed; but also to monitor the network integrity and security, e.g. as the means to ensure network reliability and restoration in the event of individual network failures. However this also highlights an ever increasingly important aspect of 5G networking, which is security, and which is also an important feature to the CHARISMA architecture. As such, suitable security and virtualised security functions (VSF's) are also being designed into the inherent CHARISMA architecture. Finally, in relation to the virtualisation of many 5G networking functions, this is generally performed via the cloudified network architecture, e.g. C-RAN (Cloud Radio Access Network) where cloud equipment (i.e. servers and associated VNF functions) is located at the central node. Thus, many 5G architectures have a tendency to be centralised in concept. However, the CHARISMA architecture has made an explicit attempt to be more distributed (decentralised) in nature with intelligence devolved towards the end user. This also has required the fundamental understanding of how best to design the CHARISMA architecture to take this into account.

The CHARISMA architecture has been designed to achieve many of the 5G KPIs as defined by the 5G-PPP programme as well as other key technology drivers. As already mentioned, in addition to the 5G KPIs, CHARISMA has been designed to emphasise 3 specific important functionalities that are also considered to be key to many important vertical sectors and the provisioning of their supporting 5G services. These 3 functionalities are to be a low-latency network, featuring security and open access (multi-tenancy) operation. These aspects and how they have influenced the particular design choices in the CHARISMA architecture are examined in greater detail in this deliverable.

This deliverable D1.1 is organised as follows:

Chapter 1 provides an introduction to the motivation and background context of the CHARISMA architecture, and describes some of the key rationales underlying the CHARISMA approach to future 5G networking.

Chapter 2 defines the multi-layered approach to the CHARISMA architecture design, based on consideration of its control plane, data plane, and service plane, and how these are managed and orchestrated by the CMO plane. The initial design for the C&M plane has already been described in the earlier deliverable D3.1 “V-Security management plane design and definition”, but a brief summary of the C&M plane is also offered in chapter 2, whilst many aspects of the SP are considered in chapter 3. Chapter 2 focuses on the data plane architecture, where the innovative technologies that will underpin the low latency, open access, and v-security performance of CHARISMA are comprehensively discussed.

Chapter 3 defines CHARISMA’s expected service and workflow lifecycle; with particular regard to automation of the whole service delivery and operations process. The UCs are assumed to be highly dynamic in nature, such that the service lifecycle requires dynamic provisioning and reconfiguration. Chapter 3 also identifies the most important actors expected to feature in the CHARISMA architecture, particularly in the context of virtualisation of physical infrastructure, network operation, resources and network functions.

Chapter 4 provides a comprehensive overview to the Use Cases that are being considered as key drivers both to the 5G paradigm, but also to how we have designed the CHARISMA architecture to satisfy their requirements. In particular, all the UCs have been selected to feature the 3 key defining functionalities of CHARISMA (namely: low latency, open access, and security). Chapter 4 also describes the requirements of the UCs (in terms of their required functionalities, performance, and their relative importance) as well as the associated KPIs, and the constraints, restrictions and technical challenges associated with each UC. As part of the analysis of the UC requirements, we have also made an initial attempt to categorise all the various requirements into common blocks, so as to ascertain which requirements are of more general importance than other (more UC-specific) requirements. The expectation is that this systematic categorization of the UC requirements will also be of general interest to a broader range of 5G architecture designers.

Finally, some concluding remarks are offered in chapter 5, with an indication of how the results reported in this deliverable D1.1 will feed into the parallel work packages of the project, and in particular influence the choice of testbed demonstrators and validators for the CHARISMA architecture in the project’s final year.

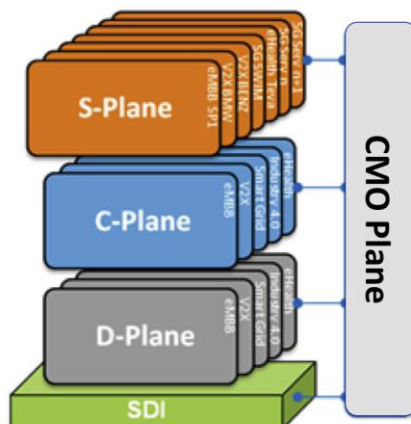
## 2. Architecture Definition

In this chapter 2 of the D1.1 deliverable we define the multi-layered approach to the CHARISMA architecture design, based on consideration of its control plane, data plane, and service plane. In particular, in this chapter we focus on the data plane architecture, with a comprehensive discussion of the innovative technologies underpinning CHARISMA's low latency, open access, and v-security performance.

### 2.1. Layered Architecture Description

CHARISMA's objective is the development of an open access, converged 5G network, via virtualised slicing of network resources to different service providers (SPs), with network intelligence distributed out towards end-users over a self-similar hierarchical architecture. Such an approach offers a means to achieve important 5G key performance indicators (KPIs) related to low latency, high and scalable bandwidths, energy efficiency and virtualised security (v-security). CHARISMA's approach for low latency and enhanced security builds upon present and future high-capacity developments that are currently being mooted for 5G deployment, such as 60 GHz/E-band, CPRI-over-Ethernet, cloud-RAN, distributed intelligence across the back-, front- and perimeteric-haul, ad-hoc mobile device interconnects, content delivery networks (CDN), mobile distributed caching (MDC) and improved energy efficiency. 5G networking is a swiftly evolving and broad concept, encompassing seamless fixed-mobile convergence with gigabit/s connectivity speeds over an intelligent open access infrastructure. CHARISMA integrates such diverse technologies into a single architecture with attendant software-defined networking (SDN) and networking functions virtualisation (NFV) amongst other important technology trends. This presents key technology challenges, while making issues such as security, energy efficiency, and scalability ever more critical. In this chapter we present the first approach to a hierarchical CHARISMA architecture, which seeks to provide a technical 5G-based solution to the issues of achieving low latency and security in an open access networking architecture.

The CHARISMA architecture can be considered in a classical multi-layer fashion as composed of the data plane (DP), control plane (CP), and service plane (SP) all above an overall software-defined infrastructure (SDI) and managed and orchestrated by the CMO plane. This is as indicated in the Figure 1 below. Here, the SDI can be considered to host all the logical implementation architectures, consisting of virtual functions connected by virtual links, each belonging to a heterogeneous set of resource domains across multiple administrations.



**Figure 1: Generic multi-plane (S-, C-, D-planes) view of 5G networking architecture**

The control plane is where routing (forwarding) decisions are made, such that network elements use the CP to exchange information on host reachability, and status etc. In addition, the CP needs to enable multi-vendor interoperability, and provide dynamic and flexible service provisioning, recovery, and concurrent network re-optimisation. The CP lies above the data plane, which is where the data flowing through the network is processed using the forwarding tables, routing tables, and queues, i.e. the hardware components (e.g. switches, routers, and processing elements) in the DP carry out the commands of the CP to configure the network. Located at the top of the architectural layers is the service plane, consisting of services ranging from mobile broadband, media (VoD, and RTSP-based video systems) streaming, gaming, and peer-to-peer file swapping, as well as newer services (e.g. machine type communications, MTC) associated with Internet of Things (IoT) and cyber-physical systems (CPS), as well as the monitoring of the network performance (QoS, QoE, latency & jitter etc.) to aid in enforcement of service level agreements (SLAs). The SP architecture and interactions are described in greater detail in the next chapter 3. All these layers (with their various functions and virtualized functions, NFVs) are managed and orchestrated by the CMO plane, which allows automated instantiation and management of the elements of each plane. This is the most ‘simplified’ version of a 5G logical and functional architecture, since the architecture could also be stratified into other layers (e.g. virtual plane, security plane, functions plane etc.); however, such more complex considerations of a future 5G architecture are beyond the scope of the current CHARISMA project. Rather, in CHARISMA we are focusing on providing a 5G networking architecture able to offer the focused benefits of low latency, security, and open access.

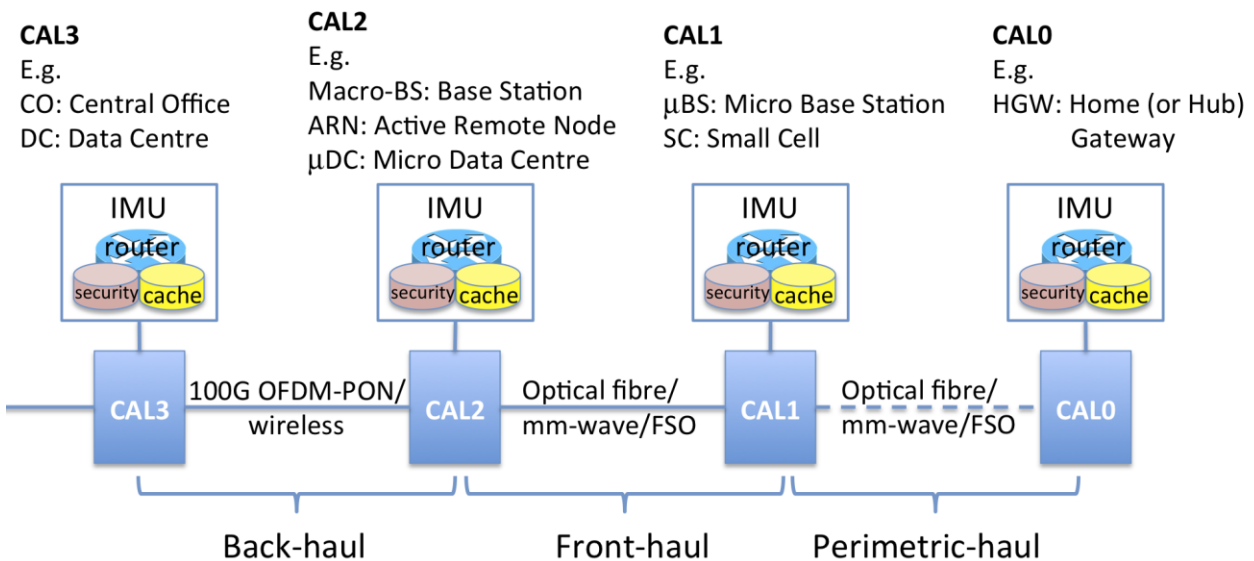
### 2.1.1.CHARISMA Aggregation Levels (CALs)

A key architectural innovation of CHARISMA is the adoption of a self-similar hierarchical approach, with active nodes intermediate to the central office (CO) and end-users. Each active node (i.e. CAL) has its own scalable intelligent management unit (IMU) performing data storage/caching, processing and routing functionalities. The CHARISMA 5G architecture described has been designed to exhibit low-latency (towards the 1-msec KPI of the 5G-PPP programme) as well as security and open access. Achieving low latency requires data to be handled (i.e. routed and/or processed) as close to where it is required (i.e. either at the receiving end, and/or at the source end). Indeed, this implies that a low-latency architecture requires network intelligence to be

located as near to the edge as possible, such that traffic which is expected to remain local never needs to travel towards the core of the network; and in this way minimizes transmission latency. Likewise, where data is frequently required (e.g. from a popular video streaming source) it makes sense to store that video data at a location close to where it is frequently accessed; in such a way, access time latency can also be minimized. Overall, this requires the CHARISMA architecture to be much more distributed in nature, as compared to more centralized 5G architectures, e.g. as typically exemplified by the purely C-RAN architecture, where intelligence is almost completely located in the CO (or Central Node). Indeed, CHARISMA is more of a distributed cloud (i.e. fog, where the cloud is typically closer to the ground, i.e. closer to end-users) type architecture. To that end, we have designed the CHARISMA architecture to be hierarchical, with a set of self-similar intelligent aggregation nodes located between the CO and end-users. Each node is labelled a CHARISMA Aggregation Level (CAL) and is designated with a number, to signify its level in the hierarchy.

**CAL: CHARISMA Aggregation Level**

IMU: Intelligent Management Unit      FSO: Free Space Optics  
 OFDM-PON: Orthogonal Frequency  
 Division Multiplexing Passive Optical Network



**Figure 2: Physical layer description of hierarchical CHARISMA aggregation levels (CALs)**

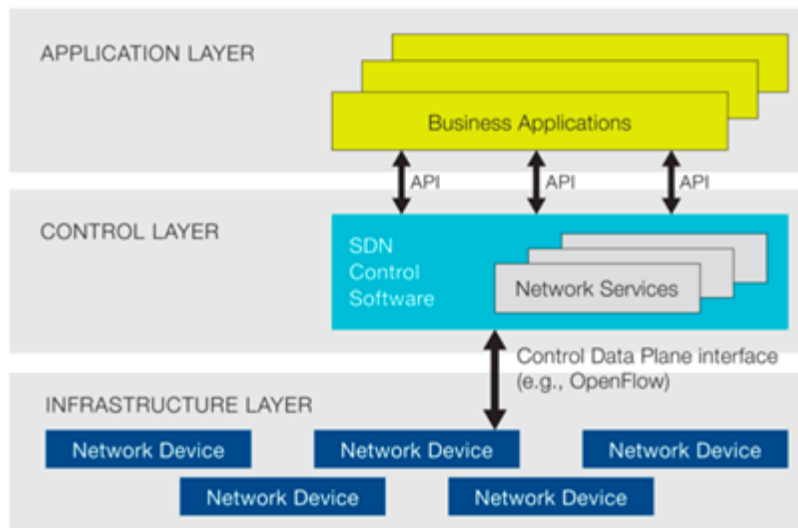
This means that data is routed, where possible, at the lowest common aggregation point, to assist in achieving low-latency networking. For example, for D2D communications, data is routed directly between the devices, whereas routing at the lowest CAL, e.g. at CAL0 (see Figure 2), means the data is routed between devices via the local (e.g. home or access) gateway. For devices within a micro-cell, routing is via the CAL1 level; within a macro-cell, it is via the CAL2 level, e.g. at the macro base station (BS) or active remote node [10]; and finally for non-local routing, this is performed at the CAL3 level, at CO or DC. Distributing intelligence ever closer to the end-user assists in reducing network latency, and allows for more precise SDN and NFV control of the CHARISMA 5G network.

It must be noted that Figure 2 presents a somewhat simplified view of a network hierarchy, as in practice there are various permutations possible. For example, a macro BS can connect to micro BS's or small cells, as a 2<sup>nd</sup> aggregation point (CAL2), but can also connect directly to UEs, skipping in this case CAL1. Similarly, the CAL1 to CAL2 link can be a fronthaul link in the case of C-RAN or a typical backhaul link. We refer to the

simplified structure of Figure 2 in order to define the main, distinct points in the CHARISMA network where we can introduce intelligence through the IMU.

## 2.2. Data Plane

CHARISMA consists of a multiple number of diverse and innovative hardware technologies, whose functionalities are key to enabling the low-latency, open access, and secure data transmission required in future 5G networking. Together, these technologies comprise an important aspect to the CHARISMA data plane architecture, and we describe these individual DP architecture elements in this chapter. Overall, the DP architecture of CHARISMA will enable the integration of these heterogeneous technologies into a single programmable, multi-tenant 5G network. The following Figure 3 shows the relationship between the application, control and infrastructure layers in a generic SDN architecture (as defined by the ONF) with the network devices comprising the infrastructure (DP) layer.



**Figure 3: Software-Defined Network Architecture as defined by ONF [1]**

The device elements singled out for particular description in this chapter are the **TrustNode** router for low-latency and secure routing (section 2.2.1); **accelerated network interface card (NIC)** (section 2.2.3); **device-to-device (D2D)** communications, for low latency featuring local (distributed) security (section 2.2.4); offloading and hierarchical **caching**, to enable low-latency video distribution and network load balancing (section 2.2.5); **mobile cloud** for low latency and scalable (virtualized, as required) networking functions (section 2.2.6); **Ethernet fronthaul** based on OFDM-PON and NG-PON2 technologies, for low latency, low cost and resilient RRH connectivities (section 2.2.8); and **reliable low-latency backhaul** providing open access connectivity between the RAN and the core network (section 2.2.10). These are now described in greater detail in the following sub-sections.

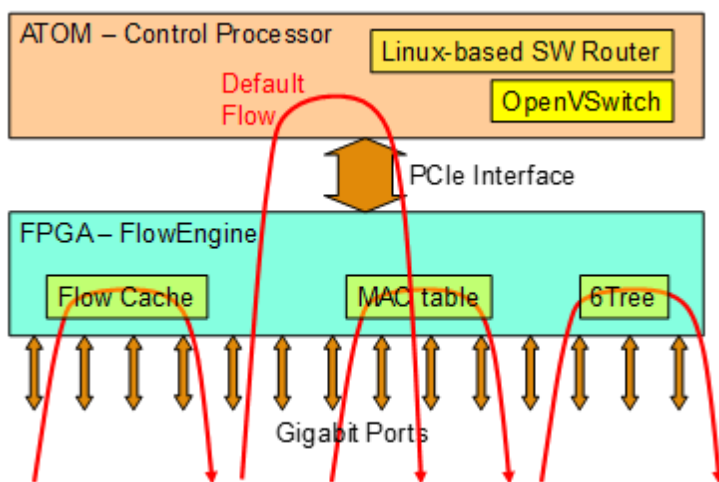
### 2.2.1. TrustNode Design

Rationale for the development of the TrustNode was a lack of open platforms for the exploration of new network functions, in particular in the data plane. The options available today all have significant drawbacks:

1. NetFPGA is too time consuming to program and results are not re-usable;
2. OpenFlow switches have limited number of functions;
3. Standard PCs have too much latency in the data plane.

The TrustNode solves these problems. Its concept is a Control Processor for packet processing supported by HW accelerators in the FPGA (Figure 4). Per default all packets from the external Gigabit (Ethernet) Ports are pre-processed by the FPGA and sent to the Control Processor via the internal PCIe interface. Some packet types are processed in the FPGA only and sent out to other external ports without burdening the Control Processor. This offloading concept should reduce the packet load of the Control Processor to 10%-20% of the external traffic. As shown in Figure 4 three types of packet flows are forwarded by the FPGA directly:

- Layer 2 Ethernet frames are switched according to IEEE 802.1D Bridging;
- IPv6 packets with the special “6Tree” coding (see below);
- Any packet flow matching one of the entries in the Flow Cache (see below).



**Figure 4: TrustNode offloading Concept**

The FlowEngine in the FPGA is a packet processor consisting of configurable blocks, which can be combined in a modular way (Figure 4Error! Reference source not found.). Key blocks are accessible to the user in source code for modification/ enhancement:

- Ingress processing: contains Flow Cache, Action Table and Counters
- Scheduler: allows implementation of intelligent scheduling algorithms
- Egress processing: packet tagging or tag removal, e.g. for VLAN or MPLS

Source code modification is simplified by the use of industry standard AXI-S interfaces with well-defined packet format and an internal (NoC) header for internal information transport. Basic functions such as Ethernet I/O, Mux/DeMux, packet delineation, FCS etc. are not intended for modification; the user can rely on stable operation of these blocks. CHARISMA partners can quickly implement new network concepts and verify them in real networks.

The TrustNode is realized as standalone device; other than NetFPGA it operates without PC.

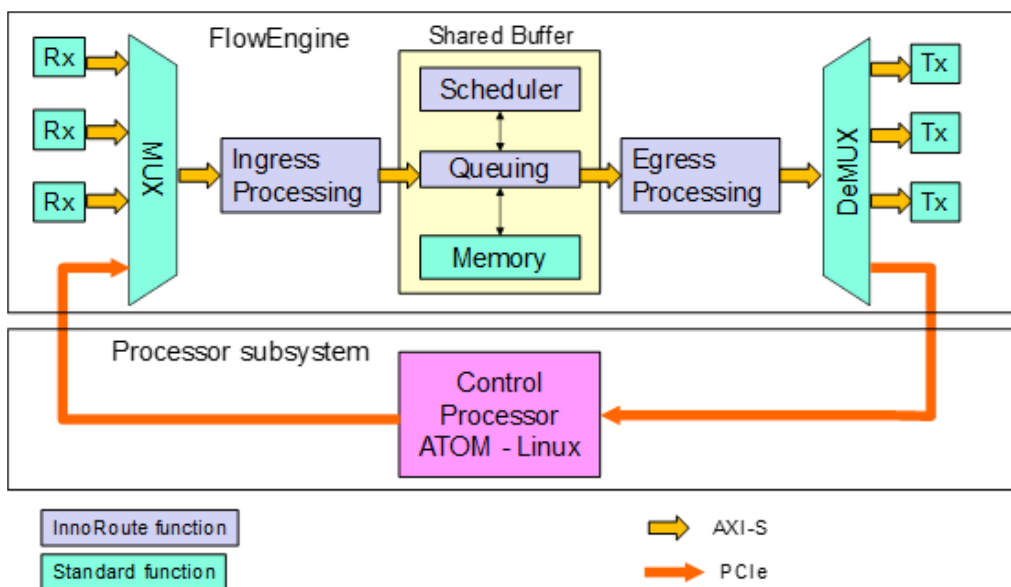


Figure 5: TrustNode Architecture

A key function of the ingress processing path is the Flow Cache. It can be used for example to implement up to four Flow Tables ( $n=3$ ) according to OpenFlow standard (Figure 5Error! Reference source not found.). The packet header fields for Flow Table lookup can be chosen arbitrarily. A built-in Parser provides all usual fields up to Layer 4. Actions can be packet tagging, prioritization, counting, colour marking etc.

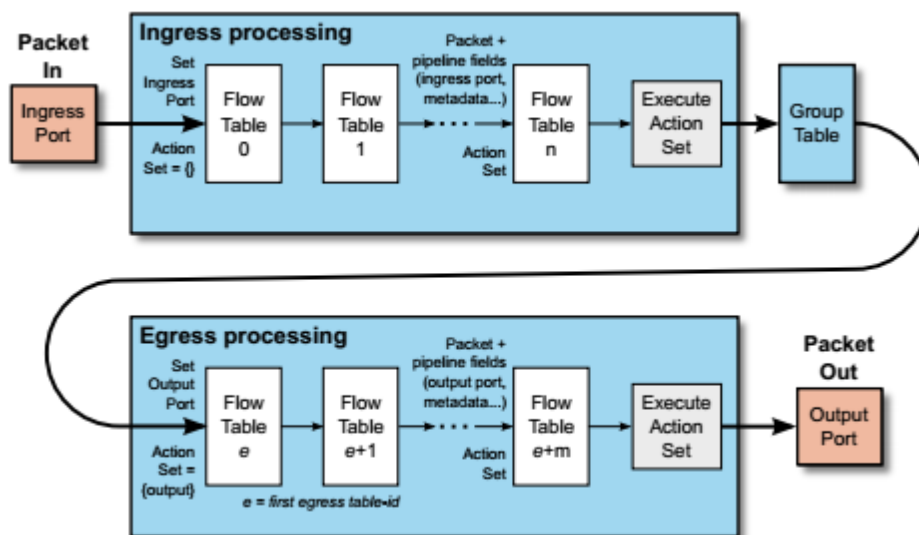


Figure 6: OpenFlow Processing Pipeline

The detailed functionality of TrustNode version 1.0 and 1.1 will be described in the CHARISMA deliverable D1.3. These functions can be considered as examples; they constitute a basis for further adaptation to project needs.

### 2.2.2. Network Slicing and Traffic Model

Network virtualisation relies on independent network slices. This concept works fine as long as bandwidth is not considered. Some services contain flows with guaranteed bandwidth. A virtualized network plane (slice) must have the possibility to check the physical network for bandwidth availability. This task is not straightforward, as the physical path is not obvious. This is outlined with the example in Figure 7, where 4 nodes are physically interconnected with three links. The first virtualised network creates a fully meshed network with six virtual links. Obviously the connection 1-3 is realised via the path 1-2-3, the connection 1-4 is realised as 1-2-4 and 3-4 realised via 3-2-4. Reserving an amount of bandwidth on the link 1-3 translates into bandwidth reservation on the physical links 1-2 and 2-3. In virtualisation plane 1 the links 1-2 and 1-4 are independent, but not in the physical network.

If a second virtualised network is created things get more complicated. Assume that the topology of the Virtualisation Plane 2 is a ring 1-2-4-3. Then a flow from 2-3 via 4 would affect the physical connection between 2 and 3, which does not exist in the Virtualisation Plane 2.

To solve this problem CHARISMA will start with a simplified QoS concept, which needs a very limited number of parameters to be managed. Ideally, one single parameter, the guaranteed bandwidth will be sufficient. To avoid a query process to request bandwidth from the physical network a certain amount of bandwidth could be assigned to each virtual link at slice creation time.

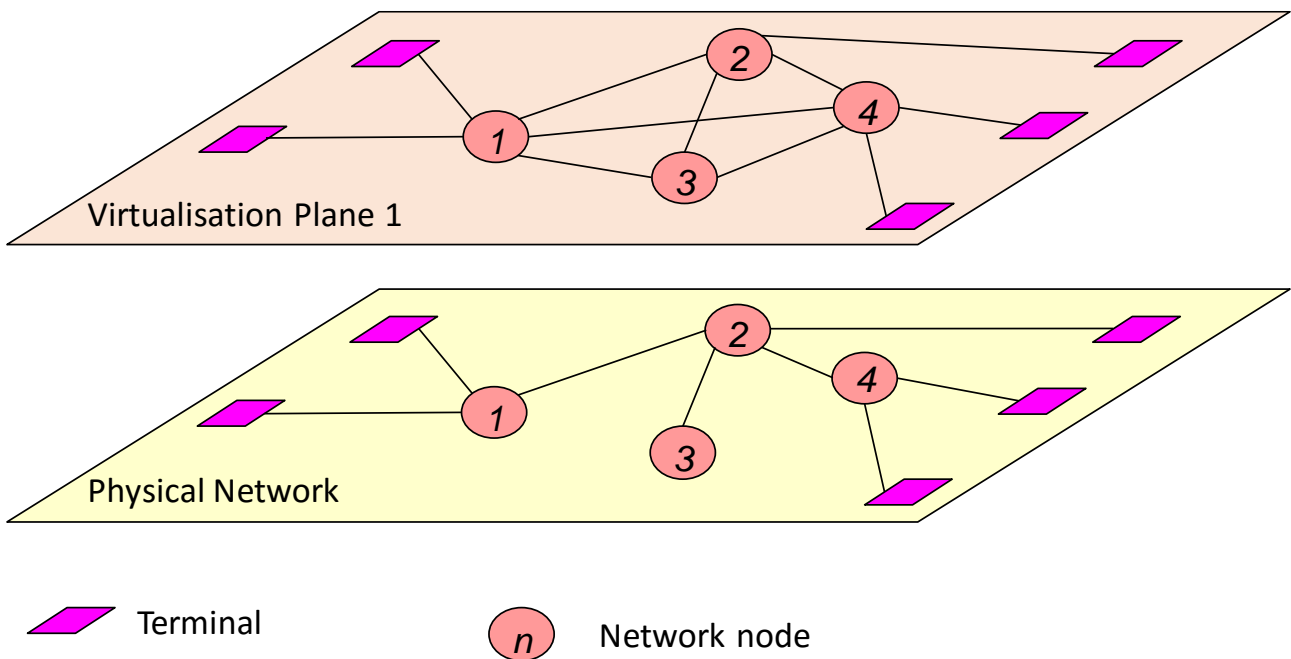


Figure 7: Physical and virtualized network

### 2.2.3. Low latency hardware acceleration

Latency is a very important issue for many applications, and represents one of CHARISMA's technology challenges. For 5G networking, the latency problem has to be solved at any point of data processing, and at any level of control. One of the main contradictions with this requirement in SDN is the fact that VNFs (virtual network functions) run on top of the CPU. The CPU is running the OS (usually Linux) with a lot of processes and threads, and even with SRIOV (short for Single Root I/O Virtualization, or SR-IOV) and within the CPU SMP mode, this requires a lot of task switching, which causes one 10th of a millisecond latency when processing a packet. Here, SRIOV is a specification that allows a PCIe device (NIC connected to Server through PCIe) to appear to be multiple separate physical PCIe devices, which optimizes the CPU vs. IO processing. In addition, Symmetric Multiprocessing (SMP) as related to the CPU, enables a computer architecture to provide fast performance by making multiple CPUs available to complete individual processes simultaneously (multiprocessing). Any of the network forwarding applications: IDS, NAT, FW etc., will take a few CPU cycles to get a decision and set the required packet editing. The same applies for tunnelling; especially if it is secured tunnelling running on a crypto engine.

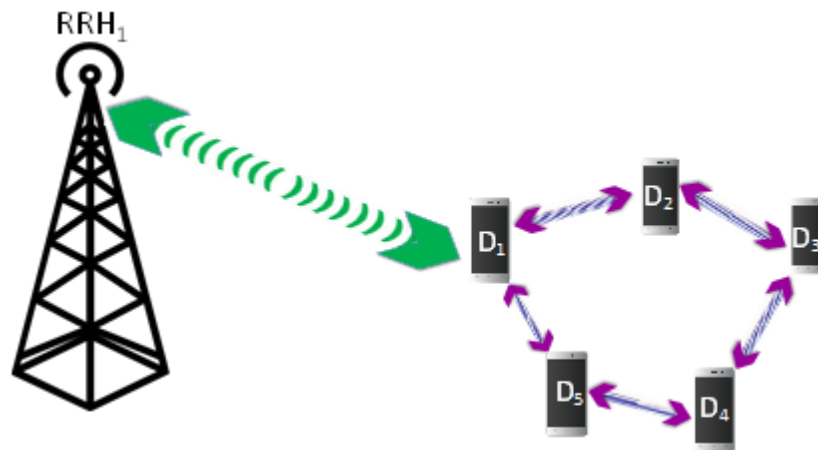
This is why CHARISMA has adopted the approach of VNFs offloading in the NIC, since such a dedicated HW solution causes only a 1-10 $\mu$ s packet latency overhead, and as a result has almost zero effect on packet propagation. Offloading the VNFs also significantly improves the performance, and reduces cooling and cabling, which is also an important consideration for DC infrastructure.

Latency can also be managed during the process of SW design and network planning, especially in the context of 5G network requirements. For example the DPDK (Data Plane Development Kit) proposed by Intel reduces the latency for any NFs (Network Functions) running on the CPU. Some applications have very tight latency requirements (for example, automotive car2car connectivity), and in this case solutions can also support some form of fog computing, where the architecture uses a collaborative multitude of near-user edge devices to carry out a substantial amount of storage (rather than storage primarily in the Cloud), communication (rather than routed over the Internet backbone), as well as control, configuration, measurement, and management (rather than have these controlled primarily by network gateways).

The optical network part of the architecture has a low latency of 5 $\mu$ s per km, which means that a 100-km span provides only 1ms round-trip latency, which is negligible as compared with host processing latency and bottleneck (network packet loss) problems. Adding HW data path offload at any point of the SD network therefore not only solves a considerable part of the latency problem, but also increases network reliability and reduces packet loss.

### 2.2.4. D2D & D2I

D2D communication allows two devices to communicate without a base station (BS) involvement. Even if the BS is involved in the communication, its involvement is limited. This form of cooperative communication is expected to be implemented in the 5G ecosystem. It therefore presents a security threat since user data might be routed through other UEs. A possible solution could be establishing a trusted environment (closed access) for devices operating under D2D.



**Figure 8: D2D & D2I example with 5 devices in a ring topology, and D<sub>1</sub> as a hub/gateway to reach RRH<sub>1</sub>**

In Figure 8, device D<sub>1</sub> acts as the gateway/hub to the other devices. This also makes it possible for the devices D<sub>2</sub>...D<sub>5</sub> to have alternative routes of communication to the RRH via D<sub>1</sub>. For example, D<sub>5</sub> can either communicate via D<sub>1</sub> to the RRH using just a one-hop route, or to go through D<sub>4</sub>, D<sub>3</sub>, D<sub>2</sub> and the device D<sub>1</sub>. This latter option might be somewhat slower (i.e. higher latency) due to the number of required hops; however, it indicates that flexibility (and resiliency) of such topological rearrangement as a means to optimise use of networking resources.

Unlike the traditional D2D communication system via WiFi and Bluetooth using unlicensed spectrum, the cellular D2D communication allows two users in proximity to form a D2D pair and communicate with each other directly by using the licensed spectrum under the assistance of the base station (BS), which means, the quality of service (QoS) in the cellular D2D communication could be guaranteed. Therefore, the D2D communication can be used to offload the cellular traffic from backhaul as well as improve the spectrum efficiency of limited licensed spectrum.

The millimetre-wave bands around 60 GHz have recently become a major option for shorter-range high-speed communication systems, with these bands offering multi-Gb/s throughput as required by multimedia consumer-oriented applications such as uncompressed video streaming and device-to-device (D2D) and device-to-infrastructure (D2I) functionalities.

The technologies offer theoretical maximum data rates of 7 Gb/s with a relatively small transmission range that allows them to work only within a small area. The short wavelengths at mm-wave frequencies, as compared with conventional cellular frequencies, also means that an antenna of the same gain requires a much smaller collection area (e.g. about 60x60 times smaller).

Obstruction loss is significant at 60 GHz, making 802.11ad certainly appropriate for line-of-sight (LoS), room-scale, low-cost, short-range, very-high-throughput applications, such as in-room uncompressed and lightly compressed multimedia wireless display, sync data/file transfer, and so on. However, 60GHz high gain antennas with low cost and small size can also be realised for point-to-point applications such as small-cell

backhaul networks. It's worth noting here that the higher frequency mm-wave E bands, between 71-76 GHz and 81-86 GHz, are also now becoming available for backhauling applications.

WiGig and 802.11ad chipsets are currently expected to be used mainly with UHDTVs and consumer electronics, to enable the transmission and transfer of data intensive high-definition signals. The technologies can also be deployed in mobile phones, laptops, and even peripherals such as printers. The first application that already demands these technologies are streaming or copying movies to a hard drive or video monitor from Blu-ray discs wirelessly, rather than over an HDMI cable.

The point-to-point high-capacity throughputs over relatively short ranges offered by 60GHz technologies offer interesting topological and networking functionalities, e.g. device-to-device (D2D) communications, ad-hoc mesh networking between multiple devices, and mobile distributed caching (MDC). Such capabilities may be utilised in order to maximally exploit available network resources (e.g. data bandwidths, processing power, data caching, and energy); as well as optimise networking aspects such as energy efficiency, load balancing, and spectral efficiency; and also provide network resilience and redundancy, e.g. alternative pathways for connectivity between a device and multiple fixed-infrastructure access points (i.e. RRHs) in the event of there being obstructions, capacity shortages, BS outages, and/or cellular dead spots.

#### ***Latency requirement***

For cellular assisted D2D communication, data traffic can be offloaded by using D2D communication. The resource management configuration parameters as well as any other control signals need to be fed back to the D2D communication pair in the downlink channel. Due to the restrictive proximity requirement of D2D communication and the variability the D2D link, the latency of signalling becomes more critical and strict for effective resource allocation in D2D communication than in cellular communication.

It may appear that there is nothing new about local-area device-to-device communication. For example, WiFi and Bluetooth have supported short-range wireless communication of this sort for many years. However, these technologies have shortcomings that would undermine their ability to support mass-market deployment of proximity-based services:

- **Unlicensed spectrum.** WiFi and Bluetooth operate in unlicensed spectrum, without any centralised control of usage or interference. This is not generally a problem when usage densities are low, but it would become a major limitation as proximity-based services proliferate. Throughput, range and reliability would all suffer.
- **Manual pairing.** WiFi and Bluetooth rely on manual pairing of devices to enable communication between them, which would be a serious stumbling block for autonomous, dynamic proximity-based services.
- **Security.** The security features of WiFi and Bluetooth are much less robust than those used in public cellular systems. They would not be adequate for major public services and they would be unsuitable for public safety applications.
- **Independence from cellular networks.** WiFi and Bluetooth operate independently from cellular radio technology such as LTE. Any form of device-to-device discovery based on them would have to

run in parallel with cellular radio operation, which would be inefficient and would become a significant drain on device batteries.

Integrating D2D into the LTE-Advanced system offers the prospect of a spectrum-efficient, energy-efficient and secure solution for proximity discovery and device-to-device communication, which would benefit from the LTE eco-system of spectrum, mobile devices and network equipment. It could put mobile network operators at the heart of the emerging market for proximity-based services, as well as satisfying the needs of public safety organisations. Some of the potential benefits of LTE D2D include:

- **Radio resource management.** Unlike Bluetooth and WiFi, LTE operates in licensed spectrum and the radio resources are carefully managed by the network, to minimise interference and maximise the performance of the system. The same mechanisms can be extended to D2D.
- **Performance.** Direct communication between nearby devices may be able to achieve even higher throughput and lower latency than communication through an LTE base station. For example, the devices may be closer to each other than either of them is to the nearest base station and a busy base station may be a bottleneck. The network can still exert control over the radio resources used for these connections, to maximise the range, throughput and overall system capacity.
- **Spectrum reuse.** D2D could enable even tighter reuse of spectrum than can be achieved by LTE small cells, by confining radio transmissions to the point-to-point connection between two devices.
- **Network load.** Relieving the base stations and other network components of an LTE network of some of their traffic-carrying responsibilities, for example carrying rich media content directly between mobile terminals, will reduce the network load and increase its effective capacity.
- **Energy efficiency.** Integrating D2D into the LTE system provides the opportunity to achieve energy-efficient device discovery, for example by avoiding the need to scan for other wireless technologies, by synchronising the transmission and reception of discovery signals to minimise their duty cycle and by waking application software only when relevant devices are found in the local area. Meanwhile, direct transmission between nearby devices can be achieved with low transmission power.
- **Security.** D2D can take advantage of the key generation and distribution mechanisms already available in LTE, to achieve high levels of security.

### ***Standardisation***

Incorporating D2D into the LTE standard will provide a common set of tools for proximity-based services, rather than a disparate set of approaches by different application providers. Public safety organisations can benefit from the worldwide economies of scale achieved by the broader LTE system.

### **2.2.5. Offloading and Caching**

Due to the increasing popularity of smart phones and emerging mobile applications, mobile Internet is dramatically expanding. Global mobile traffic will increase nearly 10-fold by 2019 as compared to 2014 [2]. The report also shows that Internet traffic from wireless and mobile devices will exceed traffic from wired devices by 2019 and nearly 67% of Internet traffic will originate from non-PC devices by then. The increase

of mobile data traffic is starting to stress the networks of mobile network operators (MNOs). Many solutions such as traffic offloading and caching in network have been proposed to reduce the network traffic and improve service latency.

Traffic offloading, often known as mobile data offloading, is used to reduce the amount of data being carried on the cellular bands, or allow users to connect to another network with better network connectivity when local cell network is poor. Triggering the offloading can be controlled either by end-user or by network operator. WiFi and femtocell are the two primary technologies for traffic offloading. Offloading traffic from microcell to AP or femtocell in fixed network can allow cellular operators to reduce the traffic on their mobile backhaul and can improve service quality.

Content caching reduces user-perceived latency as well as the transmission of redundant traffic on the network. Authors in [15] analyse the gains of HTTP content caching at the location of SGW in an LTE Wireless network. They found that 73% of the data volume and around 30% of the responses are cacheable. In fixed network, operators have deployed Content Delivery Networks (CDN) to allocate multiple caches close to the end-users in order to limit the bandwidth requirements related to video streaming distribution in the downlink. Moreover, many cloud services can also rely on data centres that are distributed within the network in order to serve demands as close as possible to the users. To meet the growing bandwidth demands of mobile users, studies on content caching in mobile backhaul networks and new infrastructures of mobile CDNs [3] are gaining a lot of attraction recently. That is the case in [4] for example, where caching is enabled in 3G RNCs and LTE eNodeBs. Through deploying in-network caching in fixed and mobile networks, it could allow network operators to enable a better QoS, reduce internal costs and offer new services.

#### **2.2.5.1. Traffic Offloading**

Techniques for offloading traffic (partially or totally) from the network of mobile network operators are currently being designed and deployed at various points of the network. Mainly, there are two types of techniques to divert traffic to offloading networks: *Wi-Fi offloading* and *Femto-offloading*. Wi-Fi offloading deals with moving traffic from macro-cells to the Wi-Fi radio interfaces, and femto-offloading focuses on moving traffic from macro to femto cells. Some examples of Wi-Fi offloading techniques are: I-WLAN and Non-3GPP Access, IP Flow Mobility (IFOM), Multi Access PDN Connectivity (MAPCON) [5][6][7][8][9] Moreover, femto-offloading techniques designed within 3GPP are Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) [10].

In CHARISMA we are focusing on the traffic offloading that is controlled by network operators. Network operators have a global view of network status and so are able to make an optimal decision for traffic offloading. The main objectives here include: 1) reducing service latency through offloading traffic from one network with poor performance to another one with good network connectivity; 2) offloading traffic from one access network to another, or to implement various load sharing policies with our proposed open access platform.

#### **WiFi Offloading**

The basic approach is covered by Interworking Wireless LAN (I-WLAN) [11] for connecting the mobile device to the 2G/3G packet core network, and Non-3GPP Access [12] for connection the EPC network. It supposes a transfer of all IP traffic between mobile network and Wi-Fi network (WLAN) under control of a mobile network operator. 3GPP defines three basic scenarios for this approach.

- *Non-Seamless WLAN offload* for the EPC, allows users to access the Internet or Intranet directly from the WLAN access, but under control of the network operators over a 3GPP AAA server that performs corresponding authentication and authorization procedures for users.
- *Untrusted Non-3GPP access* for the EPC, enables authorized users to access to the operator services or external PDNs through a secured connection towards the mobile core network. Figure 9 illustrates this scenario for the connection to the EPC where Wi-Fi is considered as a non-trusted non-3GPP access, so that a VPN/IPsec tunnel is established between the User Equipment (UE) and the evolved Packet Data Gateway (ePDG) residing in the EPC network for security reason. The ePDG is an evolution of the PDG that is involved by the WLAN 3GPP IP access to the 2G/3G packet core.

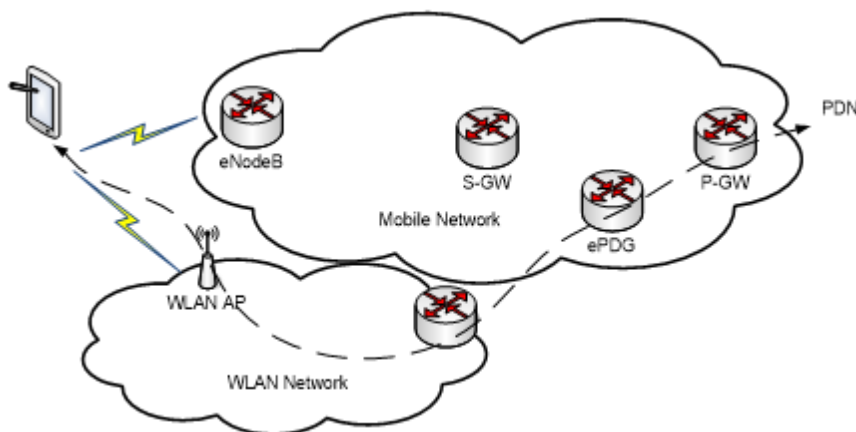


Figure 9: WLAN 3GPP IP access

- The *Trusted Non-3GPP Access* enables authorized users to access to the operator services or external PDNs, as the previous scenario. But, since the access network is considered as trusted, it does not require the ePDG to secure the EPC access. When Wi-Fi is used as the access network of this scenario, the TWAN (Trusted WLAN Access Network) specifications (in chapter 16 of [12]) is applicable to enable a connection to the EPC without the UE needs to establish any tunnel.

3GPP Release 8 introduced some features to maintain the IP sessions between mobile and WLAN networks for EPC [12]. For this purpose, two mobility schemes are supported:

- Host-based mobility: it relies on Dual-stack Mobile IPv6 (DSMIPv6).
- Network-based mobility: it mainly relies either on PMIP (PMIPv6) or GTP (GPRS Tunnelling Protocol).

It allows the user to roam independently in IPv4 and IP v6 address spaces [5]. The P-GW is considered as an anchor point to support seamless mobility. However, in 3GPP Rel'8 the user cannot communicate with the P-GW using both access networks simultaneously. The UE is connected through a single radio access (i.e., either 3GPP or Wi-Fi access) at a given time. Thus, flexible allocation of IP flows between accesses is not supported. That is, as in previous cases, all traffic related to a PDN connection should be routed through either mobile network or WLAN. However, if the UE can support simultaneously connections through

different access it can bring some additional advantages. In some scenarios it is important to allow dynamic allocation of IP flows belonging to the same PDN connection between different access networks. Currently, 3GPP is being defined *IP Flow Mobility (IFOM)* technique [6] where the mobile terminal is able to use more than one interface to send data towards the same PDN using different paths as illustrated in Figure 10.

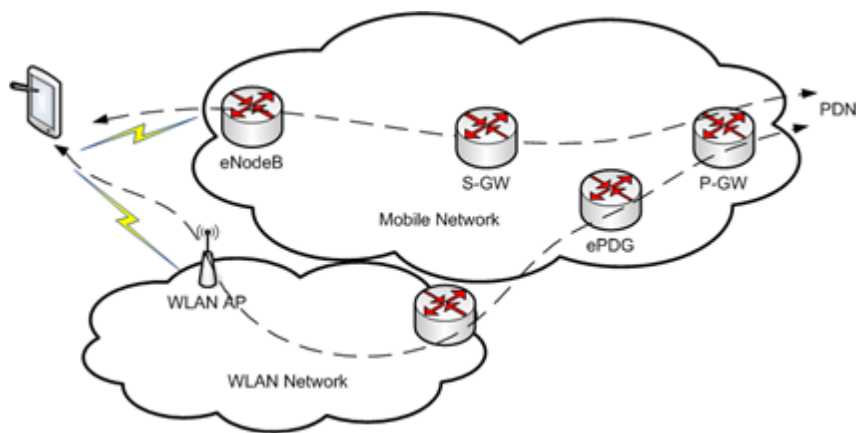


Figure 10: IFOM scenario

Based on the IFOM scenario the UE could add or remove IP flows over either of access within a PDN connection, effectively offloading data. Thus, the granularity of access system connectivity in IFOM is IP flow-based as opposed to I-WLAN PDN connection-based granularity.

While IFOM is dealing with multiple IP flows over 3GPP/non-3GPP access within a single PDN connection, the MAPCON (*Multi-Access PDN connectivity*) concept proposed recently by 3GPP [6][7][8] is oriented to support routing different simultaneously active PDN connections over 3GPP/non-3GPP access. The MAPCON scenario is shown in Figure 11. In this scenario the UE can use more than one PDN-GW to be connected to different PDN networks simultaneously.

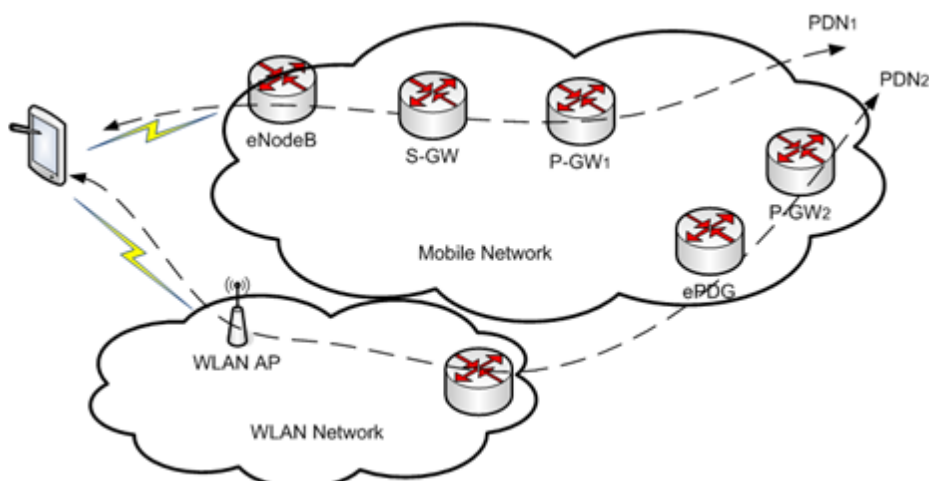


Figure 11: MAPCON scenario

**Femto-offloading**

In the 3GPP technical report [10], the concept of offloading traffic via femtos has been defined. LIPA (Local IP Access) is an offloading mechanism that does not allow traffic from a UE to traverse the mobile operator's network except Home eNode B (HeNB). An IP capable UE through a HeNB is able to exchange data with IP capable devices within its local network. The UE is also able to have an access to an external network connected to the local network [13] LIPA is realised using a local gateway (L-GW) having the P-GW functionality as shown in Figure 12. A unique PDN connection is established over the L-GW to enable a differentiated treatment of the LIPA data flow. At the same time, the UE can continue to have a data session over a macro core network over separate PDN connections. Thus, LIPA offloading supposes a PDN-based granularity. As a result, IP flow reallocation between external public network connected via local network and the macro network is not possible. The continuity of the LIPA session with mobility is not defined yet. The LIPA PDN connection is interrupted when the UE goes out of femtocell coverage [13].

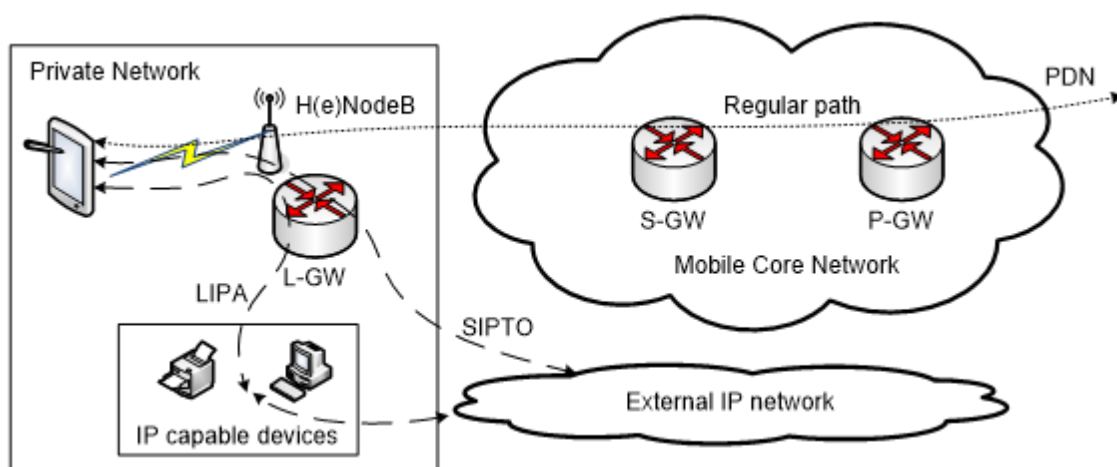


Figure 12: LIPA/SIPTO-Femto scenario

SIPTO (Selected IP Traffic Offload) is an offloading technique by means of which the mobile network operator is able to offload portions of IP traffic through a network node close to the UE's point of attachment (femtocell or H(e)NB) or another gateway in macro network [13]. Thus, there are two cases of SIPTO scenario: SIPTO-Femto and SIPTO-macro, correspondingly. SIPTO-Femto is defined to be the same as LIPA using a L-GW collocated with the H(e)NodeB in a private network as a breakout point, but with direct access to the public PDN network. The SIPTO-Femto scenario is illustrated in Figure 13. SIPTO-Macro has the breakout point at/above the RAN. The main idea is to select a S-GW and a P-GW that are topologically close to RAN and MME to offload data from involved GWs that can be located quite far from the current access network. The portion of data flows associated with a specific PDN or all active PDN connections can be offloaded through a Local P-GW/S-GW (L-P/S-GW) that in fact has a regular P-GW/S-GW functionality. Thus, the relevant PDN connection(s) is redirected towards the L-P/S-GW. Since the SIPTO-Macro scenario has a breakout point at/above RAN it does not help to reduce a traffic load on the access network. SIPTO-macro scenario is presented in Figure 13.

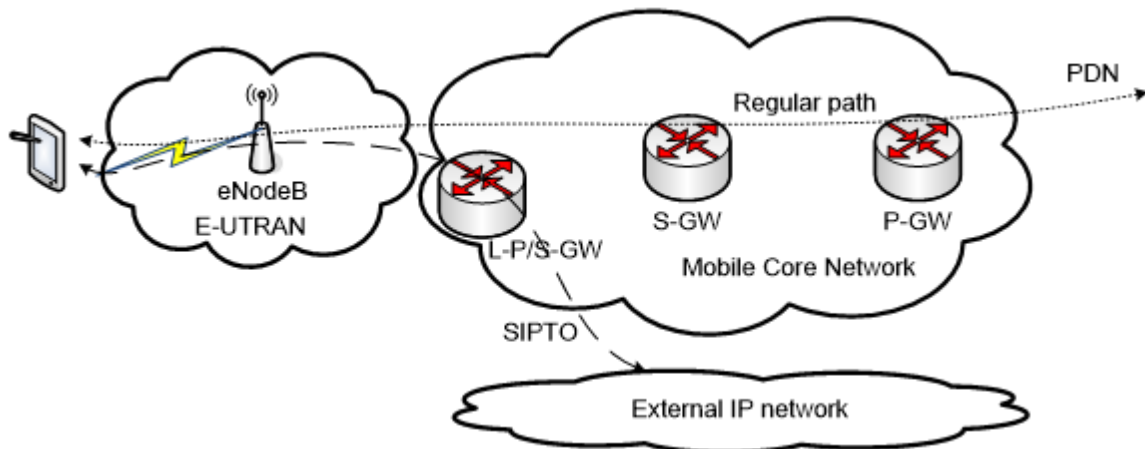


Figure 13: SIPTO-Macro scenario

#### 2.2.5.2. **Mobile distributed caching (MDC) & Hierarchical Caching**

Fixed network operators have deployed caches and data centres close to the end-users in order to efficiently serve traffic demands by limiting the bandwidth requirements on the backbone and metro networks. According to Bell Labs' paper [14], the use of distributed caches within the Metro/Aggregation and Access network segments resulted in offloading into the metro caching up to 57% of the total fixed traffic in 2012. This amount could grow to 75% by 2017. To meet the growing bandwidth demands of mobile users, commercial LTE networks are being deployed to significantly increase the bandwidth and reduce the latency experienced in the mobile network. Though LTE improves the network performance between end users and mobile network, the service latency still highly depends on the distance between the data centre and the exchange point where the mobile network connects to the Internet. Ensuring low service latency is crucial to satisfy the QoS of current applications, especially for latency-sensitive applications like audio and video services. Moreover, LTE network backhaul bandwidth will be heavily consumed by duplicated data streams when a content (such as high-popular video) is requested simultaneously and frequently. Mobile network caching could be a cost-effective solution to improve the service latency and reduce the mobile backhaul traffic by replicating popular and frequently demanded content in IP-based 3G/LTE network elements closer to mobile users.

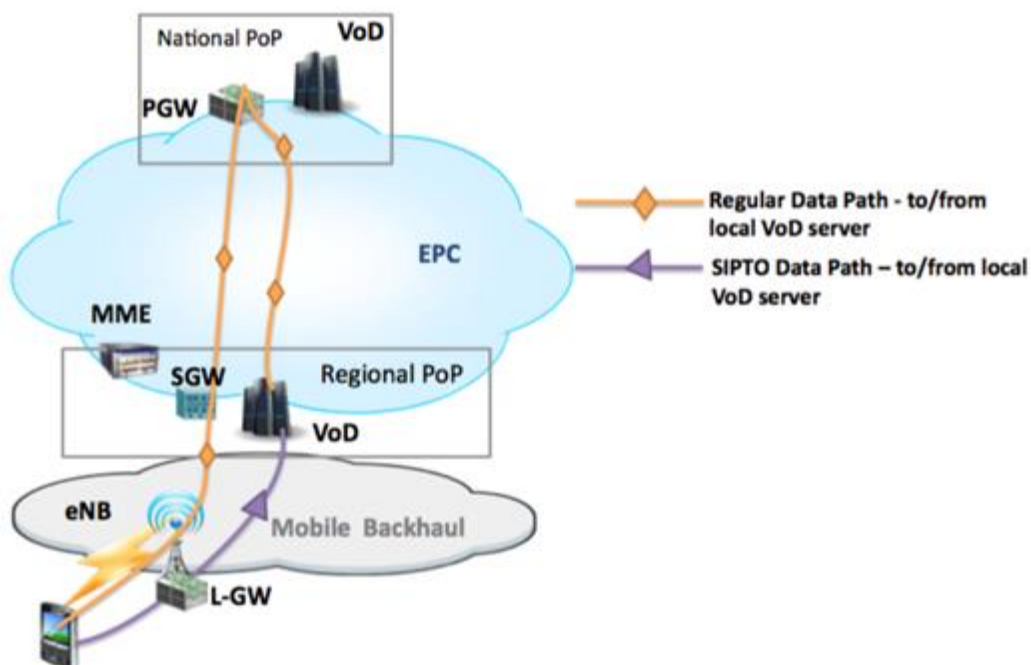
Historically content was stored in centralized locations owned and operated by the original creators of the content. As VoD and Over the Top (OTT) services increased in volume, network operators began to search for improved models with the intent to reduce the total load in the network, improve user experience and maintain customer satisfaction as well as providing a mechanism to monetize the delivery of content-based distribution. Operators therefore adopted content cache support on or collocated with less centralized, Broadband Remote Access Server (BRAS) devices until such time that a distributed approach was standardized. The broadband forum specifications for DSLAMs incorporate cache facilities, including content offload interfaces, content injection and Deep Packet Inspection (DPI, an enabler of content based functions). Such tools have supported operator business models and enabled a distributed content distribution model.

To enable caching in 5G network, a set of key network elements with caching functionality could be considered such as home/residential gateway, eNodeB, Macrocell, access gateway. First, today's dominating

technology delivering Internet to the home is based on copper access technologies, i.e. Digital Subscriber Line (DSL). A converged residence gateway integrating DSL, Wi-Fi and 3G/LTE (such as femtocell, nanocell, etc.) has been designed to provide a unified service and reduce the mobile backhaul traffic. Several advantages can be achieved because: first, a mobile device accessing to a Wi-Fi AP does not have services like SMS, telephone and mobility; second, femtocell can support well these services; however, the data are normally tunnelled between Internet and mobile network, which still consumes lot of bandwidth in mobile network, and probably deteriorates the user experience. In-network caching can be further enabled in a converged residential gateway to improve network performance, especially while the residential gateway locates in a public place or at enterprises. Second, in a mobile network, the first location that a content cache could be placed would be on the base station itself. In terms of an efficient business model and the trend towards base station hoteling, the cell-site gateway will become the natural location to host content cache facilities.

The use of caches in the mobile network is not as simple as in the fixed network due to the tunnelling between the UE and the PGW in both directions. This tunnelling implies that, even if a video server is geographically close to a UE, the downloaded video stream has to go through the EPC in order to enter the tunnel available between the UE and the PGW, which may be far from the UE (there are currently a few PGWs per mobile network). If caching is enabled in mobile access network like femtocell or eNodeB to allow cached data to be served directly from mobile access network to mobile users, there would be some functional changes needed. The possible solutions for this tunnelling issue would be as follows:

First, in order to enable caching functionality in eNodeB, PGW could be moved down to the access network from centralized PoP location. Second, mobile data offloading approaches such as LIPA and SIPTO [10] have allowed the UEs to access the external IP network using distributed Local Gateways (LGWs) closer to the UE without traversing the EPC network as shown in Figure 14.



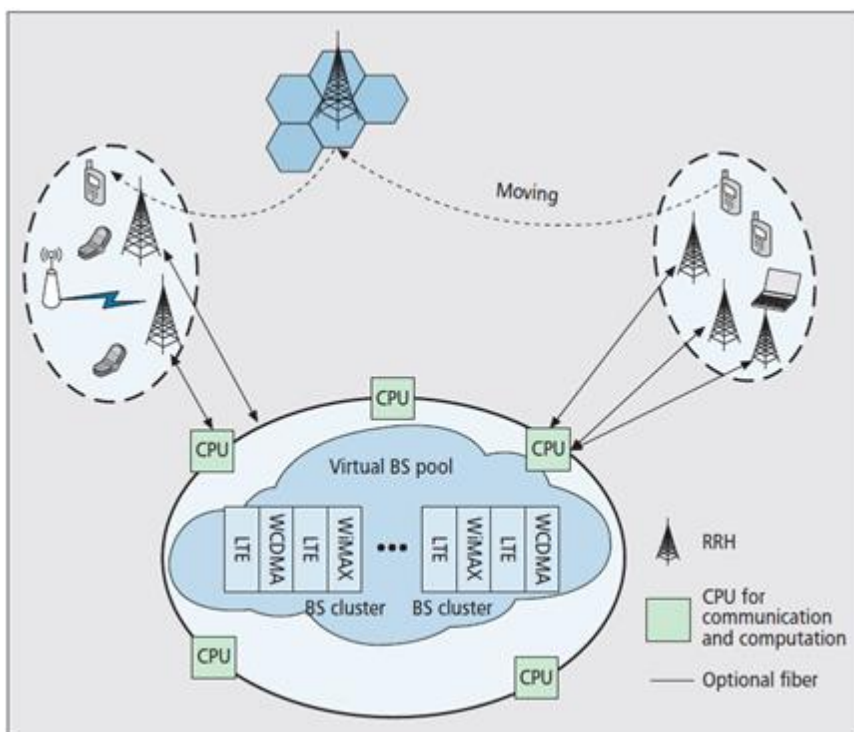
**Figure 14: Accessing a local cache with SIPTO architecture**

A cooperative hierarchical caching solution can optimize the utilization efficiency of network resource and improve the service latency. The hierarchical caching is called a cooperative hierarchical caching if caching decisions are made both locally and globally at each cache. Based on the definition of overall caching architecture and key elements enabling caching functionality, our cooperative hierarchical caching architecture can be deployed on different CAL layer (from CAL0 to CAL3).

### 2.2.6. Mobile Cloud

Mobile operators are considering the cloud in order to take advantage of the same benefits that the computing sector has gained. These advantages include scalability, efficiency and lower capital and operating expenses. On the RAN side of the network, the cloud-RAN concept (C-RAN) together with SDN technology allows the separation of the radio units, or Radio Remote Heads (RRHs), from the base station baseband units (BBUs). In C-RAN, BBUs and RRHs are separated from each other with BBUs located at central offices (CO) or master cell sites and RRHs located at the cell sites, as shown in Figure 15. This decoupling will enable mobile operators to transform the baseband functions of the base stations into VNFs providing them with the ability to easily scale their networks up and down as needed, achieving at the same time low latency and increased throughput.

By utilizing Cloud RAN, operators can centralize the control plane, which does not have extreme bitrate requirements, to bring RAN functionality closer to applications, or further distribute the physical layer closer to the antenna to enable massive beamforming [24].



**Figure 15: Cloud-RAN architecture [21]**

However, it is expected that the C-RAN/fronthaul architecture intended for 4G will not be able to handle the increased capacity requirements of 5G. To overcome this issue, the splitting of the functions of BBU and RRH should be defined differently from the way they are currently defined. Many functional split options have been proposed, as shown in Figure 15 each offering different trade-offs such as reduced fronthaul capacity, RAN virtualization gain, etc. These new network solutions are currently being tested by many operators including the Korean big 3, NTT, AT&T, etc. [22].

The functional split in cloud-RAN introduces more degrees of freedom in processing design and flexibility in the actual execution of functions. The bottom of Figure 15 exemplifies a traditional 4G C-RAN implementation where all baseband functions are centralized. However, as we move upwards and according to different needs, a more flexible functional split can be applied bringing more baseband functions closer to the RRH.

Considering the initially envisioned benefits of C-RAN however, flexible centralization has two main drawbacks:

- RRHs become more complex, and thus more expensive.
- De-centralizing the BBU processing reduces the opportunities for multiplexing gains, coordinated signal processing and advanced interference avoidance schemes.

Consequently, flexible or partial centralization will be a trade-off between what is gained in terms of fronthaul requirements and what is lost in terms of C-RAN features and overall cost [23].

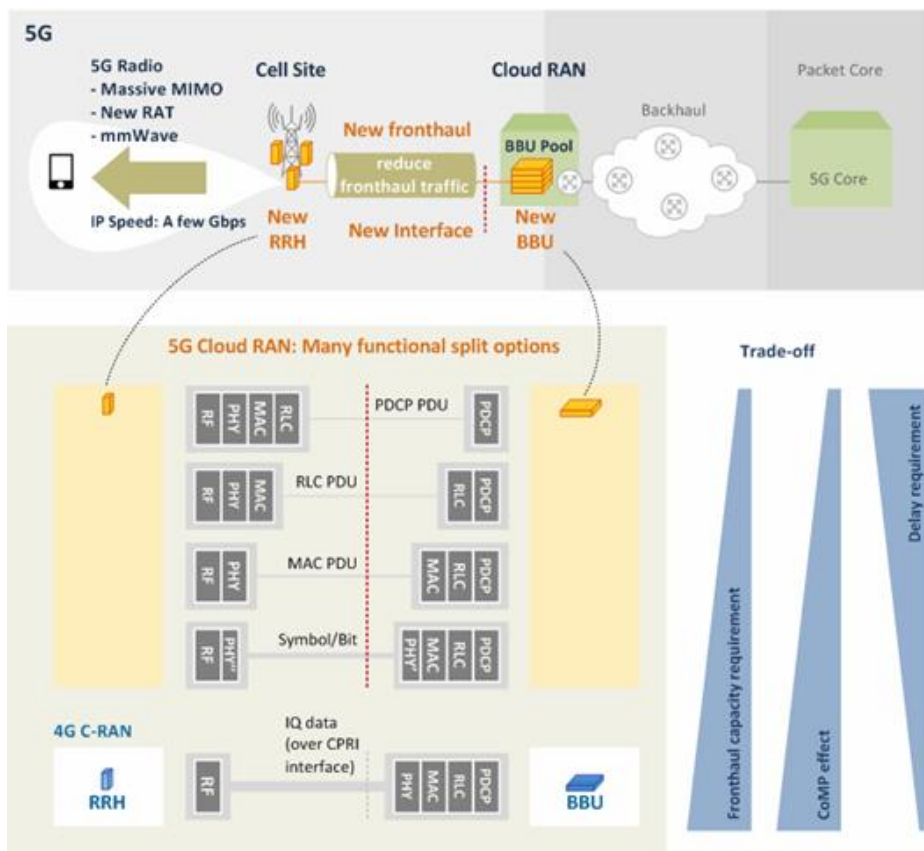


Figure 16: Cloud-RAN for 5G including functional split between BBU and RRH [22]

### 2.2.7.Fronthaul Design

Fronthaul design is currently a topic of great research interest and being intensively investigated, e.g. the project H2020 iCIRRUS (grant agreement No 644526) has performed an excellent overview of Ethernet-based fronthaul design. For more detailed information, the reader is referred to the original iCIRRUS document [16].

Currently, two specifications are used to design the radio fronthaul, namely CPRI and OBSAI. The Open Base Station Architecture Initiative (OBSAI) provides an open interface specification. It was established in 2002 by a group of base station equipment vendors to provide a complete and example modular architecture for cellular base stations. Common Public Radio Interface (CPRI) was also the result of cooperation between vendors. Here, the scope of the cooperation is specifically limited to the interface between what CPRI terms a Radio Equipment Controller (REC) and the remote Radio Equipment (RE).

At the most fundamental level any fronthaul solution must provide reliable transport of 3 basic flows:

- User Data
- Control and Management (C&M)
- Synchronisation

In current fronthaul implementations, user data is composed of digitised radio baseband waveforms (IQ data). The exact format and mapping of these samples depends on the application (Radio Access Technology), but a common feature is that the required bit rate is proportional to the target maximum provisioned user throughput (carrier bandwidth) and number of antenna-carriers (AxC) to be used, not to the actual bandwidth required at any given instant. Typically, this data is uncompressed, leading to very high fronthaul data rate requirements. CPRI currently specifies line rates up to 12.16512 Gbit/s, however extrapolating from current requirements to target requirements for 5G networks suggest that using the same techniques may require data rates in excess of 100 Gbit/s in future fronthaul networks. Because of these huge requirements using CPRI, a new functional split with a much reduced bitrate has been proposed [17]. It is estimated that an Ethernet-based new fronthaul as depicted in Figure 17 could reduce the bit rate by a factor of 20 [18].

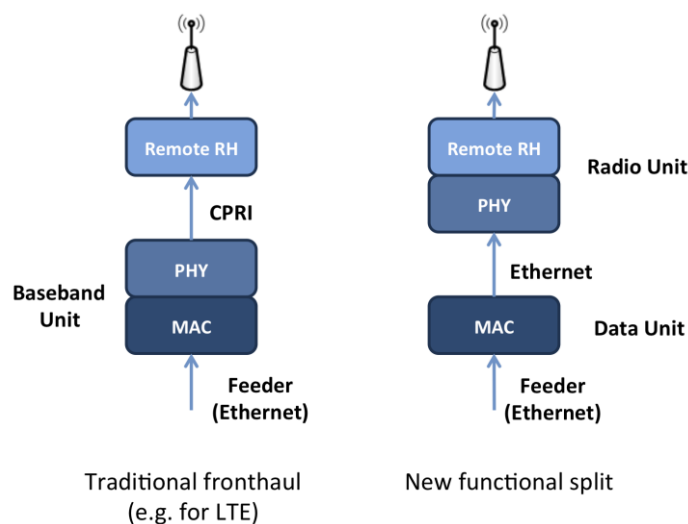


Figure 17: New functional split [17]

CHARISMA is following the recent developments in fronthaul design for 5G closely and supports the new functional split. This new fronthaul design requires an Ethernet link between the data and the radio unit.

### 2.2.8.Ethernet fronthaul

In the context of providing Ethernet in the fronthaul of the architecture, there are a number of challenges: First, Ethernet provides no inherent support for synchronisation of frequency, phase or time. Secondly, latency (delay), both in terms of absolute value and variation, can be a significant issue. Both stem from the origins of Ethernet and have conversely contributed to its cost effectiveness and adaptability. Fortunately, as Ethernet has found wider use, solutions to these issues have been developed in the form of Synchronous Ethernet (for frequency synchronisation) and higher layer protocols such as IEEE1588-2008 (for phase and time synchronisation), while other developments attempt to address the latency issues. These are now described in the following sections.

#### **Synchronisation**

The term 'synchronisation' is broadly used in telecommunications, in particular in mobile communications systems to encompass the methods that enable oscillators (clocks) at different locations to be set to the same frequency or to the same phase/time within specified limits.

As has already been noted, unlike CPRI, Ethernet in its basic form does not natively support synchronisation of any kind. While this has resulted in cost and reduced-complexity benefits for Ethernet implementations, the expansion of Ethernet into more application areas including mobile network infrastructure has driven a demand for synchronisation across Ethernet networks. This has prompted the development of extensions to Ethernet to enable frequency synchronisation, and of higher layer protocols facilitating frequency, phase or time synchronisation.

Although synchronisation is already widely deployed in backhaul networks, the additional performance requirements in fronthaul networks, coupled with more stringent performance requirements for new RAN features beyond 4G place new demands on synchronisation performance.

#### **Ethernet Latency**

Latency in an Ethernet network is defined as the time for a frame to pass the networks from transmitter to receiver. Ethernet networks have several sources of latency ([19]):

- store and forward
- processing delay (switch fabric)
- transmission delay (wireline/wireless)
- queuing delay (frame)

Store and forward refers to the basic operating principle of an Ethernet switch. The term is descriptive of its actual operation: the switch stores the received data in memory until the entire frame is received. So, the *store and forward latency* can be calculated from the Ethernet frame length and bitrate.

The internal switch fabric consists of Si-chips that implement the store and forward engine, MAC address table, VLAN handling, and service classes. The fabric introduces a *processing delay* when executing the logic that implements these functions.

Bits transmitted along a wired link travel at about  $\frac{2}{3}$  of the speed of light, whilst a wireless link operates at the speed of light. For long distances this *transmission delay* can become significant.

Ethernet switches use queues in conjunction with the store-and-forward mechanism to eliminate the problem of frame collisions. Queuing introduces a non-deterministic factor to latency since it can often be very difficult to predict exact traffic patterns on a network. The introduction of service classes help to mitigate *queuing delay*, at least for the classes with high priority.

### 2.2.9.NG-PON2

Driven by the proliferation of heterogeneous bandwidth-consuming services, passive optical network (PON) architectures have been evolving in the last decade, providing enhanced availability, data rates and services. An evidence of this fast evolution is that both IEEE 802.3 and ITU-T together with the full services access network (FSAN) group are currently working towards the standardization of next-generation PON2 (NG-PON2) [25][26]. NG-PON2 is therefore also appropriate for use in the CHARISMA network, as a means to offer a technical solution for fixed-mobile convergence, satisfying 5G KPIs, such as end-user bandwidths.

Several access technologies are currently deployed in the field, namely, EPON, 10GEPON, BPON, GPON, XG-PON and the choices have been to evolve from the legacy systems without discontinuity of the previous technology, in other words maintaining coexistence over the same fibre span to further exploit the investment [27]. Additionally, as shown in Figure 18, spectral scarcity is now becoming a reality, since most of the low loss bands of the fibre are fully exploited. Gigabit PON (GPON) technology, driven by the ITU-T, has conquered several markets and achieved high take rate. XG-PON was developed to try and improve the data rate, and due to the lack of component maturity together with tighter filtering and laser requirements, some risks were already taken. From there, a new standard is now under finalization, the time and wavelength division multiplexing PON (TWDM-PON) or NG-PON2 [26][28], representing a major change in the paradigm of previous technologies.

NG-PON2 is based on ITU-T G.989 series:

1. ITU-T G.989.1- 40-Gigabit-capable passive optical networks that contains the general requirements for the NG-PON2.
2. ITU-T G.989.2 - 40-Gigabit-capable passive optical networks (NG-PON2): Physical media dependent (PMD) layer specification, that specifies parameters for the physical layer as wavelength plans, optical loss budgets, line rates, modulation format, wavelength channel parameters and ONU tuning time classes
3. ITU-T G.989.3 - 40-Gigabit-capable passive optical networks (NG-PON2): Transmission Convergence Layer Specification.

- ITU-T G.989 (no dot) that contains the common definitions, acronyms, abbreviations and conventions of the G.989 series of Recommendations.

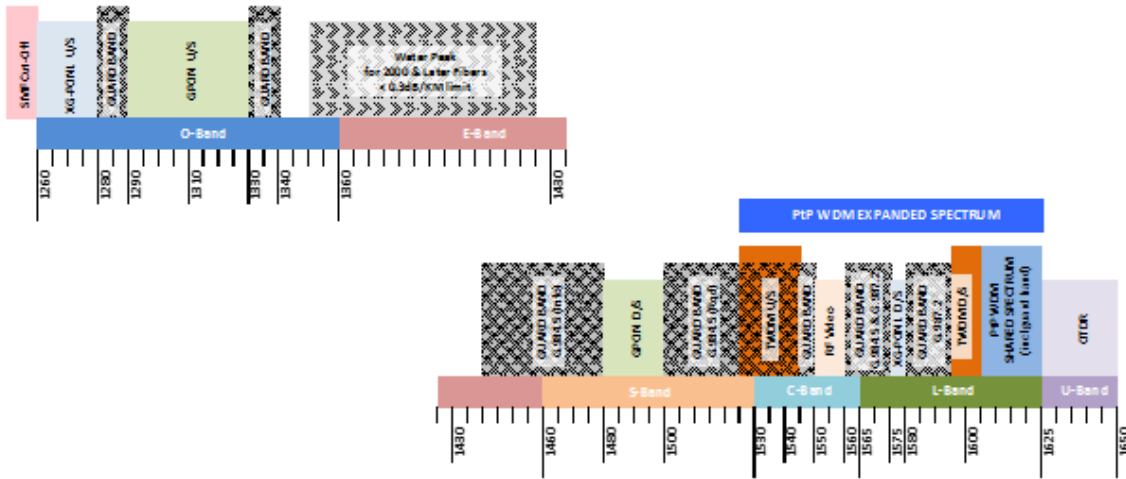


Figure 18: PON Spectrum

**Requirements and Drivers for NG-PON2**

NG-PON2 main target requirements are the increase of aggregate capacity per Optical Line Terminal (OLT) PON port, a sustainable bandwidth on any Optical Network Unit (ONU) at downstream of 1Gbit/s and upstream of 0.5 to 1 Gbit/s, support 64 or more ONUs per port, be compatible with legacy PON infrastructure, a 40 km differential reach and a smooth migration, ie, legacy PON co-existence (GPON and/or XG-PON1), support multiple applications on the same Optical Distribution Network (ODN) (residential + business+ backhaul), embedded test & diagnostics capabilities and support of PON resilience, including dual parenting [42].

TWDM-PON was selected as the primary technology solution for NG-PON2 (in April 2012). This decision was based on considerations of system cost, technology maturity, loss budget, complexity and power consumption.

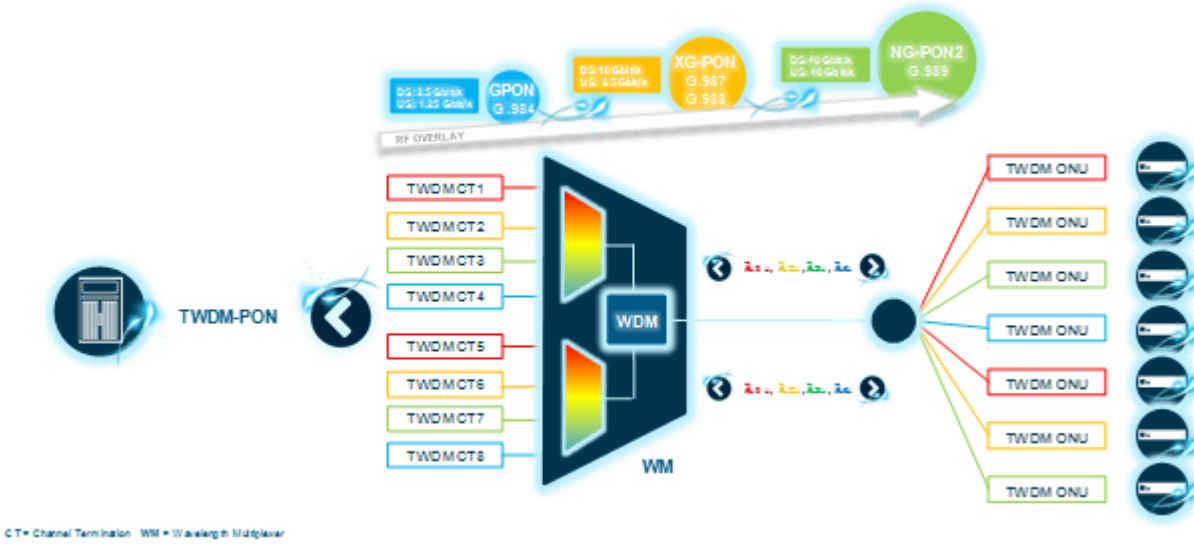
There are several applications driving the demand for next generation PONs, all of which are relevant to CHARISMA, namely:

1. FTTB for multi-dwelling units
2. Enterprises
3. Mobile Backhaul
4. Fronthaul
5. Cloud-RAN

**What is NG-PON2?**

NG-PON2 is a 40 Gbit/s Capable Multi-Wavelength PON system that can grow up to 80 Gbit/s. It has 3 types of channel rates: basic rate 10/2.5 Gbit/s and as an option 10/10 Gbit/s and 2.5/2.5 Gbit/s. ONUs are colourless and can tune to any assigned channel [42]-[45].

Figure 19 presents the basic NG-PON2 system.



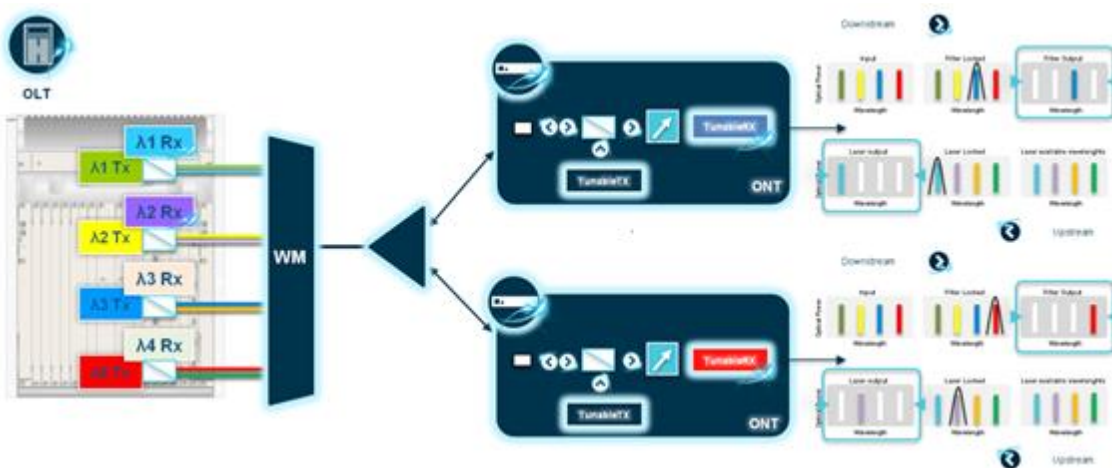
**Figure 19: NG-PON2 basic scenario**

The downstream TWDM channels, in L band, 1596-1603 nm, fit between XG-PON1 downstream and OTDR monitoring band. This enables simultaneous co-existence with legacy PON and 1550 nm RF video.

In upstream, the TWDM channels work in C band, 1524-1544 nm (wide band), 1528-1540 nm (reduced band), 1532-1540 nm (narrow band), above the WDM1r co-existence filter edge and below the 1550 nm RF video band. The use of C-band allows lower cost ONUs [42]-[45].

Upstream wavelength options are driven by differing capabilities of the ONU transmitter to control its wavelength, i.e. wide band option is usable by wavelength set approach to channel control where a DFB laser may drift over a wide range, narrow band option may be most appropriate for temperature controlled lasers *than can lock onto the assigned DWDM wavelength* [42]-[45].

In Figure 20 it is possible to see the wavelength tuning capabilities of the ONUs in the NG-PON2 system.



**Figure 20: NG-PON2 wavelength tuning**

NG-PON2 is compatible with legacy loss budget classes, i.e., B+ and C+ of GPON and N1, N2, E1, E2 of XG-PON1. It requires a minimum optical path loss of 14 dB and allows a differential reach of 40 km. The optical path loss and fibre distance classes are presented in next tables [42]-[45].

**Table 1: NG-PON2 class losses (dB)**

Class	N1	N2	E1	E2
Min loss (dB)	14 dB	16 dB	18 dB	20 dB
Max loss (dB)	29 dB	31 dB	33 dB	35 dB
Max. differential optical path loss	15 dB			

**Table 2: NG-PON2 distance classes**

Fibre distance Class	Minimum (km)	Maximum (km)
DD20	0	16 dB
DD40	0	31 dB

NG-PON2 has defined 3 classes of Tx/Rx wavelength channel tuning time and these classes were broadly defined based on known wavelength tunable technologies [42]-[45]:

1. Class 1 components may include switched laser on arrays.
2. Class 2 components be based on electronically tuned lasers (DBR);
3. Class 3 components could be thermally tuned DFBs.

**Table 3: NG-PON2 tuning speed classes**

Class 1	< 10 us
Class 2	10 us to 25 ms
Class 3	25 ms to 1 s

By wavelength agility NG-PON2 allows enhanced network functionalities unavailable in previous generations of pure TDM PONs, namely [42]-[45]:

1. Incremental bandwidth upgrade (Pay-as-you-Grow);

2. Selective OLT port sleep for power saving during low traffic periods, i.e., during times of low traffic load all ONUs can retune to a common wavelength and allow OLT ports to be powered down;
3. Resilience against OLT transceiver failures through ONU retuning, i.e., all ONUs can retune to a common standby or working wavelength under a fault condition to maintain a basic service until the fault is cleared;
4. Fast, dynamic wavelength and timeslot assignment using DWBA (extra degree of freedom c.f. DBA today) to improve bandwidth utilization efficiency.

NG-PON2 transmission convergence layer has new capabilities supported by the protocol, as multiple wavelengths, TWDM and point-to-point channels, start with a single channel adding more channels later and distributed OLT channel Terminations (CTs) that can drive a single fibre [42]-[45]. These new protocol functions allow:

1. Multiple wavelengths so protocol supports tuning;
2. New identities to distinguish system and wavelength channel;
3. New management protocol for PtP WDM and TWDM activation;
4. Dealing with ONUs with uncalibrated lasers that must not be allowed to transmit in the wrong wavelength channel;
5. Inter-channel messaging for some procedures over distributed OLT channel terminations;
6. New rogue scenarios that can be detected and mitigated.

Regarding the tuning support, the ONU state machine cover activation and channel management. PLOAM messages control tuning and new ONU parameters were added for tuning time.

Identities for multiple wavelengths and distributed OLT CTs are taken into account [42]-[45]:

1. Each downstream channel wavelength advertises channel information including channel number and an identity of the PON system that owns the channel;
2. OLT CT can feed back upstream channel identity to ONU;
3. ONU can feed back the downstream channel and system identity it is receiving to OLT CT.
4. Distributed OLT controls ONU ID uniqueness across all channels, PtP WDM and TWDM.
5. To not limit a potential future extension, the protocol has code space for 16 wavelengths even though the physical layer specifies up to 8;

NG-PON2 has an inter-channel termination protocol. The OLT CTs are distributed so that some procedures require messages to be passed between OLT [42]-[45]:

1. Synchronizing OLT CT Quiet Windows;
2. ONU tuning;
3. ONU activation;
4. Parking orphaned ONUs;
5. ONUs connected to the wrong ODN;
6. Guided hand-off of ONUs between OLT CTs;
7. Rogue ONU Isolation.

NG-PON2 covers different protection scenarios and rogue behaviours of the ONU [42]-[45]:

1. ONU transmitter hops to wrong upstream channel;
2. ONU transmitter starts transmitting at wrong upstream wavelength;
3. OLT CT transmits in the wrong downstream wavelength channel;
4. Interference from co-existing devices, either faulty ones or due to spectral flexibility;
5. Distributed OLT channel terminations can be used for protection, requiring inter-channel termination co-ordination.

*NG-PON2 major advantages*

**FTTH for everything:**

A major advantage of NG-PON2 is its ability to support different types of subscribers and applications by using different wavelengths and different bit rates on those wavelengths. It can assign a single wavelength to a particular customer, such as a business, or to a particular application, such as mobile backhaul.

**Legacy investment savings:**

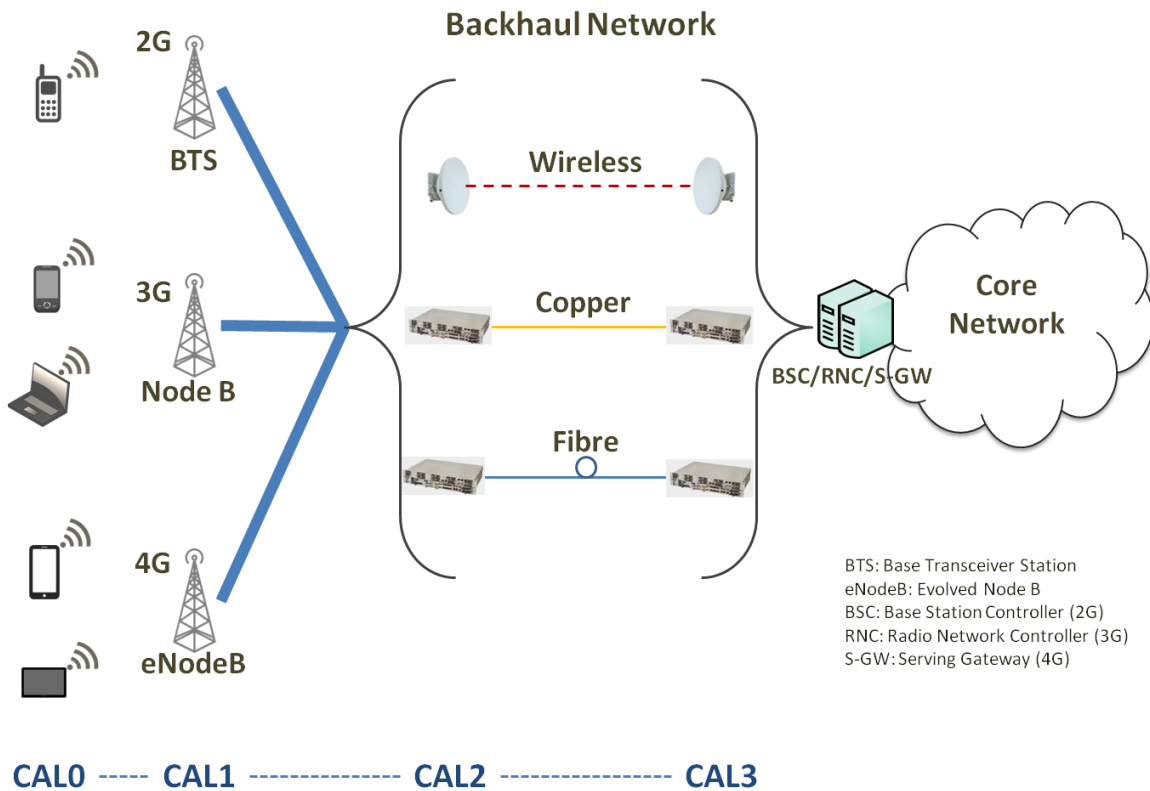
NG-PON2 coexists with legacy PON systems. No changes are required to the ODN, i.e., fibres, splitters and cabinets, as so, GPON network investments are preserved. NG-PON2 can be added over an existing GPON or XG-PON network: an existing GPON network can be upgraded gradually over time (pay as you grow). An operator could deploy NG-PON2 where it has identified new market opportunities, such as enterprise subscribers. It could use NG-PON2 for internal support of fronthaul and backhaul needs. The service provider could also option to upgrade existing high-end residential customers to NG-PON2 where it faces significant competition from other service providers promoting 1G and beyond.

**Pay-as-you-grow:**

Wavelengths can be added one by one as needed to support customer growth and high-bandwidth applications.

### **2.2.10.Backhaul**

Backhaul is the part of the network that comprises the intermediate links between the Core Network or backbone and the small sub-networks at the "edge" of the entire hierarchical network. Backhaul plays a vital role in mobile networks by acting as the link between Radio Access Network (RAN) equipment and the mobile backbone, by transferring voice and data from the access base stations to the core network.



**Figure 21: Backhaul in 2G/3G/4G Networks**

Mobile broadband penetration is growing at a remarkable rate worldwide and as a consequence data traffic in mobile networks is booming. To cope with increased traffic demand, especially in urban areas, mobile networks architecture has to be redesigned, in the effort to solve the imminent capacity crunch. An essential task when designing such high-capacity mobile access networks is the selection of the best backhaul technology solution. There are a wide variety of technologies and solutions available as carriers for backhauling traffic. Mobile Backhaul can be performed via fibre, copper and wireless. Operators might adopt more-than-one technology deploying each where most appropriate. It's critical though for the backhaul network to meet specific cost, coverage and capacity objectives, without compromising service quality.

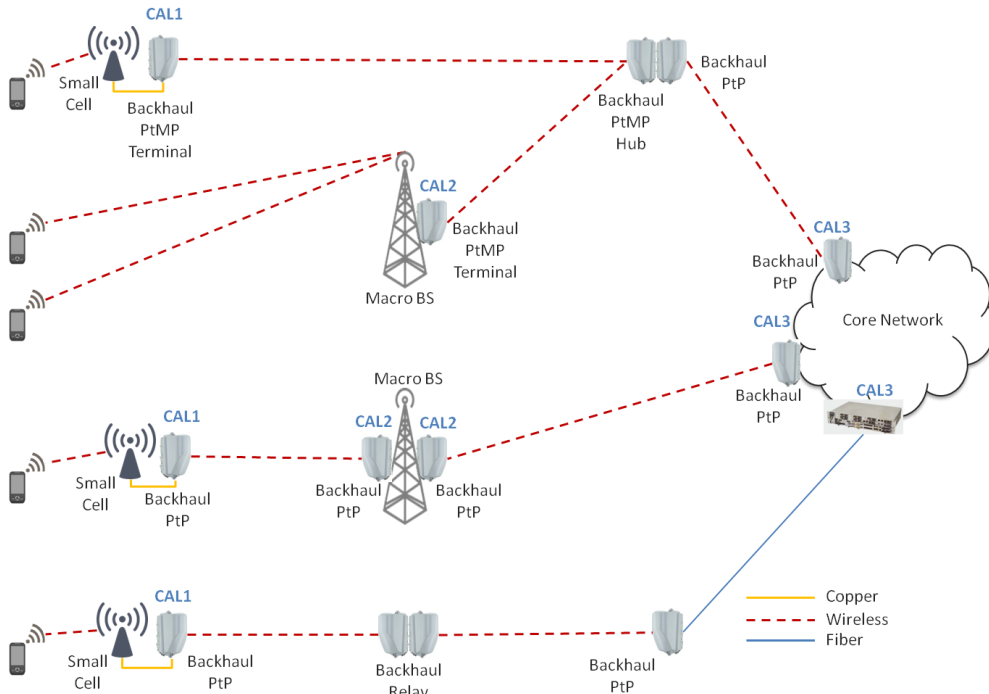
In CHARISMA, both a wireless link and an OFDM-PON will be used for the backhaul section of the network, as described below.

**Wireless backhaul**

Wireless technologies, traditionally with systems operating at microwave frequencies and recently with systems at millimetre-wave frequencies (V-band/E-band), provide operators the best options when it comes to implementing combined macro-cell and small-cell backhaul [46]. With respect to wireline solutions, wireless-based backhaul can reach any area, while offering:

- High Capacity – Up to multiple Gbit/s per link;
- High Reliability – Up to 99.999% link availability;
- Lower CapEx;

- Faster deployment;
- Higher flexibility, using the right topology mix tailored to network needs.



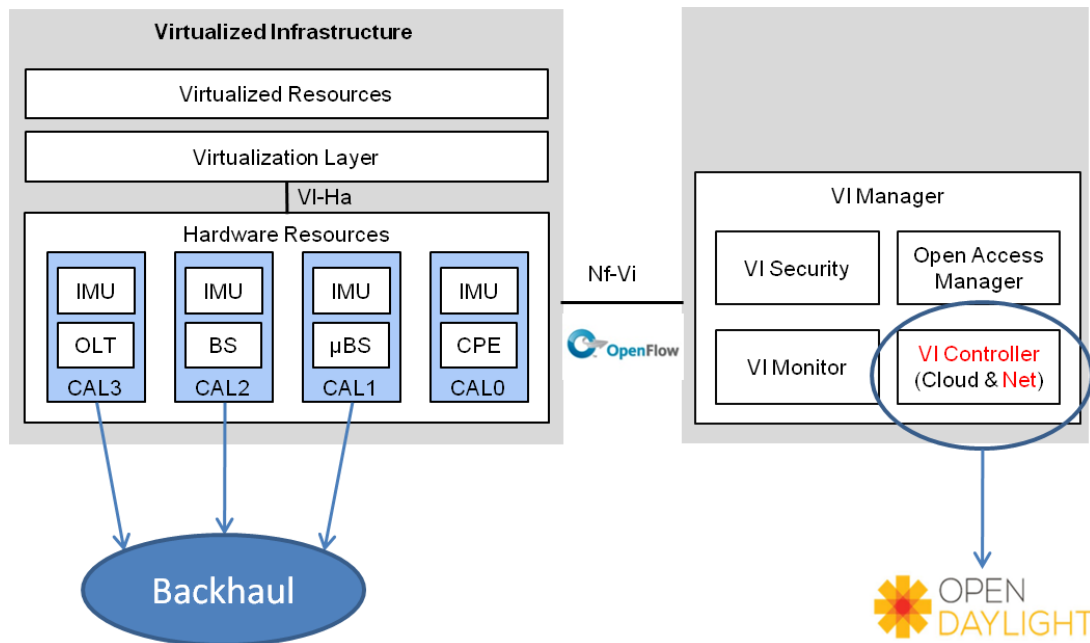
**Figure 22: Wireless Backhaul Network with PtP and PtMP Configurations and CALs**

LTE/4G Radio Access Networks (RANs) currently evolve to Heterogeneous Networks (HetNets) by seamlessly integrating macro and small cells of various technologies. Selecting and utilizing the perfect mix of backhaul solutions is a major challenge when deploying a new RAN. Packet microwave or mm-wave technologies are essential elements of HetNets, offering excessive IP capacity for backhaul. In Figure 22 we can see the two different backhaul topologies. PtP systems can also be used as relays (repeaters) in a multihop backhaul network. PtMP systems have a Central Station (Hub) that connects to a number of Terminals. Each backhaul equipment is connected to an access Base Station, as shown in Figure 22, be that a small cell, a micro-BS or a macro-BS.

Although the backhaul network could be logically abstracted as a straight pipe between the access and the core network, in reality it constitutes an aggregation domain which can have a complex hierarchical structure, considering that a high number of access base stations must be aggregated at a certain point of the core network. Various topologies can be used in a backhaul deployment depending on each specific network needs, e.g. point-to-point line, tree structure, mesh, ring and combinations of these. Reliability can be achieved by using redundancy in equipment and appropriate topologies, e.g. a ring.

With respect to the CHARISMA architecture as defined in subchapter 2.1, the wireless backhaul equipment can be positioned at any of the aggregation points CAL1, CAL2 and CAL3, according to network topology/dimensioning.

CHARISMA will investigate the introduction of functionality at the backhaul that could support the CHARISMA architectural vision for unified software defined operation and distributed intelligence across all parts of the network.



**Figure 23: Proposed architecture for SDN support at the backhaul**

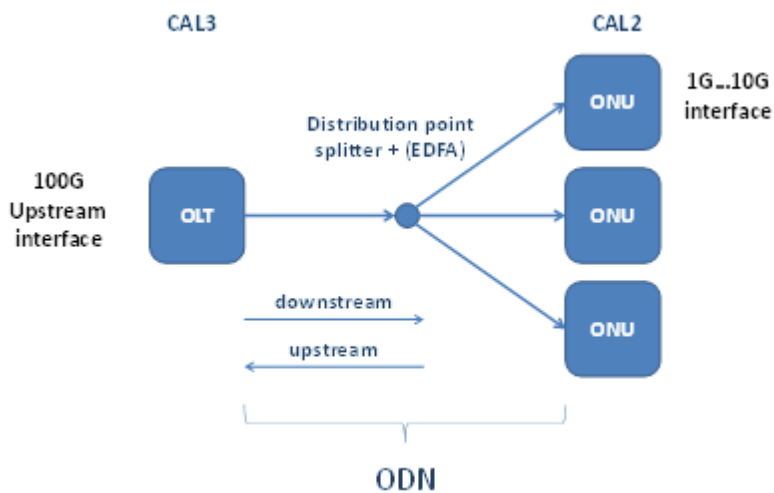
To implement this, the architecture of Figure 23 is proposed, based on the “high-level CHARISMA control and management plane” presented in Figure 4-2 of deliverable D3.1. This consists of an SDN Controller (OpenDaylight) and the switching part of the backhaul communicating via OpenFlow protocol. The switch must be OpenFlow-enabled and it can either be a software-based (virtual switch) or a hardware one. The SDN controller is the network operating system, which contains all the control logic, leaving only the forwarding logic in the switch. The controller exchanges messages with the OpenFlow-enabled switch and programs it as appropriate. As a part of the CHARISMA project, SDN-based control of the switching functionality of a Point-to-Point wireless backhaul system will be evaluated.

**OFDM-PON backhaul**

The OFDM-PON technology is a main part of the physical layer research in CHARISMA. This section describes the architectural considerations of the data and control path for the OFDM-PON. The physical layer properties of the OFDM-PON will be described in WP2 deliverables.

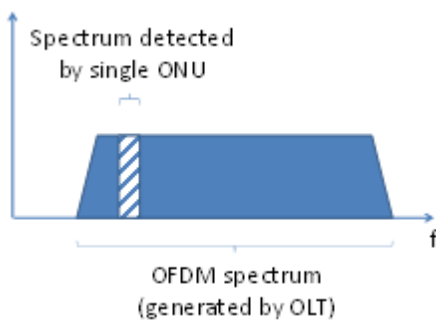
The general architecture of the OFDM-PON follows the classical PON (Figure 24), with an aggregation node at the central office (optical line terminal) OLT, an optical distribution network (ODN) including a splitting point, and several optical network units (ONU). The splitting point of an OFDM-PON might include an EDFA in order to increase the splitting ratio and/or the reach of the network. With respect to the CHARISMA architecture as defined in subchapter 4.1, the OLT would be at aggregation level 3 (CAL3), while the ONUs are at aggregation level 2. The upstream interface of the OFDM-PON OLT should carry at least 100 Gb/s,

aggregated from all ONUs connected. The ONU itself can be equipped with an interface running in the range 1...10 Gb/s, depending on the actual requirements.



**Figure 24: OFDM-PON architecture**

CHARISMA will investigate a sophisticated design, where the ONU only receives parts of the OFDM spectrum in order to reduce the costs of the digital interface. Since only parts of the spectrum are processed by the ONU, the latency can also be reduced, in contrast to other concepts where the full spectrum needs to be received and processed. Compared to TDM-PON the OFDM-PON additionally enables a 2<sup>nd</sup> dimension for the allocation of bitrate resources, which can potentially reduce the latency further.



**Figure 25: OFDM spectrum**

In a 5G network the OFDM-PON will act as distributed switch, which can allocate the resources according to the network management to different nodes. The OFDM-PON architecture allows in principle to assign bandwidth resources with a very low granularity, high flexibility and low latency.

The OFDM-PON follows a layered architecture as shown in Figure 26. It depicts the flow of data and control information.

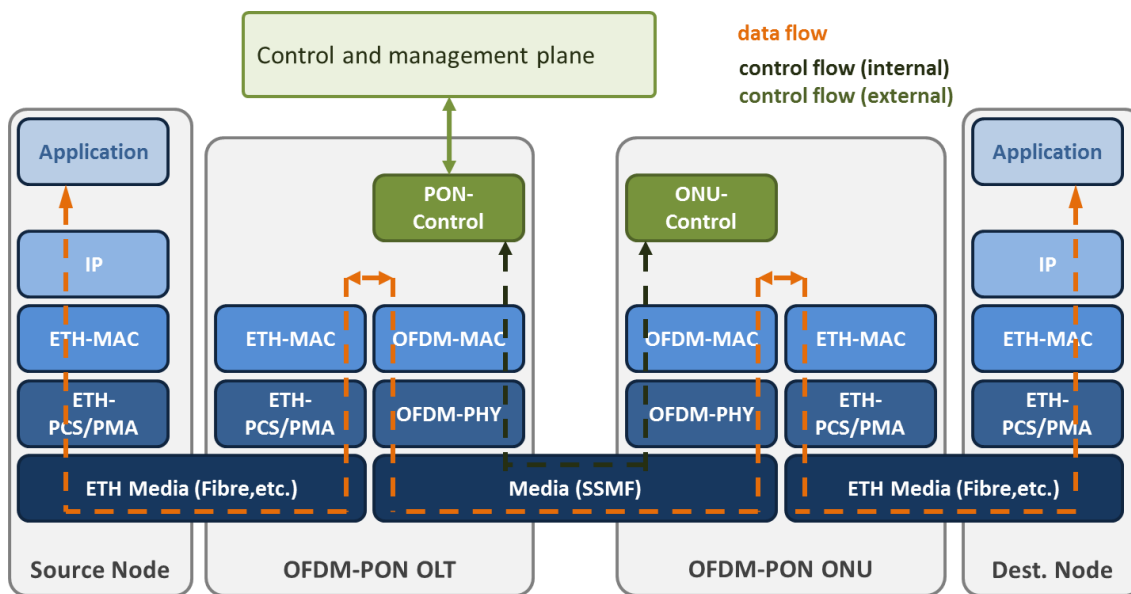


Figure 26: OFDM-PON layered architecture

*Data flow*

The flow of data for an application is shown from a source node via the OFDM-PON to a destination node. The source and destination node as well as the PON input and output layer follow the standard Ethernet/IP architecture. The main functions of OFDM-MAC and OFDM-PHY are given below. A detailed description of the OFDM-PON will be given in deliverable D2.1.

The OFDM-MAC layer (Tx) has the following main functions:

- Distribute the incoming Ethernet frames to the respective ONU.
- Add/remove PON control information to be passed to the respective ONU.
- FEC encoder
- Pass data and control information to the OFDM-PHY

The OFDM-PHY layer (Tx) has the following main functions:

- Generate the OFDM signal from incoming data and control information
- Add information to the data stream to estimate the physical channel and to perform a synchronisation at the ONU

The OFDM-PHY layer (Rx) has the following main functions:

- Synchronize the data stream reaching the ONU
- Demodulate OFDM signal
- Perform a channel estimation and correction
- Pass received information to the OFDM-MAC

The OFDM-MAC layer (Rx) has the following main functions:

- FEC decoder

- Remove control information
- Pass data to Ethernet MAC interface

The *control flow* can be separated in two parts.

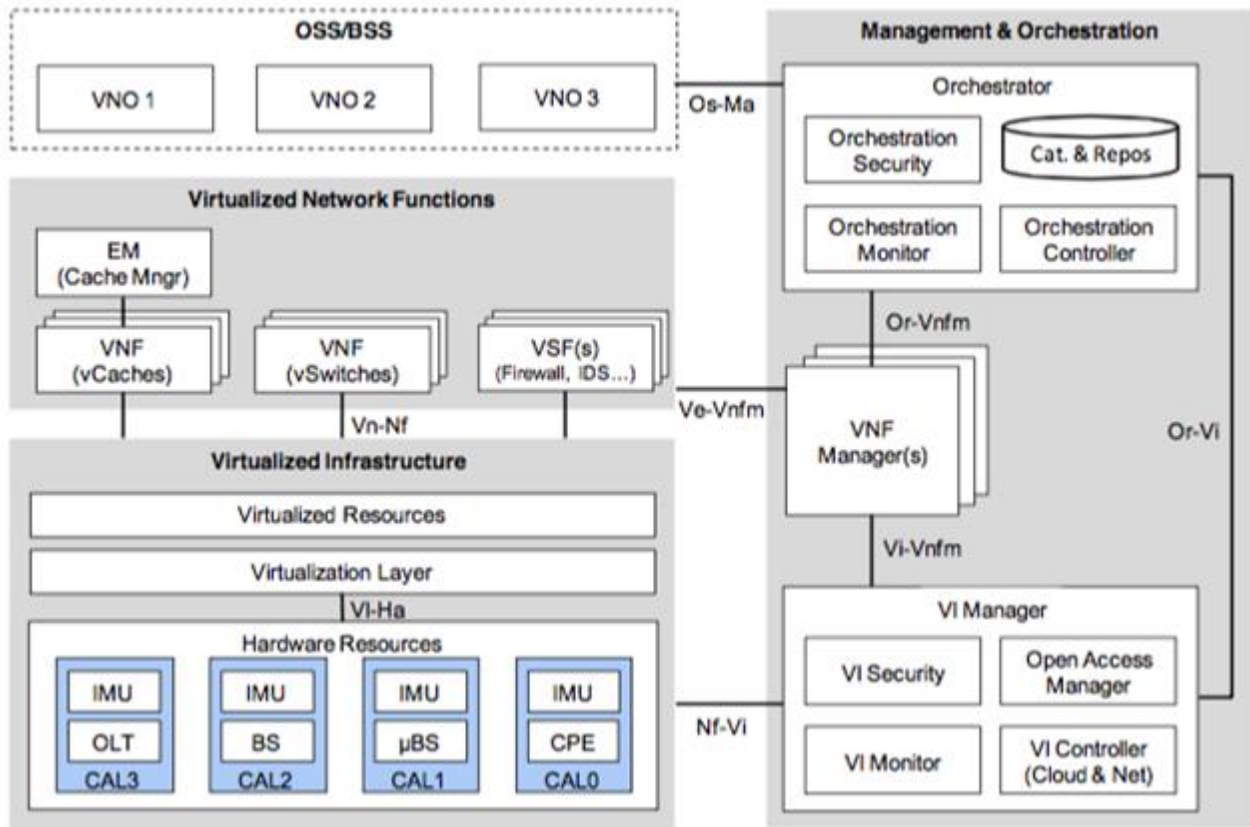
The external control flow exchanges information between the control and management plane and the PON control using an external interface Figure 26. It sets OFDM-PON parameter according to the control and management plane. This refers to SLA parameters like bitrate or spectral assignment for a certain ONU.

The internal control flow passes information between the control entities located at the OLT and ONU. It will be transported in-band over the OFDM-PON physical layer. The main function is to adapt to changing external parameters and to changes of the physical channel.

### 2.3. Control and Management Plane

In order to provision and establish end-to-end services over the CHARISMA infrastructure, an architecture for the control, management and orchestration of the available resources has been proposed. The architecture is based on advanced virtualization techniques and software-defined network programmability. Virtualization of resources -namely, network, compute and storage- and emerging software programming technologies such as Network Functions Virtualization (NFV) and Software-defined Networking (SDN) are a mean to maximize efficient utilization of network resources, achieve quicker operational functional changes, and manage the network over a quicker service provisioning time cycle. NFV enables the deployment of services that are traditionally offered via specialized hardware devices as software functions running in commodity servers. SDN, through the separation of control and data planes, migrates the traffic handling decisions from the network elements themselves to centralised software controllers (SDN controllers). SDN controllers can be programmed appropriately to offer efficient control and management of the network resources. The SDN logic constitutes the Network part of the “VI Controller”.

The proposed architectural framework provides control, management and services orchestration on top of the access network. The high-level design of the CHARISMA control and management plane is shown in Figure 27. The architecture consists of three groups of components: Virtualized Infrastructure (VI), Virtualized Network Functions (VNFs) and Management and Orchestration (MANO). It is aligned with the framework and reference points proposed by the ETSI NFV MANO WG for the management and orchestration of the VNFs.



**Figure 27: The high-level CHARISMA control and management plane**

The Virtualized Infrastructure (VI) group virtualizes the hardware resources (computing, storage, and network) via e.g., a hypervisor at the Virtualization Layer, which pools the resources and exposes them for consumption by VNFs. The hardware resources constitute the CHARISMA access network, with the notable addition of an Intelligent Management Unit (IMU) at each CAL. As explained in Section 2.1, the access network includes 4 levels of aggregation (CALs), from the Customer Premises Equipment (CPE) at CAL0 (degenerating as necessary to User Equipment (UE)) to the Optical Line Termination (OLT) at CAL3. Intermediate CALs host the (micro-, macro-, etc.) Base Stations (BS). The IMU models computing and storage resources that are either spare within access network equipment, e.g., BSs, or introduced with commercial off-the-shelf (COTS) servers.

The Virtualized Network Functions (VNFs) group comprises software components that implement network functions destined to run on the VI (and finally on the IMUs). CHARISMA will work specifically on implementing VNFs for caching, switching, and security. However, any other network function, e.g., CDN, would be able to run on the VI.

The Management and Orchestration (MANO) group includes components for the combination of VNFs into graphs implementing network services, the lifecycle management of VNFs, the coordination of allocating VNFs to virtualized resources, the homogenized control and management of the hardware resources, and the slicing of resources for supporting multi-tenancy. MANO operates under the policy set by the owner of

the hardware infrastructure and communicates with the OSS/BSS of VNO to report status and possibly to receive requirements.

A more detailed description of the CHARISMA CMO plane can be found in the earlier CHARISMA deliverable D3.1.

## 2.4. Summary

In this chapter 2 of the deliverable D1.1 “CHARISMA intelligent, distributed low-latency security C-RAN/RRH architecture” we have defined the multi-layered approach to the CHARISMA architecture design, focusing particularly on the data plane, as well as briefly the control & management plane. We have started with a high-level architectural description of the CHARISMA aggregation levels (CALs), which enable a distributed approach to the CHARISMA architecture design. Each CAL within the CHARISMA network hierarchy possesses an intelligent management unit (IMU) to allow local processing, caching and routing of data. The various network elements comprising the CHARISMA data plane have all been described, in particular concentrating on their innovative aspects and how they contribute towards helping enable the CHARISMA architecture to achieve its objectives of low-latency, open access, and security. The service plane (SP) aspect to the overall CHARISMA architecture description is now considered in the following chapter 3.

## 3. Workflows & Service Life Cycle Design

In this chapter 3 of D1.1 we consider the service plane (SP) aspect of the CHARISMA architecture. This is particularly in the context of 5G networking anticipated to require much more dynamic provisioning and reconfiguration as a means to support automation of the whole service delivery and operations process. Again, these characteristics are also a feature of the 5G use cases (described in chapter 4) that the CHARISMA architecture has been designed to enable. Within this chapter, we also identify the most important actors expected to feature in the CHARISMA architecture, particularly in the context of virtualisation of physical infrastructure, network operation, resources and network functions.

### 3.1. Service Lifecycle Modelling

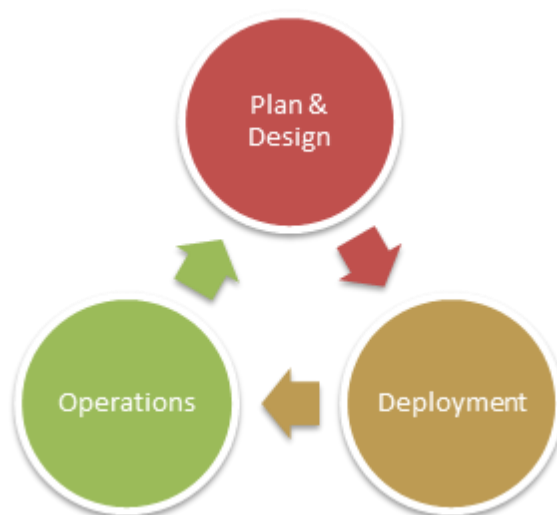
The existing services development and lifecycle management frameworks are usually oriented on traditional human-driven services development and composition. However, the network and application services envisioned in 5G, particularly for the UCs as described in the previous chapter, are highly dynamic in nature requiring automation in terms of provisioning, configurability and management. The service oriented architecture based technologies provide a good basis for creating services for dynamically provisioned and re-configurable services. The typical service lifecycle includes five stages, namely, Service Request, Service Design & Development, Service Deployment, Service Operation, and Service Termination.

A definition of different lifecycle stages allows one to use a different level of the service presentation and description at different stages and to address different aspects and characteristics of the provisioned services. However, to ensure integrity of the service lifecycle management, the consistent service context management mechanisms should be defined and used during the whole service lifecycle, including corresponding security mechanisms to protect the integrity of the services context. The problem arises due to the fact that such mechanisms are generically state dependent, which is on the contrary to a Service Oriented Architecture (SOA) environment generically defined as stateless. To address the dynamic, reconfigurable and scalability features of a service together with the automation of the provisioning of services, the TeleManagement Forum (TMF) proposed the Service Delivery Framework (SDF). The main motivation behind implementing SDF in CHARISMA is to achieve the automation of the whole service delivery and operation process, in particular:

- End-to-end service management in a multi-service-provider's environment;
- End-to-end service management in a combined, shared and optimum utilised network service environment;
- Management functions to support a highly distributed service environment. For example, unified or federated security, user profile management, allocation of services in historically different platforms such as fixed-wireless converged networks, etc.;
- Any other scenario that pertains to a given phase of the service lifecycle challenges, such as on-boarding, provisioning, or service creation.

SDF services lifecycle corresponds to the general services lifecycle management model that includes the abovementioned service lifecycle stages.

The CHARISMA service lifecycle considers dynamic provisioning, auto-management and auto-configurability as essential features. From CHARISMA perspective, the service lifecycle can be classified into three main stages, i) Service Plan and Design, ii) Service Deployment, and iii) Service Operation. These three phases feed each other in a cyclic manner as depicted in Figure 28.



**Figure 28: CHARISMA Service Lifecycle Model**

In the CHARISMA ecosystem, the Virtual Network Operator (VNO) is a customer of a Network Operator (NO). It is worth mentioning that a VNO could possibly be an Application Provider. Furthermore, for simplicity, it is assumed that the NO runs the CHARISMA solution on top of the infrastructure it owns although CHARISMA Operator can possibly be a separate role as well. Using CHARISMA, the VNO can design the required service, which includes the design of a virtual network, edge service, SLAs and configuration of desired applications. The application is designed to run as an end-to-end service, with in the virtual network that can be offered to customers of VNO, i.e., End Users. After the design phase, the virtual network is deployed via CHARISMA, i.e., virtual network and IT resources are committed by the NO according to the design and SLA. CHARISMA enables the VNO to control and manage its virtual network and edge resources by exposing appropriate interfaces to facilitate the service operations. It also provides the flexibility to the VNO to use its own Business Support System (BSS)/Operation Support System (OSS). This flexibility allows the VNO to continuously improve the service based on the information collected during the service operations phase thanks to the service monitoring function that CHARISMA offers to VNOs.

The CHARISMA service lifecycle model is aligned with the Information Technology Infrastructure Library (ITIL) v3 standard. The three stages of CHARISMA service lifecycle can be mapped to the five stages described by ITIL v3 as shown in below.

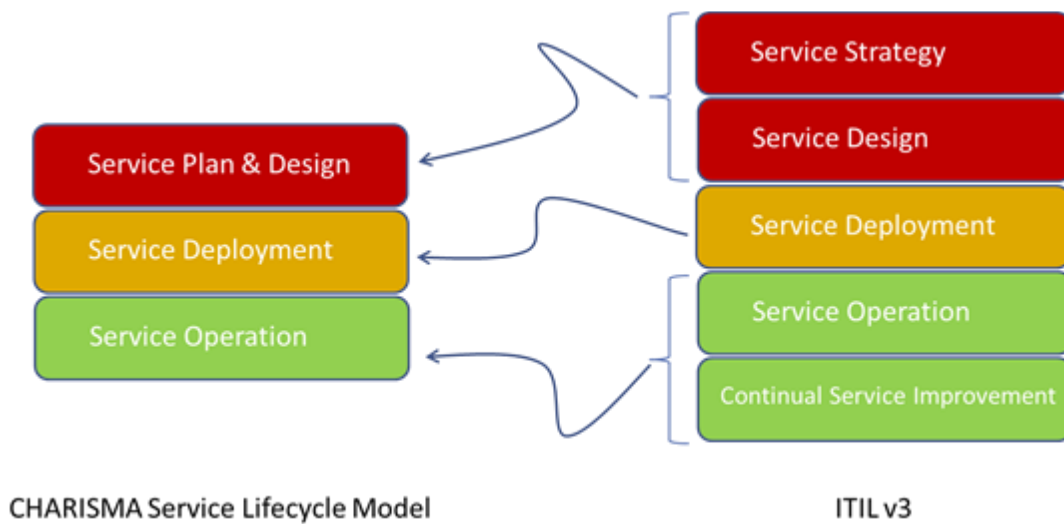


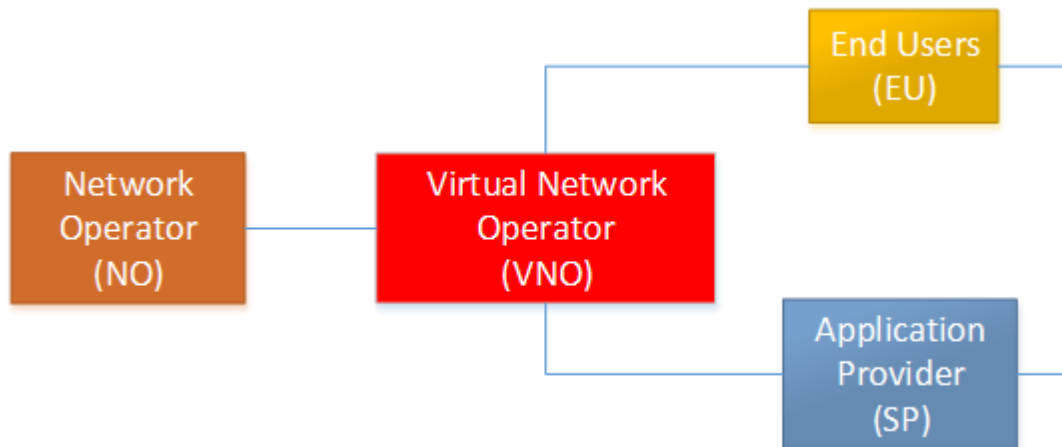
Figure 29: CHARISMA Service Lifecycle Model mapping to ITILv3

### 3.2. Actors and Stakeholders

Aligned with the CHARISMA architecture and use cases, the following actors have been identified:

- **End Users (EU):** users of the CHARISMA services, they can be either simple end users or an entity (e.g. automotive company, factory, hospital, bus company etc.)
- **Network Operator (NO):** this actor owns the physical infrastructure and equipment. The equipment is mapped into a pool of available resources that are leased to the virtual network operator in the form of virtual infrastructures.
- **Virtual Network Operator (VNO):** This actor operates a virtual infrastructure providing network services to end users. In order to achieve this, it leases resources from the Network Operator.
- **Application Provider (AP):** An entity that produces and gives to end users specialized services (e.g. platform for remote surgery, software for collision avoidance)

Among the above-identified actors there are several interactions that are illustrated in the following.



**Figure 30: Interactions between 5G networking actors**

This figure represents the simplest scenario where only one instance of each actor is represented.

### 3.3. Roles interaction

The role played by the stakeholders in the general CHARISMA architecture has been described in the previous section **Error! Reference source not found.**. The relationships between them are structured in a chain-like manner, where the different services provided by each role are consumed by the next role in the chain, all the way down from the VNO to the End User. This approach simplifies the design of an architecture that is capable to provide virtualised network resources by slicing them in layers. In this section CHARISMA is explored from the point of view of the stakeholders that will have a predefined precise role and the interactions between them. A description about their relationships and the functionalities that each one of them will accomplish in their role is given in the following subsections.

The different roles interact with the CHARISMA architecture and its elements. Starting from the Network Operator (NO), who owns the physical infrastructure and is able to create Virtual Infrastructures (VI) using an SDN based platform to provide the means of virtualisation of the physical resources. The NO creates virtual slices composed of virtualised resources offering them to the Virtual Network Operator (VNO). The VNO uses the Open Access Manager in order to operate the provisioned VIs and offer network services on top of it to their End Users. Then the Application Provider (AP) can offer their applications to be deployed over the CHARISMA VI operated by the VNO. Service Level Agreements need to be established between the different stakeholders for the negotiation, provisioning and operation of the offered services.

Following the described model, the different interactions between the involved roles take place when a given stakeholder consumes one or more services that are being offered by any other stakeholder. The most prominent and relevant service that has clearly been identified as required for CHARISMA is the network slicing service, although there will be potentially new features and services supported by CHARISMA that will be reported in the refined CHARISMA architecture deliverable (D1.2).

### 3.4. Service Workflows of CHARISMA

In this section the different workflows of the stakeholder’s interactions are explained.

#### 3.4.1.NO and VNO interaction

NO and VNO interaction is depicted in the following. In this case we assume that the NO is the CHARISMA Network Operator, meaning that this is the entity that owns and operates the CHARISMA infrastructure.

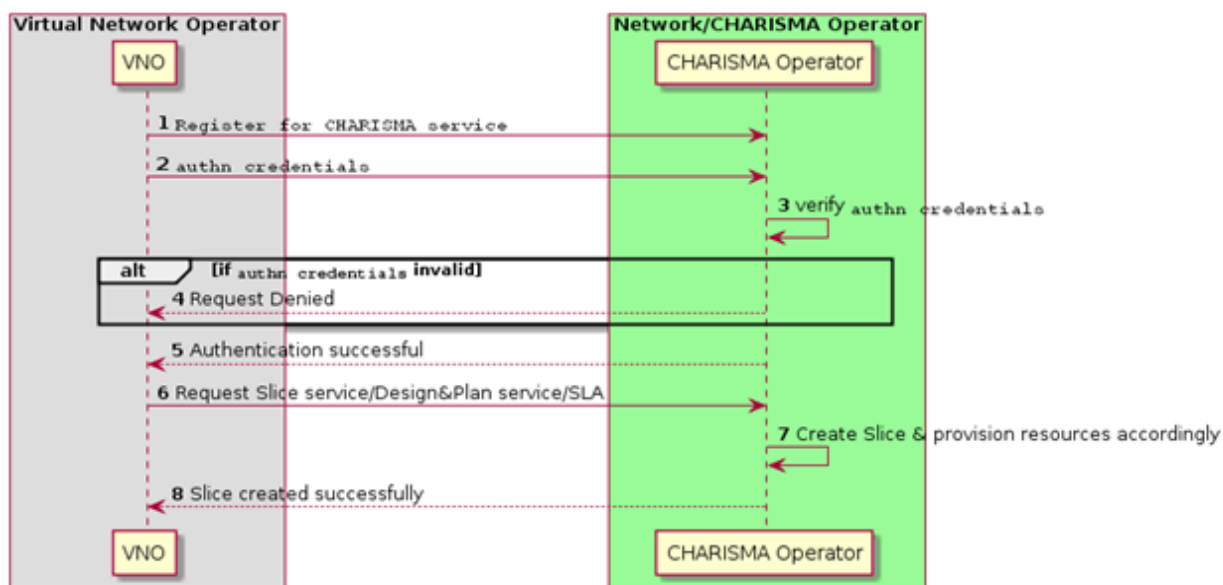


Figure 31: NO and VNO interaction workflow

The initial step would be the registration of the VNO in the CHARISMA system requesting for a new service slice for an End User. The second stage is the verification of the VNO credentials in CHARISMA. In case the credentials are not valid and the VNO is not eligible to apply for a service slice, the system will return a “request denial” message. If the VNO is authenticated successfully, then he can request the service slice and the CHARISMA system will start the process of allocating resources according to the requested service type and features. After this, the service slice is created successfully and the VNO can operate its part in the VI of CHARISMA. The service slice will have an additional feature to be able to monitor the service and its performance based on QoS implementations.

Additional features like enhanced security, content caching as well as processing and storage in different parts of the network, will also be offered by CHARISMA and could be requested by the VNO.

#### 3.4.2.VNO and AP interaction

VNO and AP interaction is depicted in the following.

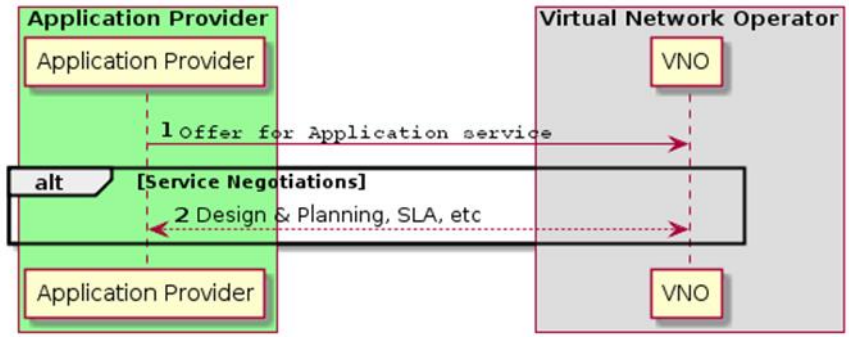


Figure 32: AP and VNO interaction workflow

The relationship between the AP and the VNO is out of scope of CHARISMA, although it will be using potentially some of the storage, processing and network features that have been mentioned in the previous section.

Their interactions are fairly simple, the AP offers an application that the VNO wants to implement and they will contract the service/product through a service provisioning agreement. Then, if required, they will sign a contract of services provisioning that can cover design, support times, SLAs, etc.

3.4.3.VNO and EU interaction

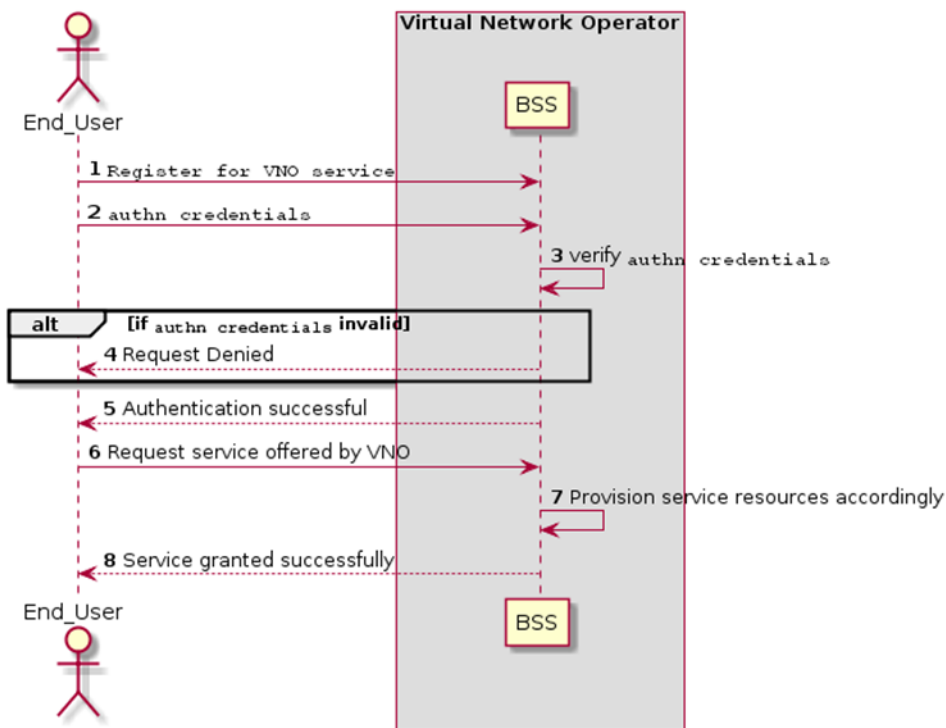


Figure 33: VNO and EU interaction workflow

The above represents the workflow of the interaction between a VNO and its customers or End-Users. The BSS/OSS systems of the VNO that deal with user’s authentication and billing are out of the scope of CHARISMA. The initial stage for this workflow is the registration of the user, in case he/she does it successfully,

he/she will be able to apply for a new service, typically a triple-play, quadruple-play will be offered for them. Then, finally, the VNO will provision the service according to the request and needs of the user.

### 3.5. Summary

In this chapter 3 we have described service plane aspects to the CHARISMA architecture, focusing in particular on the workflows & service life cycle design. In the 5G context, these need to be much more dynamic in their provisioning and reconfiguration, particular so that automation of the service delivery and the operation process is enabled. Such SP functionality as well as the virtualisation of physical infrastructure, network operation, resources and network functions, are all required for the anticipated 5G use case scenarios (as identified in the next chapter 4). In addition, as a precursor to describing the use case scenarios particularly relevant to the CHARISMA architecture, in this chapter 3 we have also identified the most important actors expected to feature in the CHARISMA network, namely: the End Users (EUs), Network Operator (NO), Virtual Network Operator (VNO), and Application Provider (AP). We have also described how the various actors interact with each other and their associated service workflows. Having described these various SP and actor aspects, we are now in a position in the next chapter 4 to expound on the specific CHARISMA use case scenarios that we have identified will most exploit the technical capabilities of the technologies as described in chapters 2 and 3.

## 4. Use Case Scenarios

### 4.1. Introduction

This chapter presents the set of 5G use cases that have been considered by the CHARISMA project as a result of the definition of the CHARISMA architecture. The purpose of these use cases is twofold:

- First, to highlight how the key innovations of the CHARISMA solution will benefit the various stakeholders (e.g., end-users, network/service providers) involved.
- Second, to be used to define the widest possible range of performance and functional requirements that the CHARISMA architecture should meet.

For the identification of the use case scenarios in CHARISMA, the following guidelines are followed:

- The use cases must be a sub-set of the potential 5G use cases that have been presented in different forums and white papers.
- The use cases must accentuate all or a sub-set of the specific goals and objectives of the CHARISMA project, which include low latency, enhanced distributed security and open access.

Taking into account the representative example use cases for 5G currently available in the literature (e.g. those developed by NGMN [55] and 3GPP [56]), as well as in the context of other 5G projects, such as 5G NORMA [57], CHARISMA considers the following use cases, as the most relevant with the scope of the Project:

1. Automotive – Trains
2. Automotive – Platooning, Vehicle Collision Avoidance
3. Automotive – Buses
4. Big Event
5. Emergency - Fire Fighters
6. Factory of the Future (IoT)
7. Video Streaming
8. Remote Surgery
9. Smart Grid

It is important to point out that the above use cases represent quite satisfactorily the large set of use cases identified for 5G. Due to the large number of these 5G use cases, Standards Developing Organizations (SDOs), like ITU and 3GPP, have attempted to group these use cases into a number of general categories that share common characteristics from a technical point of view. These general categories of use cases (taken from [58]) include the following ones:

- Massive machine type communications incorporating a large number of devices per km<sup>2</sup>

- High throughput massive broadband communications
- Ultra-reliable and low latency critical machine type communications

Each of these categories is associated with a certain dominant technical feature (e.g., number of devices connected or maximum latency), which is considered as the most crucial for each category. It is thus important that the use cases defined in CHARISMA cover the whole range of these technical features. In Figure 34 a graphical representation (taken from [57] and [58]) of the use cases is provided, taking into account the number of devices that need to be served on a per eNB basis (device density / eNB), the throughput required by the application itself and the latency/reliability needs.

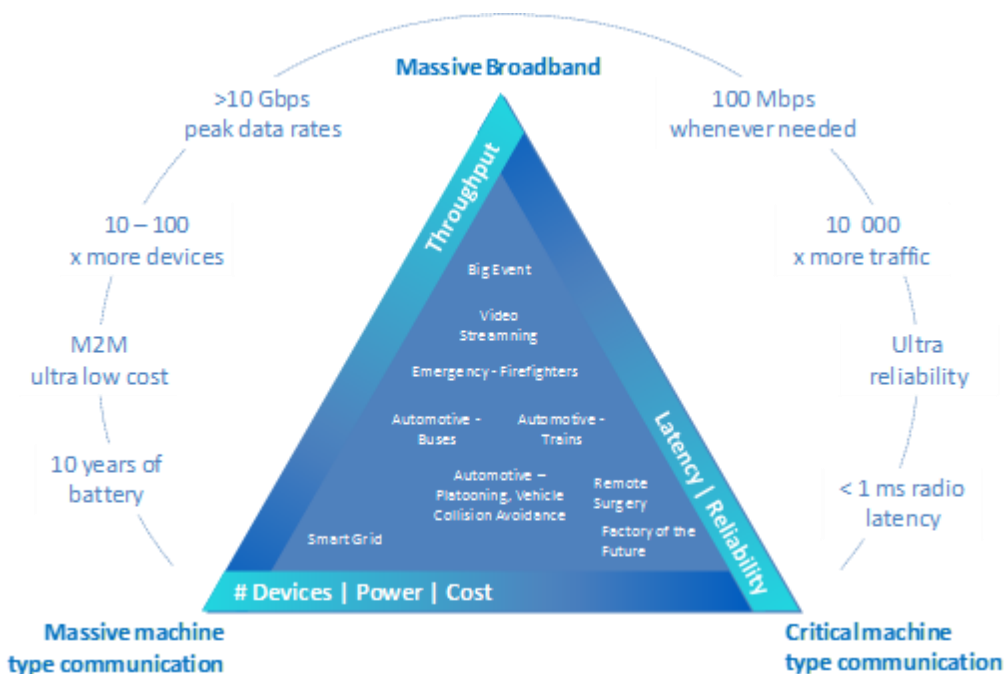


Figure 34: CHARISMA use cases within the 5G ecosystem

## 4.2. Use Case Comparative Tables

### 4.2.1. Automotive - Trains

#### Rationale of the UC, Goal and Objective

The objective of this use case is to ensure that 5G networks can support train-to-shore connectivity. High-speed railway (HSR) has brought much convenience for peoples’ travelling. To ensure safe and reliable operation of HSR, the train operation control system must maintain a reliable bidirectional communication link between the train and the ground. Dedicated mobile communication systems such as GSM for railway (GSM-R) and LTE for railway (LTE-R) play key roles. Rapid growth of future railway services and applications such as real-time ultra-high-definition (UHD) video surveillance has already gone beyond 1 Gbps data transmission rate with 100 MHz bandwidth, at least. Higher frequency bands such as mm-wave technique

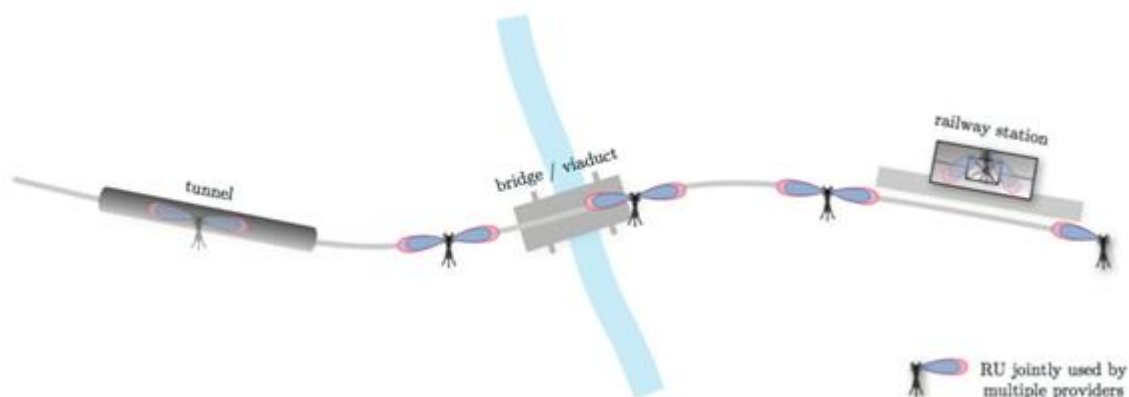
(i.e. 60GHz and beyond), the fifth generation (5G) technique and corresponding mobile communication network should be designed accordingly to provide high capacity and high data transmission rate for newly developed railway services and applications.

**Description**

Wireless communication in HSR scenarios exhibits several key differences to the traditional considerations of a coverage-oriented network. Many effects have not been fully understood and it is not clear which are the most significant in HSR scenarios.

High-speed trains could easily exceed 350km/h. This leads to a high Doppler shift, which causes several transceiver impairments such as channel estimation errors and Inter Carrier Interference (ICI) in Orthogonal Frequency Division Multiplexing (OFDM) systems.

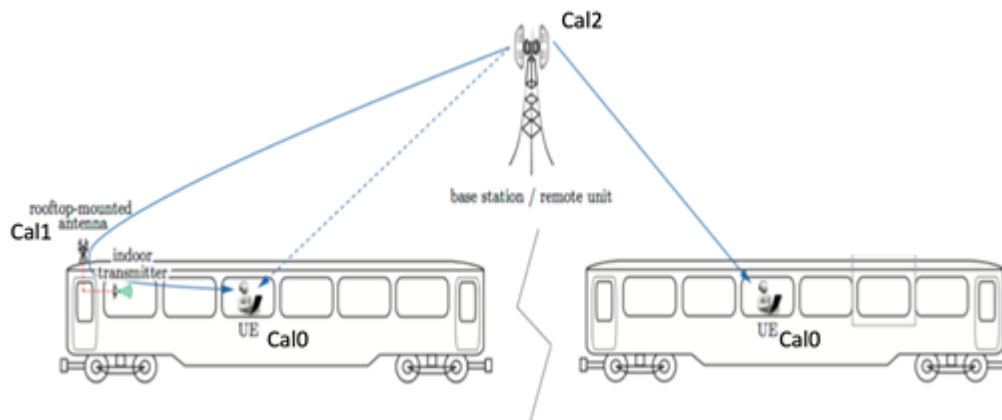
Also, the channel characteristics along the tracks vary greatly. It is considered as a noisy and challenging environment such as the 25kVA overhead line equipment (OLE), tunnels, trenches, cut-tings, stations, viaduct-like structures or bridges as shown below.



**Figure 35: Different channel characteristics for trains 5G networking**

As deployment gets increasingly dense, the huge redundant control signalling interaction caused by frequent handovers between small and macro cells reduces the efficiency of heterogeneous networks.

There are two possible connectivity cases. The first, when the user equipment (UE) directly associates with the base station along the tracks. In the second case, the link is established via a relay, as shown in below.



**Figure 36: Hierarchical CHARISMA architecture for trains**

In the relay scenario, several antennas are mounted on the outside of the train. These are connected to one or more relays, which are then distributing the signal inside the train. This approach has the major advantage that the signal is not attenuated by the windows of the carriage. This setup also allows us to configure the relay such that it appears as a single UE to the BS, thus significantly reducing the number of handovers.

The virtualization and security management provided by SDN and NFV control of CHARISMA 5G network will significantly improve network usage efficiency of public transport network and reduce service latency for train passengers. Disadvantages in network coverage will be resolved by deploying additional mobile base stations in this use case scenario as well.

### Constraints, Restrictions and Challenges

- Large penetration loss via the shield of the train. This penetration loss is expected to be 20 to 30 dB.
- Large numbers of handovers in very short time. This is due to hundreds or thousands of users needing handover from one site to another concurrently/sequentially. This phenomenon affects system stability and eats up capacity.
- High power consumption of user equipment (UE). This is because the UEs on the train need higher power to overcome the large penetration loss in uplink as well.
- Cell edge intelligence approach (due to high speed)
- Increased packet delay due to the occurrence of handovers cause service interruptions
- Communication system in high-speed railway scenario has a linear topology (implementation cost is considerably higher. Not favourable by service providers)
- Tunnel connectivity issue. (I.e. 200m tunnel, 300m train). Either leaky feeder in the tunnel or relay antennas at each end of the train are potential technical solutions.

### Relevance with CHARISMA

- Security and reliability aspect
- Low latency

- Open access

Relay scenario is preferred. This is due to the fact that the RRH will treat the rooftop antenna (CAL1) as a single user equipment

- UE (CAL0) connects to the rooftop antenna (CAL1) via an indoor transmitter
- Rooftop antenna (CAL1) connects to RRH (CAL2)

**Requirements**

The functional and performance requirements associated with this use case are the following:

**Table 4: 5G connectivity requirement for UC1**

Requirement Name	High number devices. High priority communication.
Type	Functional
Description	Each carriage should be able to connect a high number of devices to either the base station (CAL2) or preferably to the rooftop antenna (CAL1). Priority should be taken into account. For example, emergency is highest, passenger entertainment is lowest.
KPIs	5G network availability
Category	Mandatory

**Table 5: 5G real-time system requirement for UC1**

Requirement Name	Detailed public transport information
Type	Functional
Description	The 5G network should offer availability in the order of 99.9% to be able to handle real-time passenger information systems
KPIs	99.9% availability
Category	Mandatory

**Table 6: Open access requirement for UC1**

Requirement Name	<b>Open access</b>
Type	Functional
Description	The 5G network must be able to support multiple service providers simultaneously. This is crucial for safety reasons. Caching and switching may be distributed and placed along the network and user devices to be able to serve content as near as possible to user side
KPIs	Multiple operators
Category	Mandatory

**Table 7: 5G advanced security requirement for UC1**

Requirement Name	<b>5G advanced security</b>
Type	Performance
Description	The network should guarantee a high level of security in case of D2D and D2I communication
KPIs	The 5G network should offer advanced security mechanisms.
Category	Mandatory

**Table 8: 5G low latency requirement for UC1**

Requirement Name	<b>Low latency and better QoS</b>
Type	Performance
Description	The network should be able to provide a solution for the high penetration loss introduced by the structure of the train (especially legacy fleets).
KPIs	Low latency and jitter. QoS.
Category	Mandatory

## 4.2.2. Automotive – Platooning, Vehicle Collision Avoidance

### Rationale of the UC, Goal and Objective

The objective of this use case is to ensure that 5G networks can provide the low latency and enhanced security required for the provision of advanced ITS innovative services / applications (e.g. vehicle collision avoidance and platooning), necessitating the exchange of information in real-time under strict delay constraints among the vehicles / central infrastructure.

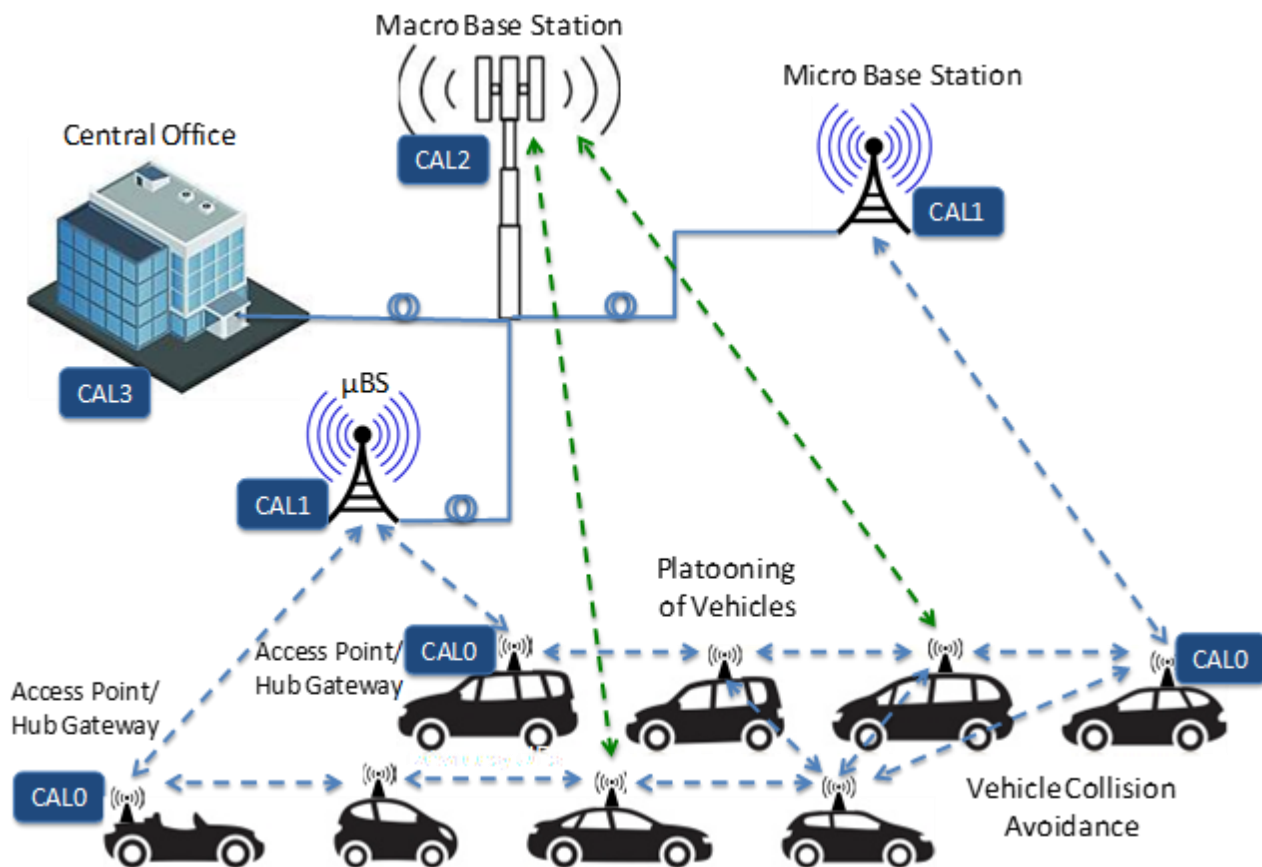
The existing SoA mobile communications technologies (4G/4G+) are not capable of supporting extra low latency (in the order of 1 msec) and security sensitive vehicular communications.

### Description

This use case (see Figure 37) involves two of the CHARISMA actors: the end users, who are the drivers, and the network operator who provides the 5G network connectivity. D2D communication refers to the CAL0 aggregation level of CHARISMA, whereas communication with micro base stations located along the high-traffic roads and serving a limited area refers to the CAL1 aggregation level. CAL2 aggregation level is associated with macro base stations that serve a wide area and finally, the CAL3 aggregation level is associated with the operator's central office.

This UC assumes a high-density platooning situation in which vehicles drive very close to each other, thus making collision avoidance a very critical and extremely useful safety-related service. To prevent collision, the vehicle of interest (VOI) must take into account other vehicles and "obstacles" in the vicinity. These vehicles can move in front or behind, on the same or the opposite lane of the VOI. They can also come from intersections along the path of the VOI. An "obstacle" is considered to be a stopped vehicle, or a vehicle moving at an extremely low speed.

In order to avoid collisions, information such as timestamp, current location (latitude, longitude), speed, bearing, altitude, acceleration / deceleration needs to be exchanged in real time among the vehicles either directly (D2D) or via 5G. In case of an imminent hazardous event, visual and/or audio alerts will be made available to warn the driver of the VOI.



**Figure 37: Intelligent Transport Services / Collision Avoidance, Platooning**

Collision avoidance could be further enhanced by the "See-What-I-See" service, that refers to the provision of automated HD live video streaming to the driver of the VOI from the vehicle in front on the same lane and within a certain distance depending upon the speed. This service will be especially helpful in cases such as:

- stopped vehicle ahead in dead spot
- vehicle ahead moving at an extremely slow speed
- vehicle ahead attempting a blind overtake.

Furthermore, in the case of an accident, the HD video/audio streaming could be automatically pushed to the nearest PSAP (Public Safety Answering Point).

On top of the above services, additional ones could be envisaged including:

- Real time positioning of vehicles moving in the vicinity (same direction, within a certain distance depending on the speed) over e.g. Google maps
- Detailed information on the car’s console/dashboard (e.g. speed, distance, acceleration/ deceleration) regarding the vehicle in front (on the same lane)
- Personalized “time to destination” based on driver profile/behaviour (average speed, average number of line changes, etc.) and current traffic statistics.

**Constraints, Restrictions, Challenges, and Risk Analysis**

- Not all vehicles may be equipped with a special Collision Avoidance Device (CAD) device.
- Even if a vehicle is equipped with a CAD device, the driver may ignore the device advice/information.
- There are certain regulatory issues that need to be clarified. For example, regulators need to address QoS, security, integrity, data protection, and privacy by setting rules that apply to all providers offering equivalent services. Also, mobile operators need regulatory frameworks that promote innovation and reward investment in novel communication networks in order to make sure that operating these networks will be a viable business, especially for the provision of the upcoming 5G and IoT services.
- Specific attention must be paid to security and privacy in the context of automotive connectivity since future ITS services will require a high degree of reliability and integrity, as well as strict personal data protection policies. It is absolutely necessary that advanced security mechanisms need to be applied including robust authentication and encryption techniques.

**Relevance with CHARISMA**

This use case is highly relevant to the CHARISMA project, in particular with regards to:

- Low latency
- Security

In addition, the network reliability and availability provided by the CHARISMA architecture are also associated with this use case.

**Requirements**

The functional and performance requirements associated with this use case are the following:

**Table 9: CAD in all vehicles requirement for UC 2**

Requirement Name	CAD in all vehicles
Type	Functional
Description	All vehicles should be equipped with a special Collision Avoidance Device (CAD) and the related application(s) should be automatically activated during vehicle engine start-up.
KPIs	CAD penetration (percentage of vehicles equipped with a CAD).
Category	Mandatory

**Table 10: CAD 5G connectivity requirement for UC2**

<b>Requirement Name</b>	<b>CAD 5G connectivity</b>
Type	Functional
Description	All CADs should have 5G connectivity including D2D
KPIs	5G network availability CADs should have 5G connectivity including D2D
Category	Mandatory

**Table 11: 5G message priority requirement for UC2**

<b>Requirement Name</b>	<b>5G message priority</b>
Type	Functional
Description	The 5G network should be able to prioritize messages related to collision avoidance.
KPIs	5G network should be able to offer different priority levels.
Category	Mandatory

**Table 12: 5G broadcast functionality requirement for UC2**

<b>Requirement Name</b>	<b>5G broadcast functionality</b>
Type	Functional
Description	The 5G network should support broadcast mechanisms to warn all the vehicles in a certain geographical area in case of a critical event.
KPIs	5G network should be able to offer broadcast functionality.
Category	Mandatory

**Table 13: 5G availability of 99.9% requirement for UC2**

Requirement Name	<b>5G availability of 99.9%</b>
Type	Functional
Description	The 5G network must offer availability in the order of 99.9% [59].
KPIs	All 5G network elements should offer availability in the order of 99.9%.
Category	Mandatory

**Table 14: 5G advanced security requirement for UC2**

Requirement Name	<b>5G advanced security</b>
Type	Functional
Description	The 5G network must provide secure communication links. Personal data regarding the driver should not be made available to 3 <sup>rd</sup> parties.
KPIs	The 5G network should offer advanced security mechanisms.
Category	Mandatory

**Table 15: 5G latency of 10ms or less requirement for UC2**

Requirement Name	<b>5G latency of 10ms or less</b>
Type	Performance
Description	The 5G network should support latency of 10ms or lower [59].
KPIs	Latency of 10ms or lower.
Category	Mandatory

**Table 16: 5G packet loss rate of 10<sup>-5</sup> or less requirement for UC2**

<b>Requirement Name</b>	<b>5G packet loss rate of 10<sup>-5</sup> or less</b>
Type	Performance
Description	The 5G network should provide packet loss rate of 10 <sup>-5</sup> or less [59].
KPIs	Packet loss rate of 10 <sup>-5</sup> or less
Category	Mandatory

**Table 17: 5G high quality video (up to 40Mbps) requirement for UC2**

<b>Requirement Name</b>	<b>5G high quality video (10-40Mbps)</b>
Type	Performance
Description	The 5G network should allow the transmission of high quality video (10-40Mbps) per vehicle [59].
KPIs	High quality video (10-40Mbps)
Category	Mandatory

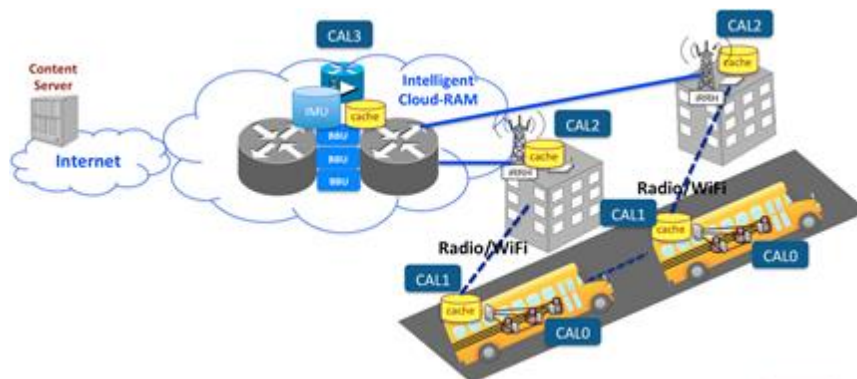
### 4.2.3. Automotive - Buses

#### Rationale of the UC, Goal and Objective

The objective of this use case is to ensure that 5G networks can provide optimized and secured Internet access in the public transport such as bus cases. The open access solutions deployed by CHARISMA will ensure user’s service continuity and low service latency in a secured solution in the mobile scenario of the bus cases.

#### Description

Public transport services like buses or metro are generally operated along a regular route and a published transport timetable. This allows provision of network services such as caching and routing to provide optimized Internet access in the public transport by reducing resources and service latency.



**Figure 38: Scenario of bus use cases**

As shown in Figure 38, the hierarchical CHARISMA Aggregation Levels (CALs) are well matched in different network devices in the bus cases. Through distributing intelligence like caching, switching and routing closer to end-users (even on user devices) assists in reducing network latency. The virtualization and security management provided by SDN and NFV control of CHARISMA 5G network will significantly improve network usage efficiency of public transport network and reduce service latency for bus passengers.

We assume that a group of users are commuting in metro or bus, for instance, and are periodically connected to access points (APs) or BSs, but are sometimes disconnected. Through deploying CHARISMA open access solutions in bus, AP/BS and C-RAN, even providing D2D communications between users by infrastructure provider, service provider is able to ensure user’s service continuity and improve QoS.

- Network controlled offloading between WiFi and mobile networks depending on network status and user profiles.
- D2D communication helping reduce consumed resources for a crowded area in traffic jam;
- Enabling cache functionalities, such that content is intelligently cached or pre-fetched according to a socially aware delivery mechanism or real use of the content;
- Cloud based flexible and dynamic deployment of media services, to ensure continuous use of content even when disconnected and meeting real-time constraints.
- Consideration of secured content distribution like content confidentiality and access privilege violation, etc.

**Constraints, Restrictions and Challenges**

- Seamless handover
- Configuration of enabling caching functionality on mobile devices.

**Relevance with CHARISMA**

This use case is highly relevant to the CHARISMA project, in particular with regards to:

- Low latency
- Security
- Dynamic provisioning

In addition, the network reliability and availability provided by the CHARISMA architecture are also associated with this use case.

**Requirements**

**Table 18: Dual network connectivity requirement for UC3**

Requirement Name	Dual network connectivity on user equipment
Type	Functional
Description	The mobile devices MUST be able to simultaneously connect to WiFi and mobile networks, and to balance the traffic over two interfaces
KPIs	Simultaneous connections for WiFi and mobile networks
Category	Mandatory

**Table 19: Required functionality close to user side for UC3**

Requirement Name	Required functionality close to user side
Type	Functional
Description	Functionalities like caching and switching MAY be distributed and placed along the network and user devices to be able to serve content as near as possible to user side.
KPIs	Caching enabled on network devices closer to end users
Category	Mandatory

**Table 20: Virtualization requirement for UC3**

Requirement Name	Required functionality close to user side
Type	Functional
Description	All resources necessary to offer the service to the VNOs, namely computing, storage and networking
KPIs	Caching functions should be virtualized

Category	Mandatory
----------	-----------

**Table 21: Cache management requirement for UC3**

Requirement Name	Required functionality close to user side
Type	Functional
Description	Efficient and secured cache management SHOULD be provided by SDN based CHARISMA management system
KPIs	Cache management should be secured and efficient
Category	Mandatory

**Table 22: performance requirement of caching and prefetching algorithms**

Requirement Name	Caching and prefetching algorithms
Type	Performance
Description	Hierarchical caching and prefetching algorithms MUST be able to make intelligent decisions for a best use of the network bandwidth and caches
KPIs	High cache ratio, latency of 10ms or lower and high quality video (10-40Mbps)
Category	Mandatory

#### 4.2.4. Big Event

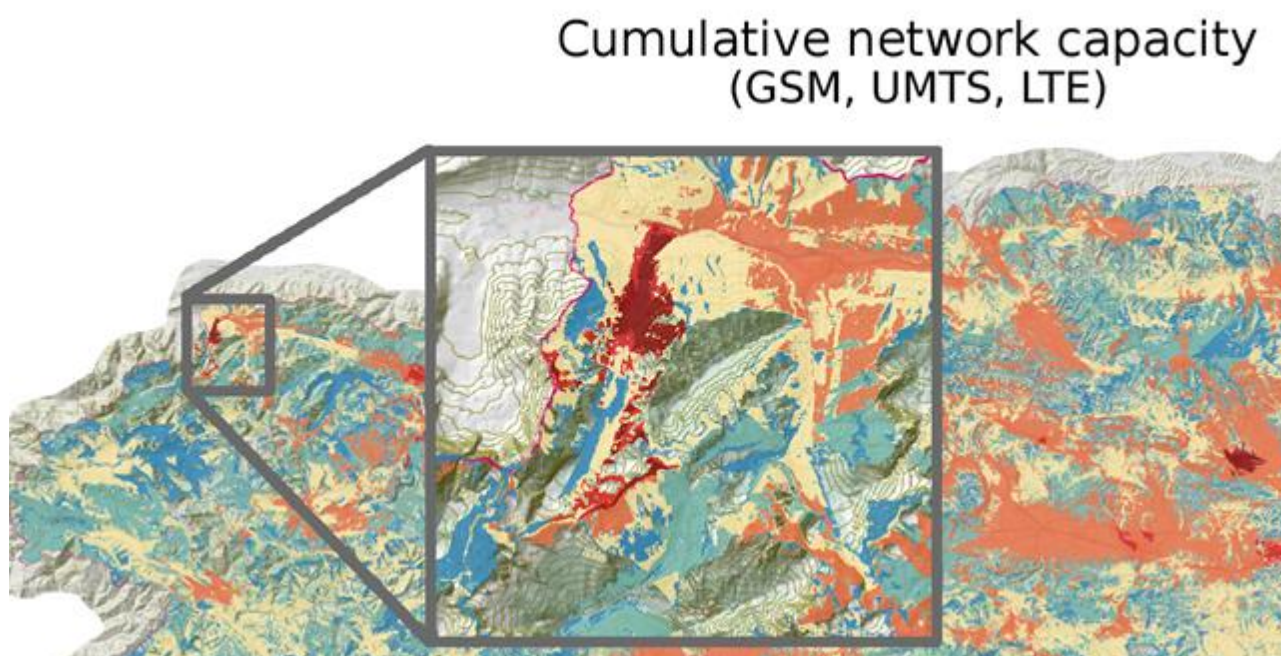
##### Rationale of the UC

The objective of this use case is to ensure that 5G networks can support big events, located in confined spaces. The problem is to correctly dimension the infrastructure to offer good service and at the same time, optimize costs. Typically, most of the time the equipment will be unused while during short periods of time requirements will be very high (during the event). Therefore, reconfigurability and infrastructure sharing are key to optimize resource utilization. Examples of this use case are: concert halls, stadiums, theatres, etc.

An example of a big event that happened in Slovenia (Planica) end of March 2016 were the finals of World Ski Jumping Competition (<http://www.planica.si/Programme>), where Telekom Slovenija installed all its capacities to cover 35,000 visitors at the same time. In terms of generated traffic the table below shows the numbers. Used radio technologies were WiFi (for free and everyone), UMTS and LTE on 800, 1800 and 2700 MHz (for Telekom users only ~ 50 % market share).

**Table 23: Big event (Telekom Slovenija) generated traffic profiles**

Technology	Max. no. of same time active connections	Max. generated traffic (UL and DL)
WiFi	700	30 Mbit/s
Mobile (3G/4G)	N.A.	70 Mbit/s (4 Mbit/s average)



**Figure 39: Extended network capacity in Planica (March 2016)**

**Description**

Events taking place in confined spaces are one of the most difficult network cases to be designed to provide good quality of experience while keeping capital and operational costs as low as possible.

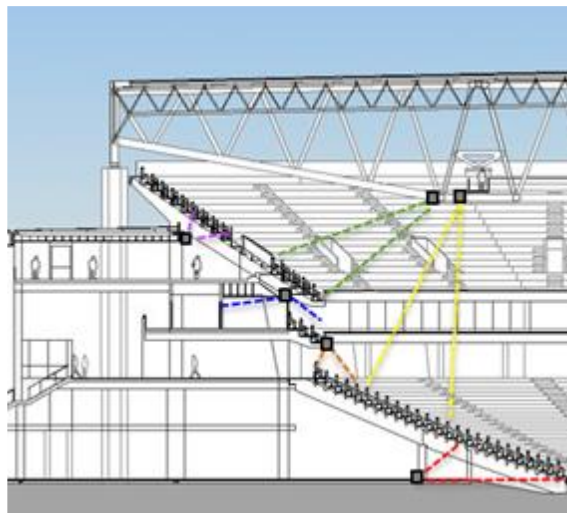
At present connectivity during entertainment events are key in order to offer a complete experience to end-users. People want to share their experiences in real time and the number of users that upload content while assisting to such events is dramatically increasing.

Many teams and clubs try to develop their own Wi-Fi infrastructure in order to provide broadband access while the fan is in their location. However, network performance tends to be poor and end users have to pay for premium services if they want to have a good network experience.

Therefore, 5G networks are a suitable technology that can, on one hand offer a consistent experience to the end user, and on the other allow network operators to keep their users connected to their networks while those events take place.

This use case is very specific and in order to be successful, the following network requirements are almost mandatory:

- Open Access and infrastructure sharing: the location will be empty most of the time, so to deploy multiple networks one for each network operator has no sense. Therefore, open access is key in order to provide a unique infrastructure for all the network providers that own a 5G license.
- High network capacity: the number of subscribers connected simultaneously to the network will be high, and statistical multiplexing factor will be low, as most of the users will want to transmit event highlights at the same time.
- Spectrum efficiency and reuse: the solution to high density and high bandwidth requirements tends to be to design small cells, so efficient network planning and spectrum reuse are key to offer good network performance.



**Figure 40: Schematic of access points in a big event (e.g. sports stadium) scenario**

- Content caching and buffering: in order to equalize peak traffic demands (specially upload of content), to locate content caching equipment close to the user may reduce overall system capacity requirements, so content can be uploaded to the network gradually, incrementing statistical multiplexing.



**Figure 41: End-user density variation in a big event context.**

From the business perspective, the following players need to be considered in order to develop this use case:

- Location owner: the infrastructure needs to be deployed in the stadium / concert hall... so an agreement with the building owner needs to be subscribed. Ideally, an Open Access operator should be the one that should sign the agreement with the location owner.
- Service providers (SPs): the different service providers should agree to use the same Open Access infrastructure to offer final connectivity services to their subscribers. A revenue sharing business model should be established between the different network operators. The network should be transparent to the different SPs.
- End users: end users should perceive no difference with the service and transparently upload and download content using their smartphones and other connectivity devices. One of the key aspects of this implementation is that the end users do not need to register to portals or websites to gain access to the

**Constraints, Restrictions and Challenges**

This UC focus their challenges in the very high transmission requirements in short periods of time. In order to cover this challenge, the network re-configurability is key.

**Requirements**

Functional:

- Open Access: The architecture should be able to work in an open Access network.
- Content caching to equalize network capacity and reduce overall uplink dimensioning
- Transparency and ease of use: end users should access to the network in the same way as when they are in other locations (no need to register to conditional access portals)

Performance:

- High capacity
- Spectrum reutilization

#### 4.2.5. Emergency - Fire Fighters

##### **Rationale of the UC, Goal and Objective**

The objective of this use case is to ensure that 5G networks can support emergency cases. In such event the overall goal is that emergency services such as fire fighters, police, rescue, first aid and others should have the best possible communication available. CHARISMA particularly considers large, unpredictable events, as they pose highest challenges to the communication infrastructure. The use case will show the benefits of the iRRH capabilities.

##### **Description**

Network overload or blackouts are characteristic for emergency situations [68][69]. After a big emergency disaster a large part of communication and energy infrastructure will be destroyed. So the first steps according to the information infrastructure will be to re-establish a basic information system for emergency helpers' coordination. To establish basic voice communication low frequency transmitters are used, the used systems differ by countries, two examples are TETRA [65] and BOS [61]. Especially in situations with structural damages in urban areas the disposability of additional communication systems, which enable the communication to trapped victims can increase their chance of survival. Jang, Lien, and Tsai [67] and Manoj and Baker [69] describe IEEE 802.11-based solutions to enable basic communication using wireless mesh networks. Braunstein *et al.* [62] identify scaling and performance challenges using mesh networks in emergency environments. Using additional remote controlled or autonomous assistance vehicles can optimize the work of emergency assistants. As shown in [55][63][70][71] additionally video surveillance can be used for terrain investigation. Also the support of the human action forces through autonomous vehicles is possible [64][66]. Typically, these devices are controlled by a centralized instance, which processes the accumulated data and generated new commands. This M2M communication servo loop implies high data rates for video data transmissions and low latency for command transmission.

The CHARISMA infrastructure will enable a robust flexible and low latency D2D infrastructure. In the case of an emergency, the existing infrastructure can be reused and extended to enable IP-communication for emergency assistants. This will facilitate the usage of additional supporting technology to optimize the handling of emergency cases. Using intelligent remote radio heads (iRRHs) it is possible to handle D2D and D2-RAN-2D communications. The flexibly deployed iRRHs, which are interconnected through wireline or wireless-technologies, are the basics for network recovery after an emergency scenario. In the case of an emergency the iRRHs can be used to establish and supervise a D2D mesh network to enable a basic communications infrastructure. Additional relay devices can be easily deployed using autonomous flying (i.e. drones) or portable devices.

##### **Constraints, Restrictions and Challenges**

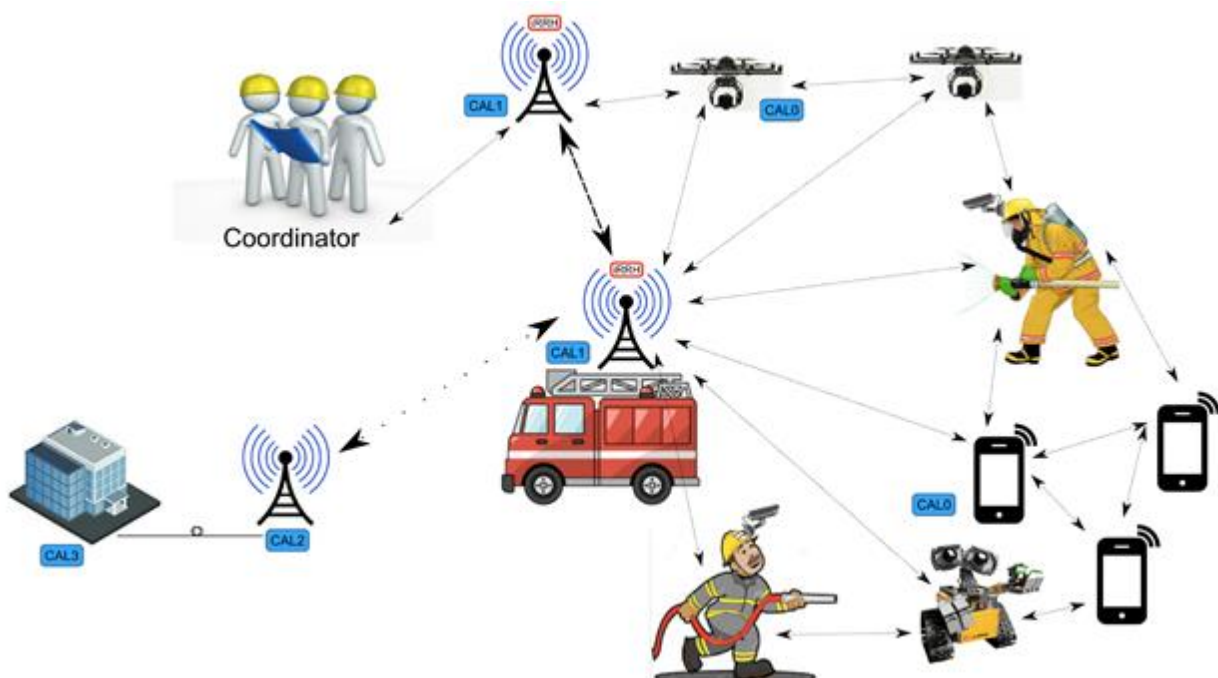
One challenge to manage this use case is to manage the D2D communications, enable a robust, flexible and low-latency D2D infrastructure, and maximize the throughput. Additional devices also need to be integrated

into the current infrastructure. In this use case, the available bandwidth additionally needs to be split into several QoS groups, for example:

- Fire fighters communications
- Technical support equipment communications
- Victims communications

The following scenario shows the related challenges:

In the case of an emergency, fire fighters arrive at the disaster spot, with an iRRH base station integrated into their vehicles or other equipment. The FF-iRRH that is logically placed in the access network establishes basic D2D communication for the rescue and audio communications equipment. The range of this D2D mesh network can be extended by deploying more D2D devices. Some of these devices can also offer a standard WiFi hotspot for victims' communications. Rescued people can connect in a safe location, with additionally information about the state of their health also able to be collected. As might be expected, there are several FF-iRRHs at the emergency spot, with additional working static iRRHs also available. Together, these iRRHs can establish a ad-hoc mesh network. At this juncture, no connection back into the core network is needed, since the FF-iRRHs are able to establish an autarchical communications infrastructure. If a backbone connection is indeed available, the QoS on this link then have to be managed to ensure proper communications according to the defined QoS groups.



**Figure 42: CHARISMA fire fighter use case – overview**

The challenges of this use case will focus on the capabilities of the iRRH to manage the D2D communication of attached devices. In the emergency case, the iRRHs also have to manage devices,

which are not directly connected; this will require additional characteristics on the used mesh routing algorithm.

**Relevance with CHARISMA**

According to the described fire fighters scenario, this use case addresses the following aspects of CHARISMA:

- Open access;
- Hierarchical D2D communication;
- Low latency (according to D2D);
- Network slicing.

Requirements

This use case requires special capabilities of wireless access equipment such as base stations or WiFi hotspot. Each access equipment should be able to:

- Establish and manage an D2D mesh network, to enable low latency D2D communication;
- Connect to wireless access equipment in case of emergency and establish an ad-hoc mesh network amongst them;
- Ensure several network slices with different QoS classes for the several types of emergency traffic;
- Host a landing page for the victims’ communications.

**Table 24: Mesh controlling capability for access equipment**

Requirement Name	Mesh controlling capability for access equipment
Type	Functional
Description	Access equipment has to manage the D2D communication of attached devices to maximize the throughput.
KPIs	Low latency D2D communication
Category	Mandatory

**Table 25: Mesh controlling capability for aggregation equipment**

Requirement Name	iRRH – mesh controlling capability for CAL0
Type	Functional
Description	If D2D devices are divided to several aggregation equipment, this equipment should provide fast routing.
KPIs	Low latency D2D communication
Category	Mandatory

**Table 26: Emergency QoS classes**

Requirement Name	Emergency network slices and QoS classes
Type	Functional
Description	CHARISMA should provide several network slices with different QoS classes for emergency communication of different groups (3 identified), which have individually defined QoS and are independent from the traffic of service providers.
KPIs	Low latency in emergency case
Category	Mandatory

**Table 27: Aggregation equipment interconnection**

Requirement Name	Aggregation equipment interconnection
Type	Functional
Description	The aggregation devices should have technologies for P2P interconnection.
KPIs	Low latency D2D communication
Category	Mandatory

**Table 28: D2D communication**

Requirement Name	User devices mesh capability
Type	Performance
Description	User/ end devices / terminals shall be enabled to form ad-hoc meshed networks under network control.
KPIs	Low latency and disposability in emergency case
Category	Mandatory

#### 4.2.6. Factory of the Future (IoT)

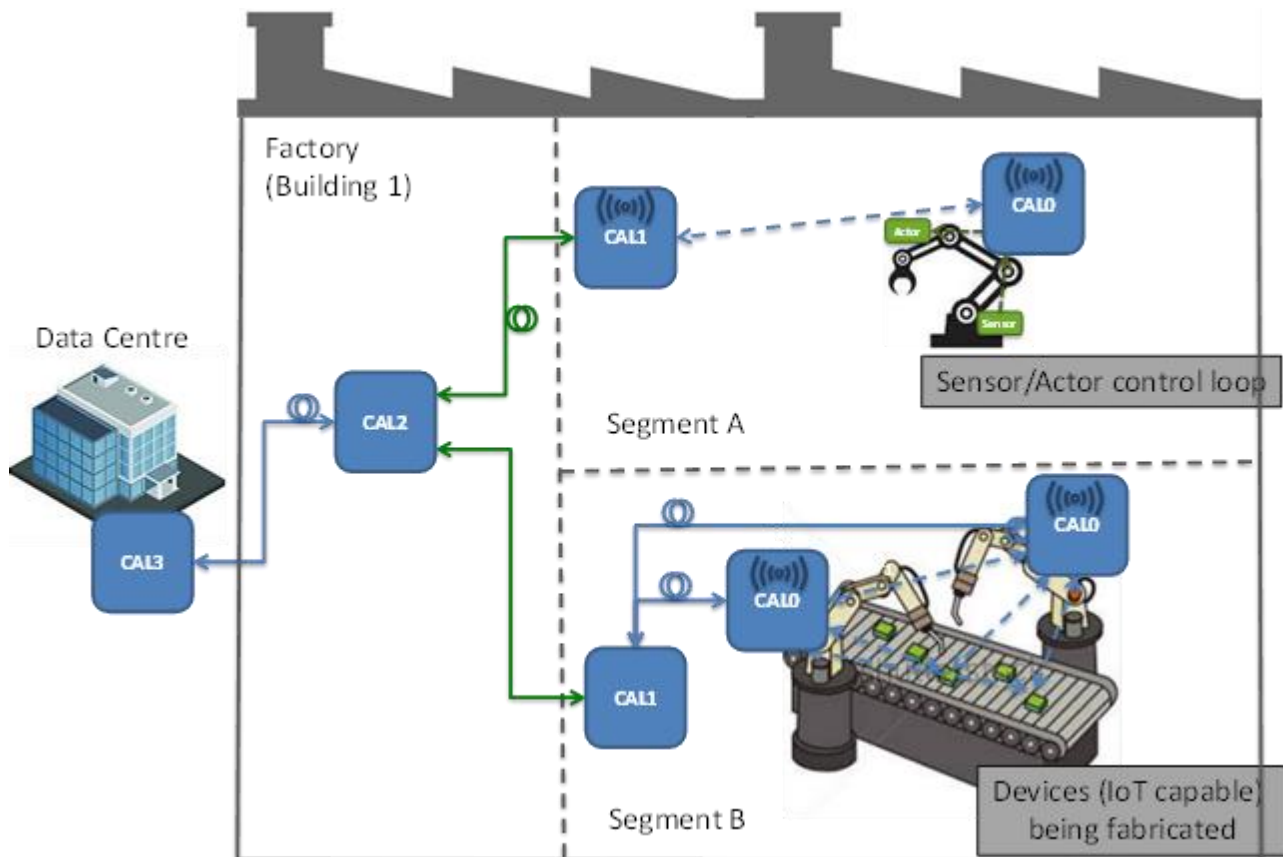
##### Rationale of the UC

The objective of this use case is to evaluate and ensure that 5G networks can support the industrial Internet (Industry 4.0) by providing secure and low latency connectivity. The 5G network should support off-loading of a control loop calculation as well as industrial production, while still keeping the security and latency requirements.

##### Description

The Industry 4.0 scenario involves customers, who design their intended products on their home computer devices using graphic tools, like configuring a brand new car. The product is the purchased via the Internet, the customized product plans are transferred to the Factory of the future, which is entirely defined by software, where the purchased product is then produced automatically according to the customer demands.

For 5G, this scenario has the implication that the whole production scenario will change and become more flexible and reconfigurable. Communications links inside the Future Factory will be more wireless, but have the same robustness, availability, security and low latency as they are usually available for wired links (Figure 43).



**Figure 43: Factory of the Future**

The principle idea of implementation is to install several wireless access points covering the area like in a small-cell mobile network deployment. These small cells are centrally controlled inside the factory (and not outside at the EPC like in current mobile networks) so that coordinated handover and interference management can be done with high efficiency and at very low latency. Because of the centralized processing, cell boundaries, which usually have high signal-to-interference ratio, disappear so that a robust wireless link can be established between multiple access point and multiple robots which can move freely in the entire area covered by all small cells. It is important to have few more access points than mobile robots to enable macro diversity gains, which further improve the robustness of the wireless link.

### Constraints, Restrictions and Challenges

In some locations of the factory of the future the usage of RF might not be desired, because of security and safety concerns. These include the fear of jamming and the RF interference with sensitive sensors.

Because of security concern it might not be acceptable to connect the factory infrastructure directly with networks of mobile operators. Therefore 5G must also support isolated wireless networks with a limited connectivity to the “public” mobile network.

The industrial Internet requires a very high reliability, since any interruption in production process might induce very high costs and is not acceptable.

**Relevance with CHARISMA**

This use case addresses CHARISMA’s following key features:

- Security – to keep sensitive information about the production process;
- Low latency – e.g. to enable fast control loops in the factory;
- Distributed intelligence – to avoid sending sensitive information outside the respective cell (improved security), and to keep the information as local as possible (low latency).

**Requirements**

The functional and performance requirements associated with this use case are the following:

**Table 29: Isolated networks**

Requirement Name	Isolated networks
Type	Functional
Description	The 5G network in a factory should provide the option to provide an isolated network, not connected with networks of mobile operators.
KPIs	Local 5G network separated from public network
Category	Mandatory

**Table 30: usage of non-RF physical layer**

Requirement Name	CAD 5G connectivity
Type	Functional
Description	5G should be open to other PHYs (optical wireless, THz)
KPIs	5G should be frequency-agnostic
Category	Mandatory

**Table 31: 5G availability of 99.99%**

Requirement Name	5G availability of 99.99%
Type	Functional
Description	The local 5G network must offer availability in the order of 99.99%.
KPIs	Local 5G network elements should offer availability in the order of 99.99%.
Category	Mandatory

**Table 32: 5G advanced security requirement**

Requirement Name	5G advanced security
Type	Functional
Description	The 5G network must provide secure communication links. Factory data should not be made available to 3 <sup>rd</sup> parties.
KPIs	The 5G network should offer advanced security mechanisms.
Category	Mandatory

**Table 33: 5G latency of 1ms or less**

Requirement Name	5G latency of 10ms or less
Type	Performance
Description	The 5G network should support latency of 1ms or lower
KPIs	Latency of 1ms or lower.
Category	Mandatory

### 4.2.7. Multi-tenant Access and Video Broadcasting Services

#### Rationale of the UC, Goal and Objective

In the context of the Network Functions Virtualization (NFV) paradigm, virtualization techniques can be used to abstract computing and network resources, allowing the support of various network and content delivery functions (e.g., CDN); such functions are realized with software (SW) implementations on top of shared commercial off-the-shelf (COTS) hardware (HW). In turn, the deployment of network functionality is decoupled from the use of dedicated, special-purpose HW and the associated HW deployment and maintenance overheads. Computing and network resources can be dynamically leased and managed at fine-grained temporal and volume granularity. As a result, these capabilities facilitate the realization of network services, fostering the emergence of Virtual Network Operators (VNOs). Building on virtualized resources, VNOs are able to rapidly deploy their services, flexibly and efficiently utilizing the required resources, and further differentiate their services against competitors by providing SW-based specialized network and CDN functionality. At the same time, network infrastructure operators are presented with the opportunity to deploy and manage COTS resources within their network, so as to enable new business interactions with the emerging VNOs, in business models resembling the cloud computing domain.

The objective of this use case is to ensure that CHARISMA can support this vision, focusing on its realization in the 5G access network infrastructure domain. Edge resources are leased to VNOs resulting in a *multi-tenancy* scenario *i.e.*, more than one VNOs may share the virtualized physical resources of a 5G network infrastructure operator. As different end users may be affiliated with different VNOs, the envisioned setup may result in *inter-domain* traffic scenarios. In the context of multi-tenancy, it follows that *peering* between different VNO domains may be realized at the edge *i.e.*, traffic crossing domain borders within the same micro-datacenter ( $\mu$ DC). The envisioned functionality is demonstrated here in the context of a video broadcasting application. Apart from baseline connectivity, in this use case, (virtual) edge network caches are introduced as additional content delivery functions, for reducing latency experience by end-users and offloading the core network.

#### Description

As shown in Figure 44, the use case involves six actors:

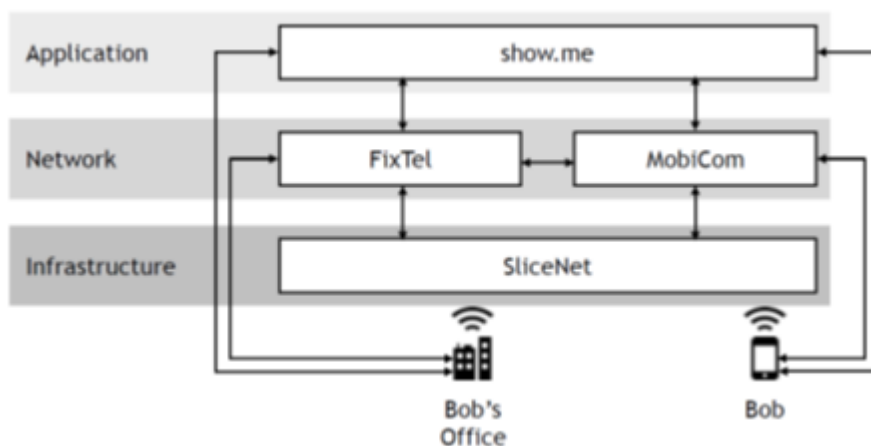
- An access network infrastructure operator, namely *SliceNet*. SliceNet is a company that owns and operates infrastructure for country-wide wireless access. SliceNet has augmented its infrastructure with compute and storage resources that form a cloud. SliceNet leases slices of that entire infrastructure to virtual network operators, like FixTel and MobiCom (see next).
- Two virtual network operators (VNOs), namely *FixTel* and *MobiCom*. FixTel provides Internet access to residential users and small businesses. MobiCom on the other hand focuses on mobile communications at a country scale. MobiCom also sells edge cloud and content delivery resources e.g., caching.
- An application, namely *show.me*. show.me is a social network application where people create their personal live video channel and watch the channels of their friends. It is similar to applications like Meerkat and Periscope. show.me does not use a content delivery network operator, but instead

leases VNO resources that are closer to the end users; in our case show.me uses caching services provided by MobiCom *i.e.*, broadcasted video from users is cached at MobiCom’s  $\mu$ DCs.

- Two end users (Bob and Bob’s office). Bob is a civil engineer at a bridge construction site. Bob is a subscriber of MobiCom. Bob’s office is one of the subscribers of FixTel. Bob is using show.me and his phone to show his team back at the office how construction is progressing.

*Baseline scenario*

Bob is a subscriber of MobiCom and frequently visits construction sites to inspect construction progress. When on site, Bob uses the show.me application to broadcast video from the site to interested colleagues either back in the office premises or on the move. The show.me application provider leases MobiCom resources to support the scalable streaming and caching of the broadcasted videos. Namely, one or more caches are instantiated at selected locations of MobiCom’s virtual infrastructure to support the broadcasting of the video stream sent by an end user’s device (in our case, Bob’s smart phone). During a visit to a site, Bob starts streaming video footage from the construction. A few minutes later, one of Bob’s colleagues joins the show.me application to view Bob’s video broadcast. As a problem seems to arise in the constructions, a team of colleagues located at another office is notified to view the video. Bob’s manager is also later notified for the solution to be fixed. As a result, a series of viewer from different locations start receiving the video broadcast asynchronously. The video streams are requested through FixTel’s virtual network. As FixTel is at several locations co-located with MobiCom, the requests hit the cached content at MobiCom’s caches.



**Figure 44: Virtual Network Operators sharing the infrastructure of an access network (including an edge cloud). The inter-domain application on top is live video broadcasting**

*Baseline setup*

An example illustration of the envisioned use case is provided in Figure 45. SliceNet provides virtualised, cloud resources at each available (small-, micro-, macro) Base Station, in the form of  $\mu$ DCs. This consists of spare resources in existing network equipment (e.g., BSs) and COTS servers. Slices of these resources are provided to FixTel and MobiCom so as to instantiate their services, namely access network services, as well as caching services for MobiCom. The show.me application provider leases such services from MobiCom to

enhance the performance experience by its users. In this context, several CHARISMA Aggregation Levels (CALs) can be defined, where the multi-tenant character of the VNO deployment enables the localization of traffic through optimised routing and/or caching. Example cases are:

- CAL0/CAL0': in this case aggregation takes place at the Customer Premises Equipment (CPE) CAL0 (degenerating as necessary to User Equipment (UE)). For instance, a single CPE interfacing a VNO (e.g., FixTel) is equipped with a caching component localising traffic within the customer premises. In another scenario, the source of the video broadcast is collocated with the recipients of the broadcast in the same 5G cell; in this case the video broadcast is directly diverted to the local recipients.
- CAL1/2: in this case aggregation takes place at the (small-, micro-, macro) level. Aggregation in this case is facilitated by multi-tenancy: in our particular scenario, Bob's video broadcast needs to traverse the borders of the MobiCom domain, so as to enter the FixTel domain and reach Bob's office. A subsequent video broadcast request can be later served by a cache at MobiCom's domain, which also results in crossing the VNO's borders. Both traversals happen at the  $\mu$ DC level. This aggregation level will constitute the main focus area of this use case, as it is focused on the access network domain.
- CAL3: in this case aggregation takes place at the Central Office (CO) / Evolved Packet Core (EPC).

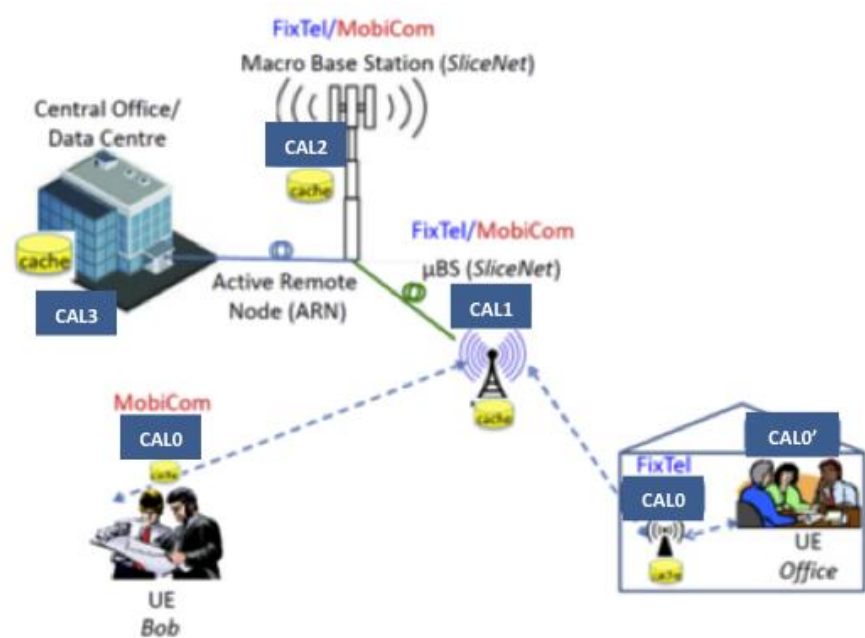


Figure 45: Multi-tenancy in a video streaming application

### Constraints, Restrictions and Challenges

- Orthogonal operation of multiple tenants: security and isolation between the various VNOs are of paramount importance in this UC.
- Security and privacy for end users: video broadcasting necessitates user privacy and security protection.

**Relevance with CHARISMA**

This use case is relevant to the CHARISMA project, with respect to:

- Multi-tenancy  
The use case focuses exactly on the sharing of physical resources by different VNOs, via means of virtualization, thus enabling multiple tenants on the physical infrastructure.
- Security  
The use case aims at highlighting issues of resource isolation among multiple tenants. Focus here is on mitigating attacks related to the shared nature of the physical infrastructure *e.g.*, intrusion attacks, DoS attacks, etc.

**Requirements**

The functional and performance requirements associated with this use case are the following:

**Table 34: Virtualization of resources requirement for UC7**

Requirement Name	Virtualization of resources
Type	Functional
Description	All resources necessary for VNOs, namely computing, storage and networking, have to become “virtualized”, so that they can be allocated dynamically and assume various roles/functions. To this end, cloud-based infrastructure has to be deployed in place of the existing customized hardware.
KPIs	N/A (There is no KPI for such a requirement)
Category	Mandatory

**Table 35: Multi-tenancy requirement for UC7**

Requirement Name	Multi-tenancy
Type	Functional
Description	The infrastructure owner has to be able to offer its virtual resources in a way that multiple operators can coexist and function independently from each other. To this end, virtual resources should be easily bundled together into slices of the physical

	infrastructure so that each slice constitutes an independent virtual edge network and cloud for a VNO.
KPIs	VNO slice instantiation delay (ms/s), <i>i.e.</i> the time required to instantiate VNFs as well as apply all network, compute and storage resource configurations.
Category	Mandatory

**Table 36: Security requirement for UC7**

Requirement Name	Security
Type	Functional
Description	Telecommunication resources should be appropriately isolated from IT resources (compute and storage) at the infrastructure layer to contain malicious or malfunctioning virtual functions. The infrastructure operator should be distinct from any VNO, as their business models differ significantly. VNOs should not be able to interfere with each other (except through peering) according to current practice. Operational security (e.g., intrusion detection, access control, policing) on the other hand could be a shared resource.
KPIs	VNO service availability: should remain unaffected by the instantiation (or resource reconfiguration) of other VNOs on the same infrastructure.
Category	Mandatory

**Table 37: Throughput requirement for UC7**

Requirement Name	Throughput
Type	Performance
Description	Throughput is a key parameter for a large part of existing and envisaged applications, as is in this case, video broadcasting. High-definition video is already the norm -with higher resolutions coming up- especially for receivers with large screens, so bandwidth requirements are considerable and will become more so in the near future.
KPIs	Throughput (Mb/s)

Category	Mandatory
----------	-----------

**Table 38: Routing requirement for UC7**

Requirement Name	Routing
Type	Functional
Description	When appropriate, traffic should be routed as close to the edge as possible to minimize hops and hence traffic impairments.
KPIs	Path length (hop count) Latency (ms)
Category	Mandatory

**Table 39: Routing requirement for UC7**

Requirement Name	Performance
Type	Non-Functional
Description	Virtualization, multi-tenancy, and security should not come at the expense of performance. In fact, compute and storage resources at the edge should be exposed to applications (via e.g., caching, analytics, processing) to improve their performance.
KPIs	Above performance metrics (i.e., throughput, latency) should remain unaffected by the instantiation (or resource reconfiguration) of other VNOs on the same infrastructure.
Category	Mandatory

#### 4.2.8. Remote Surgery

##### Rationale of the UC

The objective of this use case is to ensure that 5G networks can support the vertical industry of health in the area of remote surgeries.

Remote surgery is foreseen to play a significant role in the future systems of e-health. The adoption of remote surgery systems will allow high trained experts that are available in a few hospitals to perform operating procedures without the need to be physically present at the operation location. The surgeons of the future will be able to perform complex operations from their offices using the 5G networks and will be able to collaborate with other doctors. Surgeons will have a live feed through the network, communication with other members of the team, access to patient data and control of the robotic mechanism.

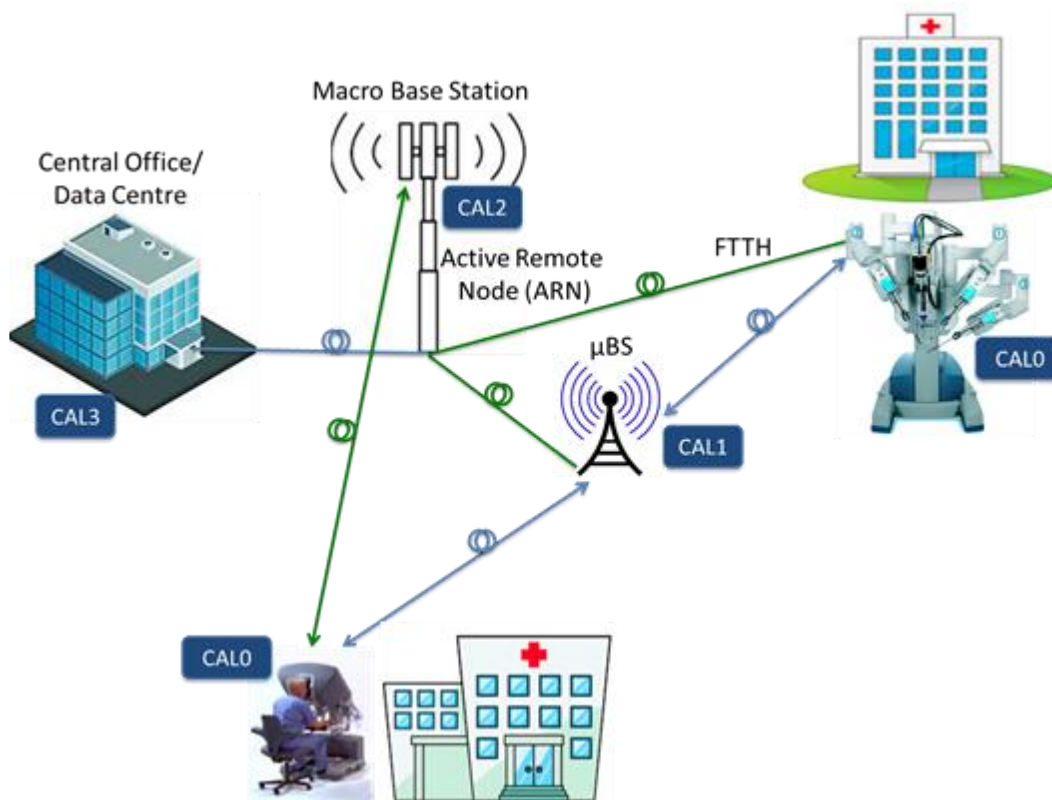
But in order to be able to perform remote surgeries, the latency of the communication system must be reduced below the limit of 200ms. In addition, the communication link must be able to offer high availability, reliability and security.

The latency of current operating systems, such as the DaVinci system is in the order of 180ms. According to the other studies [72] the impact of the delay is related also to the difficulty of the procedure. An overall rule is that delays between 100 and 200ms have no significant impact on the operation procedure. Delays higher than 500 ms lead to an increase in the surgical risk, while is recommended to avoid performing surgeries if the delay is higher than 700ms. Future systems are expected to operate below 30ms.

Security and privacy is also crucial since sensitive personal medical data will be transferred. All the data that will be exchanged must be checked for consistency and the system must be intolerant to new security threats.

### **Description**

This use case is illustrated at the next figure and involves all the CHARISMA actors. The doctors are the end users of the telecommunication services that are provided from the Virtual Network Operator that utilises the resources it rents from the Network Operator. The application provider develops specialised software for controlling the robot that performs the surgery and also tools for collaboration between doctors.



**Figure 46: Remote surgery architecture**

The doctor that will perform the surgery is located at the CAL0 point of the CHARISMA architecture, and is connected either to CAL1 or CAL2 with a wireless or a fibre link. The machinery that is used for the surgery is also located at CAL0 level of architecture. These CAL0s can be connected to the same aggregation point CAL3 or to different ones. This UC assumes that the CHARISMA architecture will ensure a dedicated link between the CAL0s levels with guaranteed low latency, reliability and security. Through this communication link a high quality video feed flows from the machine cameras to the doctor. The doctor at the remote location controls this machine and also communicates with other doctors.

### **Constraints, Restrictions and Challenges**

Until now there have been cases of remote surgeries but they all used wired private networks in order to achieve the above requirements a solution that requires specialized equipment and is of high cost. 5G will come and provide a platform capable of fulfilling the challenges that rise and make remote surgery a reality.

### **Requirements**

The performance requirements associated with the remote surgery case are presented at the following tables:

**Table 40: Remote surgery connectivity requirement**

Requirement Name	Connectivity
Type	Functional
Description	Doctors and machine should be connected
KPIs	
Category	Mandatory

**Table 41: Remote surgery low latency requirement**

Requirement Name	Low Latency
Type	Performance
Description	The network must ensure low latency
KPIs	Latency below 30ms
Category	Mandatory

**Table 42: Remote surgery high availability requirement**

Requirement Name	High Availability
Type	Performance
Description	The network must ensure high availability
KPIs	99.99x% availability
Category	Mandatory

**Table 43: Remote surgery high reliability requirement**

Requirement Name	High Reliability
Type	Performance
Description	The network must ensure high reliability
KPIs	99.99x% reliability

Category	Mandatory
----------	-----------

**Table 44: Remote surgery high security requirement**

Requirement Name	High Security
Type	Performance
Description	The network must ensure high security. There are sensitive personal medical data that must not be available to others. Also none should be able to intervene and take over of the machine that performs the surgery.
KPIs	Security mechanisms
Category	Mandatory

**Table 45: Remote surgery high quality video requirement**

Requirement Name	High quality video
Type	Performance
Description	The network must allow the transmission of high quality video
KPIs	100Mbps
Category	Mandatory

**Table 46: Remote surgery low cost requirement**

Requirement Name	Low cost
Type	Other
Description	The network must provide low cost services
KPIs	
Category	Desirable

### 4.2.9. Smart Grid

#### Rationale of the UC, Goal and Objective

Due to the development of renewables, new challenges are appearing for the energy distribution networks. Indeed, renewable production is uncertain and variable during the day by nature due to weather conditions (e.g., sun, wind). In addition, renewable production is much more distributed than central power plants that are based on e.g. nuclear or fossil fuel. In order to avoid blackouts and to optimize the use of renewables a real time dynamic routing of electricity flows will be needed. This routing will require new electrical equipment but also a renewed supervision and control network for electricity distribution networks. This supervision and control network will be required to transmit and process distributed data such as measures from meters (for production units but also demand units or even weather sensors) in real time. It could make sense to mutualize infrastructures with other sectors to execute this distributed transmission and processing of data. Indeed, this requirement is also appearing for water or gas distribution networks and also in some manufacturing transformations, as well as more broadly in the Cloud industry and in the Internet of Things domain. 5G technology could support efficiently all these services and sectors within a unified infrastructure while providing sufficient flexibility in order to deploy specific virtual network functions and ensure dedicated technical performances (with related SLA) such as constant latency for each sector/domain. 5G is envisioned to be the first global technology standard that will in mind address the variety of future use cases from energy sector, where even more data is predicted to be generated and smartly used, by ensuring that the both radio and core network performance requirements can be met in terms of (end to end) latency, reliability, availability for different services. Robust and reliable handling of data traffic offered to the 5G network by the multitude of supported services will be achieved from data plane and control plane isolation. Reliability-of-service will have to be orders of magnitude higher than in current wireless access networks, usually in combination with stringent E2E latency requirements, e.g. for the grid backbone communication network domain below 5 ms, while the acceptable downtime per year must not exceed 5 minutes, and data rates in the order of Mbps or even Gbps are required. Smart Grid includes diverse use cases ranging from system protection that requires ultra reliable and low latency communication to smart meters that require support of massive number of network connected devices with relaxed latency and reliability requirements. LTE Radio Access Network (RAN) and Evolved Packet Core (EPC) are not designed flexible enough to simultaneously meet requirements of such diverse use cases economically and technically. Thus, programmable and flexible network architecture is required which can enable handling reliability, security and performance (including QoS) requirements of diverse subset or even each Smart Grid application over a single platform. As consequence, the increasing demand for low round trip latency and ultra-high reliability appears as a decisive factor for 5G implementation with respect to mission-critical communication within the smart grid. Security and confidentiality solutions, which prevents cyber-attacks, still maintaining the latency requirements, is a critical function for the future power grid communication network.

#### Description

Smartgrid network proposed (considered Sunseed FP7 project pilot within Telekom Slovenije) is implemented so that communication antenna of the gateway (CALO) is mounted either inside or outside the electrical box or the object where WAMS (Wide Area Measurement and Supervision) is mounted to

overcome the Faraday cage/shield effect. The gateway is a modem which connects to the LTE network via CAL1 or CAL2 base station, which depends on the availability of the existing infrastructure on site.

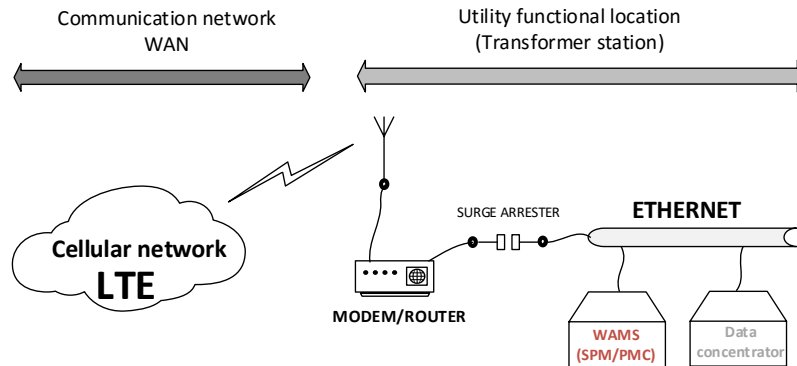


Figure 47: Smartgrid (Sunseed FP7 project) use case

**Constraints, Restrictions and Challenges**

The specific requirements of smart grid data traffic that can pose challenges to existing cellular networks, relate to:

- Massive number of devices;
- Low latency communication; and
- Ultra-reliable communication.

**Relevance with CHARISMA**

- Security and reliability/availability aspect;
- Low latency.

**Requirements**

A performance requirements associated with the smartgrid use case are presented in the following tables:

Table 47: Smart grid network availability requirements

<b>Requirement Name</b>	<b>Dense network of measurement nodes (e.g.: smart meters) and network availability.</b>
Type	Functional
Description	Each carriage should be able to connect a high number of devices to either the corresponding base station (CAL1 or CAL 2). Priority with certain QoS and SLA agreements should be taken into account. (e.g.: real time communication and time synchronous measurements are expected).

KPIs	5G network availability and QoS/SLA agreements
Category	Mandatory

**Table 48: Smart grids security requirements**

<b>Requirement Name</b>	<b>Dense network of measurement nodes (e.g.: smart meters) and networks security.</b>
Type	Functional
Description	Number of nodes in smart grid rises dramatically, where each node can be potential target for DDoS or on site tempering and vulnerability injection. This is especially true with user in-house installed smart sensors and programmes running grid optimisation.
KPIs	5G network end-to-end security
Category	Mandatory

**Table 49: Smart grids latency requirements**

<b>Requirement Name</b>	<b>Low latency high availability communication due to smartgrid standards.</b>
Type	Functional
Description	Managed demarcation router (CAL0), at location IP network with protection functionality.
KPIs	8 ms or less latency and 99.999 % availability.
Category	Mandatory

### 4.3. Requirements & Specifications

The following table presents a homogenised list of all the different requirements extracted from the use cases described in the previous section. Similar requirements are grouped together and in cases where

different KPIs are considered for the same requirement, the strictest KPI is taken into account and included in the table below.

**Table 50: CHARISMA requirements**

Number	Requirement	CHARISMA support
1	CHARISMA shall offer low latency services	CHARISMA’s architecture shall support low latency services via: <ul style="list-style-type: none"> <li>• Routing of data at the lowest common aggregation point</li> <li>• Devolved offload strategies for device-to-device, device-to-remote-radio, device-to- baseband, device-to-central office/metro, cloud-to-cloud/cellular, etc.</li> <li>• Mobile distributed caching</li> <li>• Trust Node enabled secure hierarchical and ID routing</li> </ul> Typical value of latency $\leq 1\text{ms}$
2	The system shall support advanced end-to-end security	CHARISMA’s architecture shall support distributed (decentralized) security, as opposed to centralized security in 4G, as well as physical layer security. The CHARISMA virtualized OpenNaaS-based architecture-level design provides a C&M plane offering improved security. A holistic security approach is proposed where the underlying infrastructure is virtualized and shared among several SPs, who operate simultaneously the same physical resources.
3	CHARISMA shall support open access	CHARISMA’s architecture enables ubiquitous multi-provider, multi-user, multi-technology, and multi-service scenarios. The open access CHARISMA infrastructure has a unified virtualized network management system capable of allocating slices and offering accessible service interfaces for novel and differentiated services to end-users, as the basis for supporting innovative business models.
4	High bandwidth video streaming services shall be supported	CHARISMA’s architecture shall support data-rates up to 10 Gbps for SMEs and residential users and up to 1 Gbps for mobile end-users, through the use of a hierarchical intelligent data processing approach at the C-RAN and RRH, where statistical multiplexing, aggregation, and caching allow access data volumes to be significantly increased. In addition, CHARISMA’s architecture shall incorporate mm-wave (60 GHz

		<p>and E-band technologies), as well as optical LoS and non-LoS (NLoS) final-drop technologies, including converged wireline (FTTH) connections from the RRH and/or the C-RAN to end-user premises.</p> <p>Typical value of data-rate for video streaming: 100Mbps.</p>
5	The proposed system shall provide seamless and ubiquitous connectivity	The system proposed by CHARISMA shall be able to offer seamless and ubiquitous 5G services in both densely- and under-populated areas thanks to a highly diversified (heterogenous) networking architecture (including 60 GHz and optical LoS communications) with higher bandwidths available in the wireless/fixed access networks.
6	High availability	All network elements employed in the CHARISMA's architecture will have an availability of 99.99%.
7	High reliability	All network elements employed in the CHARISMA's architecture will have a reliability of 99.99%.
8	Virtualization of resources	CHARISMA's architecture shall make extensive use of resource virtualization. The Virtualized Infrastructure (VI) group will virtualize the hardware resources (computing, storage, and network) via e.g. a hypervisor at the Virtualization Layer, which pools the resources and exposes them for consumption by VNFs. The Virtualized Network Functions (VNFs) group comprises software components that implement network functions destined to run on the VI. Virtualization will also be applied on the RAN with the utilization of C-RAN. Finally, CHARISMA will put effort on implementing VNFs for caching, switching, and security.
9	The users shall be provided with different levels of priority for emergency communications	CHARISMA 's architecture shall support several QoS classes for emergency communications, assigning to users different levels of priority.
10	Advanced D2D communications shall be supported	In CHARISMA's architecture each iRRH shall be able to establish and manage a D2D mesh network, to enable low latency D2D communication. In addition, each iRRH shall be able to connect to other iRRHs in case of emergency and establish a CAL1 mesh network between several iRRHs.

11	Low packet loss rate	The 5G system proposed by CHARISMA shall provide packet loss rate of $10^{-5}$ or less.
12	Broadcast functionality support	The 5G system proposed by CHARISMA shall support broadcast mechanisms in order to be able to warn all users in a certain geographical area in case of a critical event.

#### 4.4. Summary

In this chapter we have provided a comprehensive overview of the Use Cases that are particularly relevant to the CHARISMA architecture. Building upon the architecture design parameters of the earlier chapters, the UCs have been chosen to particularly feature and require the 3 key defining functionalities of CHARISMA, namely: low latency, open access, and security. The list of CHARISMA UCs considered in this chapter were:

- Automotive – Trains
- Automotive – Platooning, Vehicle Collision Avoidance
- Automotive – Buses
- Big Event
- Emergency - Fire Fighters
- Factory of the Future (IoT)
- Video Streaming
- Remote Surgery
- Smart Grid

We have described the requirements of the UCs in terms of their required functionalities, performance, and their relative importance, and have also tabulated their associated KPIs. The constraints, restrictions and technical challenges associated with each UC have also been described. In addition, we have categorised all the various UC requirements into common blocks, so as to ascertain which requirements are of more general importance than other (i.e. more UC-specific) requirements; the expectation being that such a categorization of the CHARISMA UC requirements will also be of broader interest to the designers of 5G networking architectures.

## 5. Conclusions

In this deliverable D1.1 “CHARISMA intelligent, distributed low latency security C-RAN/RRH architecture” we have provided a comprehensive overview of the architecture that we have adopted in the CHARISMA project. In particular, in designing an architecture suitable for 5G purposes we have also outlined the 5G Use Cases that will particularly exploit and find useful application for the CHARISMA architecture design. The CHARISMA architecture has been designed to feature three particular characteristics that are anticipated to be of importance in future 5G networking: low latency, open access, and security. To that end all of the Use Cases have been chosen to particularly require these three particular features. In addition to these three fundamental features of the CHARISMA architecture, which are common to all the Use Cases, each of the UCs has its own distinguishable requirements (in terms of functionality, performance, and its relative importance/criticality) and their associated KPIs, as well as the constraints, restrictions and technical challenges associated with each UC. These have all been outlined in this deliverable. Taken together, all these various requirements and constraints have also acted to influence the design of the CHARISMA architecture. An initial systematic categorization of all the various requirements has also been performed to ascertain which requirements are of more general importance than other (more UC-specific) requirements. These particular results will be of general interest to a broader range of 5G architecture designers.

In order to define the CHARISMA architecture, we have followed a multi-layered approach to the architecture design, based on consideration of its control plane, data plane, and service plane, and how these are managed and orchestrated by the CMO plane. The data plane architecture for CHARISMA is comprehensively considered in chapter 2, where the innovative technologies that will underpin the low latency, open access, and v-security performance of CHARISMA have been described. In particular, at the overall architecture level, we have also described how the CHARISMA architecture has been designed to be hierarchical and quasi-distributed in nature, via the use of four self-similar CHARISMA aggregation levels (CALs). Each of these CALs (from CAL0 to CAL3) have been mapped onto the key physical and functional nodes of a 5G network, and also explicitly identified for each UC scenario. Each active node (i.e. CAL) has been designed to possess its own scalable intelligent management unit (IMU) performing data storage/caching, processing and routing functionalities. Data is routed, where possible, at the lowest common aggregation point, so as to assist in achieving low-latency networking. Distributing intelligence ever closer to the end-user also assists in reducing network latency, and allows for more precise SDN and NFV control of the CHARISMA 5G network.

The initial design for the control & management plane has already been described in the earlier CHARISMA deliverable D3.1 “V-Security management plane design and definition”, but a brief summary of the C&M plane has also been given in chapter 2, whilst the service plane (SP) has been considered in chapter 3. Here, we have also defined the expected service and workflow life-cycle that CHARISMA will have to support; in particular with a view to automation of the whole service delivery and operations process. With the UCs being highly dynamic in nature, the service lifecycle requires dynamic provisioning and reconfiguration. Alongside the service workflows, we have also identified the most important actors expected to feature in the CHARISMA architecture, with particular regard to the virtualization of physical infrastructure, network

operation, resources and network functions. Together the design of the CHARISMA architecture to be compliant with VNF and SDN capabilities has also been fundamental to its development.

The specifications for the CHARISMA architecture described in this deliverable are now being used to feed back into the other parallel work packages such as WP2 for the CHARISMA physical layer design, WP3 for realizing the CHARISMA CMO plane design with its v-security features, and also into the CHARISMA demonstrators design of WP4. Here, the most appropriate UC scenarios are also now being adopted to best showcase the CHARISMA architecture features in the final year of the project.

## References

- [1] [http://www.ict-strauss.eu/deliverables/D3.1.v.3.0\\_final.pdf](http://www.ict-strauss.eu/deliverables/D3.1.v.3.0_final.pdf)
- [2] Cisco VNI report, "Cisco Visual Networking Index: Forecast and Methodology, 2014–2019" 27, May 2015.
- [3] Malandrino, F.; Casetti, C.; Chiasserini, C., "Content Discovery and Caching in Mobile Networks with Infrastructure," IEEE Transactions on Computers, vol.61, no.10, pp.1507,1520, Oct. 2012
- [4] Hasti Ahlehagh and Sujit Dey, "Video caching in Radio Access Network: Impact on delay and capacity," IEEE Wireless Communications and Networking Conference (WCNC), pp.2276-2281, April 2012.
- [5] White paper "3G/Wi-Fi Seamless Offload", Qualcomm Inc., 2010.
- [6] 3GPP TR 23.861 "Network based IP flow mobility", V1.7.0 (2012-11).
- [7] 3GPP TS 22.278 "Service requirements for the Evolved Packet System (EPS)", V12.2.0 (2013-03).
- [8] 3GPP TR 23.882 "Report on Technical Options and Conclusions" V8.0.0 (2008-09).
- [9] T. Ahmed, S. Antoine, S. Dong, D. Barankanira, "Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS), in proc. of WCNC-2010, 2010.
- [10] 3GPP TR 23.829, "Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)", V10.0.1 (2011-10).
- [11] 3GPP TS 23.234, 3GPP system to Wireless Local Area Network (WLAN) interworking, V11.0.0 (2012-09)
- [12] 3GPP TS 23.402, "Architecture enhancements for non-3GPP accesses", V12.0.0 (2013-03).
- [13] C. B. Sankaran, "Data offloading techniques in 3GPP Rel-10 networks: a tutorial", IEEE Communication Magazine, June 2012.
- [14] "Bell Labs Metro Network Traffic Growth: An architecture impact study", White Paper, Alcatel-Lucent 2013.
- [15] B. A. Ramanan, L. M. Drabeck, M. Haner, N. Nithi, T. E. Klein and C. Sawkar, "Cacheability analysis of HTTP traffic in an operational LTE network," Wireless Telecommunications Symposium (WTS), 2013, Phoenix, AZ, 2013
- [16] Peter Turnbull, et al. "Verification of Ethernet as a Transport Protocol for Fronthaul/Midhaul", iCIRRUS, Deliverable D3.1, 2016
- [17] Philippe Chanclou, et al. "iCIRRUS – Intelligent C-RAN Architecture", iCIRRUS, Deliverable D2.1, 2015
- [18] N. J. Gomes, V. Jungnickel, P. Chanclou, J.-P. Elbers, P. Turnbull, A Flexible, Ethernet Fronthaul for 5th Generation Mobile and Beyond, Optical Fiber Conference 2016 (invited paper).
- [19] Siemens: "Latency on a Switched Ethernet Network", Application Note 8
- [20] "V-Security Management Plane Design and Definition", CHARISMA deliverable D3.1, January 2016
- [21] Jun Wu, Zhifeng Zhang, Yu Hong, and Yonggang Wen, "Cloud Radio Access Network (C-RAN): A Primer", IEEE Network, January/February 2015
- [22] <http://www.netmanias.com/en/?m=view&id=blog&no=8153>
- [23] <http://www.eurecom.fr/en/publication/4841/download/cm-publi-4841.pdf>
- [24] <http://www.ericsson.com/res/docs/whitepapers/wp-cloud-ran.pdf>

- [25] IEEE P802.3av task force, [www.ieee802.org/3/av/](http://www.ieee802.org/3/av/).
- [26] ITU-T recommendation: [www.itu.int/rec/T-REC-G.989.2](http://www.itu.int/rec/T-REC-G.989.2).
- [27] P. Chanclou, A. Cui, F. Geilhardt, H. Nakamura, and D. Nessel, "Network operator requirements for the next generation of optical access networks," IEEE Netw. Mag., vol. 26, no. 2, pp. 8-14, Mar. 2012.
- [28] D. Nessel, "NG-PON2 technology and standards," in Eur. Conf. Opt. Commun. (ECOC), Cannes, Sep. 2014, tutorial paper Mo.4.1.1.
- [29] Miller, S.E.: 'Integrated Optics : an introduction', Bell Syst. Tech. J., 1969,488, pp. 2059-2069
- [30] Smit, M., Leijtens X., Bente E., et al: 'Generic foundry model for InP-based photonic', IET Optoelectronics,2011, Vol. 5, Iss.5, pp 187-194
- [31] Smit, M., Leijtens, X., Ambrosius H., et al: 'An Introduction to InP-based generic integration technology', Semiconductor Science Technology, 2014, pp 41
- [32] Koren U et al: 'WDM light sources with integrated QW tunable lasers and optical amplifier', Applied Physics Letter, 1989, 54, 2056-8
- [33] Duthi P J et all:'Guided wave switch array using eleco-optic and carrier depletion effects in Indium Phosphide', Electronic Letters,1991, 27, 1747-8
- [34] Kaiser R:'Monolithically integrated 4x4 InGaAsP/InP laser amplifier gate switch arrays', Electronic Letters, 1994, 30, 1446-7
- [35] Smit M K: 'New focusing and dispersive planar component based on an optical phased array', Electronic Letters, 1988, 24, 385-6
- [36] Nagarajan, R., Joyner, C. H., Schneider, R. P., et al.: 'Large-scale photonic integrated circuits', IEEE J. Sel. Top. Quant. Electron. JSTQE, 2005, 11,(1), pp 50-65
- [37] EuroPIC, <http://europic.jepix.eu>
- [38] Tavares,A. , Lopes, A., Rodrigues, C. et al : 'Photonic integrated transmitter and receiver for NG-PON2', AOP , 2014
- [39] Rodrigues, F., Tavares, A., Lopes,A. Et al : 'Photonic integrated transceiver for Hybrid PONs', IEEE proceedings from Networks 2014, 2014
- [40] Almeida, L.,Kumar, N., Parca, G. Et al: 'All-optical image processing based on Integrated Optics', ICTON 2014, 2014
- [41] Richter, A., Mingaleev,S., Koltchanov,I. : 'Automated design of large-scale photonic integrated circuits', SPIE Newsroom, 2015
- [42] Carrol, M., Nessel,D, Dawes,P. : ' FSN Highlights & NG-PON2 standards Update', FSN and IEEE NG-EPON/1904 ANWG Joint Session, February 4,2015
- [43] ITU-T recommendation: G.989.3
- [44] ITU-T recommendation: G.989.1
- [45] ITU-T recommendation: G.989
- [46] Microwave Technology Innovations Enabling Efficient and Homogeneous LTE Macro & Small-Cell Backhaul, White Paper, 2013 Intracom S.A. Telecom Solutions ([http://www.intracom-telecom.com/en/products/wireless\\_network\\_systems/WP/Microwave\\_Technology\\_Innovations.htm](http://www.intracom-telecom.com/en/products/wireless_network_systems/WP/Microwave_Technology_Innovations.htm))
- [47] <http://whatis.techtarget.com/definition/network-management-system>

- [48] <https://en.wikipedia.org/wiki/FCAPS>
- [49] [http://docwiki.cisco.com/wiki/Simple\\_Network\\_Management\\_Protocol](http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol)
- [50] NGMN Alliance, “NGMN 5G White Paper,” White paper, Feb. 2015. [Online]. Available: [http://ngmn.org/uploads/media/NGMN\\_5G\\_White\\_Paper\\_V1\\_0.pdf](http://ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf)
- [51] 3GPP TR 22.891, “Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)”, November 2015
- [52] 5G NORMA D2.1 Use cases, scenarios and requirements, [https://5gnorma.5g-ppp.eu/wp-content/uploads/2015/11/5G-NORMA\\_D2.1.pdf](https://5gnorma.5g-ppp.eu/wp-content/uploads/2015/11/5G-NORMA_D2.1.pdf)
- [53] ITU-R Recommendation M.2082-0, “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond,” September 2015. Available: [https://www.itu.int/dms\\_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-!!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-!!!PDF-E.pdf)
- [54] <https://technet.microsoft.com>
- [55] NGMN Alliance, “NGMN 5G White Paper,” White paper, Feb. 2015. [Online]. Available: [http://ngmn.org/uploads/media/NGMN\\_5G\\_White\\_Paper\\_V1\\_0.pdf](http://ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf)
- [56] 3GPP TR 22.891, “Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)”, November 2015
- [57] 5G NORMA D2.1 Use cases, scenarios and requirements, [https://5gnorma.5g-ppp.eu/wp-content/uploads/2015/11/5G-NORMA\\_D2.1.pdf](https://5gnorma.5g-ppp.eu/wp-content/uploads/2015/11/5G-NORMA_D2.1.pdf)
- [58] ITU-R Recommendation M.2082-0, “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond,” September 2015. Available: [https://www.itu.int/dms\\_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-!!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-!!!PDF-E.pdf)
- [59] <https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf>
- [60] Ahmad Jaelan Alif Aizat Azraie and Abdul Hafiihz. “Smart Drone for emergency monitoring and disaster relief”. In: (2015). url: <http://dSPACE.unimap.edu.my/xmlui/handle/123456789/40412>.
- [61] BDI. *Bestimmungen für Frequenzuteilungen zur Nutzung für das Betreiben von Funkanlagen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS)*. Bundesministerium des Innern, 2005. url: [http://www.digitalfunk-sh.de/DFSH/userfiles/files/bos\\_funkrichtlinie\\_2009.pdf](http://www.digitalfunk-sh.de/DFSH/userfiles/files/bos_funkrichtlinie_2009.pdf).
- [62] B Braunstein *et al.* “Challenges in using distributed wireless mesh networks in emergency response”. In: *3rd International ISCRAM Conference*. 2006, pp. 30–38.
- [63] Kyoungah Choi and Impyeong Lee. “A UAV-based close-range rapid aerial monitoring system for emergency responses”. In: *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci* 38 (2011), pp. 247–252.
- [64] Gabriele Ermacora *et al.* “A cloud robotics architecture for an emergency management and monitoring service in a smart city environment”. In: (2013).
- [65] ETSI. “TETRA”. In: (2007). url: <http://www.etsi.org/technologies-clusters/technologies/tetra?highlight=YToxOntpOjA7czo1OiJ0ZXRxYYSI7fQ==>.
- [66] R.B. Haarbrink and E. Koers. “Helicopter UAV for photogrammetry and rapid response”. In: *International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences, ISPRS Workshop of Inter-Commission WG I/V, Autonomous Navigation*, Antwerp, Belgium. Citeseer. 2006.

- [67] Hung-Chin Jang, Yao-Nan Lien, and Tzu-Chieh Tsai. "Rescue information system for earthquake disasters based on MANET emergency communication platform". In: *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*. ACM. 2009, pp. 623–627.
- [68] Yao-Nan Lien, Hung-Chin Jang, and Tzu-Chieh Tsai. "A manet based emergency communication and information system for catastrophic natural disasters". In: *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on*. IEEE. 2009, pp. 412–417.
- [69] Balakrishan S. Manoj, and Alexandra Hubenko Baker, "Communication challenges in emergency response". In: *Communications of the ACM* 50.3 (2007), pp. 51–53.
- [70] Francesco Nex and Fabio Remondino. "UAV for 3D mapping applications: a review". In: *Applied Geomatics* 6.1 (2014), pp. 1–15.
- [71] Pedro A. Rodriguez et al. "An emergency response UAV surveillance system". In: *AMIA Annual Symposium Proceedings*. Vol. 2006. American Medical Informatics Association. 2006, p. 1078.
- [72] Rayman, Reiza, et al. "Effects of latency on telesurgery: an experimental study." *Medical Image Computing and Computer-Assisted Intervention–MICCAI 2005*. Springer Berlin Heidelberg, 2005. 57-64.

## Acronyms

<b>Acronym</b>	<b>Definition</b>
3GPP	3rd Generation Partnership Project
5G	Fifth Generation
AP	Access Point
AP	Application Provider
API	Application Programming Interface
ARN	Active Remote Node
AxC	Antenna Carrier
BBU	Base Band Unit
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BRAS	Broadband Remote Access Server
BS	Base Station
BSC	Base Station Controller
BSS	Business Support System
BTS	Base Transceiver Station
C&M	Control and Management
CAD	Collision Avoidance Device
CAL	CHARISMA Aggregation Level
CapEx	Capital Expenditure
CDN	Content Delivery Network
CHARISMA	Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access
CMO	Control, Management & Orchestration
CO	Central Office
COTS	Commercial Off The Shelf
CP	Control Plane
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CPRI	Common Public Radio Interface
CPS	Cyber Physical Systems
C-RAN	Cloud Radio Access Network
CT	Channel Termination
D2D	Device-to-Device
D2I	Device-to-Infrastructure
DBA	Dynamic Bandwidth Allocation
DC	Data Centre
DL	Downlink
DP	Data Plane
DPDK	Data Plane Development Kit
DPI	Deep Packet Inspection

DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSMIPv6	Dual-stack Mobile IPv6
DWBA	Dynamic Wavelength and Bandwidth Allocation
DWDM	Dense Wavelength Division Multiplexing
EDFA	Erbium Doped Fibre Amplifier
eNodeB	Evolved Node B
eNB	Evolved Node B
ePDG	evolved Packet Data Gateway
EPC	Evolved Packet Core
ETH	Ethernet
EU	End User
FCS	Frame check sequence
FEC	Forward Error Correction
FF	Fire Fighter
FPGA	Field Programmable Gate Array
FSO	Free Space Optics
FTTB	Fibre to the Building
FTTH	Fibre to the Home
FotF	Factory of the Future
FW	Firmware
GPON	Gigabit PON
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GTP	GPRS Tunnelling Protocol
HD	High Definition
HeNB	Home eNode B
HetNet	Heterogeneous Network
HGW	Home (or Hub) Gateway
HSR	High Speed Railway
HTTP	Hyper Text Transfer Protocol
HW	Hardware
ICI	Inter Carrier Interference
ICT	Information, Computing, & Telecommunications
ID	Identification
IFOM	IP Flow Mobility
IMU	Intelligent Management Unit
IoT	Internet of Things
IP	Internet Protocol
IPSec	IP Security
IQ	In-phase and Quadrature
iRRH	Intelligent Remote Radio Head
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITS	Intelligent Transport System

ITU	International Telecommunications Union
KPI	Key Performance Indicator
LAN	Local Area Network
L-GW	Local Gateway
LIPA	Local IP Access
LoS	Line of Sight
LTE	Long Term Evolution
mBS	Micro Base Station
mDC	Micro Data Centre
MAC	Media Access Control
MANO	Management and Orchestration
MAPCON	Multi Access PDN Connectivity
MDC	Mobile Distributed Caching
MME	Mobility Management Entity
MNO	Mobile Network Operator
MPLS	Multi-Protocol Label Switching
MTC	Machine Type Communications
N/A	Not Applicable
NaaS	Network as a Service
NAPT	Network Address and Port Translation
NF	Network Function
NFV	Network Functions Virtualisation
NGMN	Next Generation Mobile Network
NG-PON2	Next-Generation Passive Optical Network 2
NIC	Network Interface Card
NO	Network Operator
NoC	Network Operations Centre
NP	Network Provider
OA	Open Access
OBSAI	Open Base Station Architecture Initiative
ODN	Optical Distribution Network
OFDM	Orthogonal Frequency Division Multiplexing
OLE	Overhead Line Equipment
OLT	Optical Line Termination
ONF	Optical Networking Forum
ONT	Optical Network Termination
ONU	Optical Network Unit
OpenNaaS	Open Network as a Service
OS	Operating System
OSS	Operations Support System
OTDR	Optical Time Domain Reflectometry
OTT	Over The Top
PC	Personal Computer
PCIe	Peripheral Component Interconnect Express
PCS	Physical Coding Sublayer

PHY	Physical Layer
PMA	Physical Medium Attachment
PDN	Packet Data Network
P-GW	Packet Gateway
PIP	Physical Infrastructure Provider
PLOAM	Physical Layer Operations, Administration and Maintenance
PMD	Physical Media Dependent
PMIP	Proxy Mobile IP
PON	Passive Optical Network
PPP	Public Private Partnership
PSAP	Public Safety Answering Point
PtP (P2P)	Point-to-Point
PtMP (P2MP)	Point-to-Multipoint
QoS	Quality of Service
QoE	Quality of Experience
RAN	Radio Access Network
RAT	Radio Access Technology
RE	Radio Equipment
REC	Radio Equipment Controller
RNC	Radio Network Controller
RRH	Remote Radio Head
RTSP	Real Time Streaming Protocol
Rx	Receiver
SC	Small Cell
SDF	Service Delivery Framework
SDI	Serial Digital Interface
SDN	Software Defined Networking
SDO	Standards Developing Organisation
SGW	Serving Gateway
SIPTO	Selected IP Traffic Offload
SLA	Service Level Agreement
SMP	Symmetric Multi-Processing
SoA	State of Art
SOA	Service Oriented Architecture
SP	Service Plane
SP	Service Provider
SR-IOV	Single Root In/Out Virtualisation
SW	Software
TDM	Time Division Multiplexing
TETRA	Terrestrial Trunked Radio
TMF	TeleManagement Forum
TWAN	Trusted WLAN Access Network
TWDM PON	Time and Wavelength Division Multiplexed PON
Tx	Transmitter
UC	Use Case

UE	User Equipment
UHDTV	Ultra-High Definition Television
UL	Uplink
UMTS	Universal Mobile Telecommunications System
VI	Virtual Infrastructure
VIM	Virtual Infrastructure Manager
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VNFM	Virtual Network Functions Manager
VNO	Virtual Network Operator
VoD	Video on Demand
VOI	Vehicle of Interest
VPN	Virtual Private Network
VSF	Virtualised Security Functions
WAMS	Wide Area Measurement and Supervision
WDM	Wavelength Division Multiplexing
WG	Work Group
WLAN	Wireless Local Area Network
WP	Work Package
XGPON	10-Gigabit/s PON

**<END OF DOCUMENT>**