MOBILIZADOR 5G

Components and services for 5G networks

Project nº 24539

Deliverable D2.1

Use cases and requirements for solutions targetting 5G network core

Relatório D2.1

Casos de uso e requisitos de soluções para redes core de redes 5G

PPS	**Produtos e serviços para o core da rede**
Activity	**A2 – Especificações Técnicas**
Dissemination level	**Public**
Date	**March 2018**
Version	**1.0**

Cofinanciado por:

Lisb@20 20 COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Project Lider:
Altice Labs, S.A.
Rua Eng. José Ferreira Pinto Basto
3810-106 Aveiro – Portugal
http://www.alticelabs.com
Tel: +351 234 403 200
Fax: +351 234 424 723

Sumário executivo

O documento D2.1 fornece uma primeira visão geral das áreas de pesquisa alvo, soluções subjacentes e os requisitos de alto nível associados. Além disso, exemplos de casos de uso que integram as soluções identificadas são apresentados, com o objetivo de demonstrar como as múltiplas soluções alavancam os múltiplos avanços arquiteturais das redes core 5G, assim como interagem e dependem umas das outras para fornecer valor aprimorado em futuras redes 5G.

A primeira contribuição do Deliverable é a análise dos seguintes tópicos:

- Gestão de políticas

- Orquestração de serviços e recursos

- Garantia de serviço

- Segurança

- Serviços de suporte

- Plataforma de Virtualização

Para cada um dos tópicos referidos, o contexto necessário é fornecido, contribuindo com a informação prévia necessária antes de introduzir o foco de trabalho, as funcionalidades e mais-valias alvo.

A segunda contribuição do Documento é uma descrição na forma de história de dois casos de uso - 1) serviço vCDN e 2) Internet of Things (IoT) em serviços Public Protection and Disaster Recovery (PPDR). Cada um dos casos de uso contém um conjunto de subcasos com o objetivo de demonstrar o papel dos componentes anteriormente referidos em diferentes eventos e contextos. É também pretendido mostrar a relevância que cada subcase apresenta na ótica das futuras redes 5G.

Finalmente, e impulsionado pelo trabalho de integração desenvolvido nos casos de uso, são apresentados requisitos não finais de alto nível associados a cada um dos tópicos abordados.

Executive Summary

Deliverable D2.1 provides a first overview of the target research areas, underlying solutions and the associated high level requirements. Furthermore, example use cases, integrating the identified solutions, are presented, with the objective of demonstrating how the multiple solutions leverage the multiple architectural advances of the service-based 5G core networks, how they interact and depend on each other for delivering enhanced value in future mobile networks and applications.

The first contribution of the Deliverable is the analysis of the following addressed topics:

- Policy management
- Service and resource orchestration
- Service assurance
- Security
- Support services
- Virtualization Platform

For each of the referred topics, the necessary context is provided, contributing with essential prior information before entering in the work focus, target functionalities and associated gains.

The second contribution of the Deliverable is a story-like description of two use cases: 1) vCDN service and 2) IoT in PPDR services. Each of the use cases contains a set of subcases, with the goal of depicting the role of the previously referred components over different events. Care is taken in showing the relevance that each subcase is perceived to have in future 5G networks.

Finally, and driven by the integration work developped in the use cases, the non-final and high-level list of identified requirements associated to each of the addressed topics is presented.

Table of Contents

List of Figures

List of Tables

Glossary

5GC	5G Core
AAA	Authentication, Authorization and Accounting
AF	Application Function
AI	Artificial Intelligence
AMF	Access and Mobility Function
ANN	Artificial Neural Network
API	Application Programming Interface
BSS	Business Support System
CAPEX	Capital Expenditure
CCC	Command Control Center
CERT	Computer Emergency Response Team
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
DC	Data Center
D2D	Device to Device
DDoS	Distributed Denial of Service
DÉCOR	Dedicated Core Network
DevOps	Development and Operations
DNN	Deep Neural Networks
DNS	Domain Name Server
E2E	End-to-end
ECA	Event/Condition/Action
eMBB	Enhanced Mobile Broadband
EMS	Element Management System
EPC	Evolved Packet Core
FCAPS	Fault, Configuration, Accounting, Performance, Security
FW	Firewall
GAN	Generative Adverserial Network
GPU	Graphics Processing Unit
IDPS	Intrusion Detection and Protection System
IoT	Internet of Things
KPI	Key Performance Indicadot
LTE	Long Term Evolution
MANO	Management and Orchestration
MCPTT	Mission Critical Push to Talk
MEC	Multi-acess Edge Computing
ML	Machine Learning
NEF	Network Exposure Function
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFVO	Network Function Virtualization Orchestrator
NGMN	Next Generation Mobile Networks

NRF	Network Repository Function
NS	Network Service
NSI	Network Slice Instance
NWDAF	Network Data Analytics Function
O&M	Operations and Management
OODA	Observe-Orient-Decide-Act
OPEX	Operational Expenditure
OSS	Operations Support System
OTT	Over-the-top
PAP	Policy Administration Point
PCC	Policy and Charging Control
PCF	Policy and Charging Function
PCRF	Policy and Charging Rules Function
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PLMN	Public Land Mobile Network
PNF	Physical Network Funcion
PPDR	Public Protection and Disaster Recovery
PPS	Product, Process or Service
ProSE	Proximity Services
QoS	Quality of Service
RAM	Random Access Memory
RBM	Restricted Boltzmann machines
RNN	Recurrent Neural Networks
SON	Self Organized Networks
SA	System Architecture
SIEM	Security Information and Event Management
SDN	Software Defined Networking
SLA	Service Level Agreement
SMF	Session Management Function
TETRA	Terrestrial Trunked Radio
TR	Technical Report
TS	Technical Specification
UDR	User Data Repository
UHD	Ultra High Definition
vCDN	Virtualized Content Delivery Network
VIM	Virtualized Infrastructure Manager
VoD	Video on Demand
VNF	Virtualized Network Function
VNFC	Virtualized Network Function Component
VNFD	Virtualized Network Function Descriptor
VNFM	Virtualized Network Function Manager
WLAN	Wireless Local Area Network

1 Introduction

Recent advances and propositions in networking, including software defined networking (SDN), network function virtualization NFV) or even Multi-access Edge Computing (MEC) have all emerged and raised the Telecom industry interest with their promising advantages. Multiple selling points have been listed - and even hyped -, such as the potential CAPEX reduction enabled by the usage of generic equipment, greater scalability, high flexibility unlocked through network programability, OPEX reduction enabled by automated operation, quick service deployment and update, or even new monetization sources by means of disruptive and attractive business models. However, the shift to or adoption of these novel models by Mobile Operators has been slow and challenging, in much part due to inertia resulting from existing business chains and operational processes. One such source of inertia is the mobile architecture itself. The Evolved Packet Core (EPC), responsible for session and mobility management or security in 4G networks, is centered on rigid and business-constraining point-to-point interfaces which introduce strong dependency between functions, and consequently network "ossification"; this implies that the modification of a specific deployed network function requires reconfiguration and testing of each adjacent function before operating live. Thus, seeking to maximize the alignment with SDN and NFV, 5G Core follows a Cloud-native design and introduces a service-based model, where network functions interacting with other network function as required through the exposure of service-based interfaces. In other words, 5G architecture shifts from monolithic applications into loosely coupled (micro)services. Other key characteristics of 5G architecture which are aligned with the goals of SDN/NFV include the control and user planes separation or modular and reusable function design. With the architecture standardization almost complete, it is an adequate time for designing and identifying products (i.e. virtualized network functions and services) which fully leverage the mentioned benefits of the novel 5G mobile architecture.

This Deliverable studies use cases and associated requirements within the context of next generation (5G) mobile core networks, focusing in the following aspects:

- Policy management
- Service and resource orchestration
- Service assurance
- Security
- Support services
- Virtualization Platform

Moreover, and in order to more clearly demonstrate the capabilities expected both from 5G in general and specifically from the solutions being defined under PPS2, compelling scenarios are necessary. With this in mind, the deliverable then presents a set of use cases centered in different application contexts (e.g. content delivery using vCDNs, IoT and PPDR in 5G), in order to illustrate how the different components pertaining to the different areas - service and resource orchestration, network and service monitoring, security and authentication, support services - are expected to interact. For each use case, its relevance with respect to 5G context is presented, before providing a step-by-step description.

The document is organized as follows:

- Section 2 presents the scope addressed by PPS2, reflecting the considered 5G vision, and delimiting the areas in which contributions are provided;
- Section 3 presents in a detailed way each of the addressed topics, including background information and their relevance to future mobile networks;

- Section 4 introduces potential use cases of interest, exercising the multiple areas and their relationship. Each use case considers multiple steps where a preliminary vision of the interactions between modules / blocks - to be defined in Deliverable D2.2. - is shown;
- Section 5 presents and organizes multiple requirements derived both from the use cases and the operation of identified components.
- Finally, Section 6 concludes the Deliverable.

2 5G Networks and PPS2 scope

2.1 Introduction

5G architecture under the 3GPP standardization work has a much more strict scope than what is commonly referred in related industries or academia. Technological paradigms such as SDN, NFV or IoT have a close relationship with 5G, with the latter leveraging them and at the same time enabling them. Thus, the label 5G is usually used as a placeholder for all these new network-based technologies, creating a common path in terms of network evolution.

Considering the paramount role which mobile networks increasingly have across all sectors and environments, the value and impact expected from PPS2 products will not be restricted to that of the mobile network domain. Referring to the overall interest from Network Operators on a single common core infrastructure where all owned networks (e.g. wireless and fixed) converge using native interfaces, the 5G Core Network - and all Network Functions leveraging it - is expected to effectively employ a central / core role for every communication provider and service.

The contents and solutions addressed in PPS2 focus different components which are expected to employ a relevant role in a fully operational 5G core network. Such components may either represent:

1) components partially or fully implementing specific 5GC network functions, potentially extending it with additional capabilities; or

2) components interacting with 5G Core, coexisting in a 5G ecosystem but whose scope and operation goes beyond that of mobile domains.

It is thus important to highlight that PPS2 scope is not restricted to "3GPP's strict 5G", meaning that the resulting solutions are not exclusively applicable to 5G mobile access – an implicit consequence from the minimized dependency between access and 5G core networks.

Nevertheless, it is essential to introduce essential background on relevant standardization advances on 5G Architecture, Core and its management. Given its relevance in the mobile network management, orchestration and monitoring, a brief summary of ETSI NFV is also presented.

2.2 3GPP Standardization Work on 5G

The standardization of system and service aspects related to the next generation mobile system (5G) is addressed within 3GPP's TSG SA group. The scope includes the specification of service, feature and requirements, as well as the support of network management, security, charging and accounting, both from the user's and network functions' perspective (referred as Stage 1 and Stage 2, respectively; Stage 3 defines switching and signalling capabilities needed to support services from stage 1).

Greatly motivated by the need to take advantage of the developments in SDN and NFV technologies, 5G system, defined in 3GPP SA2, is the first mobile system adopting a service based model. As a consequence, all architecture elements may be defined as network functions whenever required, enabling them to offer their services via interfaces of a common framework to any other network functions - which may or not access the services, depending on permissions [1]. Besides the previously seen, commonly used reference points based architecture figures, which represent the specific interactions between network functions for providing system level functionality, and show inter-PLMN interconnection across various network functions, 5G service based principles can be depicted in

service-based architecture representations, which draw the (Core) Network functions with a single connection to the rest of the system. These architecture diagrams can be found in [2]. SA2's 5G stage 2 level specifications ([2], [3], [4]) include the overall architecture model and principles, eMBB data services, subscriber authentication and service usage authorization, application support in general, but also specifically for applications closer to the radio as edge computing. The 5G system architecture model uniformly enables user services with different access systems, like fixed network access or WLAN, from the onset. The system architecture provides interworking with and migration from 4G, network capability exposure and other functionalities.

The normative work on service-oriented management concept, architecture and provisioning, as well as all the functionalities required for management and charging for 5G networks [5] are currently being defined ([6], [7], [8] and [9]) under the umbrella of 3GPP SA5, and will be part of 3GPP Release 15. 3GPP SA5 addresses the management aspects of 5G networks and adopts the network slice concept defined in SA2. Network slicing is about transforming a PLMN from a single network to a network where logical partitions are created, with appropriate network isolation, resources, optimized topology and specific configuration to serve various service requirements.

This Deliverable addresses blocks pertaining to 3GPP SA5 (e.g. Network Management) and SA2. At this point in time, TSG SA specifications are still in a draft status, i.e. currently defined modules are either subject to change or completely undefined (e.g. SA5). Thus, the potential alignment of the introduced solutions, presented at a high level through the use cases, is scoped for a latter stage, and will be documented in Deliverable D2.2.

2.3 ETSI ISG NFV

Recent developments in the field of virtualization have been evolving, bringing a necessity of uniformization and standardizing these techniques and technologies. The ETSI model for NFV (illustrated in Figure 1) aims at uniform the usage and management of network function virtualization mechanisms. This model provides a base on which a development consensus can be built among operators and manufacturers.

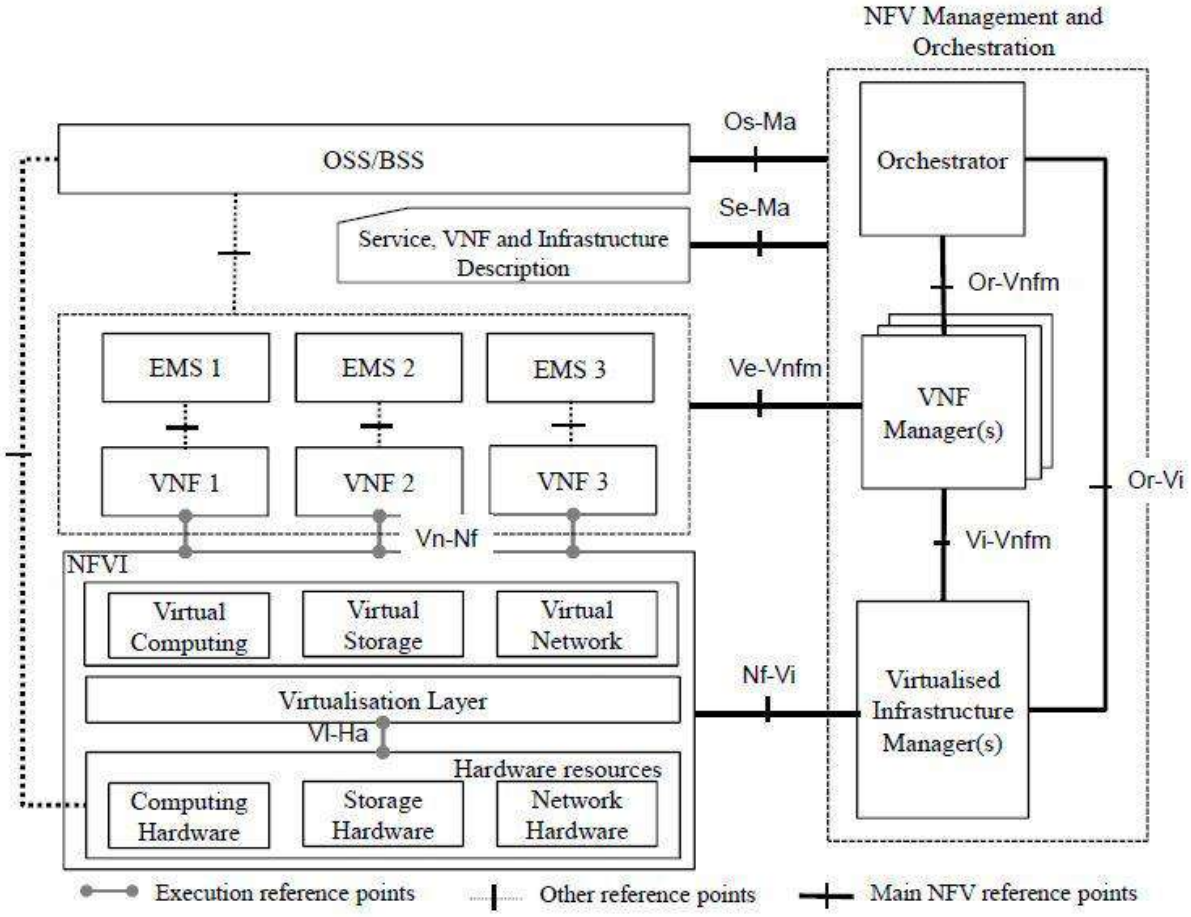

Figure 1 - ETSI NFV reference architecture [10]

This architecture can be divided into three main functional domains:

- NFV Infrastructure (NFVI) – Abstracts the computing, storage, and networking resources (using COTS equipment – Commercial Off The Shelf, accelerators, hypervisors) to provide support to VNF instantiation.
- Virtual Network Function domain contains the VNF instances, which are instantiated on the NFVI, including the Element Management System (EMS) that aids the integration with OSS and BSS systems.
- The NVF Management and Orchestration (MANO or M&O), which deals with the orchestration and management of hardware and software resources that support the virtualization infrastructure.

This architecture has a base a NFVI layer that using the physical resources, is capable of providing virtual resource pools (compute, storage and networking) using a virtualization layer. These resources will be used by the VNF (managed by the EMS). The MANO domain is transversal to the several layers of the virtualization architecture, being responsible for the management of virtualization tasks. Is composed by several components including VNF Managers that deal with the VNF instances lifecycle. It is also composed by the VIM, which manages the NFVI layer resources.

2.3.1 5G Network Slicing

One of the key concepts of the 5G evolution in comparison with the 4G is the network slicing capability [11]. In the new scenarios enabled by the 5G specification, network slicing becomes a relevant concept. In the NGMN (Next Generation Mobile Networks) definition [12], network slicing is a paradigm that enables an operator to subdivide its network into several logic sections [13]. These logic network sections/segments operate on a network infrastructure through an abstraction.

The division of the multiple network segments can follow several criteria such as isolation between logic network segments or several requirements such as throughput, latency, reliability. The requirements can have an impact on how the resources are instantiated (such as node location in a low latency scenario or the number of service instances in a redundancy scenario). The initial NGMN proposal divided network slicing into three main layers [12]:

- Service Instance Layer – Represents the services to be supported
- Network Slice Instance Layer – Can be composed by zero or more sub-network instances (that can be shared among many network slices)
- Resource layer – Composed by the physical resources

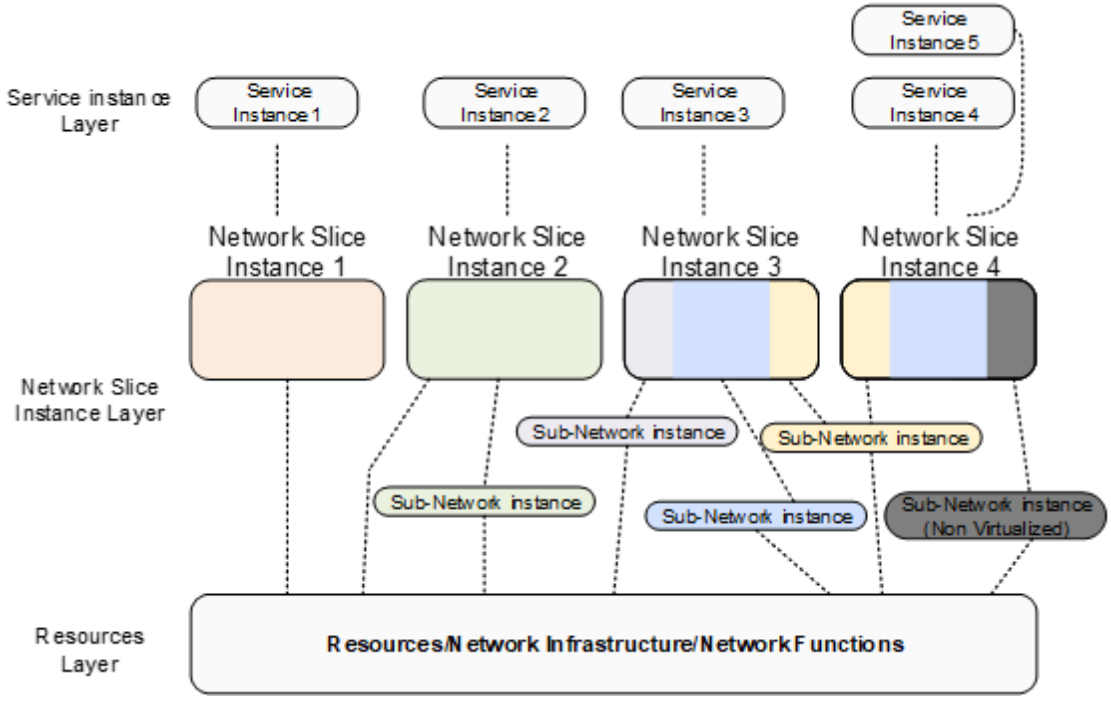

Figure 2 - Network Slicing Layers (adapted from [12])

The network slicing concept follows a set of seven main principles in terms of concept and operation [11]:

- Automation – Enables the on-demand configuration of network slicing without manual intervention
- Isolation – One of the fundamental properties, assuring the tenant safety
- Customization – Assures that the resources allocated to a tenant are used efficiently to achieve the service requirements
- Elasticity – Base principle to adjust the resources allocated to a specific network slice, enforcing an SLA defined for that service.

- Programmability – Enables the control of the services allocated to a network slice by third parties through APIs.
- End-to-End – Intrinsic property of network slicing, ensuring service delivery from its provider to the end client.
- Hierarchical abstraction – Property of recursive abstraction on which the resource abstraction is repeated in several hierarchical layers, each one offering a higher abstraction with a broader scope.

2.3.2 Mapping Network Slicing to ETSI NFV Architecture

The NFV and SDN paradigms are good candidates to implement network slicing [14]. Analysing the layers above represented in Figure 1 a mapping of the network slicing layers can be made to the ETSI NFV architecture [13]. This approximation can serve as base to support the necessary functions to enable the use of network slicing, namely for instantiation and operation. This mapping is illustrated in Figure 3 below.

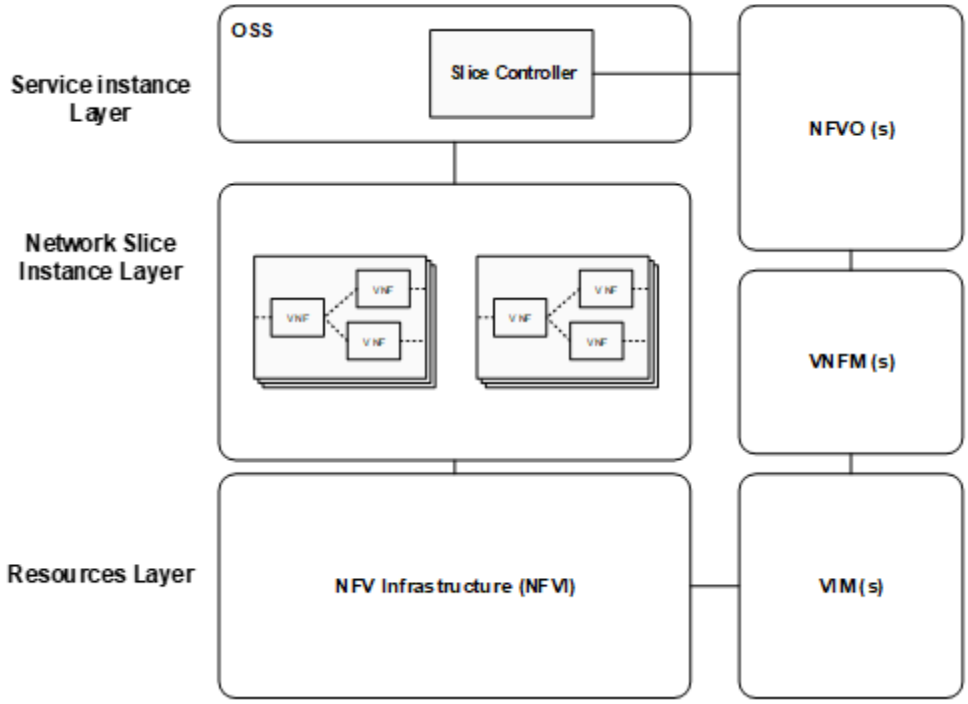

Figure 3 - Network Slicing mapping on the ETSI NFV model (adapted from [13])

Mapping the network slicing components on the ETSI NFV model can be done in the following manner [13]:

- Resource Layer is mapped in the NFVI and VIM components
- Network Slice Instance Layer is related with the network services managed by the NFV MANO functions
- The Service Instance Layer is a functional block of the OSS, which includes the Slice Control, being this a component responsible to assign network slices to services and to manage their lifecycle

This partial mapping can be fitted to some 5G scenarios. To be fully adapted some extensions to the ETSI NFV model may be needed [15].

2.3.3 Network Slicing in 3GPP

Previous mobile architectures attempted to introduce similar flexibility to that which Network Slicing provides, namely through specifications such as Décor (Dedicated Core Networks) or evolution eDecor (Release 14). However, previous specifications had several limitations comparatively to the Network Slicing introduced in the context of 5G architecture:

- Customization / configuration limited to the Control Plane and its procedures, i.e. services were bound to the same functional architecture
- No access for slice behavior configuration by third-parties (e.g. "verticals")
- No User Plane isolation
- UE bound to a single specífic Network Slice

In on-going 3GPP specifications [2], the behaviour of a Network Slice is realized via network slice instances (NSIs), i.e. activated network slices. Each NSI is composed by one or more Network Slice Subnet Instances (NSSI), which represent different segments or domains (e.g. Core, Access Network). This modularity enables independent lifecycle management of NSIs and NSSIs, with each instance going through "Preparation", "Instantiation, Configuration and Activation", "Run-time" and "Decommissioning" stages. Network slices (or subnet) instances lifecycle is depicted in the figure below:

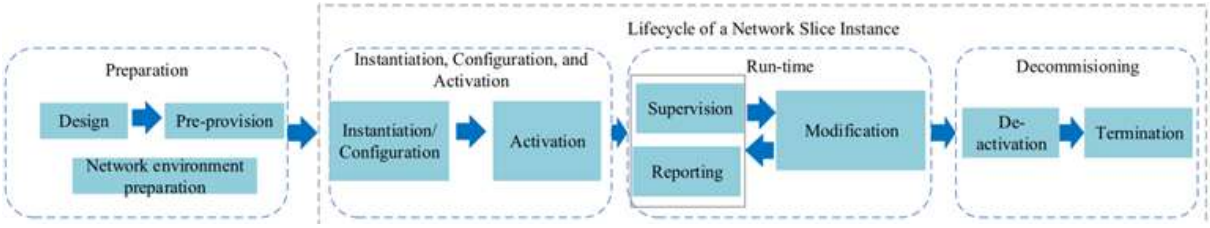

Figure 4 - Lifecycle phases of a NSI [16]

3 Addressed Areas

3.1 Introduction

The work in PPS2 is organized in six main technical subjects which are addressed from the perspective of 5G networks:

- Policy management and control
- Service definition and orchestration
- Service assurance
- Support mechanisms
- Security
- Virtualization platforms

The areas do not represent "independent" blocks, rather representing the focused objective or purpose. This has several implications in the relationship between the different technical areas, which will become clearer in future specifications. The motivation and vision for each of the referred areas is described below.

3.2 Policy Management and Control Mechanisms in 5G Networks

3.2.1 A context for Policy Management and Control

Network and service behavior is determined by rules that are applied at various levels whenever a decision needs to be made, either by humans, hardware systems or running software.

These rules are part of policies that are usually determined as a function of business or operational orientations, which should be structured in such a way that relations between them are clear and accountable. Unfortunatelly this is usually not the case, with policies and their associated rules being defined and managed for limited scopes, very far from a holistic approach.

In general terms, policy management and control structure is defined by a limited set of roles:

- Policy Administration Point (PAP): is responsible for the management of policies: the mechanisms for their creation, update and removal, and all the necessary validations. The PAP is also responsible for deploying policies to the entities that will carry on the decisions (PDP).
- Policy Decision Point (PDP): Makes decisions according to the established policies and checks whether they are properly enforced.
- Policy Enforcement Point (PEP): Applies the decisions of the PDP.

In 5G, an architecture for policy control has already been defined (refer to next subsection) for the scope of session management, charging, service data flows (gating, QoS, credit control), access and mobility.

In the project, policies and their interrelations will be explored in a wider scope, including policies related to operations management and control, like those associated with service orchestration, and policies related to the virtualized infrastructure management, and to network programmability.

The Use Cases proposed hereby describe scenarios broader then the strict policy management and control. Hence, key aspects of policy are disributed across the Use Cases, but no exhaustive UC enumeration is done for this subsystem.

3.2.2 Policy Control for 5G

For Release 15, 3GPP has already defined the stage 2 (Architecture) of a Policy and Charging Control (PCC) Framework for the 5G System [4]. In this recent Technical Specification, the functions of a Policy Control Function (PCF) are described in some detail, as well as the relations that this functional block has to keep with each function of the rest of the 5G Core.

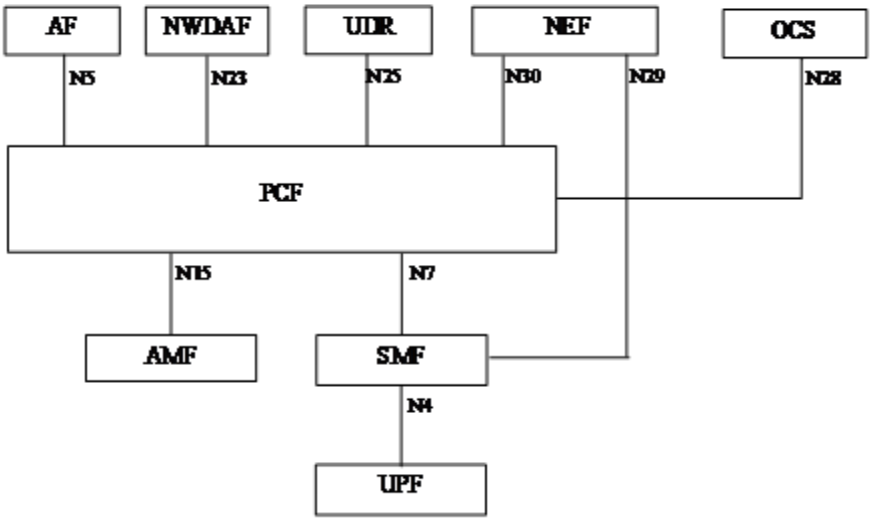

Figure 5 - PCF Framework reference points [4]

This figure highlights the relations that a PCF will have with other functions. The shown reference points represent integration points between a 5G PCF and other functions, which are particularly relevant to guarantee a functional Core for this project. Some, of particular importance in the scope of this project are:

- AF-PCF (N5): Corresponds to the interface that is used by network applications to make requests to the PCF (eg, requesting QoS for a particular session/flow) and receive notifications of relevant events. This is the basic interface to be used for making service related requests to the PCF in Use Cases that involve requesting for a specific QoS at session time or subscribing to specific network events.
- NWDAF-PCF (N23): Corresponds to the interface between network monitoring and analytics and the PCF for the events/reports that will trigger policy decisions on the PCF. Use Cases that involve collecting, processing and analyzing data from various sources and feeding it to the PCF policy motor will use this interface.
- UDR-PCF (N25): To access and store policy control related information from/to the UDR
- NEF-PCF (N30): Interface for the negotiation of policy and charging control behavior between PCF and NEF, like Service specific policies, sponsored data connectivity, or AF-influenced traffic steering.

- AMF-PCF (15): Interface to provide Access and Mobility Management related policies to the AMF, and to collect mobility and registration/deregistration information to the PCF
- SMF-PCF (N7): This is the functional interface of PCF to session control, used mostly for conveying the enforcement of policy decisions made by the PCF that are related to session control, either on its establishment or running state. Also session related network events are carried from the SMF to the PCF through this interfaces, as well as its filtering rules from the PCF to the SMF

Like in the overall 5G architecture, the functional - reference point based - architecture is complemented with a service-oriented view, which favours an IT-based software approach.

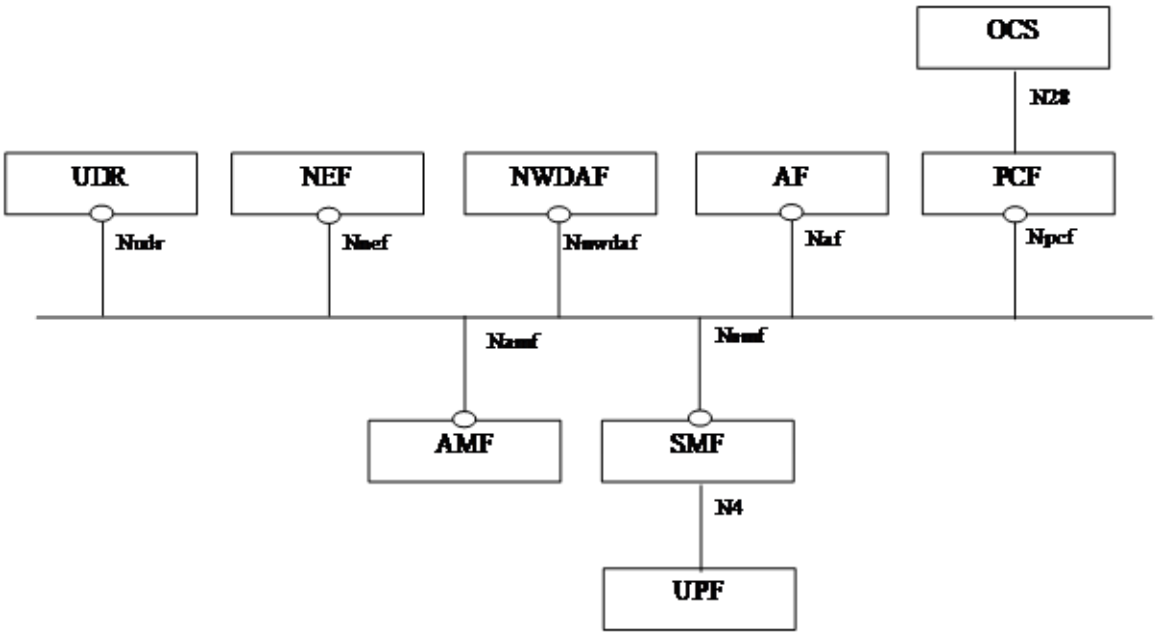

Figure 6 - PCF Framework Service View [4]

This PCC architeture sets the standard and determines the path to be followed from the 4G PCRF function to a 5G Core Policy Control Function. Nevertheless, the ambition of the policy framework being proposed here is bigger than just the control aspects of 5G sessions. For the sake of clarity and to have an evident separation of what is strictly 5G Control plane from other management aspects, the PCF function will be henceforward represented separated from a more general Policy Framework, as proposed in the next section.

3.2.3 A wider approach

Apart from Policy Control at the 5G core, as briefly described in the section above, policies are present everywhere, from low-level protocol behavior, to strategic management. They are described using different languages and applied under distinct paradigms, and managing them as a consistent and coherent whole is often considered an impossible mission… Nevertheless, to achieve the desired autonomic behavior, policies have to be addressed – if not as a whole – at least as a manageable universe.

The ongoing work of ETSI ISG ENI (Experiential Network Intelligence) [17] point to the use of mechanisms like those of Artificial Intelligence to deal with this problem. Also, projects like ONAP (Open Network Automation Platform) [18] try holistic approaches for policy creation and administration.

For NFV, ETSI NFV Industry Standards Group make important considerations on how policies may be distributed within the MANO ecosystem [19]. Also, in its principles, SDN which relies on centralized policies, needs to manage these policies in a way that assures its consistent application to a logically centralized controller (although physically distributed).

In the scope of this project, a Policy Framework (PF) that can be used as a common Policy Administration Point as well as a Policy Decision Point for some high level management policies is proposed. The 5G Policy Decision Point (PCF) is kept separated, as a control-level entity that receives its policy rules from the PF. Both entities (PCF and PF) are proposed in the scope of PPS2. A PF is naturally supposed to manage/administer policies that are decided upon by other Core or Management functions, also present in the PPS2 ecosystem.

The following figure illustrates the roles of PF and PCF in the context of an overall policy architecture for PPS2:

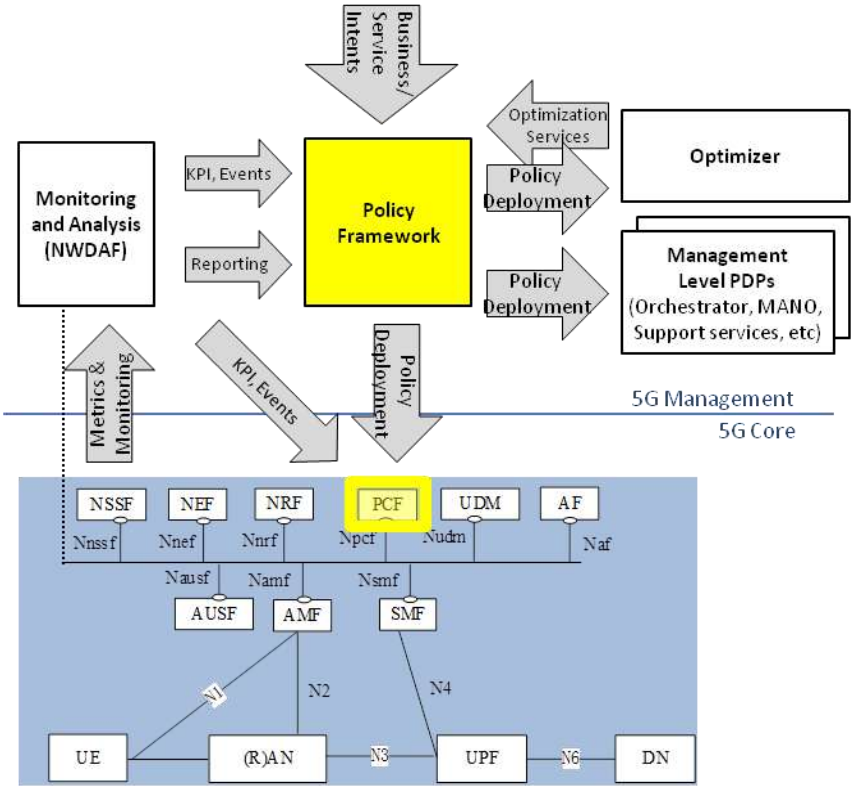

Figure 7 - Policy Framework context in PPS2

For the general Use Cases that are proposed in this documents, Policies are expected to flow from the PF into the PCF and other PDPs, where they are installed and determine decisions, typically in an ECA (Event/Condition/Action) manner.

3.3 Service Definition and Orchestration Mechanisms in 5G Networks

3.3.1 Introduction

A telecommunications operator's architecture is logically divided in several layers, in which the upper layers deal with products and marketing domains and the bottom ones relate to resources. TM Forum Frameworx [20] is the most known architecture model and is the current reference for most service providers. Typically, it is divided in two systems:

- Business Support Systems (BSS) – it includes all components realizing the service provider business model and is where all the interfaces towards the customer are located. It comprehends four main processes: product management, customer relationship management, revenue management and order management
- Operation support Systems (OSS) – it includes all components involved in resource and service management. The components present here collaborate to provide the following functionalities: infrastructure management and planning, service provisioning, monitoring and assurance, billing and customer care.

The Orchestration domain addressed in this document is limited to OSS systems, which means that details relating to service provider's business model will not be taken into account.

Traditionally, the word Orchestration in telecommunications refers to the coordinated execution of workflows, consisting of operations on top of services and resources which may be contained in several domains. Within the scope of ETSI ISG MANO, the word Orchestration takes a similar but distinct meaning as it regards operations on top of virtualized resources, normally located in datacenters. To distinguish between the different meanings of Orchestration [21], [22], the concept of End-to-End Orchestration was introduced to refer to multi-domain orchestration, while NFV Orchestration relates to ETIS ISG MANO specification, see Figure 8.

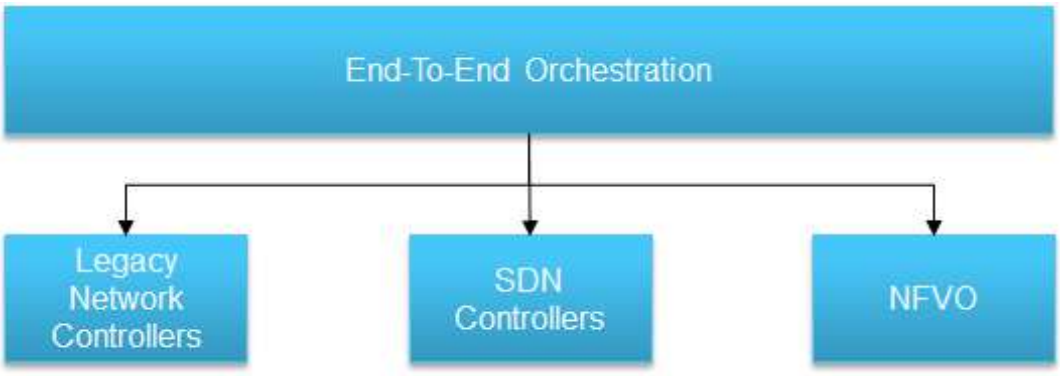

Figure 8 - End-to-End Orchestration overview

The following components are shown on the figure above:

- Orchestration E2E – component in charge of infrastructure mediation, enabling the complete lifecycle management of all domains and services under the administration of network operators
- Legacy Network Controllers – network controllers for specific and non-virtualized technologic domains, normally they also provide that domain's FCAPS interfaces. Nevertheless, since a

running virtualized network function (VNF) should not be distinguishable from their physical counterpart , they can also be used to control VNFs

- SDN Controllers – network controllers for domains where the control plane is decoupled from the data plane, typically SDN domains, independently of the network elements being virtualized or not
- NFVO – orchestration component for NFV domains following ETSI ISG NFV specification

It could also be considered the component responsible for slice orchestration, i.e. Slice Orchestrator, but it is not clear at the moment if there will be an explicit component for this role or if its functionality will be spread between the other components. If there is a component responsible for the realization and management of slices, it could be placed in parallel with the NFVO and interfacing the southbound of the E2E Orchestrator.

3.3.2 Service Provisioning

The process of provisioning a service consists on the execution of a variable number of operations on top of resources, in which the final result is classified as a success when the end client is able to use the contracted service.

Independently of the event that triggers a service provisioning – it may be the result of a client's request through the traditional customer channels or through a subscription portal – at the OSS level it usually starts with a request made to the E2E Orchestrator. The figure bellow showcases the usual steps performed during a service provision prior the infrastructure mediation, highlighting the main interactions between the various components. The step zero shown in the figure comprehends the distribution of policies by the Policy Framework before any service request being made. Every time a policy is created, updated or deleted from the Policy Framework, it will distribute all new or updated policies to relevant policy decision points, e.g. Optimization Framework.

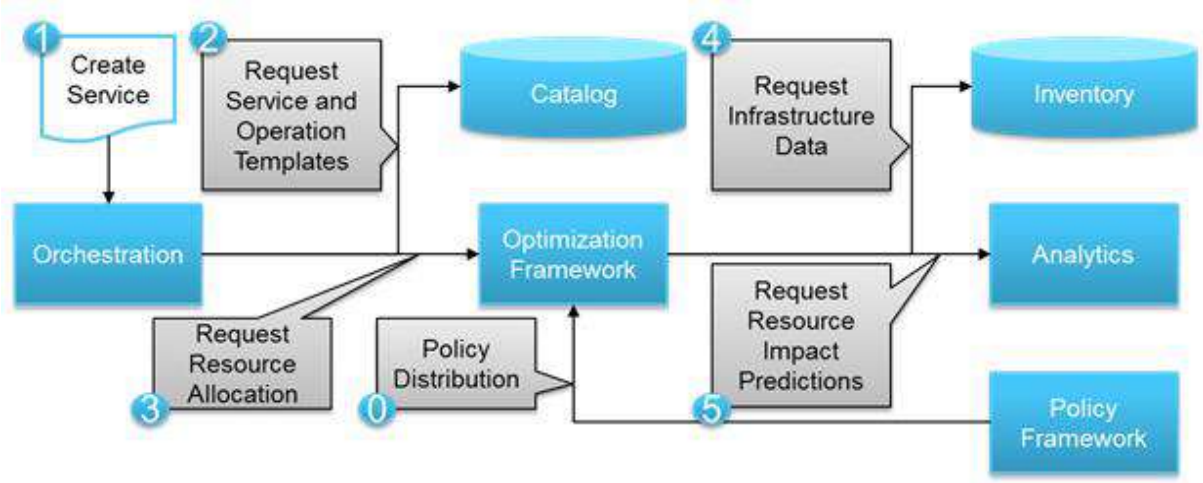

Figure 9 - Service provisioning generic workflow

The following steps are shown in the figure (with the exception of step 0):

1. The Orchestrator receives a request to provision a service
2. The Orchestrator will retrieve the operation template stored on the catalogue and after validating the service request, it will start the execution of the workflow defined for the operation
3. The resource allocation process defined on the operation workflow, is performed by the Optimization Framework

4. After receiving the request for the service resource allocation, the Optimization Framework retrieves all relevant infrastructure data from inventory systems so that it can map the resources defined on the template in available infrastructure resources
5. To mitigate future constraints on the infrastructure and/or services, the Optimization Framework uses Analytics to estimate the impact of the Service Provisioning operation

At the end of the step 5, the Optimization Framework processes all the gathered information to formulate a recommendation to the Orchestrator identifying all the resources allocated to the service. In turn, the Orchestrator is able to provision the various service components using the recommendation provided by the Optimization Framework and the information stored on the operation template.

3.3.2.1 Services and Resources Optimisation

Service and resource optimization is part of the major operational challenges network operators have to face [23]. At the OSS level, being the resource allocation one example, decision-making is based on static rules, which brings severe constraints to efficiency by not taking into account the operation's context. With the network evolution according to the 5G architecture, and considering technologic paradigms such as SDN and NFV, the loss of efficiency is further augmented. Services and resources in 5G environments are foreseen to be highly customizable, making individual deployments very context-driven which makes even harder their generalization. Thus, it is imperative to address the need for services and resources continuous optimization and take advantage of the more granular control enabled by the logically centralized architecture of SDN and of the efficiency and dynamicity associated with the NFV model.

The evolution for the next generation OSSs is happening in parallel with the evolution for 5G networks, and among the key aspects the following three are included [24]:

- Services model-driven integration – the newer languages for service templates are more oriented towards recursivity and reutilization of component models, which allow more agile approaches for service integration (i.e. faster time-to-market) and the decoupling between service definition and implementation
- Analytics driven by Artificial Intelligence (AI) – the use of cognitive mechanisms in analytics strengthen a richer context-aware characterization of services and resources while fostering learning at the OSS level
- Policy-based Management – the new policy systems make use of declarative policies and intents to enable distinct teams, ranging from business to engineering, to define policies to govern autonomous processes at the services and resources management layer

Taking into account these aspects, an Optimization Framework should integrate different data sources (such as inventories and/or analytic applications depending on the optimization algorithm) policy systems and orchestration templates for a more holistic approach, see Figure 10. The ONAP Optimization Framework Project [25] is one example of this approach regarding optimization in network management.

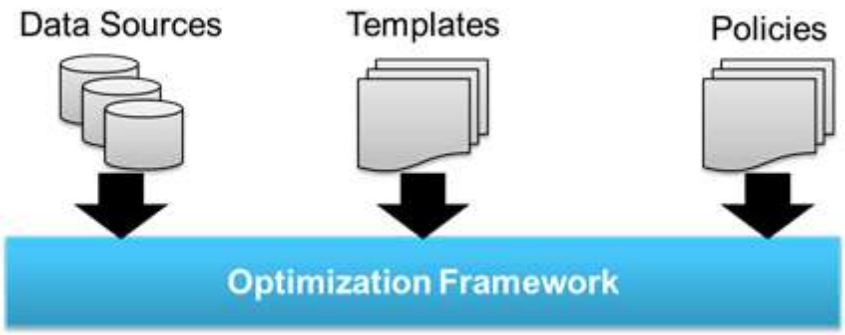

Figure 10 - Data source examples for Optimization Framework

Still on the subject of next generation OSS, an Optimization Framework should be seen as support service which can be invoked by any of the remaining components when necessary, see Figure 11. It should also adopt a modular approach regarding implementation to enable the integration of new optimization algorithms, extending existing ones and the integration with different orchestration-based systems.

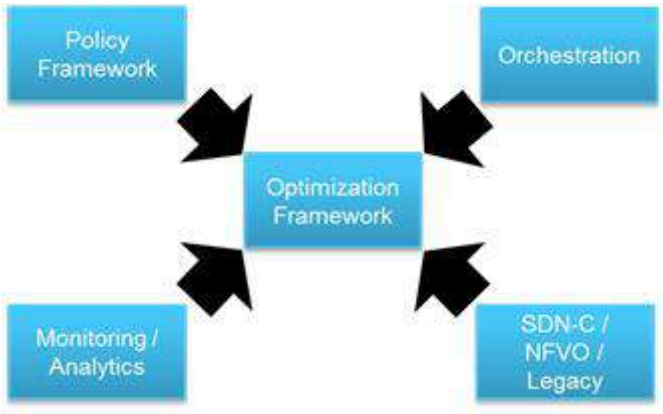

Figure 11 - Optimization Framework operational context

The foreseen transformation for the next generation OSSs, in which the continuous optimization is included, will allow network operators to improve efficiency by using policies to govern services and resources management. For example, a network operator may design a policy that says that resource optimization should maximize performance during peak hours and minimize energy consumption for the rest of the time. This is just an example on how to enable continuous optimization and dynamic adaptation to context and related goals. From the 3GPP perspective regarding 5G Networks the following use cases are being considered for network and radio optimization [26], [27]:

- Coverage and capacity optimization
- Mobility load balancing
- Mobility robustness optimization
- Inter-cell robustness optimization
- Energy saving management
- Random Access Channel (RACH) optimization
- Self-Organized Networks (SON) for Adaptive Antenna Systems (AAS)

3.3.3 Service Scaling

One of the greatest advantages brought by virtualization is the capability to scale services depending on the resources and service usage. Although network operators have been using alternative mechanisms and strategies to overcome these challenges in legacy networks, e.g. overprovisioning of resources, they should not be compared with the dynamicity of the ones available with virtualization. In case a service shows signs of high resource usage, two different responses may be used:

- Vertical or horizontal resource scaling - if there are resources available on the infrastructure, the orchestration components can request vertical scaling, by increasing the number of resources assigned to individual instances of components (e.g. increasing CPU or RAM in single VM), or horizontal scaling, by increasing the number of instances of individual components (e.g. deploy a second instance of a specific VNF)
- Scaling using neighbor infrastructure - if there are no available resources in a specific zone of the network operator infrastructure, it may use an adjacent zone to provide the needed resources. In this case, the adjacent zone may be used to provide only the needed resources or alternatively to be used for a complete or partial service migration.

From the service and resource management point-of-view, the figure below showcases how the several components may interact to support the before mentioned scaling operations.

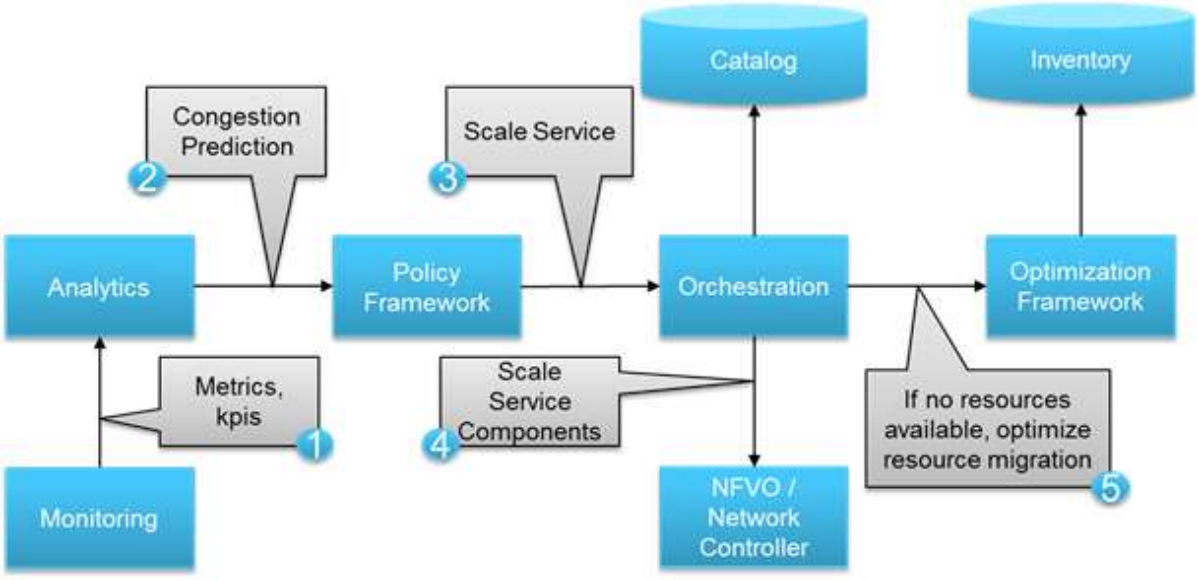

Figure 12 – Service Scaling generic workflow

The following present a more complete description of the various steps:

1. The monitoring components realize the data collection and aggregation while making all the data available for Analytics
2. Analytics predict a congestion scenario (basing on service and infrastructure usage history) and notify the Policy Framework
3. The Policy Framework evaluates all active policies and requests the Orchestration components to scale the service
4. Depending on the type of components to be scaled, network or compute based, Orchestration components send the appropriate request to network controllers or the NFVO respectively

5. In case there are no resources available, Orchestration components may invoke the Optimization Framework to optimize the resources allocated to services within the area, thus triggering a complete or partial migration of low-priority services

Although, neither the catalogue nor the inventory are explicitly referenced, these components contain the required information for normal functional behavior of Orchestration and Optimization systems. As in the previous scenario, the distribution of policies by the associated system is implicit and prior the start of this scenario.

3.3.4 Small and Big Orchestration Loops

The use of the E2E Orchestrator in service level operations enables all management capabilities through the coordination of all involved domains. Nevertheless, in some situations the response to a network event might be constrained to a single domain, making the use of the E2E Orchestrator redundant. In these situations and as long as the inventory is updated with all relevant changes, i.e. preserving the consistency of the stored data, it is possible to directly invoke the northbound interface of the NFVO or network controller and bypass the E2E Orchestrator. The latter represents the small orchestration loop while the former, using the E2E Orchestration, is called big orchestration loop.

One example of an operation using the small orchestration loop is when a VNF stops responding and a healing operation is triggered. In this case, the healing operation is limited to the datacenter domain and all resource orchestration is limited to the NFVO, see Figure 13.

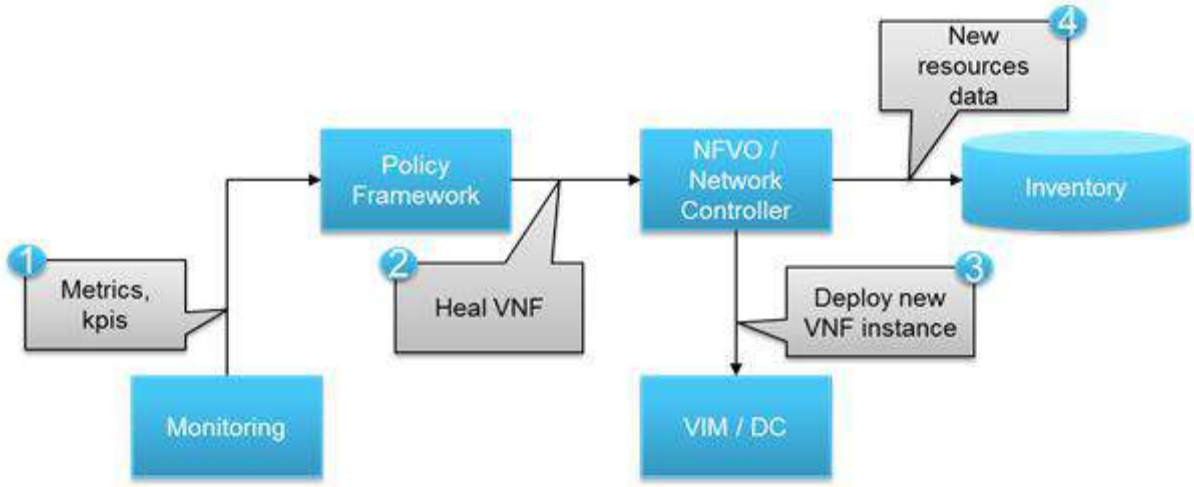

Figure 13 - Management systems control loop example

The steps shown are the following:

1. The monitoring components through the various available sensors identifies a problem with a VNF and generates an alarm which is captured by the Policy Framework
2. By analyzing the alarm, the Policy Framework determines the need to heal the VNF and interacts with the NFVO
3. The NFVO receives the request to heal the VNF: it starts destroying the VNF instance and afterwards deploys a new instance of the VNF
4. The NFVO updates the central inventory with the ids of the new resources related with the service

At the end of step 3 and on normal circumstances, the service will be up and running again, thus resolving the problem with the use of the small orchestration loop. Nevertheless, in some cases the

NFVO might be unable to resolve the problem, which means a new alarm must be generated. The response to the second alarm should involve the E2E Orchestrator, this way the response to the alarm can use more complex operations such as the partial or complete migration of the service. If the worst case scenario becomes true and the E2E Orchestrator is not able to heal the service, then it must send a notification to the other systems about the inability to resolve the problem.

It should be noted that if the NFVO is also a policy decision point (PDP), then monitoring components may invoke directly the NFVO instead of the Policy Framework.

3.3.4.1 Observe-Orient-Decide-Act Loop

Current network are evolving into Self-Organized Networks (SONs) by using the Observe-Orient-Decide-Act decision loop (OODA). This transformation is being performed gradually by making service and resource management more autonomous, and consequently reducing the cost of managing networks which are becoming more complex and dynamic [28]. The OODA Loop"is a learning system, a method for dealing with uncertainty (...) or put another way, the OODA Loop is an explicit representation of the process that humans beings and orgganizations use to learn, grow, and thrive in a rapidly changing environment", which was developed by Coronel John Boyd during the analysis of combat scenarios [29]. The four points present in the loop are the following:

1. Observe – data collection
2. Orient – data analysis
3. Decide – decision-making
4. Act – decision enforcement

The OODA loop is a vital point in the process of making network management more autonomous, because it enables the use of mechanisms based on AI to assist when making decisions.

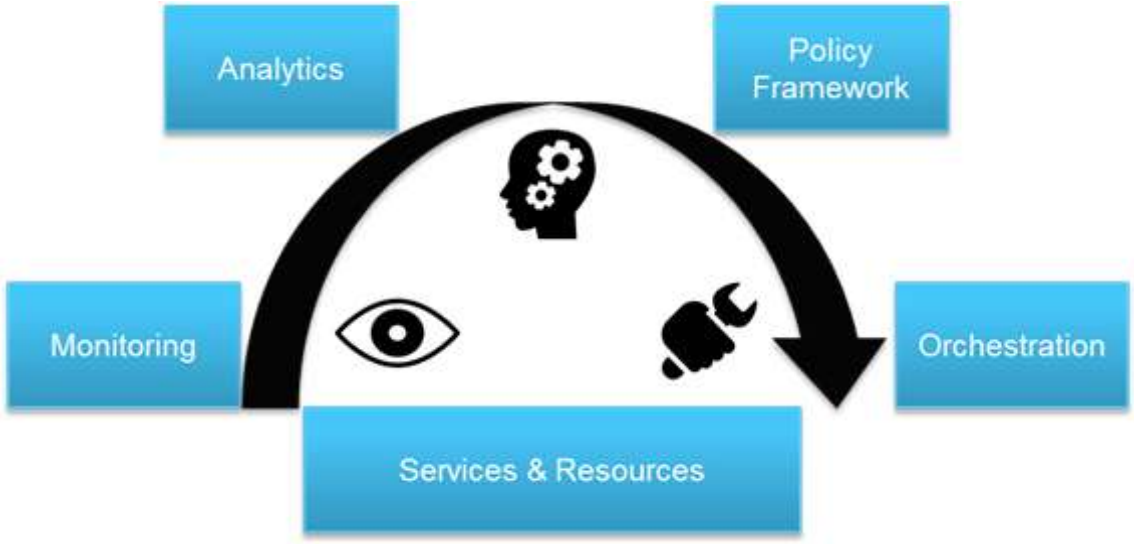

Figure 14 - Continuous OODA loop in Network Management

The loop is realized in continuous loop that involves monitoring, decision making and orchestration in a way that enables learning, see Figure 14. The vision in the loop is realized using monitoring and analytic components, being the latter able to obtain non-direct information and learn, usually by using machine learning mechanisms. Afterwards, by combining analytics and policies, a decision is made to be enforced by orchestration components. Finally, after the enforcement, the loop is once again restarted, with the monitoring and analytic components assessing the success and efficiency of the decision, thus enabling the system to learn and to correct previous decisions.

3.4 Assurance in 5G Networks

3.4.1 Introduction

Telecom Operators has historically struggled both economically and operationally with the dependence on proprietary hardware for service provisioning. The cost of the devices, the logistics required for its installation, space, energy and specialized personnel for integration and operation, were all contributing to make the launch of new services in the market a slow and difficult process.

In order to overcome this problem new virtualization paradigms were needed, which led to the consideration of the Network Function Virtualization (NFV) model. The paradigm allows the consolidation of proprietary equipments for Telecommunications services into generic equipments, leaving operators free to worry only about the development of new software services. In this way, a service can be decomposed into a set of virtual network functions (VNF), which can be implemented in software and made available on one or more virtualized servers. VNFs can be reallocated to different network locations without the need for new hardware installations, thus providing greater flexibility for the operator's network.

Cloudification and automation are now keys to push the limits of 5G technology and manage the massive number of network connections with different requirements. It will help networks to efficiently automaticly scale on demand across core and edge and have inteligent algorithms to address all the network complexity.

Service assurance, will garantee that services offered over networks meet a pre-defined service quality level for an optimal subscriber experience, encopassing the following:

- Fault and event management
- Performance management
- Probe monitoring
- Quality of service (QoS) management
- Network and service testing
- Network traffic management
- Customer experience management
- Service level agreement (SLA) monitoring
- Trouble ticket management

The new 5G features will require service assurance application to adapt to the new reality, where managed elements will grow exponential and the vertical bussinesses on the network will need to be addressed separately using the new slice paradigm. The next chapters will detailed the main addressed areas for assurance.

3.4.2 Multi-Tenancy O&M Support for 5G Networks

The 5G network slices are designed from the ground up to offer and support classes of services (e.g. eMBB, mcIoT). This is a paradigm shift from past networks, which were primarily built to offer connectivity. With this approach, the 5G network slices will have unique capabilities that are required for the supported group of services. Moreover, the capabilities of each slice can be dynamically optimized to meet the specific needs of individual services.

Dynamic 5G network slices can be easily designed by packaging the necessary network capability units into a forwarding graph. Network slices can be created dynamically by orchestrating these forwarding

graphs on a distributed cloud infrastructure using proven orchestration and management technologies. A template-based approach can be used to ease the creation of slices and to eliminate routine errors. The templates can be used to create various Network Slice Instances and then each NSI can be further customized based on the needs of supported services, use cases, or business models.

Creating more network slices inherently adds complexity to network operations and ongoing optimization efforts. Therefore, the dynamic network slices are designed to enable maximum possible automation of operations and optimizations. Automation is enabled by analytics, machine learning, network big data, and network programmability. For proper automation of O&M functions, an overall view of the physical network is needed to respond to the requirements of the hosted NSIs. Availability of aggregated monitoring data from all NSIs will be accomplished by multi-tenancy support at the monitoring application level.

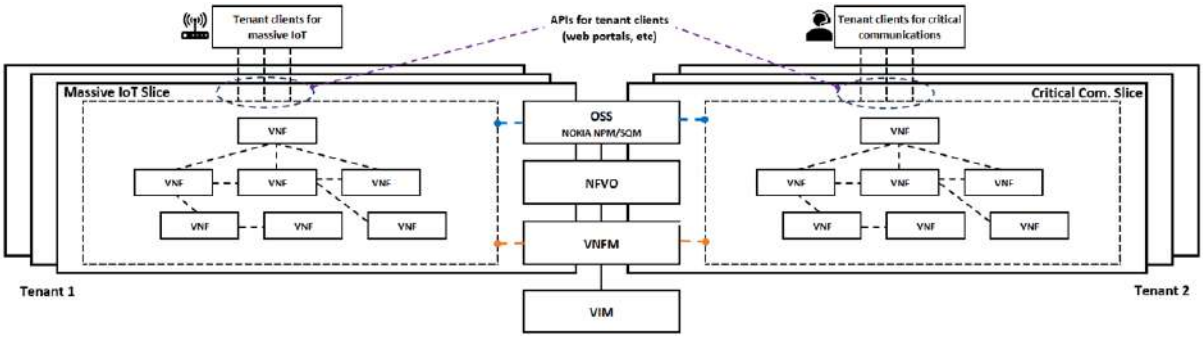

Figure 15 - Multi-tenancy support for 5G monitoring applications

Software-defined networking (SDN) and network function virtualization (NFV) will play an important role in the shift to network slicing. Virtualization will enable separation of the software from the hardware and offer the possibility to instantiate many functions on a common infrastructure. With this approach, the infrastructure can be shared by different tenants and provide different services.

Multi-tenancy support is at the core of the cloud architecture, it enables VNFs to share the same resources by reducing the overhead over multiple single-tenant application instances. Maximized usage of resources will lead to reduction in investment cost which will create savings for operators and hence will make the cloud architecture more attractive. With a multi-tenant architecture, performing centralized updates, maintenance and customization is possible, and the level of granularity using common tenant management tools is significantly higher when compared to single tenant applications that can require multiple management tools aligned with the application versions deployed on the field. In this regard, the concept of DevOps will assume a major role.

However, developing a multi-tenant application is significantly more complex. Some of the common arguments raised against multi-tenancy can be reconciled to the simple fact that customer data resides in the same application and or database. Despite the vast array of fail-safes, security measures, and encryption techniques available to mitigate risk, in the end a shared resource is being used and that means there will be some (at least theoretical) security and performance trade-offs in certain circumstances.

3.4.3 FCAPS data integration for 5G elements management

Fault, Configuration, Accounting, Performance, Security (FCAPS) data integration for 5G network VNFs/PNFs will face new challenges and will need to fulfill new requirements. Open interfaces and

standard metadata specifications are needed due to the new dynamic 5G architecture and for the support of the new functional and lifecycle capabilities of the VNFs.

Element Management (EM) will be the central piece and standard FCAPS need to to be extended to support the new 5G features:

- Alarm correlation (between application and VM-level alarms)
- Real time data ingestion (that will enable the development of advanced analytics and machine learning use-cases).
- Auto VNF integration, configuration, topology-update and termination.

3.4.4 O&M integration for 5G networks

ETSI has defined a standard and base architecture for companies - e.g. both traditional vendors and software companies - to create NFV-based products and protocols. In this sense, new monitoring solutions require the support of the necessary interfaces defined by this organism to provide management functions for the new entities NFV Orchestrator and VNF Manager (VNFM).

Cloudification and automation are now keys to push the limits of 5G technology and manage the massive number of network connections with different requirements. VNFM needs to support automatic instatiation and scaling of VNFs in the network and NFVO needs to provide arbitration capability for the increasingly dynamic nature of the cloud to help networks to efficiently scale on demand across core and edge. Automation introduces/requires a template-driven approach where VNF properties can be described in a metadata model allowing for support for new VNF releases without software updates to O&M and have this model artefacts consumed by various O&M components (NFVO, VNFM, EM).

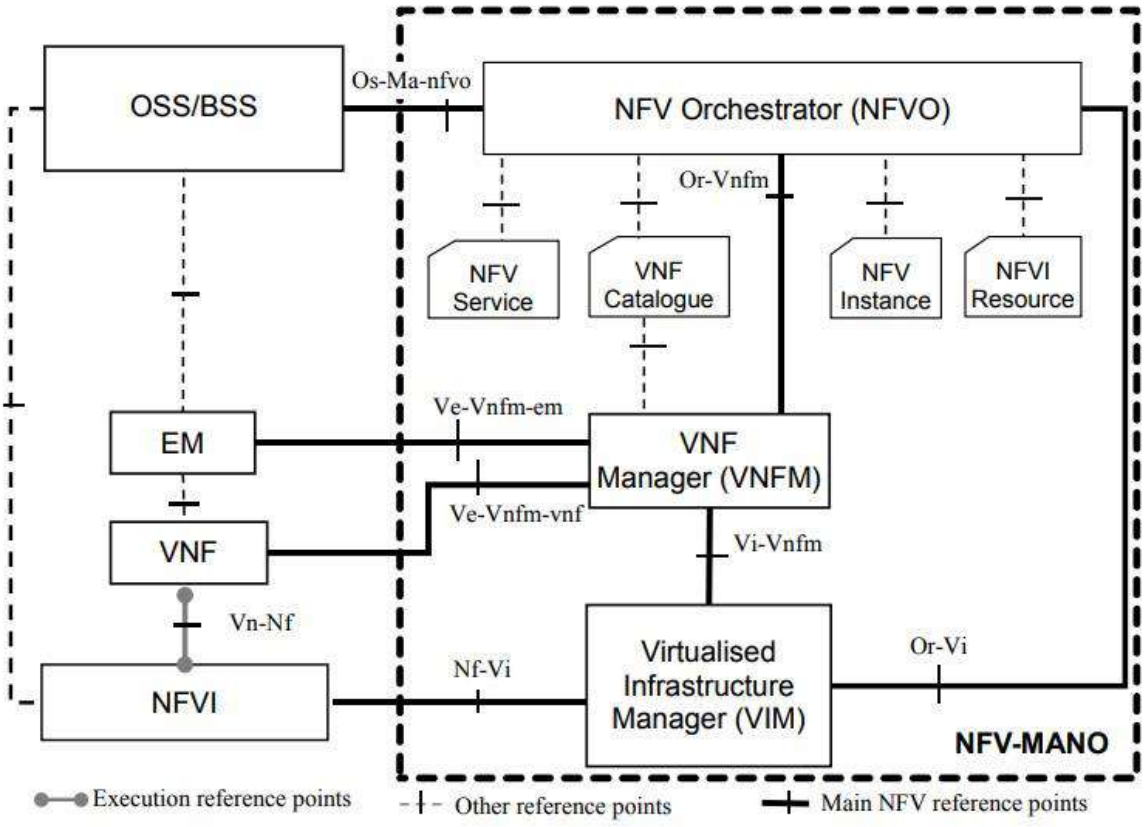

Figure 16 - The NFV-MANO architectural framework with reference points [30]

For assurance purpose, products will need to provide standard interfaces to enable OSS/BSS and EM comunication with the MANO NFVO and VNFM new elements. The ETSI reference model will be used as base.

3.4.4.1 OSS/BSS and NFVO

The Os-Ma-nfvo MANO reference point is used for exchanges between the OSS/BSS and the NFV Orchestrator (NFVO), and on this project the following interfaces will be addressed:

- NS Performance Management: This interface allows providing of performance information (measurement results collection and notifications) related to network services. Performance information on a given NS results from either collected performance information of the virtualised resources impacting the connectivity of this NS instance or VNF performance information, resulting from virtualised resource performance information, issued by the VNFM for the VNFs that is part of this NS instance.
- NS Fault Management: This interface shall allow the NFVO to provide alarms related to the NSs visible to the consumer. An alarm on a given NS results from either a collected virtualised resource fault impacting the connectivity of the NS instance or a VNF alarm, resulting from a virtualised resource alarm, issued by the VNFM for a VNF that is part of this NS instance
- Network Service (NS) Lifecycle Change Management: This interface allows the OSS/BSS to invoke NS lifecycle management operations towards the NFVO.

3.4.4.2 Element Management and VNFM

The Ve-Vnfm-em MANO reference point is used for exchanges between EM and VNF Manager, and on this project the following interfaces will be addressed:

- VNF Lifecycle Management: This interface performs the lifecicle management of VNF based on requirements defined in the template. It includes several VNF functions like instantiation, scaling update upgrade and termination.
- VNF Lifecycle Change Notifications: This interface will notify all VNF changes like, VNF information attribute value change as well as the creation/deletion of a VNF instance identifier and the associated instance of a VnfInfo information element.
- VNF Performance Management: This interface allows providing performance management (measurement results collection and notifications) related to VNFs. Performance information on a given VNF/VNFC results from performance information of the virtualised resources that is collected from the VIM and mapped to this VNF/VNFC instanc
- VNF Fault Management: This interface shall allow the VNFM to provide alarms related to the VNF(s) and its VNFC(s) visible to the consumer. Virtualised resource alarms collected by the VNFM well be filtered, correlated and modified by the VNFM and mapped to the corresponding VNF instance, resulting in alarms on the corresponding VNF and its VNFC(s).
- VNF Configuration Management: This interface allows the EM to provide configuration information for a VNF instance and its VNFC instance(s), or individual VNFC instances. The scope in this project will be to only subscribe to VNF configuration changes.
- VNF Indicator: This interface allows the VNF to provide information on value changes of VNF related indicators. VNF related indicators are declared in the VNFD.

3.4.5 Traffic Monitoring using SDN and NFV

Recently much attention has been given to the effectiveness of combining NFV and SDN for network packet monitoring and inspection. In traditional network architectures, network functions requiring packet monitoring often require dedicated physical appliances leading to high capital and operational costs. The network operator needs prior knowledge over the entire network configuration, has to have a high degree of expertise and extensive knowledge regarding all the device types in the network. Network topologies have evolved to complex and intricate meshes of computational elements often translating into multi-vendor proprietary network device environments where each has different configuration instructions and different user interfaces. Managing complex traditional network topologies is an error-prone process where a simple mistake can lead to severe network security implications. In some cases, the complexity of network configuration and the absence of common standards for programming and configuring network equipment has forced companies to commit to single network equipment vendors. In such vendor lock-in environments the potential for innovation is greatly reduced. It is also important to mention that even if traffic inspection is achieved via dedicated appliances connected via device mirroring ports other issues such as network contention and the link layer and exhaustion of computational resources are also likely to happen while, at the same time, the configuration complexity still remains. In order to better illustrate the potential of using SDN and NFV for traffic monitoring, the first part of this subsection will be primarly focused on an Openflow-centric perspetive. The aims at providing an introduction, which could be eventually provide the basis for a proof-of-concept implementation which is relatable for most readers, since OpenFlow constitutes one of the oldest proposals for an SDN protocol. For the sake of completion, a discussion about the P4 [31] protocol will also be included towards the end of this subsection.

With Software Defined Networking, as the control plane is removed from the forwarding elements (network switches) and shifted to a logically centralized location (the network controller) a global topology view, global state awareness and network programing capabilities are available at the network control layer. Considering an Openflow-centric approach, this opens up multiple possibilities for traffic monitoring in SDN applications which roughly can be categorized in three main groups:

1. Exploiting Openflow counters in a passive manner
2. Taking advantage of the packet headers for all packets sent to the controller prior to packet output decision
3. Steering network packets to dedicated monitoring assets

A simplistic representation of an OpenFlow enabled switch is provided in Figure 17.

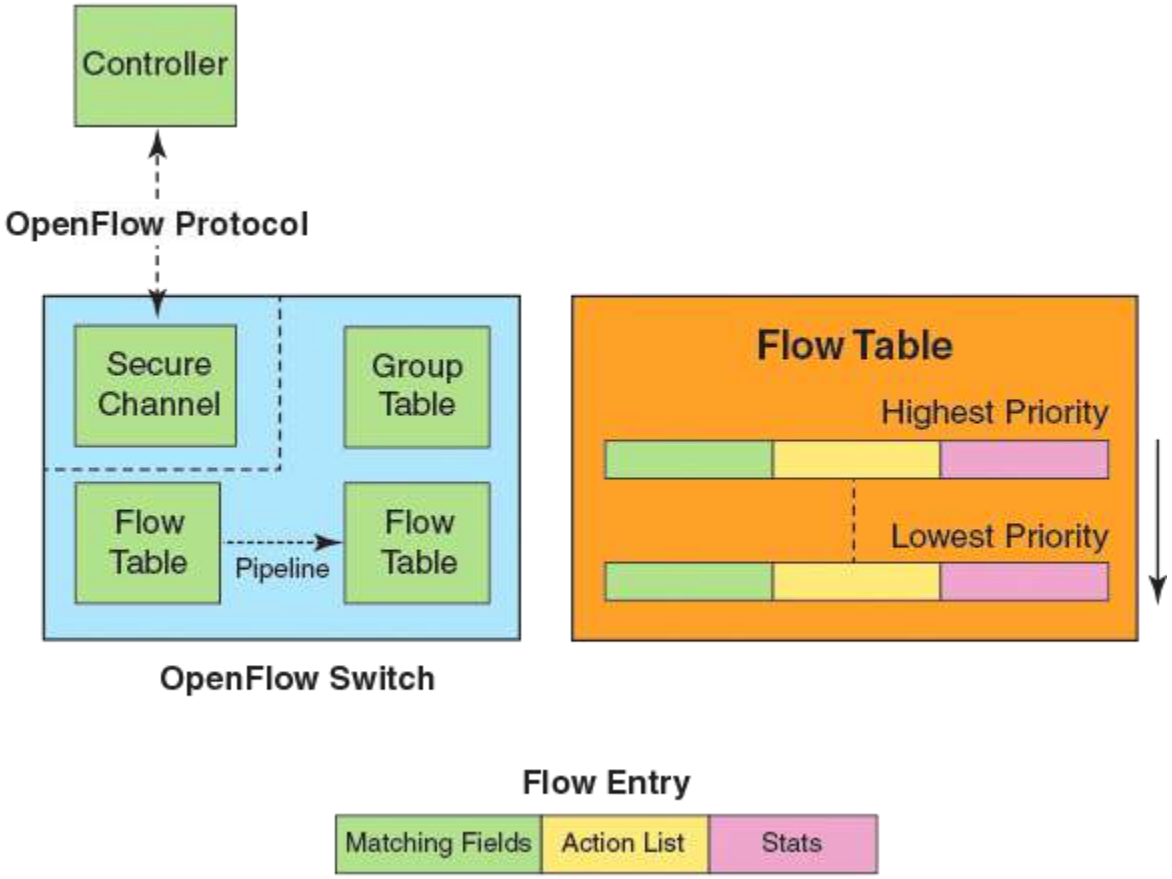

Figure 17 - Simplistic representation of an Openflow enabled switch [32]

Regarding option 1, the OpenFlow protocol, as the de-facto SDN protocol has standardized the way the network controller communicates with network devices and established a common interface for gathering device statistics. The OpenFlow protocol standard defines three different types of messages for device communication [33]: controller-to-switch, asynchronous messages and symmetric messages. While asynchronous messages allow the switch to inform the controller about a change in its state without the controller soliciting it (e.g. a change in a port capacity or the instant unavailability of a switch port), controller-to-switch messages can be exploited to periodically request statistics (packet and byte counters) from the switch. These counters are updated internally by the switch on constant time intervals on a granulometry that can go from a switch port up to each device installed flow rule. In an SDN controlled network, network flows are programmed by means of flow rules in a match-action manner (Figure 17). Hence, counters (stats) can be used as a monitoring tool with neglectable footprint on the network throughput performance and with a precision similar to the one achieved through the match fields of a flow rule. Thus, the granulometry of OpenFlow counters can be used by the network controller to profile the network traffic patterns. Counters available at an OpenFlow enabled switch are summarized in Figure 18. Note that counters are even available for the OpenFlow QoS mechanisms namely queues and meters.

Counters	Bits	Required
Per flow table		
Reference Count (active entries)	32	✓
Packet Lookups	64	
Packet Matches	64	
Per Flow Entry		
Received Packets	64	
Received Bytes	64	
Duration (seconds)	32	✓
Duration (nanoseconds)	32	
Per Flow Port		
Received Packets	64	✓
Transmitted Packets	64	✓
Received Bytes	64	
Transmitted Bytes	64	
Received Drops	64	
Transmit Drops	64	
Receive Errors	64	
Transmitted Errors	64	
Received Frame Alignment Errors	64	
Received Overrun Errors	64	
Received CRC errors	64	
Collision	64	
Duration (seconds)	32	✓
Duration (nanoseconds)	32	
Per Queue		
Transmit packets	64	✓
Transmit bytes	64	
Transmit overrun errorrs	64	
Duration (seconds)	32	✓
Duration (nanoseconds)	32	
Per Group		
Reference count (flow entries)	32	
Packet Count	64	
Byte Count	64	
Duration (seconds)	32	✓
Duration (nanoseconds)	32	
Per Group Bucket		
Packet Count	64	
Byte Count	64	
Per Meter		
Flow count	32	
Input packet count	64	
Input byte count	64	
Duration (seconds)	32	✓
Duration (nanoseconds)	32	
Per meter band		
In band packet count	64	
In band byte count	64	

Figure 18 - Openflow counters [33]

This kind of technique for network monitoring has gained enough track recently due to the advances on artificial intelligence. Multiple authors [34], [35] and [36] have been using the statistical data provided by OpenFlow counters to train machine learning classification algorithms. Some [35] even classify such

systems as lightweight intrusion detection systems since the system does not process network packets and does not impose a significant network overhead. The overall conclusions are that OpenFlow counters can be used to find deviations to the usual traffic patterns with a high degree of efficiency and can be used as an alternative way to detect security threats even if the network packets flowing in the network are encrypted. The effectiveness of these detection techniques prove even more useful in network topologies where the traffic pattern is constant and the connection matrix is somehow static.

Option 2 relates to the use of packet headers for the profiling of network flows. One of the big advantages of SDN is the fact that Openflow switches are able to send packet headers to the controller (PACKET_IN asynchronous messages) while waiting for the packet treatment decision issued by the controller (being the full packet stored in the switch internal buffers). Multiple SDN applications can co-exist in the network controller each having different roles (and priorities) regarding packet processing. Applications can simply exist as of observers of PACKET_IN messages processing the packet headers of each message for statistical purposes. One example of such an application is [37], which does not modify the output treatment of the default controller reactive flow application while still having access to each packet header arriving at the controller. The application simply implements custom counters, i.e, incrementing variables in a data store for each packet flowing to the controller - by ethertype and protocol.

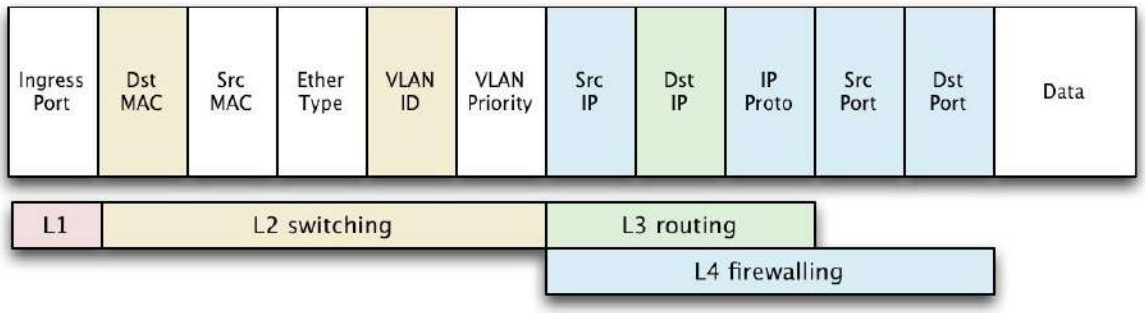

Figure 19 - Openflow packet header match fields [38]

Many authors have been proposing systems (implemented as controller modules/applications) to monitor the traffic flows in SDN by exploiting switch PACKET_IN messages. Use cases are often found in the network security domain. [39], for example, uses deep learning techniques as an intrusion detection system mechanism built into an SDN installable application. The dataset for the model is built upon the information extracted from the network packet headers. As this reactive approach brings significant data into the controller application space, issues related with the scalability of such systems have also been identified [40] [41]. Forcing all network packets headers to the control plane can bring significant overhead and can be exploited as DDoS attacks against the network controller [42].

The third option, which has recently received a lot of attention in the research domain, is to couple SDN with Network Function Virtualization mechanisms (Figure 20) in order to promote traffic steering to dedicated virtual appliances. The orchestration layer can be implemented directly in the network controller (as a regular SDN application) or can be part of an external layer to which the network controller communicates. Having the orchestration of virtual assets available to the network controller means the network operating system can no longer just serve as a means to program the network but can also request the instantiation and automatic provisioning of new virtual elements in the network (to which network packet copies are offloaded). The orchestration layer defines the type of virtual assets that are instantiated. Traditionally, virtualization has been almost a synonym of hypervisor-based virtualization and virtual machines. Nowadays a trend begins to appear targeting the use of microservices and container based virtualization due to their small instantiation times, high performance (low resource overhead) and the ready-availability of containerized versions of popular open-source

software packages. Despite the different types of VNFs, the most popular network controllers have built-in virtual network subsystems to orchestrate network functions via high level abstractions such as those provided by the OpenStack framework (Neutron and Nova modules) [43] [44].

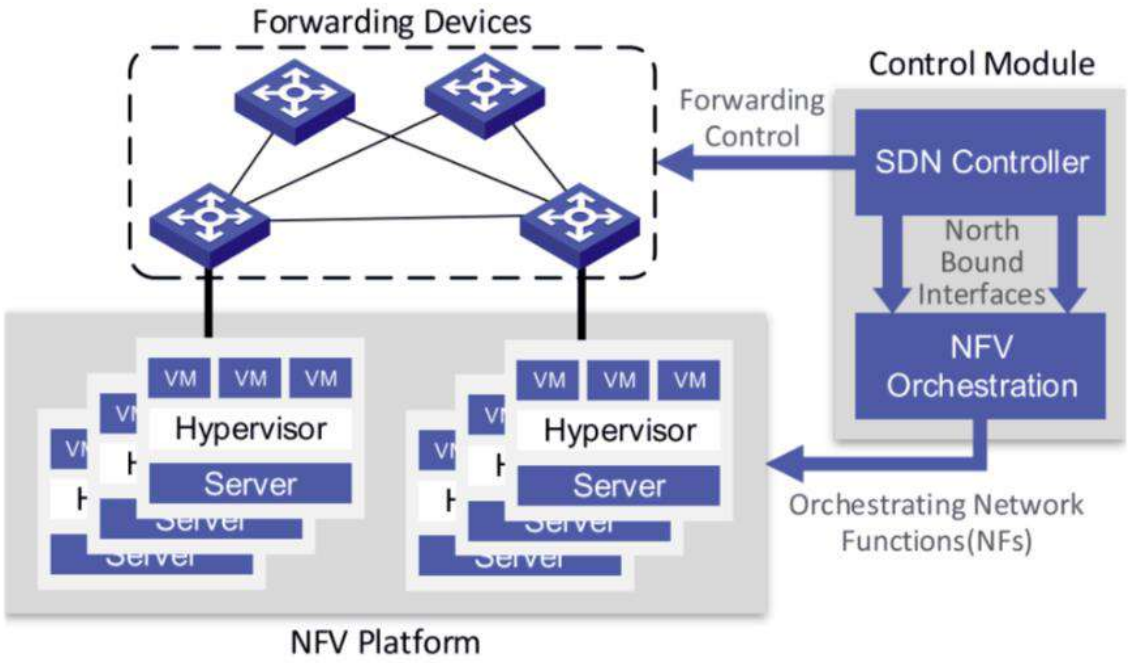

Figure 20 - Using SDN and NFV to orchestrate virtual network functions [45]

By coupling SDN and NFV, several advantages of the cloud computing model become accessible to network operators: network services can become elastic with the ability to grow and shrink based on policy, with no impact to applications. The network controller can instantiate a new virtual machine (or a new container) and automatically program the underlying network: the installation of rules in the switch fabric to ensure connectivity between the VNF and the other hosts in the network, to simply provide traffic copies to dedicated vNFS or even to chain traffic across multiple vNFs. This approach can apply a proactive approach to network flow programming since the network controller, by means of the topology graph, knows exactly the location of each element in the network. The impact in the control plane is greatly reduced and resource usage is optimized as VNFs are consolidated in the datacenter infrastructure.

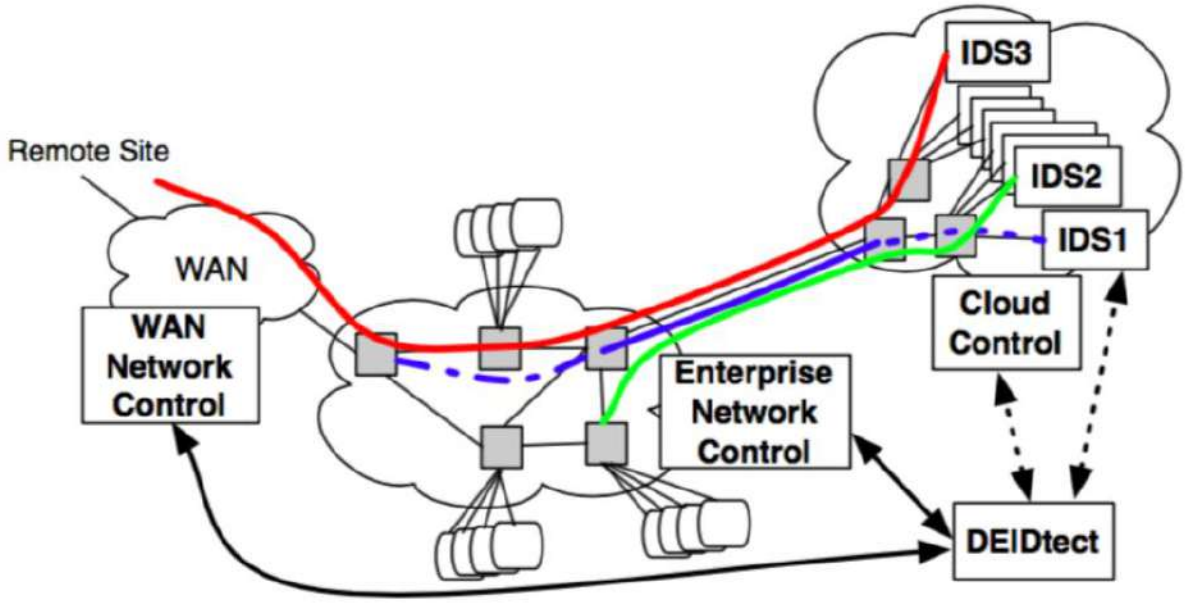

Figure 21 - A scalable SDN based IDS from [38]

As an example of this monitoring methodology, the work of [38] (Figure 21) can be mentioned. The authors recognize current traffic inspection mechanisms are inflexible and do not scale in regards to computational and networking resources. Furthermore, the authors point out that in some cases it is preferable to analyse the same traffic with the aid of multiple monitoring software packages, which is difficult to achieve in traditional networks due to the dependency of physical monitoring assets. As a result, the authors propose to offload traffic copies belonging to multi-site enterprises to the dedicated VNFs using the OpenFlow protocol, and borrowing resources from the cloud as the traffic load scales.

Besides the Openflow protocol, the P4 programming language constitputes a notable development which has been subject to considerable development in the past few years. P4 (the name spawns from the original paper title, “Programming Protocol-Independent Packet Processors”) is a language designed for programming network device dataplanes, allowing to express how packets are processed by a forwarding element. Unlike Openflow, which is a procotol that provides the means to describe flow-oriented rules, P4 is a domain-specific programming language designed in a protocol-neutral fashion (Figure 22).

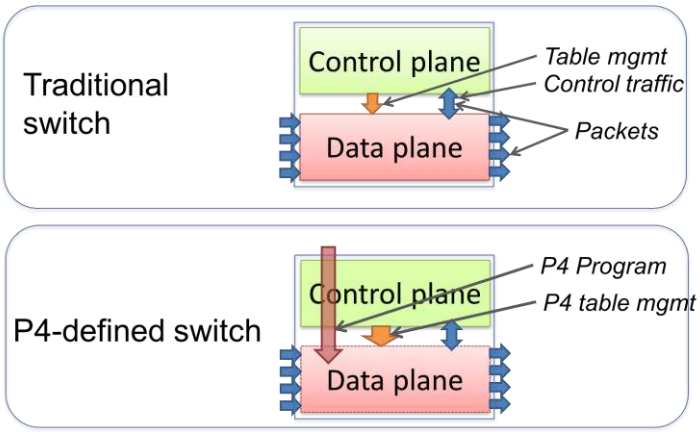

Figure 22 – Traditional switch vs. P4 programmable switch from [46]

P4 was solely designed to specify and implement the data plane functionality of a target, also encompassing the partical definition of the interface between the control and data planes. On a P4 switch, the data plane (which has no built-in knowledge about any protocol) is not defined in advance, but rather established by a program. Also, the communication between the control and the data plane is not based on fixed tables and objects, being defined by a P4 program which also takes charge of generating the corresponding API.

To a certain extent P4 can be considered to be complentary to the Openflow paradigm: while the former is concerned with expressing forwarding behaviour, the latter is focused on decoupling the control plane, by specifying a protocol for implementing a API to express behavioural rules. Despite this, and due to some insatisfaction with Openflow functionality and developments, as well as the limits imposed by fixed-function forwarding equioment, the P4 community has implemented a P4 framework for runtime control of P4 devices with a gRPC [47] API (p4runtime.proto) [48] whose support has been included in the ONOS network controller. In this sense, ONOS will provide (pretty much in the same way as its done with Openflow) the means to abstract the southbound API and/or protocol heterogeinity from applications. The first demonstration of a physical network for this scenario was done in November, 2017 [49].

Considering such developments, it becomes feasible to foresee the implementation of similar SDN/NFV monitoring mechanisms as the ones previously described for Openflow scenarios, by using P4-compliant forwarding elements. Moreover, the ongoing specification of P4 telemetry format [50] as well as support for In-band Network Telemetry (INT – also supported by ONOS) allows for real-time and fine-grained end to end monitoring directly in the data plane. INT allows to collect and report telemetry information directly from the data plane, by attaching information to the packets flowing through the devices, whis is later extracted and the end switch. This approach provides several advantages over the limits of Openflow counters, being independent from the packet processing pipeline implemented in the switch, while also reducing device overhead and providing a convenient way of acquiring flow-specific telemetry data.

3.4.6 Intelligent actions for 5G Networks

With the advent of 5G networks and massive IoT a huge spike in data traffic is expected, as much as a 10-fold increase. In addition, 5G technology, with its millimeter wavelengths traveling shorter distances, will create many more network "edges" even as the IoT connects billions more devices from which data can be collected and analyzed.

Creating a network capable of automatically responding to its own issues -- congestion, equipment failure, traffic spikes -- is one of the goals of the ongoing virtualization push. Artificial intelligence (AI) and machine learning (ML) are key elements of this effort today, and they become even more critical going forward into 5G.

3.4.6.1 Artificial Inteligence and Machine Learning

Machine learning can be characterized as the computation methods employed by software applications to achieve artificial intelligence. ML itself involves processing of data with the aim to learn a representation model (a function) that can mathematically and computationally describe the pattern of data observed, or to represent the behaviors of the system that generates the data.

The field of AI has undergone a resurgence in the last decade, thanks mostly to the advances of deep learning techniques. There was a period known as the “AI-winter” (1970s to mid-1990s) in which neural

networks and expert systems essentially over promised and under delivered. Overcoming the challenges from the previous era, recent successes with artificial neural networks (ANN) can be attributed to these following factors:

- Invention of backpropagation and gradient descent techniques: allow ANN weights to converge with an automated process. The modern art of data science has now shifted from hand-crafted feature engineering to network (neural) engineering.
- Big labelled data: the availability of reasonably large set of labelled data particularly in the image, textual, and speech domains.
- GPU: the somewhat "accidental" discovery in that graphic processors are also suitable for neural network's vector processing, which helps accelerate training of large ANN.

Such factors allow many deep and interesting ANN architectures to emerge including convolution neural networks (CNN), recurrent neural networks (RNN), restricted Boltzmann machines (RBM), generative adversarial networks (GAN), autoencoder, etc. Image classification competitions have produced increasingly impressive results, which is now roughly at par with human recognition performance, based on these architectures.

While deep neural networks (DNN) are making great strides in pattern recognition problems, traditional statistics learning-based ML algorithms (Decision-Tree, Random Forest, Bayesian, Support Vector Machines, etc.) are also well utilized by data scientists across many different verticals. These traditional ML techniques have successfully been applied to many forecasting, inference and predictive analytics problems. The two underlying ML fields of AI have both matured tremendously over the last decade.

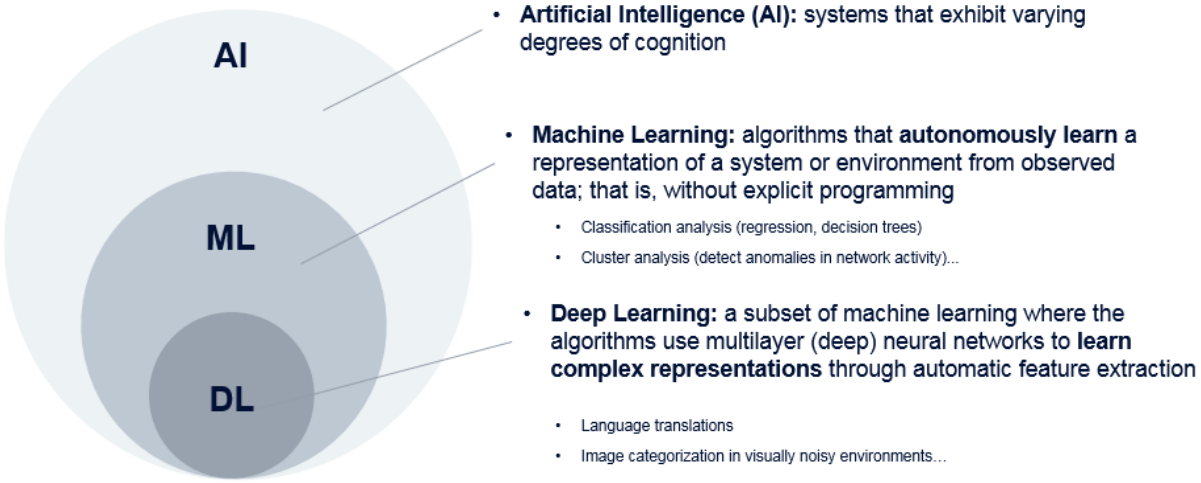

Figure 23 - Artificial inteligence scope

In general, the following types of problems can be addressed by AI/ML techniques. Although many public domain materials match problems to algorithm choices, the matchup tends to oversimplify the problem. The final selection of algorithm is heavily dependent on the available data, performance objectives, and the context of the problem one is trying to solve.

This list below is not meant to be exhaustive. In practice, a real-life problem might fit multiple AI/ML tasks.

- Classification: Categorizes a data point or event into a class or multiple classes. This is typically set up as a supervised ML problem especially when sufficient label data is available.
- Inference: Help fill in missing data or predict a data point in the future. Time series forecasting or sequential data prediction can be considered a form of inference.

- Optimization: Identify a different operating point in which the new operating state is better than the present state - given certain pre-defined objectives. The more optimal operation point might or might not be a local/global minimum. Multiple changes/actions might be required in order to "move" towards that new operating point.
- Recommendation: This is traditionally associated item-based recommendation in various content delivery settings. In the context of telecom domain, this might be policy changes or monetization recommendations.
- Knowledge discovery: This is typically associated with documents or content discovery of some sort. Data mining of care and support tickets for prevention or proactive corrective actions falls under this class of approach.
- Reasoning: Generally refers to a system that behaves in a human-like fashion in which it exhibits perceived cognition. Different type of chatbot using Natural Language Processing (NLP) technology would fall under this category. Some of these use cases are tied with a knowledge discovery backend system.

3.4.6.2 Machine Learning for service assurance

In the context of this project, the different nature of 5G network data and the target use cases will determine the AI algorithmic approach to be used. Below are some example families of use cases that can be explored:

- Autonomous network: Fast response time, human-less, self optimization based on multi-dimensional objective functions. Automate "observe-analyze-action" cycles such as in 5G RAN optimization (SON). Focus is on localized sub-domain initially and needs to be careful with multiple-overlay feedback loop effects.
- Causality chaining: Automate causation tracing from one network domain (e.g. 5G core) into other sub-domain (e.g. 5G RAN system).
- Predictive anomaly: Instead of anomaly detection, predict onset of anomaly with lower false positive/negative rates.
- Augmented recommendation: Utilize reinforcement learning style of techniques to recommend 5G network policy recommendations. Actions enacted with human in the loop (usually longer term policy actions). Support "what-if" scenario analysis as part of the overall features.
- Advanced autonomous care: Provide human like reasoning for direct care support interaction with subscribers; or to assist human care agents.

The product should be able to provide the following key functionalities:

- Data curation as a norm: At heart, all AI projects involve algorithm selection/design work. These design works start with having data. Quality, richness, and size of the data play an essential role that affect the final system design and ultimately product performance. The notion of "garbage in, garbage out" still holds true.
- Efficient data sharing: Once data is available for use on a regular basis; these data sets should be warehoused and catalogued properly to facilitate maximum sharing; whilst respecting the privacy and access privilege requirements. What and where data set is stored, for whom to use, and for what purposes should be easily explorable by all data users.

3.5 Support Mechanisms in 5G Networks

3.5.1 Introduction

Support services are employed by Telecom Operators, service providers, cloud operators in their networks to assure that all the pre-conditions required by the service portfolio is fulfilled. Such pre-conditions can include other services common to several networks like DNS, AAA, or are specific to 5G networks such as NEF and NRF.

The following subsections present the details of support services in 5G networks, highlighting the requirements, scenarios and conditions for the deployment of DNS and NEF.

3.5.2 DNS as a support service in 5G Networks

Support services such as DNS are essential to all types of networks, including the 5G. DNS provides resolution of names so that the endpoints can be reached via their IP addresses (either IPv4 or IPv6). The architecture of 5G follows a Service Based model [51], where services can be considered as network functions which functionalities are exposed over HTTP like interfaces. In this context, DNS is relevant to store the information where such services (i.e. IP addresses) can be reached. Additionaly, DNS can provide its services in secure interfaces, as most recent specifications aim to secure the information provided by DNS through secure channels like HTTPS [52].

In the context of 5G, DNS acts as a support service with different deployment models, as depicted in Figure 24. The main functionality of DNS is to store information of services, applications/networks functions, so that any element in the 5G network can have information regarding the reachability of a given service. Regarding deployment models considered by the telecom operator, DNS can be collocated with other services, like Network Repository Function (NRF), being deployed on the core network.

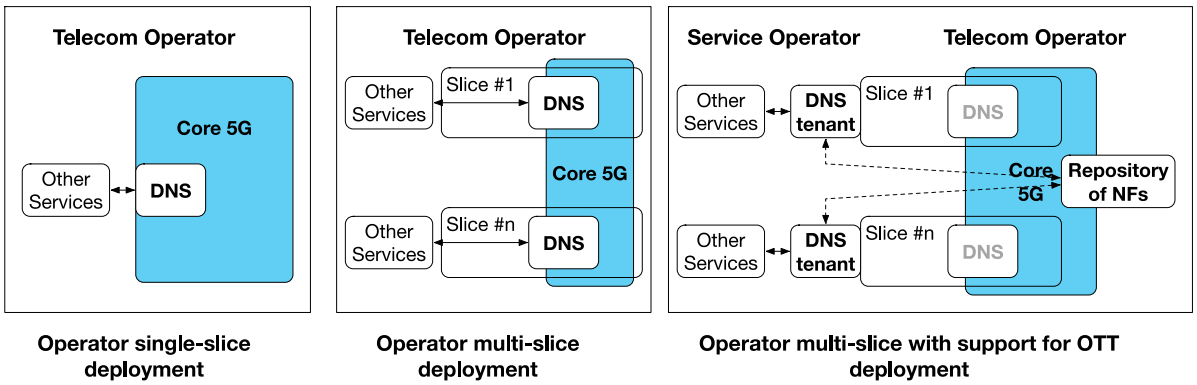

Figure 24 – Deployment scenarios of DNS service in 5G

Telecom operators that explore the benefits of 5G can also deploy the support services on a slice basis; in such cases, DNS is deployed in each network slice (as depicted in Figure 23) wihin the operator multi-slice deployment. In such cases, 5G services interact with the DNS in the respective slice.

With the advent of cloud computing paradigm, further enhanced with 5G, DNS can also be deployed as an Over the Top (OTT) solution, where the tenant can customize the DNS information via APIs. The costumization of such DNS can be based on the “service images” available in the Network Functions

(NF) repository of the Telecom Operator. In such repository, each tenant has available all the information to deploy DNS and to customize it to better suit the DNS service to its needs.

3.5.3 The role of the Network Exposure Function in 5G Networks

3.5.3.1 Contextualizing Network Exposure Function

In the context of new telecommunication paradigms, concepts such as SDN and VNF have emerged and currently started playing a key role in the introduction of flexible and scalable network deployments. Following this trend, 3GPP has defined a 5G System with a very modular architecture, splitting functionalities into different Network Functions (NFs) and thus enabling the full virtualization of the 5G core network and its connectivity with software-defined links.

The capability of deploying distributed and flexible Network Exposure functions (NEFs) allows both for multiple entry points in the network for Application Functions (AFs) and very low latencies for distributed NFs reporting and communicating with NEF. Moreover, multiple NEFs can exist, depending on operator policies, to serve multiple slices. This ensures that the load is also distributed, allowing for a dynamic and responsive set of functionalities.

3.5.3.2 Network Exposure for 5G

The Network Exposure Function (NEF), specified in 3GPP Release 15 is instrumental in providing an open 5G platform that can be leveraged for several players and services, providing the means for customers to interact with the network. It constitutes an evolution of the Service Capability Exposure Function (SCEF), which was originally defined as a node in the Evolved Packet Core specifications (according to 3GPP Release 13 [52]. NEF is essentially an API gateway designed to interact with the network functions, designed to provide third parties (such as service or partner operators) to provision, enforce and monitor application-level policies within the operator network. Moreover, it optionally can be the point where PFDs are managed.

NEF's services are described in detail in 3GPP Release 15, together with the relations with other functions in the rest of the 5G System.

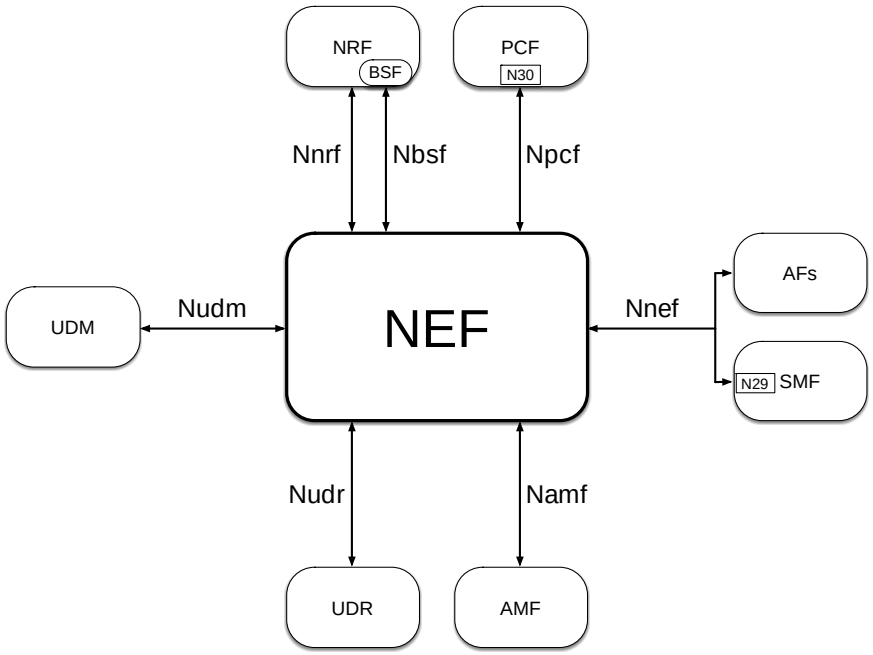

Figure 25 – NEF in the 5G System

This figure highlights the direct relations NEF has with other network functions, representing a functional architecture with a service-oriented paradigm that perfectly suits a software web service approach:

- Nnrf: Useful for the registration/deregistration of the NEF functions, together with the discovery and notification of registration of other NFs. This allows the communication with other NFs via their endpoints.
- Nbsf: Corresponds to the function that is used to discover the correct PCF for a given PDU session. This becomes paramount for the N30 interface with PCF.
- Npcf (N30): Interface for the negotiation of policy and charging control behavior between PCF and NEF, like Service specific policies, sponsored data connectivity, or AF-influenced traffic steering.
- Nnef: Interface with the exposure of NEF functionalities to AFs, namely event exposure, parameter provisioning to the 5G System and trigger services. Optionally, the N29 interface with SMF is also in Nnef to enable PFD management.
- Namf: This interface is mostly used for the enforcement of access and mobility functions, and also for transferring policies to UEs.
- Nudr: Corresponds to the interface to be used when PFD management is handled in NEF, using UDR as a storage point for PFDs.
- Nudm: This interface is used to obtain event exposure from UDM, as well as to discover the NF serving a specific UE.

This architeture is the standard and provides a basic definition of the path to be followed to upgrade from 4G SCEF to 5G NEF. However, many aspects are still undefined or open to implementation choices/operator's policies. Hence, a basic implementation of NEF should focus on the most important aspects and ensure that the key functionalities are implemented. This is the goal of the definition of NEF in this project, and also the starting point for the definition of the use cases to be evaluated.

3.6 Security mechanisms for 5G services and networks

3.6.1 Introduction

The security of a complex system like an operator network, especially one that introduces such a disruptive technology such as the upcoming 5G, is a very complex subject and will always be a work in progress due to the nature of the subject. Each discovered threat requires the evaluation of its impact on the network considering the security mechanisms already in place, auditing if the current security measures are or not enough to thwart the threat (usually in the case of a new class of threat). Upon this analysis, if needed, new security elements or procedures that aim to reduce or completely nullify the threat must be designed and implemented.

The evolution from 4G to 5G brings several high profile changes to the way operator's core network is managed. The change with the greatest impact from the security standpoint is the introduction of mechanisms that aim to bring flexibility to the network. The introduction of NFV technology as a driver for the implementation and management of network elements allows the operator to allocate its resources in a flexible way, enabling network elements to be instantiated closer to the data they process and in different scales, constantly adjusting to the load at the network. However, this increase in flexibility requires an increased connectivity between different segments of the operator's network, and some segments that were previously isolated from the Internet may now require connectivity to the Internet. That scenario, on a traditional network, would certainly be seen as a security issue. This extended connectivity of operator's network is nevertheless a required driver for the implementation of NFV, especially in scenarios with multiple VIM or POP under the control of a single MANO system. This evolution has already been the target of considreable work, both by the ETSI NVF and by the 3GPP communities. Both of these released a set of documents with security in mind, [53] specifies a series of threats to the NVF reference points and a corresponding set of requirements to counter the threats. [54] specifies a set of requirements for the 5G core functions and radio, with the definition of a series of security domains and procedures within each domain. Both of these documents are of special importance to the suppliers of two of the components of the network, the NFV MANO that will manage the infrastructure, and the 5G core that will manage the communications. However, an operator is composed by more than just those two systems, and other methodologies can and should be used to harden the components of the network.

Common malware at the end client's network is usually of no concern to the operator's network, and its traffic can be regarded as usual traffic. However, if the amount or type of traffic impacts the operator's ability to supply its portfolio of services, it will be mandatory to detect and disrupt malware generated traffic, for instance, by stopping a specific malware from communicating with its control system in order to stop a running DDOS attack. This kind of activities, performed at an operator level, have the primary goal of stopping the increase of traffic generated by this type of attack from impacting the quality of the operator's supplied services. In some cases, these protective activities may be performed in a cooperative way by multiple operators, usually coordinated by a Computer Emergency Response Team (CERT).

Attackers can normally be divided into two separate and very different goal oriented groups. The first group can be considered as the benign ones, "red teams" and penetration testers formed by ethical hackers hired by an operator or enterprise to test the effectiveness of the security mechanisms in place on a given infrastructure or service. The second group contains malicious hackers acting without the consent of affected parties, with the intention to find vulnerabilities on a given service or infrastructure,

to either discredit an organisation publicly or try to monetize on the detected vulnerabilities. This monetization can be performed, for instance, by selling the acquired information or data to interested parties or by hijacking the control of the service/infrastructure, requesting a ransom fee to give it back. Both groups follow the same methodology, varying however on the scope of the attack. While penetration testers usually operate under a very strict scope, hackers and red teams use whatever vectors they can. As previously and briefly mentioned, the outcome of the attack is also considerable differentiated. Although benign attackers report back and normally collaborate/suggest on protective measures to the identified vulnerabilities, hackers usually do not. The actions of an attacker on a network follow a set of common steps in a more or less structured way. The set of steps is common for different kinds of networks, from the end client's network to the core of the operator's network. Attackers usually only have to adjust the level of sophistication to the target's network perceived dimension and level of security. The figure below displays this methodology and steps followed by attackers while trying to gain illicit access to a given asset or data.

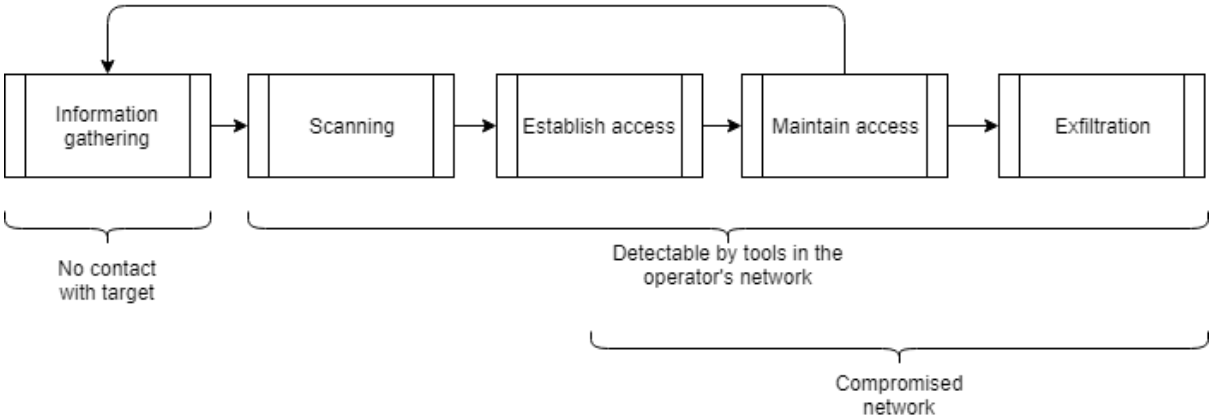

Figure 26 – Attacker's workflow to gain illicit access

The objective of a good security strategy is the prevention, detection and thwarting of malicious activity as soon as possible, if possible before any system is compromised. In case the prevention or early detection fails, the detection of data exfiltration becomes paramount as the objective shifts to the minimization of the impact of the attacker or malware on the business.

The supplied products and services should be enough to encompass the vast majority of the technical threats targeting the operator's network. In the next chapter, a few simple user stories with a big impact on the area of security are presented. From those user stories, a set of requirements will be elicited and on a later stage an analysis of the adequation of the products to the objectives will be performed, with the goal of detecting any gaps in the defence strategy.

3.6.2 Detection and mitigation of malicious activities

Its easy to understand the importance of the following statements (non exhaustive) when designing the security aspects of an operator network:

- As a platform administrator I expect to be notified of malicious activities in the core of the network.
- As a platform administrator I want to be alerted in case any system is attacked by malware.
- As a platform user I expect my subscribed services to be available at all times.
- As a platform user I expect that my communications will remain private.

Based on the above statements, the security mechanisms will always have the primary purpose of detecting an unexpected activity that can lead to problems with the service availability or to the unintentional disclosure or destruction of information. The second purpose is stopping a threat before it becomes a problem, mitigating it as early as possible. If it is not possible to thwart a thread on an initial stage, the threat becomes a compromise and the task at hand becomes one of damage control. The goal becomes preventing the compromise from spreading, and eventually restoring the system to a known good state, introducing measures to prevent the same threat form causing problems.

3.6.3 Core network threats

From the security point of view, the core of the network has a wider meaning than what is proposed by 3GPP or ETSI NFV alone. The core of the network (when it comes to security) encompasses all the systems that are involved in the delivery of the service to the end client, as well as any system that deals directly or indirectly with the metadata or private information regarding the client. A compromise of any of these systems can cause outages or information leaks, something that has a direct impact on the image of the operator with the public. The internal architecture of the operator is paramount to stop the progression of a threat of this category. The separation of different components into separate network segments with different access control measures is the first barrier to the progression of an attacker in the operator's network. The segmentation implies the creation of interconnection points, where stronger perimeter measures can be put in place with the explicit purpose of preventing the progression of such threats.

3.6.4 Volumetric and resource exhaustion threats

This groups includes all threats that lead to the degradation of the service due to resource exhaustion. This class of threat is usually transient in nature, and can be either localized or affect all the clients or services depending on its technical characteristics. In some cases, the operator by itself may not have the ability to respond to a volumetric attack having to request assistance from upstream providers or participate in a coordinated defensive response. This class of threat is usually mitigated via the filtering of traffic as close to its source as possible.

3.6.5 Threats to the privacy of the customers

This class of threat is usually sophisticated in nature and may have a huge impact on the life or business of the target. Its detection is essential for various reasons. The first reason is because it is the operator's duty to ensure the integrity of its network, and any attack that affects its integrity can be seen as an attack to the operator itself. A second reason is that the client has expectations of privacy when using the operator's network, and other than lawful interception, the operator should guarantee that the client's communications remain private.

3.7 Virtualization Platform in 5G Networks

3.7.1 Introduction

As mentioned in previous sections, 5G Networks will rely heavily in a performante and fast to adapt platform where the needed workloads can be fully automated, including the network requirements.

In legacy “physical-centric” networks, server provisioning would take from weeks to months. Replacing a server was a time consuming task, and reacting to an increase in workload demand was limited to a disruptive vertical scale limited by the allowed physical resources. Virtualization technologies helped solving some of this limitations, as the physical resources in a virtual platform belong to a global pool of resources (compute, storage, network) that can be allocated to the required workload in a moment, and can return to the pool after being released.

A logical slice of the pooled resources is consumed by allocating them to a virtual machine. A virtual machine acts like a real computer with an operating systems of its own, isolated from the underlying resources. The application running inside a virtual machine is also isolated from the underlying system and other virtual machines sharing the same compute host. The physical compute host runs a software layer called Hypervisor that manages the resources allocation and the running virtual machines, also called guest machines.

Virtualization technologies introduced some features that are valuable to dynamic workloads, which will benefits the management of 5G network workloads. The following sections provides an overview of some relevant features of virtualization technologies.

- Faster provisioning - In a Virtualization Platform, a new virtual machine can be provisioned in minutes using automated procedures, reducing immensely the time it takes to have a new server.
- Live Migration - If virtual machines are fighting over resources in a compute node, this can impact their
- performance. To address this issue, a Virtualization Platform is capable of live migrating virtual machines to compute nodes with more available resources, with “Live” meaning without restarting the guest operating system.
- Failover - If a compute node malfunctions or crashes, virtual machines can be restarted on available compute nodes, thus increasing the availability of the service provided.
- Templates - Templates of virtual machines can be prepared and be ready to deploy new instances, reducing the time it takes to have a new guest virtual machine ready to produce, avoiding the configuration phase of a vanilla operating system.

3.7.2 Traditional Virtualization vs Cloud Computing

Having the Virtualization Technology as a base, two paradigms exist based on this technology:

- Traditional Technology - A traditional Virtualization Platform aims mainly at the legacy applications that used to be deployed on physical servers, and have now migrated to the virtual world, i.e., one or more fixed number of frontends, and one or more fixed number of backends/databases. This design scales only vertically and if the databases die, the service is down.
- Cloud Computing - A Cloud Computing Platform was designed for a different kind of workload, a new paradigm.

A Cloud Application does not rely on a specific virtual machine, in this context, also known as an instance. The platform provides a reliable load balancer (as a service) that distributes the load across all frontends. This frontends can scale horizontally, i.e., instead of increasing the resources (vertical scaling) of a fixed number of virtual machines, the platform automatically add more frontend instances to help with an increased load. The backend/database follow the same principle. A Cloud Application does not rely on a fixed number of virtual machines to host the application data. Instead, the data is spread across several instances that can also scale horizontally. It is important to emphasize that if a single instance fails / crashes the application continues to operate: the Cloud Platform simply replaces the failing instance with a new one.
An added advantage of this design is that it allows for scaling down when the increased load decreases. This can lead to important savings for the paying customer, if appropriate.

3.7.3 Virtualization Platform in this project

The Virtualization Platform should be seen as resource provider (compute, storage, network) and must be decoupled as much as possible from higher levels of orchestration, as defined by the ETSI NFV reference architecture (see section 2.2). The Virtualization Platform is a means to deliver resources to the overlying layers, and must allow integration with automation and orchestration component.

4 Use Cases

4.1 Introduction

This section presents illustrative use cases, aiming to showcase the usage of the different addressed components. The use cases are set under two main higher-level scenarios, vCDN and PPDR, and cover different lifecycle stages of the services and events, namely:

- QoS service startup and dynamic configuration
- Congestion management and avoidance
- vCDN surrogate deployment in MEC
- Privacy invasion and application security

The use cases are intended to be illustrative – and not fully representative - of the expected functionalities to be provided by PPS2 components.

4.2 Use case 1 – vCDN Service Orchestration in 5G

4.2.1 Context

Nowadays, the majority of services and related resources are statically provisioned, which means that they do not change during the complete lifecycle of service instances except in case of failure or performance degradation. The end result is that network operators are forced to invest on infrastructure and customer care in order to prevent and handle scenarios that could be remedied by service and resource optimization.

Although monitoring and analytic systems already collect large quantities of data from the infrastructure, OSS systems do not make use of such data for the characterizing of service and resource context or to react to issues in real-time. An example for the need for optimization is video transmission, whose traffic volume is a concern to network operators [55]. Furthermore, in short to medium term, the expectation is that things are going to get worse due to combined effect of ultra-high definition video (UHD), mixed reality applications, and the massive number of connections resulting from IoT. Adding to that, Network Operators are usually considered the culprits when end clients face problems watching Internet-based video content; consequently, end clients see the delivery quality of video services as a differentiating factor when choosing their network provider, despite the fact that most video services belong to OTT providers. This case shows the role of different network mechanisms and procedures during multiple stages and events occuring during a vCDN system operation.

4.2.2 Motivation for 5G Networks

The predicted evolution for 5G networks is based on a set of artifacts that allows network operators to explore innovative services and optimize infrastructure management. Among the artifacts, the following are particularly relevant for CDN-based services:

- MEC - Cloud Computing is moving towards the edge of the network and closer to the RAN, which means content can be made available closer to the users

- Virtualization – the virtualization of CDN functions (vCDN) enables highly customizable deployments, ‘when’ and ‘where’ needed
- Network Slicing – the ability to deploy virtualized and isolated mobile networks, i.e. network slice, that is optimized for highly demanding content transmission, being video the most representative type of content.
- QoS - In order to assure satisfying performance of distinct services (e.g. live video vs VoD vs mission-crítical communications), the forwarding plane must differently handle packets based on the traffic type and other information.

Furthermore, vCDN represents one of the ideal scenarios whose evolution is greatly impacted and improved by these and other architectural 5G advances, as shown in the following subcases.

4.2.3 Sub-case 1: QoS Service Configuration

4.2.3.1 Description

Each application consumed by customers has a minimum quality of service which the network must satisfy for assuring a satisfying user experience. Depending on the type of service, the network must guarantee distinct levels of Quality of Service. This use case addresses the policy distribution procedures, taking place between the various network elements that support the service, required for fulfilling the contracted QoS.

4.2.3.2 Initial Scenario

As a precondition, the customer service is provisioned, and the use case is initiated when the customer accesses the service.

4.2.3.3 Step-by-step scenario

1. User registers on network, and requests the visualization of a particular video.
2. PCF receives from SMF the indication of session start.
3. PCF identifies the service profile for the customer.
4. PCF determines the policy to be applied depending on the profile and the entire context.
5. PCF installs policies on the required network elements, for differentiated QoS control of the services data flow.

4.2.3.4 Final Scenario

The use case ends when the user accesses the services, and the QoS rules are configured in all the network elements involved, in order to guarantee the desired result.

4.2.4 Sub-case 2: Congestion Management

4.2.4.1 Description

Congestion on a network can occur due to several reasons. Some of the situations that can cause congestion may be benign such as a sudden gathering of people due to a public one time event, while

others can be hostile in nature such as a DDoS attack that may exhaust all of the operator resources with junk traffic, leading to the degradation of the supplied service. Both of the above situations can however lead to some sort of service degradation (more or less localized), which may have the ultimate consequence of legal action in the event of a breach of SLA. While both these scenarios may require some kind of corrective action from the operator, the methodology used to return the network to a normal operation condition can be quite different. With the introduction of network slicing, a new way of causing congestion becomes possible as well: If two slices have a strict ingress priority established, by forcing traffic on the highest priority slice, it is possible to cause the degradation of the service on the lowest priority slice. This can be seen as an indirect methodology of inducing congestion with an ultimate goal of causing a perceived degradation on the quality of the provided service.

This example intends to establish a set of actions that take place when congestion situations are detected in the access network. This congestion condition is typically detected by analyzing the frequency of rejection situations in the access network due to lack of resources and/or packet drops across network nodes, but a more in-depth analysis and a richer context may lead to the detection of less immediate conditions (e.g. periodic trends). These situations are treated differently by multilevel policies according to their nature. For example, detection of a "simple" congestion condition may trigger the PCF to apply a policy that limits access in a given area while at the same time the policy framework may determine resources realocation to cope the problem in hand. In a long term approach, the policy framework may identify a trend of systematic congestion in this area and trigger higher-level policies, leading for example to the deployment of new resources in the area in question. Note that “Systematic Congestion” may range from a long term trend of growing traffic over months to an episodic situation caused for the occurrence of a particular “popular event”, like fairs, congresses, sports events, etc.

Some scenarios may even lead to the modification of existing policies or creation of new ones.

Note: Identifying network congestion situations is not something that can be done just by monitoring network data, and typically requires a deeper analysis, which is usually performed by analysis functions that specialize in congestion detection. A higher level of analysis would look at the profile of such congestion detections and correlate it with other information, like that produced by contextual data, to produce higher level indications.

4.2.4.2 Initial Scenario

This use case starts when there is a notification signaling the occurrence of congestion in the network. As a precondition, the 5G network must be dimensioned so that resources can be scaled dynamically.

4.2.4.3 Step-by-step scenario

1. A Congestion analysis system notifies that a congestion condition has been detected in a particular network segment
2. The notification is received by the PCF, where it triggers the application of a policy for immediate reaction to congestion, e.g. disable the establishment of new sessions in the affected area. The action is enforced to the SMF.
3. The same notification is also received by the Policy Framework, and there, together with other conditions, it triggers a policy together with other conditions, that will lead to a more structural intervention.
   In the scope of this super Use Case (**Error! Reference source not found.**) it is assumed that he congestion situation is caused by the localized consumption of a certain content that is provided by a vCDN that doesn’t have a cache close to the edge where the consumption occurs, thus causing too much traffic at the interconnections.

4. The PF uses the Optimization Framework services to identify the Edge Data Centers (MEC) that serve the impacted location(s).
5. The PF requests to the Orchestrator the instantiation of the vCDN nodes at the required location(s). This corresponds in fact to the Sub UC described in 4.2.6 - Sub-case 4: vCDN surrogate deployment in MEC host.
6. The Orchestrator takes the necessary actions for the instantiation (also as per 4.2.6)
7. The content is replicated to the involved vCDN edge nodes, either by the automatic vCDN caching mechanisms or by an orchestrated action, as described in 4.2.5 - Sub-case 3: Congestion avoidance through Intelligent Content Replication.
8. If this course-of-action is successful, the congestion indication is widthdrawn, leading the PCF to reestablish access.

4.2.4.4 Final Scenario

The configuration/instantiation result of the network elements involved/necessary has succeded and the congestion situation is resolved.

The vCDN topology was adapted to geographical aspects of content consumption.

4.2.5 Sub-case 3: Congestion avoidance through Intelligent Content Replication

4.2.5.1 Description

Video-based services are typically deployed in CDN infrastructures, either from network operators or third parties, to benefit from improved delivery and QoE for end users. The evolution of CDN infrastructures has been focusing on the following approaches [56]:

- More efficient caching mechanisms
- Use of technologies for the dynamic control of video bitrate basing on user device and network quality
- More efficient protocols for the compression and transmission of contents

However, network operators are in privileged position in terms of infrastructure to offer a solution that complements the previous ones. One of the most decisive factors to improve the performance of CDNs, especially when dealing with video content, consists of getting the content closer to the consumers instead of storing them in centralized datacenters. This movement of applications and contents towards the consumers allows improving the video quality without a direct increase in resource usage and also reduce the volume of traffic in transport networks.

With the evolution towards 5G networks, telecommunication infrastructures are expected take a distributed approach regarding datacenter topology, enabling network operators to benefit from their closeness to end users. Moreover, with the increasing heterogeneity of computing infrastructure, the opportunities and challenges for optimization of CDN services for the delivery of video content increases. The following are some examples:

- Different DC topologies with support for different technologies will make even more complex the allocation of resources
- The dynamic criteria (e.g. energy consumption, infrastructure usage, …) for the allocation of resources brings more need for continuous optimization

- Each operator has different policies which must be enforced during autonomous processes regarding lifecycle management of services and resources
- 5G networks will enable the offer of new services to verticals under a common shared infrastructure, these will be critical services and cannot be managed using manual processes to control resource sharing

With this in mind, it is imperative to make management more intelligent to fulfill the requirements of providers, content producers and consumers. In this evolution, the OODA loop is a good solution to establish a bridge from monitoring and analytics to actuation and orchestration. This 'bridge' is realized by components that make use of policies to govern decision making processes, in a way that the rules imposed by different teams, e.g. business, engineering, development, …, are fulfilled.

4.2.5.2 Initial Scenario

The figure below depicts a congestion scenario on the transport network, where the OSS systems respond by replicating video content to DCs that are closer to the user from the network point-of-view.

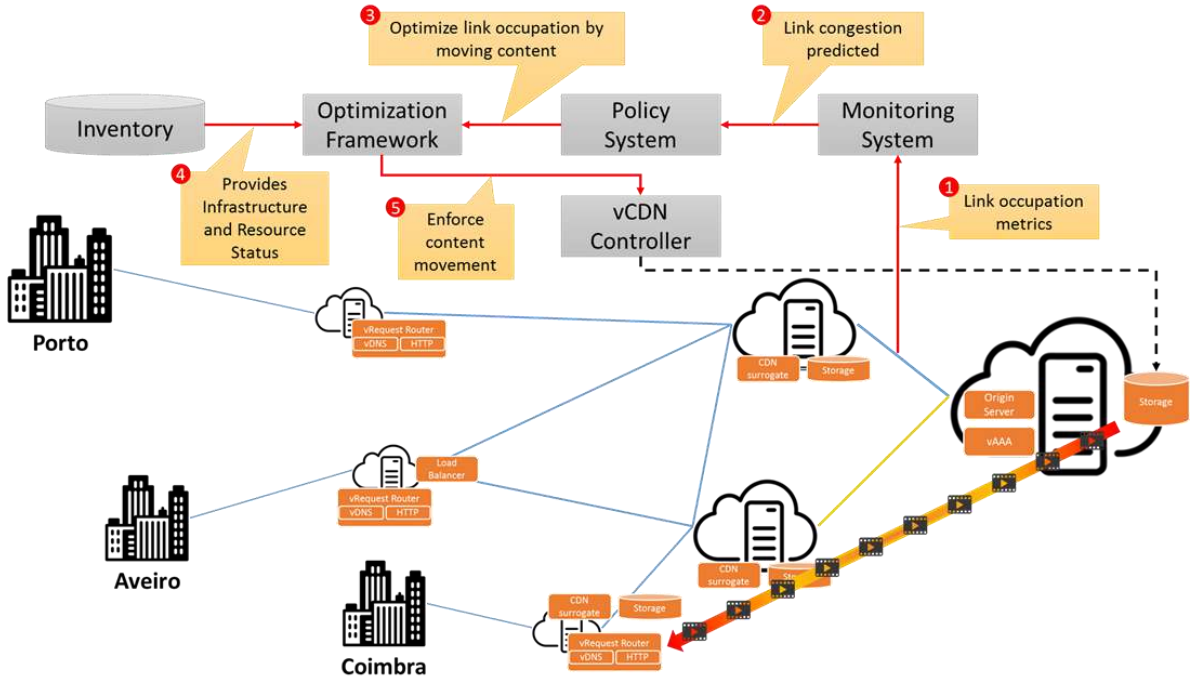

Figure 27 - OSS systems response to a congestion prediction

A CDN service is provisioned on a network slice optimized for the delivery of multimedia content, i.e. high throughput and low latency. To guarantee the service delivery, the monitoring systems are continuously collect data from the network and datacenter infrastructures.

At a given point, the metrics regarding a physical link between a regional DC and a centralized DC indicate an increase of bandwidth usage.

4.2.5.3 Step-by-step scenario

1. The metrics collected by the monitoring components are sent to analytics, which use machine learning to identify the causes and to provide predictive scenarios regarding the link usage

2. The analytics components predict an increase of requests for specific video contents that will lead to a congestion on the transport network near the central DC which may disrupt other services sharing the same infrastructure
3. The Policy Framework assesses the event which indicates the possibility of a network congestion and according to the current active policies determines that best action is to replicate the video contents on DCs closer to the consumers. To enforce the action, the Policy Framework notifies the Optimization Framework to replicate the contents deployed on the vCDN service with the goal of minimizing the bandwidth usage on the transport network.
4. The Optimization Framework choses the appropriate algorithm for the operation according to the goal defined by the Policy Framework. To accomplish that goal, it requests the necessary information from inventory and analytics systems to understand the current status of the network and DC infrastructure.
5. After running the optimization algorithm, the Optimization Framework requests the vCDN controller to trigger the execution of the operations of content replication with the identification of the content and DCs
6. Finally, the Optimization Framework triggers the MEC Orchestrator to enforce the redirection rules for the user's content requests.

4.2.5.4 Final Scenario

After the replication of content on the DCs that are hosting vCDN functions closer to the users, the collected metrics indicate a reduction on the occupied link bandwidth in vicinity of the centralized DC. The analytic applications after the content replication operation indicate that the potential network congestion has been avoided and store all the information regarding the sucessful operation for continuous learning.

4.2.6 Sub-case 4: vCDN surrogate deployment in MEC host

4.2.6.1 Description

It is intended that when instantiating an application in the edge computing environment the resources management be guaranteed so that the availability of the service fulfills the QoS requirements.

4.2.6.2 Initial Scenario

It is considered as a precondition that the network elements are installed and ready to be properly configured, starting the use case when the Orchestrator is requested to scale the vCDN service by deploying a new VNF instance. Moreover, prior the requests it is assumed that the Policy Framework has onboarded policies on all systems such as the Optimization Framework.

4.2.6.3 Step-by-step scenario

1. After the request validation, the Orchestrator requests from the Optimization Framework a recommendation for the deployment of the new VNF instance
2. The Optimization Framework uses the following information to identify the optimal location for the deployment of the new VNF instance:

a. Previously onboarded policies that impact the governance of the deployment of the new VNF
b. Information stored in inventories to assess the current usage and allocation of resources on the infrastructure
c. Information from analytics to assesss future usage and impact on other services deployed on the same shared infrastructure
d. Information from Orchestration templates to identify the needed resources for the new VNF instance

3. The Optimization Framework delivers to the Orchestrator the recommended location for the deployment of the new VNF instance, which in this case consists of a MEC DC located at the edge of the network
4. Orchestration prepares the operating environment at the edge. Namely, making sure that the enforcement of charging mechanisms and network policies are in place at that particular environment. If they are not, cater for their creation
5. Orchestration takes care of the instantiation of the VNF
6. Orchestration setss up data plane connectivity to the new VNF
   The new vCDN VNF is started (it will either connect autonomously to the CDN it belongs to or the Orchestration will take care of that)

4.2.6.4 Final Scenario

All network elements are properly configured and provisioned for the correct service provision in the DC edge. The DC edge also ensures the right network QoS resources and the service is correctly provided.

4.2.7 Sub-case 5: Invasion of Privacy hypervisor attacks

4.2.7.1 Description

This type of attacks aims at the disclosure of information about something that should not be available to a given entity or at the disruption of the service supplied by another VNF component. The vectors for such an attack are either very new at the time of writing, or unknown in the case of some complex tools that are expected to be introduced with the 5G network. This can be argued to be a part of a directed attack scenario, however the most likely scenario is that such an attack will have opportunistic characteristics where a random VNF component instance or hypervisor is targeted.

The recent discovery of viable attacks based on the architecture of the CPU, such as spectre and meltdown triggered all cloud providers to take counter measures in order to mitigate the new threat, however due to the high complexity of the current cloud infrastructure (which impacts the complexity of NFV), from hardware up to the multiple abstraction layers of the cloud operating system, new vulnerabilities are expected to be found. Hence, considering this class of attacks in the scope of this use case that requires running VNF component instances provided by a CDN operator, that may not be subject to the same scrutiny as the ones that run the core network, will enable the elicitation of a set of requirements that could otherwise be less than obvious or completely skipped.

4.2.7.2 Initial Scenario

The VNF component instances of a vCDN are running on the same infrastructure as other VNF component instances that handle different tasks.

4.2.7.3 Step-by-step scenario

1. The attack vector is discovered (note that this kind of attack can not be twarted via network tools)
2. If an ongoing attack is detectable, the operator may choose to isolate or completely stop VNF component instances that are are performing the attack
3. The operator scans all physical and virtual infrastructure for vulnerable instances
4. The operator migrates the virtual work load off each physical instance in turn, patching it without forcing a service interruption
5. The operator requests new (patched) VNFs from the suppliers if needed
6. The operator forces the service to fail over to patched VNF instances

4.2.7.4 Final Scenario

As the process finishes, all the infrastructure, both physical and virtual is patched against the newly found vulnerability. The VNF component instances from multiple VNF can coexist on the same infrastructure even if some of them try to perform such an attack it will not be successful.

4.3 Use case 2 – PPDR leveraging IoT in 5G

4.3.1 Context

The 5G networks bring support for differentiated scenarios, including IoT devices, machine-to-machine communications (M2M), critical infrastructures, optimized mobility for users, among others. These scenarios introduce different requirements that impact 5G networks. The communication of such requirements to the 5G network, allow that the 5G network to provide conditions to satisfy the requirements of applications. For instance, 5G is able to provide support for services with a certain delay, with certain packet loss ratios, or even to prioritize certain flows. . In such context, applications can communicate requirements according to the QoS model of 5G (classes for video, voice, or data), as documented in 3GPP TR 23.501.

In actual networks (3G, 4G, LTE) the configuration of the quality of service requires the intervention of an operator, which controls the full network and does not provide APIs to allow the dynamic configuration of the network, neither the communication of requirements. The NEF (Network Exposure Function) component in the 5G network allows the communication of requirements in a secure form [2], [3], considering the policies configured by an operator (e.g. assure authentication of Application Functions requests). With NEF it is possible to use 5G in critical missions scenarios, like the PPDR missions (e.g. police, firefighter, civil protection).

With the growing number of provisioned services in the 4G networks, and more recently in 5G, aspects related with the security at the service level and applications are becoming more relevant. With the implementation of services asVNFs that support value added services (such as PPDR in this use case), it is a matter of time until the discovery of a vulnerability or an employee (of the operator or one of the vendors) causes a severe impact on the core of the operator network the same way as cloud service providers have seen in the past. This creates the need to go beyond the upstream (NFV & 3GPPP) specified security mechanisms that focus only on how to build a secure system mostly via architectural constructs, and plan on how to manage existing vulnerabilities, as well as monitoring the network for unexpected activities in an attempt to detect any problems before they cause a disruption of service or impact the operator public image. This means that tools and methodologies that are usually seen on the

Internet or corporate networks become of interest for deployment on some layers of the operator network. The coordination of systems with different abilities such as traffic analysis, user behavior gathering or audit, and the cross reference of the events generated by those systems with external sources of information is expected to allow the detection of complex malicious behaviors that could otherwise remain undetected.

4.3.2 Motivation for 5G Networks

The transition of 5G networks brings a set of innovations, already started in 4G, like the support for critical communications in PPDR scenarios. The most relevant innovations that are possible with NEF are:

- Optimization of resources for critical missions: NEF allows that the conditions required for PPDR missions are properly configured in the 5G networks. In particular, allows the prioritization of flows to assure the safety and security of PPDR agents.
- Multi-vendor support: NEF acts as the entry point for 5G networks, avoiding vendor-lock for PPDR solutions over 5G networks.
- Network Policies more efficient and secure: The network can be configured to assure that the network traffic associated with NEF uses specific routes, or is distributed to allow load balancing, or is even sent to IDPS to assure the detection of possible attacks.

The transition to 5G networks brings a set of components, services and applications that reinforce the need for advanced security mechanisms:

- Slicing: The slicing mechanisms are new for 5G, as with all new services, it will come with a new set of challenges, some of those challenges may not yet be obvious. This may lead to new classes of attacks that may impact only one slice, or use a slice to impact the service provided by other slices in non trivial ways.
- Virtualization: the security tools can be virtualized and orchestrated according the concept of X-as-a-Service, which facilitates its placement and scalability.
- External exposure: The NEF component facilitates the exposure of the 5G network to external services, applications, but on the other hand puts an emphasis on the need for efficient control and security mechanisms.
- Monitoring: Various components already have interfaces (APIs) or auditing capabilities that allow the creation of security events, what is missing is a common way to read, parse and make sense of the generated information.

4.3.3 Sub-case 1: dynamic QoS configuration

4.3.3.1 Description

The 4G networks already include some support for critical missions [57], which usually is only found on Public Mobile Radio networks like TETRA and TETRAPOL. The support in LTE include support for group communications (R13 – GCSE), proximity services (R13 – ProSE) for device to device (D2D) communications, Mission Critical Push to Talk (MCPTT), among others.

The scenario herein defined includes support for IoT devices which can be used by fireman or other agents. In particular, the Bodykit allows the collection of data from biosensors, environmental sensors and allow the communications of voice and video with Command Control Centres (CCC). One of the relevant functionalities included in the Bodykit is the monitorization of safety of PPDR agents, where

alarms regarding safety are sent to the CCC. Such alarms can include the detection of man-down events (e.g. falls of PPDR agents), or even the presence of adverse and dangerous atmospheric environmental conditions like high temperatures.

The NEF component allows the configuration of prioritized flows like for the safety alarms. These flows must have a fixed allocated bandwidth and must be prioritized over other flows since they contain information that is crucial to the safety and security of PPDR agents. A full situational awareness is important in CCCs, as such commanders and operators in the CCCs may request pictures, photos, or even videos from the field. Such kind of information allows more informed operational and tactical decisions.

The QoS configuration is fundamental to guarantee the diverse operations of PPDR.

4.3.3.2 Initial Scenario

The NEF component/service is provisioned in the core of the 5G network and is available to PPDR terminals. NEF can be provisioned in a network slice or can be deployed according to other possible configurations of an operator.

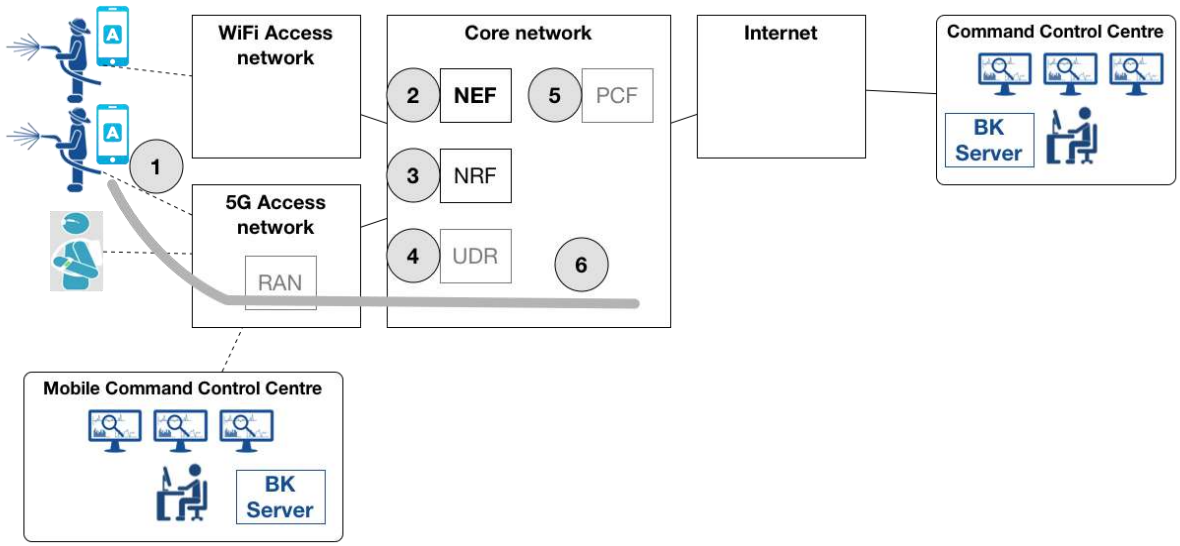

Figure 28 - Dynamic QoS scenario

All the remaining services in the core of the 5G network are properly provisioned and configured. For instance, the NRF – Network Resource Function is employed to allow the identification of service's endpoints (like PCF, AUSF, UDR, among others).

Afterwards, IoT devices (Bodykit) start and conclude with success all the procedures of connecting to the 5G network (network attach). In this phase, they receive a default flow with the default levels of QoS configured for the PDU sessions.

4.3.3.3 Step-by-step scenario

1. The Bodykit Server detects the presence of new devices in the network (through the authentication of devices and users in the Bodykit system). For each authenticated device, the Bodykit server asks to the NRF the endpoint of NEF.
2. The Bodykit Server, with the information of the NEF endpoint, starts the negotiation with NEF to assure the configuration of three types of flows by default to each device: 1-flow for priority

data (i.e. alarms), 2-flows for communications in real-time of voice and video; 3-flow for sensor data.

3. The NEF component receives information of the PCF endpoint responsible for the network slice where NEF is deployed, and responsible for the PDU session where the device is attached. This phase is important to allow the configuration of the QoS requirements.
4. NEF communicates the requirements received to the responsible PCF so that QoS flows are properly configured in the respective PDU sessions of the devices. PCF exposes an interface that enables the UE or network to explicitly request a certain level of QoS for the service session in which it is involved. From the perspective of PCF, the following procedure takes place
    a. PCF determines the policy to be applied in the network, due to the new requirements of the service
    b. PCF installs policies on the necessary network elements for differential QoS control of the data stream of the service session.
    c. PCF confirms to NEF the result of the operation (success or failure).
5. The flows are configured in the 5G network. The devices receive a notification that the QoS configuration is finalized. Such notification is sent by the AMF and PCF.

4.3.3.4 Final Scenario

After the configuration of the three types of flows, the device can start using the respective flows. The prioritized flow is employed for alarms.

The disposal of the QoS configuration is perform at request, from the Bodykit device upon defined thresholds of keepalive mechanisms, upon logout procedures. The removal of the priority flows can be subject to network policies.

4.3.4 Sub-case 2: Security for Application Functions

4.3.4.1 Description

The 5G networks already include some architectural components to assure the security like AAA and throttle control [2] as well as the separation of control and data plane interfaces. Nonetheless, these focus only on the access control and do not provide support for the detection and prevention of malicious behaviours.

The scenario herein presented introduces an Intrusion Detection and Protection System (IDPS) and Security Information Event Management (SIEM) composed by multiple tools and tailored for 5G networks. This allows the placement of probes in essential components, in particular in NEF, where services are exposed to the exterior, in the application functions that use NEF and in other components of the core of the 5G network such as network gateways or even side by side with other VNFs. The probes already present in the release 15 will be used to support the analysis by the security systems. This IDPS and SIEM should be composed of multiple tools that allow the detection and mitigation of complex behaviours potentially spanning multiple systems. Examples of detectable behaviors that would not be detected using only the upstream security mechanisms include but are not limited to: Scanning a subnet for vulnerabilities; accessing a system out of scheduled maintenance periods; and detecting known malware activity on the network.

The figure bellow depicts the applicational IDPS+SIEM in the architecture of a 5G network.

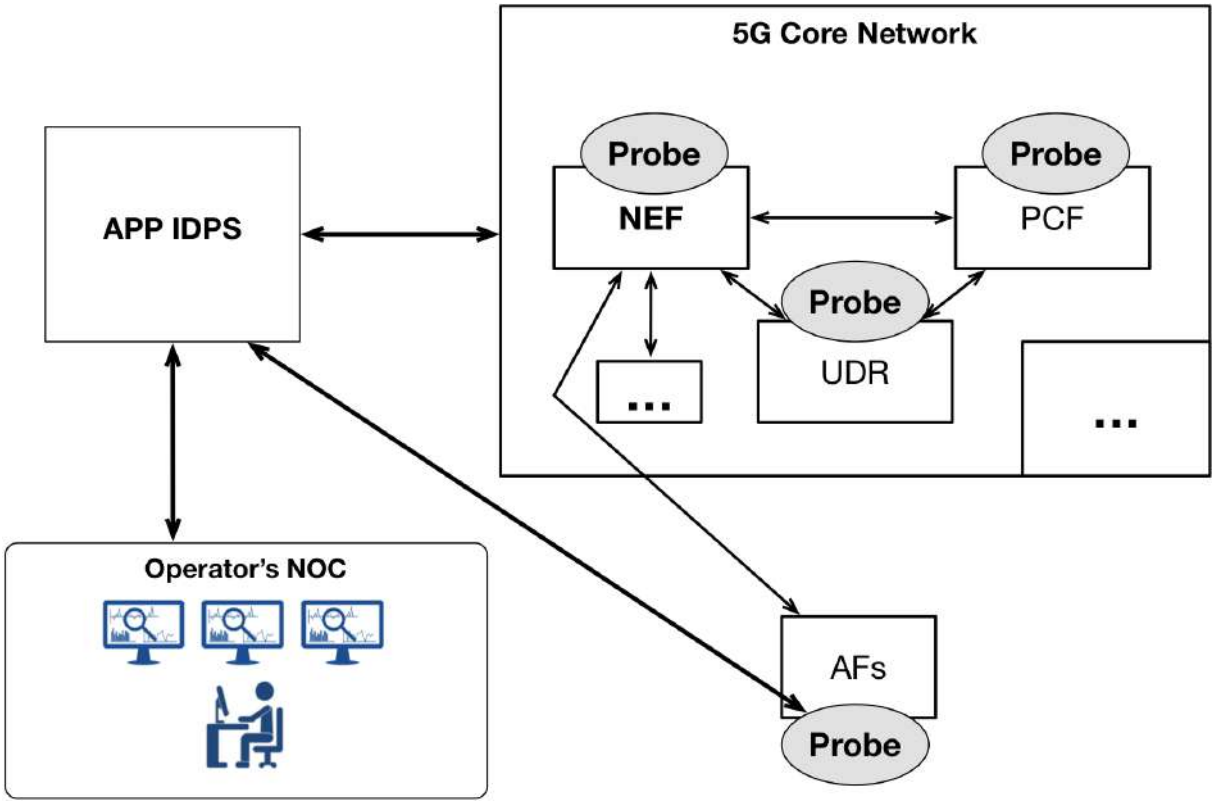

Figure 29 - IDPS deployment to secure 5G Network Core

4.3.4.2 Initial Scenario

The IDPS+SIEM engine is provisioned in the core of the network, or in a slice. This component consists in a centralized part which contains a set of policies and pre-configured rules to allow the analysis of events sourced from multiple sources and locations on the service network. Events coming from system audit tools, network traffic analysis, or profiling tools such as honeypots feed the central engine, that can detect both common patterns such as malware activities as well as advanced correlated patterns such as the establishment of a valid session by a sysadmin outside of a scheduled maintenance window.

Probes monitor diverse parameters and network links configured in the system, with the information of the probes being sent to the centralized part of the APP IDPS. The analysis process runs continuously as events arrive from the data sources. These events may be primary events, such as access control audit information, or can take the form of a pre-processed event such as the case of the detection of an ongoing attack where a traffic pattern is analyzed by another tool and the contents of the analysis are indicative of known malware. On a correlation phase, the IDPS engine checks the multiple events that are received to assure a better precision and significance. The analysis process verifies if any configured rule or policy is violated, in which cases a trigger for prevention actions is sent. Examples of violations which are addressed in this scenario include:

a. Multiple consecutive requests for a service or allocation of resources;
b. Communications from the core of the network to known command and control servers;
c. Port scanning on the control plane;

4.3.4.3 Step-by-step scenario

This subsections details the brief steps of this scenario, with particular emphasis on the types of triggers / violations and corresponding prevention measures:

1. The prevention actions can be sent to the target components or policy framework, and can be sent to the NOC of the operator (or entity responsible for the handling of such events) for posterior analysis and human confirmation. The prevention actions for each type of attack, or correlation result, and their application must be confirmed by the operator in the NOC[1], and may include the following:
    a. Multiple login failures of a specific account → deactivation of the account;
    b. Network scans on a service → throttling packets from source IP;
    c. Irregular use of network resources (e.g. high volume of traffic) → shutdown and blocking of irregular network connections.
    d. The exploit of web services, web applications vulnerabilities (e.g. SQLinjection, Cross Site Scripting) → deactivation of certain vulnerable functionalities in such applications or blocking such kind of requests.
    e. Brute force attacks on sensitive services (e.g. AAA) → throttling connections ore redirect such kind of traffic to honeynets for further analsysis (see section **Error! eference source not found.**).
2. At last, the IDPS component registers the taken action and verifies its effectiveness (enforcement).

4.3.4.4 Final Scenario

After the detection of a violation event of the rules or policies, an action is taken automatically or with human intervention. The normal operation of the network is established and any ongoing attack is prevented. A final step in this scenario includes storing all the information associated with the historic analysis component to allow a better recommendation for similar occurrences.

[1] The examples of the prevention actions are not exhaustive and may be modified according to the implementation of the security mechanisms for 5G services.

5 Requirements

5.1 Introduction

This section presents the high level requirements from the perspective of each of the addressed components, reflecting what is needed to support the envisioned functionalities and use cases. Potential information considered within the requirements includes the managed information, available actions, interactions with and dependencies on external entities (e.g. expected role or particular functionalities).

Thus, the contained information paves the path for the definition of PPS2 architecture in the upcoming Deliverable D2.2.

5.2 Policy Management and Control Mechanisms Requirements

Table 1 - List of Policy Management and Control Mechanisms Requirements

Requirement ID	Requirement description
Pol_1	The Policy Framework must be able to know the several ecosystem network functions
Pol_2	The Policy Framework must be able to know the ecosystem management functions
Pol_3	The Policy Framework must allow the creation and management of policies associated to a given function
Pol_4	The Policy Framework must be able to know the services delivered in the ecosystem
Pol_5	The Policy Framework must allow the creation and management of policies for the different services
Pol_6	The Policy Framework must be able to break down high-level intents into elementary policies at the various levels and points of decision
Pol_7	The Policy Framework must be able to check dependencies and validate the consistency of the policies at the different levels of decision (e.g.: NFVO and VIM)
Pol_8	The Policy Framework must be able to check dependencies and validate the consistency of the policies at the different points of decision (e.g.: PCF and FW)
Pol_9	The Policy Framework must be able to interpret, validate and process policies descriptions in order to apply the configured policies
Pol_10	It should be possible for an external system to configure policies into the Policy Framework using a specific description language
Pol_11	The Policy Framework must expose an interface to receive incoming notifications of conditions change (e.g., notification of high traffic load from monitoring system)

Requirement ID	Requirement description
Pol_12	The PCF should follow the requirements specified in 3GPP standards, namely implementing the following interfaces: a. N5 (AF) b. N7 (AMF) c. N15 (UDR) d. N23 (NWDAF) e. N25 (SMF) f. N30 (NEF)
Pol_13	The Policy Framework should be capable of making decisions about products, services or resources in order to avoid non-compliance with previously defined policies
Pol_14	The entire history of successful and unsuccessful actions resulting from operational decisions should be kept by the Policy Framework
Pol_15	The Policy Framework must distribute active policies to relevant systems, e.g. Optimization Framework, PCF, prior their use
Pol_16	The Policy Framework must implement a policy distribution mechanism
Pol_17	All changes to active policies must be distributed to relevant systems using the policy distribution mechanism

5.3 Service Definition and Orchestration Mechanisms Requirements

Table 2 - List of Service Definition and Orchestration Mechanisms Requirements

Requirement ID	Requirement description
Orc_1	Orchestration components must use descriptors or templates to describe services and associated operations
Orc_2	Orchestration components must be able to deploy individual applications and network functions based on the information stored in descriptors or templates as part of a service level operation
Orc_3	Orchestration components must be capable of resolving dependencies in service operations, e.g. the VNF must be deployed before applying a configuration
Orc_4	Orchestration components must be able to configure rules or other relevant artifacts on applications and network functions
Orc_5	Services and associated operations may use a common language to reference services, resources and other artifacts to facilitate the interaction between components within the management and control layer

Requirement ID	Requirement description
Orc_6	The optimization system should be able to communicate with a policy repository in order to obtain policies relevant to a given context that will be the focus of an optimization algorithm
Orc_7	The optimization system should be able to communicate with inventory systems in order to obtain the necessary information about the current state of products, services, resources, applications or infrastructure
Orc_8	The optimization system should be able to interact with orchestration systems and / or application controllers in order to apply optimization actions
Orc_9	The optimization system should support different algorithms developed for specific optimization contexts
Orc_10	The optimization system should support the dynamic management of algorithms

5.4 Assurance Applications Requirements

Table 3 - List of Assurance Applications Requirements

Requirement ID	Requirement description
Ass_1	It will be possible to collect metrics from both the network infrastructure and the computing infrastructure, i.e. DCs
Ass_2	It will be possible to aggregate metrics by service, network slices, and resource groups
Ass_3	The Monitoring System shall be capable of producing the network and computing infrastructure KPI's identified as necessary, for the measurement of the QoS and SLA assurance.
Ass_4	Collected metrics and KPI's must be available to analysis applications
Ass_5	It will be possible to map the location of the different users in the access network
Ass_6	The analysis applications should integrate machine learning mechanisms that allow to predict potential scenarios of failure and degradation of service in time for proper actions
Ass_7	It must be possible to collect metrics and events in the diverse core components of 5G (e.g. NEF).
Ass_8	The placement of probes in 5G components (for instance in NEF) must be possible
Ass_9	The placement of probes in Application functions, services external to 5G network must be possible
Ass_10	It should be possible to receive information about requests for end user content

Requirement ID	Requirement description
Ass_11	Applications and Network Functions may use a specific interface to the Monitoring Systems to access enriched information to enhance their capabilities
Ass_12	The history of actions on products, services and resources should be used by the analysis components to enable inference
Ass_13 (a-d)	The multi-tenancy related requirements for the monitoring system shall include: a. The monitoring system must support true multi-tenancy, i.e. provide data separation, content separation, settings such as time-zone, locale, first day of week, busy hour (BH) definitions, aggregation settings, retention periods for different tenants. b. It must allow authorization per tenant c. It must allow authentication per tenant d. Data retention shall be configurable per adaptation and aggregation. This should be configurable per tenant.
Ass_14	Purge function to remove excessive data stored on the system shall be configurable. This should be configurable per tenant.
Ass_15	The Ve-Vnfm-em reference point shall support the VNF Lifecycle Change Notification interface produced by the VNFM.
Ass_16	The Ve-Vnfm-em reference point shall support the VNF Performance Management interface produced by the VNFM.
Ass_17	The Ve-Vnfm-em reference point shall support the VNF Fault Management interface produced by the VNFM.
Ass_18	The Ve-Vnfm-em reference point may support the VNF Indicator interface produced by the EM.
Ass_19	The Ve-Vnfm-em reference point shall support the VNF Configuration Management interface produced by the VNFM.
Ass_20	The Os-Ma-nfvo reference point shall support the NSD Management interface produced by the NFVO.
Ass_21	The Os-Ma-nfvo reference point shall support the NS Lifecycle Change Notifications interface produced by the NFVO.
Ass_22	The Os-Ma-nfvo reference point shall support the NS Performance Management interface produced by the NFVO.
Ass_23	The Os-Ma-nfvo reference point shall support the NS Fault Management interface produced by the NFVO.

5.5 Support Mechanisms Requirements

Table 4 - List of Support Mechanisms Requirements

Requirement ID	Requirement description
Sup_1	Application and Network Functions must be able to communicate the QoS requirements to NEF
Sup_2	It must be possible to store the information of flows that are associated to the PDU session of each device
Sup _3	NEF's interface to PCF (N30) must be available for the configuration of QoS
Sup_4	NEF's interface to NRF must be available for obtaining information regarding endpoints like PCF
Sup_5	NEF's interface to AMF must be available
Sup_6	NEF's interface to UDR must be available
Sup_7	NEF's interface to UDM must be available
Sup_8	NEF's interface to SMF (N29) must be available
Sup_9	NEF must expose its interface (Nnef) to Application Functions
Sup_10	NEF must be always available implementing mechanisms of high availability
Sup_11	A record of flows that are admitted and not admitted for each device and PDU session must be kept.
Sup_12	One NEF instance must exist for each slice or a single NEF will handle all requests, depending on the selected option.
Sup_13	NEF must support probes for different purposes such as monitoring or security.
Sup_14	For an OTT scenario, DNS requires a repository for the images of the Network Functions.
Sup_15	DNS, if acting as NRF requires the availability of status option to test the reachability of services.
Sup_16	For scalability purposes, DNS requires Database as a Service to hold the information of resources.
Sup_17	5G services security must be in place to secure DNS, as a critical support service.
Sup_18	DNS must be always available implementing mechanisms for high availability.

5.6 Security Mechanisms Requirements

Table 5 - List of Security Mechanisms Requirements

Requirement ID	Requirement description
Sec_1	Dataplane congestion must be detectable a. one slice should not be allowed to grow so much in resource usage that it impacts the service on other slices.
Sec_2	The source of dataplane congestion must be characterized (via traffic sampling)
Sec _3	The Policy framework must have the capacity to change traffic priority on the dataplane (prioritizing known “good” traffic while a potential attack is analysed)
Sec_4	The Policy framework must have the capacity to block traffic that has specific characteristics (directly blocking malicious traffic)
Sec_5	The Policy framework must be able to override certain DNS entries (common technique to disrupt communication with command and control servers)
Sec_6	Dataplane tools that allow the gathering of traffic samples should be permanently deployed, or dynamically deployable on strategic network locations
Sec_7	Dataplane tools that perform policy based packet filtering should be permanently deployed or dynamically deployable on strategic network locations
Sec_8	The DNS service should allow policy-based overriding of entries
Sec_9	All the policies that manipulate traffic due to specific security problems should have an expiration date in order to allow the network to automaticaly return to normal operation.
Sec_10	Traffic inspection tools should be permanently deployed (or deployable on demand) on strategic locations of the network
Sec_11	Application-specific event gathering tools should be included in as many functions as possible and the gathered information should be analyzed and cross checked with other sources of information
Sec_12	Multiple sources of security ionformation should be correlatable, so that complex attack patterns can be detected
Sec_13	The pattern of communication between a function and the outside of the network (such as license checks) should be well known, so that unexpected communications can be easily detectable
Sec_14	Internal network scanning or mapping activities should be detectable and be treated as a potential security breach
Sec_15	The operator should always keep an updated list of known vulnerabilities in the infrastructure (both physical and virtual) so that he can: a. Plan on how to patch or mitigate each b. Isolate those that can not be patched

Requirement ID	Requirement description
Sec_16	(Potential) Security breaches should be automatically thwarted if the action does not impact the service

5.7 Virtualization Platform Requirements

Table 6 - List of Virtualization Platform Requirements

Requirement ID	Requirement description
Virt_P_1	Open REST/API for full automation of tenant workloads, namely: - Creatuib if tenant networks, - Creatuib if tenant VMs (or containers), - Allocation of tenant storage.
Virt_P_2	Open automation capabilities for: - Decommissioning of compute nodes from the Virtualization Platform, - Scaling the physical cluster with a compute node.
Virt_P_3	Open REST/API for monitoring and reporting on resources usage.
Virt_P_4	Built-in security features to allow for workloads isolation

6 Conclusion

This document provides the description of the cornerstone research areas and considered components to be addressed within PPS2, two example scenarios illustrative of the role employed by the functional components, and the target requirements derived from each research area.

The targetted components are expected to fully leverage the capabilities and availability of service-based 5G Core, which *per se* is defined to be agnostic to the access network – thus its huge potential for enabling novel business models spanning multiple vertical industries (e.g. automotive). As such, some of the solutions and associated features (e.g. Network Optimizer) herein addressed may themselves be exploitable and differently applicable under different environments and by stakeholders with differentiated targets (e.g. efficiency vs reliability). Considering 5G Core-enabling components, two different approaches are following: the pursuit of a NEF solution follows a service-centric approach, i.e. aiming to enrich the base functionality taking into account a específic service context (e.g. PPDR). Using a different approach, the Policy Framework aims to extend the PCF functionality by overcoming the policies diversity and complexity, exploring recent development in intent-based interfaces. Moreover, the set of security-related solutions are expected to encompass the vast majority of the technical threats targeting the operator's network.

The presented information will support the upcoming architectural specification stage, which will be documented in document D2.2 by M6.

7 References

[1] F. Mademann, “System architecture milestone of 5G Phase 1 is achieved,” 3GPP, 2017. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1930-sys_architecture. [Acedido em April 2018].

[2] “System Architecture for the 5G System - TS 23.501,” 3GPP, 2018.

[3] “Procedures for the 5G System - TS 23.502,” 3GPP, 2018.

[4] “Policy and Charging Control Framework for the 5G System; Stage 2 - TS 23.503,” 3GPP, 2018.

[5] T. Tovinger, “Management, Orchestration and Charging for 5G networks,” 3GPP, 2018. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1951-sa5_5g. [Acedido em April 2018].

[6] “Management and orchestration of networks and network slicing; Concepts, use cases and requirements - TS.28.530,” 3GPP, 2018.

[7] “Management and orchestration of networks and network slicing; Provisioning; Stage 1 - TS 28.531,” 3GPP, 2018.

[8] “Management and orchestration of networks and network slicing; Provisioning; Stage 2 and stage 3 - TS 28.532,” 3GPP, 2018.

[9] “Management and orchestration of networks and network slicing; Management and orchestration architecture - TS 28.533,” 3GPP, 2018.

[10] “ETSI GS NFV 002 v1.2.1: Network Functions Virtualisation (NFV); Architectural Framework,” ETSI, 2014.

[11] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini e H. Flinck, “Network Slicing & Softwarization: A Survey on Principles, Enabling Technologies & Solutions,” *IEEE Communications Surveys & Tutorials,* p. 1, 2018.

[12] NGMN Alliance, “Description of Network Slicing Concept,” NGMN Alliance, 2016.

[13] B. Chatras, U. S. T. Kwong e N. Bihannic, “NFV enabling network slicing for 5G,” em *Proceedings of the 2017 20th Conference on Innovation in Clouds, Internet and Networks (ICIN)*, 2017.

[14] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca e J. Folgueira, “Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges,” *IEEE Communications Magazine,* pp. 80-87, May 2017.

[15] M. K. Shin, S. Lee, S. Lee e D. Kim, “A way forward for accommodating NFV in 3GPP 5G systems,” em *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 2017.

[16] “Telecommunication management;Study on management and orchestration of network slicing for next generation network - TR 28.801,” 3GPP, 2018.

[17] “Improved operator experience through Experiental Networked Intelligence (ENI),” ETSI, 2017.

[18] “ONAP,” The Linux Foundation , 2017. [Online]. Available: https://www.onap.org/. [Acedido em April 2018].

[19] “ETSI GR NFV-IFA 023 v3.1.1: Network Functions Virtualisation (NFV); Management and Orchestration; Report on Policy Management in MANO; Release 3,” ETSI, 2017.

[20] “TM Forum Clickable Model,” 2018. [Online]. Available: http://casewise.tmforum.org/evolve/statics/frameworx/index.html.

[21] “End-to-End Service Instantiation Using Open-Source Management and Orchestration Components,” Intel, 2016.

[22] R. Guerzoni e e. al, “Analysis of end-to-end multi-domain management and orchestration frameworks for software defined infrastructures: an architectural survey,” *Transactions on Emerging Telecommunications Technologies,* pp. Volume 28, Issue 4, 2016.

[23] M. Ranganathan, “Operators agree: SON pivotal as networks transform to 5G & Cloud,” Nokia, 2016.

[24] “ECOMP (Enhanced Control, Orchestration, Management & Policy,” AT&T, 2016.

[25] “Optimization Framework Project,” 2017. [Online]. Available: https://wiki.onap.org/display/DW/Optimization+Framework+Project.

[26] “Self-Organizing Networks – current features and evolution,” 2016. [Online]. Available: https://www.grandmetric.com/2016/08/25/self-organizing-networks-features-and-evolution/.

[27] L. G. Jessica Moysen, “From 4G to 5G: Self-organized Network Management meets Machine Learning,” *CoRR,* p. abs/1707.09300, 2017.

[28] “Future OSS - Providing the AGILITY to support operations transformation of hybrid networks,” Huawei, 2017.

[29] “OODA Loop: A comprehensive guide,” 2014. [Online]. Available: https://www.artofmanliness.com/2014/09/15/ooda-loop/.

[30] “ETSI GS NFV-IFA 009 V1.1.1: Network Functions Virtualization (NFV); Management and Orchestration; Report on Architectural Options,” ETSI, 2016.

[31] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese e D. Walker, “P4: programming protocol-independent packet processors”,” em *SIGCOMM Comput. Commun. Rev. 4*, 2014.

[32] “Overview of OpenFlow v1.3.0,” [Online]. Available: http://docs.ruckuswireless.com/fastiron/08.0.70/fastiron-08070-sdnguide/GUID-031030CA-62EC-4009-A516-5510238EF8F4.html.

[33] “OpenFlow Switch Specification v1.5.1 (protocol version 0x06),” 2015. [Online]. Available: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf.

[34] G. Chehab, A. Ajaeiya, N. Adalian, I. H. Elhajj e A. K. a. A., “Flow-based Intrusion Detection System for SDN,” em *2017 IEEE Symposium on Computers and Communications (ISCC)*, 2017.

[35] A. A. a. B. Pranggono, “Machine learning based intrusion detection system for software defined networks,” em *2017 Seventh International Conference on Emerging Security Technologies (EST)*, 2017.

[36] N. L. M. v. A. Kuipers, C. Doerr e F. A., “OpenNetMon: Network monitoring in OpenFlow Software-Defined Networks,” em *2014 IEEE Network Operations and Management Symposium (NOMS)*, 2014.

[37] “ONOS Packet-Stats SDN application source code repository,” 2018. [Online]. Available: https://github.com/opennetworkinglab/onos/tree/master/apps/packet-stats.

[38] P. K. Shanmugam, N. D. Subramanyam, J. Breen, C. Roach e J. Van der Merwe, “DEIDtect: Towards Distributed Elastic Intrusion Detection,” em *Proceedings of the 2014 ACM SIGCOMM Workshop on Distributed Cloud Computing*, 2014.

[39] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi e M. Ghogho, “Deep learning approach for Network Intrusion Detection in Software Defined Networking,” em *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2016.

[40] A. Bianco, P. Giaccone, R. Mashayekhi, M. Ullio e V. Vercellone, “Scalability of ONOS Reactive Forwarding Applications in ISP Networks,” *Computer Communications, Vol. 102, Issue C,* pp. 130-138, 2017.

[41] A. Bianco, P. Giaccone, A. Mahmood, M. Ullio e V. Vercellone, “Evaluating the SDN control traffic in large ISP networks,” em *2015 IEEE International Conference on Communications (ICC)*, 2015.

[42] X. Wu, M. Liu, W. Dou e S. Yu, “DDoS attacks on data plane of software-defined network: are they possible?,” *Security and communication networks, vol. 9, issue 18,* pp. 5444-5459, 2016.

[43] “ONOS virtual network subsystem,” 2016. [Online]. Available: https://wiki.onosproject.org/download/attachments/6357849/VirtualNetworkSubsystem.pdf?version=1&modificationDate=1470869909080&api=v2.

[44] “OpenStack and OpenDaylight,” 2018 . [Online]. Available: https://wiki.opendaylight.org/view/OpenStack_and_OpenDaylight.

[45] Y. Li e M. Chen, “Software-Defined Network Function Virtualization: A Survey,” *IEEE Access, vol. 3,* pp. 2542-2553, 2015.

[46] “P4 Language Consortium, “P4 Language Specification, version 1.0.0”,” [Online]. Available: https://p4.org/p4-spec/docs/P4-16-v1.0.0-spec.html. [Acedido em April 2018].

[47] “gRPC: a high-performance, open-source universal RPC framework,” [Online]. Available: https://grpc.io/. [Acedido em April 2018].

[48] “P4 Consortium, P4 Runtime,” [Online]. Available: https://p4.org/p4-runtime/. [Acedido em April 2018].

[49] “ONOS and P4Runtime - SDN/NFV world congress (L123) - Technical Demo,” October 2017. [Online]. Available: https://www.youtube.com/watch?v=BE_y-Sz0WnQ&feature=youtu.be. [Acedido em April 2018].

[50] “P4.org Applications Working Group, Telemetry Format Specification version 1.0,” [Online]. Available: https://github.com/p4lang/p4-applications/blob/master/docs/telemetry_report.pdf. [Acedido em April 2018].

[51] “5G System; Technical Realization of Service Based Architecture; Stage 3 – TS 29.500,” 3GPP, 2018.

[52] “"DNS over HTTPS" IETF Working Group,” [Online]. Available: https://datatracker.ietf.org/wg/doh/about/.

[53] “ETSI GS NFV-SEC 014 v0.015: Network Functions Virtualisation (NFV); NFV Security; Security Specification for MANO Components and Reference points,” ETSI, 2018.

[54] “Security architecture and procedures for 5G System – TS 33.501,” 3GPP, 2018.

[55] Cisco, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021,” 28 March 2017. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[56] D. Helfrick, D. Hodson, A. Lynch e E. Robinson, “CDN 3.0: The Next Generation of Content Delivery,” IBB Consulting Group.

[57] B. Bhatia, “ITU Role in 5G and PPDR,” 2017. [Online]. Available: http://www.bharatexhibitions.com/en/5GI2017/SpeakerPresentations/SESSION%202/Bharat%20Bhatia.pdf.

[58] P. Almeida, Melhorar aspetos funcionais dos modelos de documentação, Aveiro: PT Inovação e Sistemas, 2014.

[59] P. Almeida, "Um bom exemplo de uma referência bibliográfica," PT Inovação e Sistemas, Aveiro, 2014.

[60] S. F. Monica Paolini, “Mastering Analytics: How to benefit from big data and network complexity,” Senza Fili Consulting, 2017.

[61] “ETSI GS NFV-IFA 009 v1.1.1: Network Functions Virtualisation (NFV); Management and Orchestration; Report on Architectural Options,” ETSI, 2016.

[62] M. G. Kibria, “Big Data Analytics and Artificial Intelligence in Next-Generation Wirelesss Networks,” *CoRR,* vol. abs/1711.10089, 2017.

[63] J. P. Sr., “What Is a SIEM?,” 2016. [Online]. Available: https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/.

[65] “SDN Guide,” 2016. [Online]. Available: https://www.sdnlab.com/sdn-guide/14736.html.

[66] “Architecture enhancements to facilitate communications with packet data networks and applications - TS 23.682,” 3GPP, 2018.

Authors List

Partner	Author
Altice Labs, S.A.	Francisco Fontes, Jacinto Vieira, Rui Calé, Miguel Santos, José Cabaça
Altran	Sérgio Figueiredo, Bruno Parreira
IT	Susana Sargento, Carlos Senna
IT Center	Rui Teixeira, Rui Gouveia
Nokia	Hugo Vieira, João Fragoso Rodrigues
Onesource	André Gomes, Bruno Sousa, Luís Cordeiro, Pedro Silva, Vitor Fonseca
PDM&FC	Diogo Costa, João Pires, Ricardo Pinto
Ubiwhere	Tiago Batista, Ricardo Preto
Universidade de Coimbra	Tiago Cruz, Jorge Proença, Miguel Freitas

Document history

Version	Date	Description
0.1	12-04-2018	First version including all partners' contributions.
0.2	18-04-2018	First document revision, comments and references.
0.3	23-04-2018	Second revision including partners' contributions improvements.
0.4	07-05-2018	Revision by Project Leader (Francisco Fontes)
1.0	07-05-2018	Final version