Deliverable D2.4

Management Plane System Definition, APIs and Interfaces

Editor:	Imen Grida Ben Yahia, Orange Labs Networks (France)
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	30th April 2018
Actual delivery date:	8th of May 2018
Suggested readers:	Infrastructure Providers, Communication Service Providers, Digital Service Providers, Network Operators, Digital Service Customers, Vertical Industries, Telecommunication/ICT Professionals
Version:	1.0
Total number of pages:	95
Keywords:	5G, network slice, slice management and orchestration, management plane, control plane, cognitive network management, multi-domain slice, slice information model, slice template.

Abstract

This document defines and specifies the general architecture of the management plane system to manage network slicing in the context of 5G networks. The proposed management plane enables not only intra-domain but also inter-domain end-to-end network slice management and orchestration. To facilitate the design of the modules for slice management, an information model in the context of SliceNet's network slicing is defined. A cognitive network slice management sub-plane with its inner modules is specified towards achieving cognition-based, machine learning enabled management for QoS and QoE awareness and optimisation, in relation to slice and service management for network operators, vertical users, and other stakeholders with different roles in the 5G system. The management plane, information model concepts including the slice template, the inter and intra domain considerations as well as SliceNet roles are instantiated for the project use cases, namely, eHealth, Smart City, Smart Grid.

Disclaimer

The research leading to these results has received funding from the European Union Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/761913.

Impressum

[Full project title] End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks

[Short project title] SLICENET

[Number and title of work-package] WP2- SLICENET System Definition

[Number and title of task] T2.3 - Management Plane System Definition, APIs and Interfaces

[Document title] Management Plane System Definition, APIs and Interfaces

[Editor: Imen Grida Ben Yahia, Orange Labs Networks (France)]

[Work-package leader: Marius Iordache, Orange Romania]

Copyright notice

Executive summary

Network slice management in a 5G system is challenging and complicated, taking into account the various intra- and inter-domain deployment scenarios, divergent use cases of different QoS/QoE requirements, stakeholders of different roles and business models, the immaturity of standards, the complexity of integrating it with network slice control, among other issues. The SliceNet management plane presented in this document targets to address some of these highlighted challenges. By taking a twofold design approach, both bottom-up and top-down, we present an advanced network slice management system that is capable of handling both intra- and inter-domain slices, supporting various slice-based representative use cases, differentiating stakeholders' roles, integrating with the defined SliceNet control plane, and leveraging and advancing related standards etc.

Specifically, this document is defining and specifying:

- We design the management plane by advancing the state of the art through positioning the add-ons of SliceNet and filling the gaps in the ongoing standardisation to ease the participation and contribution of the project to relevant SDOs;
- We define the management modules including cognition and orchestration;
- We define the information manipulated within those blocks as part of the SliceNet information model;
- We define the roles of the main stakeholders in the network slice enabled 5G ecosystem;
- We show how the proposed management and orchestration fits the project use cases: Smart city, eHealth and Smart Grid.
- We ensure the mapping of the definitions and specifications of the overall SliceNet architecture and the SliceNet control plane architecture to those of this SliceNet management to create an integrated slice control, management and orchestration system;
- We explore how inter-/multi-domain network slices can be managed.

List of authors

Company	Author	Contribution
CREATIVE SYSTEMS ENGINEERING (C.S.E) MONOPROSOPI EPE, Greece	Konstantinos Koutsopoulos Athanasios Kokkinis John Vavourakis	
ORANGE SA	Imen Grida Ben Yahia Bruno Chatras	Deliverable editor; definition of the information model; cognitive and policy management, overall interaction with orchestration and QoE/SLA management.
NEXTWORKS	Giacomo Bernini Pietro G. Giardina	
UNIVERSITAT POLITECNICA DE CATALUNYA	Fernando Agraz, Albert Pagès, Salvatore Spadaro, Joan M. Gené	Section 5: Definition and specification of the QoE/SLA manager, monitoring system and interactions between QoE/SLA manager with orchestration sub-plane
ALTICE LABS SA, Portugal	Gonçalo Gaspar, José Cabaça, Pedro Neves, Rui Calé	SliceNet Roles, Management Architecture, Multi-Domain Architecture
UNIVERSITY OF THE WEST OF SCOTLAND	Jose Maria Alcaraz Calero; Qi Wang; Zeeshan Pervez; Hector Marco	Abstract; Executive Summary; Introduction; Information Model; Multi-domain Scenarios and Considerations; Overall Management in Multi-domain
ORANGE ROMANIA SA	Marius Iordache Vlad Sorici Ana Rosu Catalin Brezeanu	Smart City use case description, and correlation with the management modules
Dell EMC INFORMATION SYSTEMS INTERNATIONAL	Zdravko Bozakov Thuy Truong	Management view considering multi-domain aspects, roles and Information model for eHealth UC.
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD	Katherine Barabash Valleriya Perelman Dean H Lorenz	

Deliverable Reviewers

EURESCOM-EUROPEAN INSTITUTE FOR RESEARCH AND STRATEGIC STUDIES IN TELECOMMUNICATIONS GMBH	Anastasius Gavras
HELLENIC TELECOMMUNICATIONS ORGANIZATION S.A. - OTE AE	Agapiou Yiorgos
NEXTWORKS	Giacomo Bernini

Table of Contents

Executive summary 3
List of authors 4
Deliverable Reviewers 4
List of tables 7
List of figures 8
Abbreviations 10
1 Introduction 16
1.1 Objectives 16
1.2 Approach and Methodology 16
1.3 Document Structure 17
2 Related work 18
2.1 IETF Common Operations and Management on Network Slices 18
2.1.1 COMS architecture 18
2.1.2 Technology Independent Information Model for Network Slicing 20
2.1.3 Gateway Function for Network Slicing 21
2.2 ETSI NFV Network Slicing Support 23
2.3 3GPP Slicing concepts 25
3 SliceNet Roles Considerations 29
3.1 SliceNet Roles Definition 29
3.1.1 Network Service Provider Role 29
3.1.2 Digital Service Provider Role 31
3.1.3 Digital Service Customer Role 32
3.2 Overview of Multi-domain considerations 34
3.3 SliceNet Roles applied to Multi-Domains 34
3.4 Considerations about the SliceNet Management Architecture and Roles 35
3.4.1 DSP & NSP Standalone Actors 36
3.4.2 DSP & NSP Combined Actor 39
4 SliceNet Information Model for Slices 43
4.1 Service-Slice-Resource concepts definitions 43
4.2 Information Model Diagrams 46
4.3 SliceNet Slice Template 50
5 Management System Definition 52
5.1 Orchestration and Information components 54
5.1.1 Slice Service Orchestrator overview 55
5.1.2 Network Domain Orchestrator 58

5.1.3 QoE/SLA Manager 62
5.1.4 P&P Manager 63
5.2 Monitoring components 65
5.3 Cognitive management components 67
5.3.1 Aggregation modules 68
5.3.2 Analytics modules 69
5.3.3 Policy Framework Modules 70
6 Preliminary management view for SliceNet use cases 74
6.1 Multi-domain considerations applied to SliceNet use cases 74
6.2 Smart City 75
6.2.1 Use case description 75
6.2.2 Management modules overview 76
6.2.3 Use case considered SliceNet Roles 77
6.3 Smart Grid 79
6.3.1 Use case description 79
6.3.2 Management modules overview 80
6.3.3 Use case considered roles 82
6.4 eHealth 84
6.4.1 Use case description 84
6.4.2 Management modules overview 85
6.4.3 Use case considered roles 86
7 Conclusion 89
References 90
Annex A 92
A.1 Control Plane and APIs 92

List of tables

Table 1 Slice related Concepts 43
Table 2 associations between main concepts 44
Table 3 Slice template 50
Table 4 Multi-domain requirements from SliceNet use cases 74
Table 5 Mapping of NGMN multi-domain categories to SliceNet use cases 74
Table 6 General Smart City UCs KPIs 75
Table 7 Smart City KPIs 75
Table 8 Mapping the management modules and the operations realized for the use case 76
Table 9 Use-case performance requirements 80
Table 10 mapping the management modules and the operations realized for the use case 80
Table 11 Proposed SliceNet KPIs for eHealth UC 84
Table 12 management modules for the use case 85

List of figures

Figure 1 COMS overall architecture and technology agnostic orchestration approach 19
Figure 2 COMS network slice YANG model. 20
Figure 3 COMS “netslice:service-instance” (left) and “netslice:slice-level-attributes”(right) models.. 21
Figure 4 COMS SLG approach for network slice subnets interconnection 22
Figure 5 Inter-Domain (ID) SLG for inter administrative domain network slice subnets interconnection 22
Figure 6 Deployment of SLG functions (and control) in NFV environments. 23
Figure 7 3GPP and NFV information models potential mapping (source ETSI GS NFV-EVE 012) 23
Figure 8 3GPP and NFV management components potential relationship (source ETSI GS NFV-EVE 012)..... 25
Figure 9 3GPP Dedicated Core 26
Figure 10 3GPP information modeling of a slice 27
Figure 11 5G Core Network Functions and Service based architecture..... 28
Figure 12 Network Service Provider Role - High-Level Perspective 30
Figure 13 Network Service Provider Role - Detailed Perspective 30
Figure 14 Digital Service Provider Role - High-Level Perspective..... 31
Figure 15 Digital Service Provider Role – Detailed Perspective 32
Figure 16 Digital Service Customer Role - High-Level Perspective..... 33
Figure 17 Digital Service Customer Role - Detailed Perspective 33
Figure 18 SliceNet Roles Applied to Multi-Domain - High-Level Perspective 35
Figure 19 SliceNet Roles Applied to Multi-Domain – Detailed Perspective..... 35
Figure 20 Management Responsibilities vs SliceNet Roles (DSP & NSP Standalone) 36
Figure 21 Management Architecture Components – DSP Standalone Perspective 37
Figure 22 Management Architecture Components – NSP Standalone Perspective 38
Figure 23 Management Responsibilities vs SliceNet Roles (DSP & NSP Combined)..... 39
Figure 24 Management Architecture Components – DSP & NSP Combined Perspective 40
Figure 25 Management Architecture Components – Instantiation Example (Combined Actor & Standalone Actor)..... 42
Figure 26 Service-Slice-Resource view 46
Figure 27 Service Level 47
Figure 28 Service Slice-Level..... 48
Figure 29 Slice-Resource Level 49
Figure 30 SliceNet management and orchestration overall view 54
Figure 31 SliceNet Orchestration overview..... 55
Figure 32 SS-O high level functional split 56

Figure 33 MEC in NFV approach and NMR-O NFV and MEC combined orchestration 59
Figure 34 NMR-O high level functional split..... 60
Figure 35 NMR-O high level functional split and positioning with respect to SliceNet CP 61
Figure 36 QoE/SLA Manager high level functional view 63
Figure 37 P&P Manager high level functional split 65
Figure 38 Summary of monitoring sub-plane components 66
Figure 39 Zoom on the cognitive Subplane..... 68
Figure 40 Zoom on the aggregation module..... 69
Figure 41 Zoom on Analytics 70
Figure 42 Policy Framework Modules..... 71
Figure 43 SliceNet Policy Architecture Entities 72
Figure 44 a) high level architecture; b) Roles considered by the Smart City use case..... 78
Figure 45 Smart City view..... 78
Figure 46 Smart-grid self-healing UC Overview 79
Figure 47 Multi-domain view of the Smart Grid use case..... 82
Figure 48 UC Roles Overview 83
Figure 49 Multi-domain view of the eHealth UC..... 85
Figure 50 Roles mapping in eHealth UC..... 87
Figure 51 Roles mapping in National Ambulance Service in Ireland..... 88
Figure 52 Demo Plan for eHealth UC 88

Abbreviations

3G	Third Generation (mobile/cellular networks)
3GPP	3G Partnership Project
4G	Fourth Generation (mobile/cellular networks)
5G	Fifth Generation (mobile/cellular networks)
5G PPP	5G Infrastructure Public Private Partnership
AF	Application Function
AMF	Access and Mobility Function
AN	Access Network
API	Application Programming Interface
AUSF	Authentication Server Function
BBU	Baseband Unit
BER	Bit Error Rate
BES	BlueEye Service
BoF	Birds of Feather
BS	Base Station
BW	Bandwidth
CFS	Customer Facing Service
CFSI	Customer Facing Service Instance
CFST	Customer Facing Service Template
CN	Core Network
CNN	Convolutional Neural Network
CoAP	Constrained Application Protocol
COMS	Common Operations and Management
COTS	Commercial Off-The-Shelf
CP	Control Plane
CPU	Central Processing Unit
CQI	Channel Quality Indicator
CQI	Channel Quality Indicator
CSP	Communication Service Providers
CU	Central Unit
CUPS	Control User Plane Separation
DC	Data Center
DCN	Dedicated Core Network

DECOR	Dedicated Core
DF	Deployment Flavors
DN	Data Network
DPI	Deep Packet Inspection
DSC	Digital Service Customer
DSP	Digital Service Provider
E2E	End-to-End
ECA	Event Condition Action
eDECOR	Enhancements for Dedicated Core
eMBB	enhanced Mobile broadband
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
EVE	Evolution and Ecosystem
FCAPS	Fault, Configuration, Accounting, Performance, Security
FFNN	Feed Forward Neural Network
GW	Gateway
HDD	Hard Disk Drive
HIS	High Speed Internet
HSS	Home Subscriber Server
I/O	Input/Output
IA	Artificial Intelligence
IaaS	Infrastructure as a Service
ICT	Information and communication technology
ID	Identifier
I-Ds	Internet-Drafts
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPTV	Internet Protocol television
KPI	Key Performance Indicator
LCM	Lifecycle Management
LSTM	Long Short Term Memory
LTE	Long Term Evolution

M2M	Machine to Machine
MANO	Management and Orchestration
MAPE	Monitoring Analysis Planning and Execution
ME	Mobile Edge
MEAO	Mobile Edge Application Orchestrator
MEC	Mobile/Multi-access Edge Computing
MEO	Mobile Edge Orchestrator
mIoT	massive IoT
ML	Machine Learning
MME	Mobility Management Entity
mMTC	massive Machine Type Communications
MP2MP	Multi-Point-to-Multipoint
MP2P	Multi-Point-to-Point
MPLS	Multiprotocol Label Switching
MVNO	Mobile Virtual Network Operators
NAS	National Ambulance Service
NB-IoT	Narrow Band IoT
NC	Network Core
NDRS	National Digital Radio Service
NE	Network Element
NEF	Network Exposure Function
NETCONF	Network Configuration Protocol
NF	Network Function
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NGCN	Next Generation Core Networks
NGMN	Next Generation Mobile Networks
NMR-O	Resource and ulti Network segment Orchestrator
NR	New Radio
NRF	Network Repository Function
NS	Network Service; Network Slice
NSaaS	Network Slice as a Service
NSD	Network Service Descriptor
NSEP	Network Slice Provider
NSI	Network Slice Instance

NSMF	Network Slice Management Function
NSO	Network Service Orchestrator
NSP	Network Service Provider
NSS	Network Slice Subnets
NSSAI	Network slice selection assistance information
NSSF	Network Slice Selection Function
NSSI	Network Slice Subnet Instance
NSSMF	Network Slice Subnet Management Function
NSST	Network Slice Subnet Template
NST	Network Slice Template
OAM	Operations, administration and maintenance
ONAP	Open Network Automation Platform
OPEX	Operational Expenditure
OS	Operating System
OSS	Operations Support System
P&P	Plug & Play
P&P IM	P&P Instance Manager
P2MP	Point-to-Multipoint
P2P	Point-to-Point
PAP	Policy Administration Point
PCA	Principal Component Analysis
PCC	Policy and Charging Control
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PDP	Policy Decision Point
PDU	Packet Data Unit
PEP	Policy Enforcement Point
PGW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
PNF	Physical network Function
PNFD	PNF Descriptor
PoP	Point-of-Presence
QoE	Quality of Experience
QoE-I	QoE optimization Instance
QoS	Quality of Service

RAB	Radio Access Bearer
RAM	Random-Access Memory
RAN	Radio Access Network
REST	Representational State Transfer
RO	Resource Orchestrator
RRC	Radio Resource Control
RRU	Remote Radio Unit
SD	Service Descriptor; Slice Differentiator
SDK	Software Development Kit
SDN	Software Defined Networks
SDO	Standards Developing Organization
SGW	Serving Gateway
SI	Service Instance
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SLG	Slice Gateway Function
SliceNet	End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks
SLO	Service Level Objective
SMF	Session Management Function
S-NSSAI	Single Network slice selection assistance information
SON	Self-Organizing Networks
SS-O	Slice Service Orchestrator
SST	Slice Service Type
ST	Service Template
TAS	Telestroke Assessment Service
TETRA	Terrestrial Trunked Radio
TMF	Telemanagement Forum
UC	Use Case
UDM	Unified Data Management
UE	User Equipment
UL	Uplink
UPF	User Plane Function
URLLC	ultra- reliable low latency communication
V2X	Vehicle-to-everything

VAS	Value Added Services
vBBU	virtual BBU
vCPU	virtual CPU
vEPC	virtual Evolved Packet Core
vHSS	virtaul HSS
VIM	Virtual Infrastructure Manager
VLD	Virtual Link Descriptors
VM	Virtual Machine
VM	Virtual Machine
vMME	virtaul Mobility Management Unit
VNF	Virtual Network Function
VNFD	VNF Descriptors
VNFD	VNF Descriptors
VNFFG	VNF Forwarding Graphs
VNFM	VNF Manager
VNFO	VNF Orchestrator
VoIP	Voice over IP
vP-GW	virtual Packet Gateway
vS-GW	virtual Serving Gateway
WG	Working Group
WP	Work Package

1 Introduction

Network slicing has been widely recognised as a fundamental cornerstone technology in the emerging softwarised and virtualised 5G mobile networks to enable independent end-to-end logical networks on a shared physical infrastructure. Therefore, effective and efficient management of 5G network slices is crucial for the success of 5G deployment in delivering varied services customized for a wide range of vertical businesses with diverging QoS/QoE/SLA requirements.

To substantially reduce the operational expenditure (OPEX), cognitive network slice management and orchestration is entailed to realize fully/highly automated slice management and orchestration through machine learning and other artificial intelligence technologies and utilizing a carefully-defined MAPE loop model and the associated policy framework.

Moreover, some use cases demand slice-based service deployment over a large geographical area that may span across multiple 5G network domains managed by different administrative organizations/network service providers/operators. A 5G management system is thus required to deal with such challenging scenario through well-defined cross-domain slice management mechanisms as well.

Furthermore, the 5G network slice management system needs to seamlessly interwork with the slice control plane and orchestrate the operations to close the control/management loops in the system. It is important to note that the network slicing paradigm further opens up the telecommunication/ICT market and introduces a number of stakeholders, and their roles and relationships need to be clearly defined from the management perspective.

1.1 Objectives

This deliverable aims to achieve the following specific objectives by defining the management plane for the overall SliceNet framework:

- Design the management plane by leveraging and advancing the state of the art and relevant standards;
- Define the management modules that are composing the cognitive and orchestration plane defined in D2.2 [2]
- Define the information manipulated within those blocks as part of the SliceNet information model;
- Define the roles of the main stakeholders in the network slice enabled 5G ecosystem;
- Ensure the mapping of the definitions and specifications of the overall SliceNet architecture and the SliceNet control plane architecture to those of this SliceNet management to create an integrated slice control, management and orchestration system;
- Investigate how the proposed management and orchestration fits the project use cases [1];
- Explore how both inter-/multi-domain network slices can be managed, especially the multi-domain scenarios for the use cases.

1.2 Approach and Methodology

To fulfil the above objectives, we adopt standards compliant methodology and follow both top-down and bottom-up design approaches, as explained below:

- Standards compliance: Network slice management is currently under standardisation processes in various leading SDOs whilst a number of informative technical specifications or drafts have already been released. This task has benefited from studying these documents and applied the recommended design principles and guidelines to the proposed SliceNet management plane.

- This methodology facilitates the justification of the design choices, ensures the compatibility of the proposed system with the emerging standards, and helps the project to identify gaps in the standardisation and thus potential contributions from the project.

- Both top-down and bottom-up design approaches
  - Overall SliceNet architecture informed: The management plane proposed in this deliverable is an integral part of the overall SliceNet architecture, which has been defined in D2.2, where the high-level vision of the management plane has been provided and further advanced in this deliverable. The specification of the management plane herein is clearly informed by the high-level vision in the overall architecture.
  - SliceNet use case informed: The project takes a "verticals in the whole loop" approach, and thus the verticals' perspective is also reflected in the design of the management plane. In particular, the SliceNet use cases defined in D2.1 have been reviewed to inform the investigation, in terms of P&P management for verticals, multi-domain network slice/service management and orchestration for use cases and so on.
  - 5G/4G technologies informed: Finally, the design of the SliceNet management plane is informed of the underlying 5G/4G technologies by taking into account the implications of the evolutionary nature of 5G deployments. This bottom-up approach is complementary to the above top-down approach where use cases and overall architecture have served as the starting points, thereby offering a more complete view for the management plane definition.

1.3 Document Structure

The remainder of the document is organized as follows:

- Section 2 reviews the state-of-the-art related work focusing on the emerging standards from leading standardization bodies (IETF, ETSI, 3GPP, etc.).
- Section 3 defines the main stakeholder roles concerned in the project (Network Service Provider, Digital Service provider and Digital Service Customer).
- Section 4 defines the network slice information model together with the slice template.
- Section 5 presents the modules in the management plane to cover the key functionalities including orchestration, SLA/QoE management, P&P management, monitoring, cognitive management and policy framework, and the interfaces and workflows among the components of the blocks.
- Section 6 applies the management plane to the defined SliceNet use cases with the multi-domain scenario highlighted.
- Finally, concluding remarks are provided in Section 7.
- In addition, a summary of the defined SliceNet control plane is appended to provide the context and reference in relation to the interworking of management and control planes in the SliceNet architecture.

2 Related work

2.1 IETF Common Operations and Management on Network Slices

During 2017 a group of network management and control experts coming from industry and academia across the world formed a discussion group within IETF to tackle network slicing aiming to find an initial consensus of IETF definition of the term network slicing. This brought to the creation of a discussion mailing list called “netslices”[4], where network slicing problems and gaps to be covered for facilitating interoperation across different operator and vendor solutions were discussed.

As a result, early 2018, an IETF Birds of Feather (BoF) called Common Operations and Management on Network Slices (COMS) was approved to further, aiming to properly position the ongoing activities within IETF, i.e. either by creating a new Working Group (WG) or joining others relevant.

COMS targets to produce and promote a technology-independent and resource-centric management plane for network slices. In particular, COMS aims to describe an overall architecture for network slicing, with information models that enable the design of service delivery and customer service interfaces. Also, COMS plans to specify network slicing OAM as well as data plane functionalities required to enable the delivery and operation of network slices as required by industry verticals.

As a general approach, COMS define a network slice as a set of infrastructure resources and service functions with customized and specific attributes designed to address the requirements of an industry vertical or a more generic end to end service. In the COMS view, network slices can span across multiple administrative domains, and may use heterogeneous technologies. Following other standard bodies definitions, COMS envisages end-to-end network slices as composed by one or multiple network slice subnets, which are basically single domain portions of the whole network slice, being them either technology domain or administrative domain subnets.

In this direction, at the time of writing, COMS has produced a set of relevant Internet-Drafts (I-Ds) that tackle network slicing from different perspectives, from overall management and operation architecture to information models and cross-provider challenges and approaches in multi administrative domain scenarios. The following sub-sections provide a brief summary of the I-Ds identified as relevant for the SliceNet management and orchestration architecture definition.

2.1.1 COMS architecture

The overall COMS architecture is presented in the draft-geng-coms-architecture I-D [5], where a top level network slice orchestrator enables a technology independent network slice management on top of a heterogeneous infrastructure. The COMS architecture approach is shown in Figure 1; it is worth to highlight that COMS is applied in Transport Network regions scenarios, and it assumes that end-to-end network slice and slicing in general refer to slicing across multiple Transport Network domains. As depicted in Figure 1, a top level orchestrator receives network slice service profiles, which include technology agnostic operation and management requests for network slices, and map them into technology specific configuration information to be enforced through properly selected network slice controllers and orchestrators.

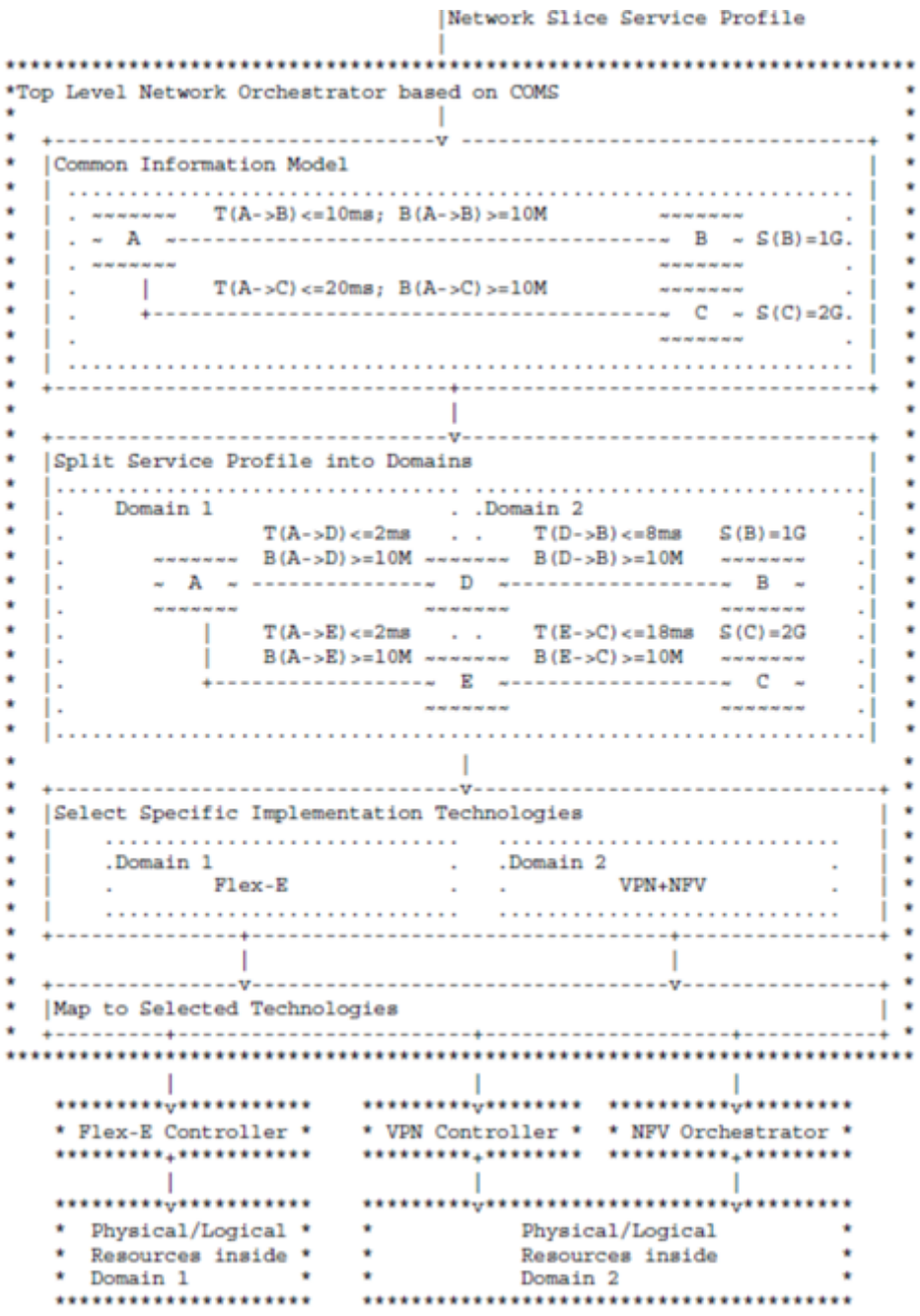


Figure 1 COMS overall architecture and technology agnostic orchestration approach

In particular, this COMS approach is built around four main layers and macro-components in the technology agnostic top level orchestrator, as shown in Figure 1. The first one is the common information model, which basically provide the description language and format of network slice service profiles in a technology independent way. In the second macro-component, the end-to-end slice profile is split into technology agnostic single domain service profiles that the COMS top level orchestrator can manage with technology specific and domain specialized controllers and orchestrators. For this, in the third macro-component, the most appropriate available implementation of a per-domain specific controller or orchestrator technology is selected according to end-to-end slice requirements and per-domain service profile attributes. At the fourth component, the technology translation towards the selected controller or orchestrator is applied to implement the necessary mapping to enforce the specific slice requirements and attributes.

As a main takeaway for SliceNet, this COMS overall architecture follows a technology independent orchestration approach where end-to-end slice and service profiles are split into per-domain actions and configurations to be enforced through technology specific controllers and orchestrators that can play as an example in the context of SDN network domains and NFV environments.

2.1.2 Technology Independent Information Model for Network Slicing

Following the COMS overall architecture introduced above, a dedicated COMS I-D proposes the technology independent information model to describe the entities building a network slice [6]. This model also includes properties, attributes and operations on each entity, as well as how network slice elements relate to each other in an end to end network slice that may span across multiple technology domain. In general, COMS envisages a network slice as the composition of heterogeneous resources (compute, networking, storage, service functions, etc.) that can be described together as kind of topology of connected entities.

The COMS network slice information model is described through YANG, and following the above considerations, is built on top of the data model for network topologies [8]. The main elements composing the COMS network slice information model are: connectivity resources, storage resources, compute resources, service instances and function blocks, network slice level attributes. These elements are arranged in a tree structure of attributes following the YANG principles, and the new COMS attributes on top of those defined in are marked with "netslice:" namespace, as shown in Figure 2.

The COMS network slice information model is a composition of basic resources, comprising nodes, links, compute units and storage units which are augmented with service instances and slice level attributes. A whole network attribute represents a network slice instance, while nodes and links describe virtual nodes and links exposed to the slice user.

```
module: ietf-network
+--rw networks
   +--rw network* [network-id]
      +--rw network-id                          network-id
      +--rw network-types
      +--rw supporting-network* [network-ref]
      |  +--rw network-ref
      +--rw node* [node-id]
      |  +--...
      |  +--rw netslice:compute-unit* [compute-unit-ref]
      |  |  +--rw netslice:compute-unit-ref    compute-unit-ref
      |  +--rw netslice:storage-unit* [storage-unit-ref]
      |  |  +--rw netslice:storage-unit-ref    storage-unit-ref
      |  +--rw netslice:service-instance* [service-instance-ref]
      |     +--rw netslice:service-instance-ref    service-instance-ref
      +--rw nt:link* [link-id]
      |  +--...
      |  +--rw netslice:link-qos
      |     +--...
      +--rw netslice:compute-unit* [compute-unit-id]
      |  +--...
      +--rw netslice:storage-unit* [storage-unit-id]
      |  +--...
      +--rw netslice:service-instance* [service-instance-id]
      |  +--...
      +--rw netslice:slice-level-attributes
         +--...
```

Figure 2 COMS network slice YANG model.

With reference to SliceNet, the new “netslices” attributes proposed by COMS are relevant and in particular those related to link QoS (bandwidth, jitter, latency), service instances and function blocks,

slice level attributes. Figure 3 shows the YANG model related to COMS generalized function blocks that are used to describe service instances associated to a network slice. Some examples are firewalls, load balancer, DPIs, etc. Figure 3 also shows the tree structure of the slice level attributes, which includes slice start/end time, lifecycle status, access control, availability against SLA, etc.

Moreover, COMS defines a set of operations on top of the network slice technology agnostic information model: In principle, each element inside network slice also should be able to be operated individually.

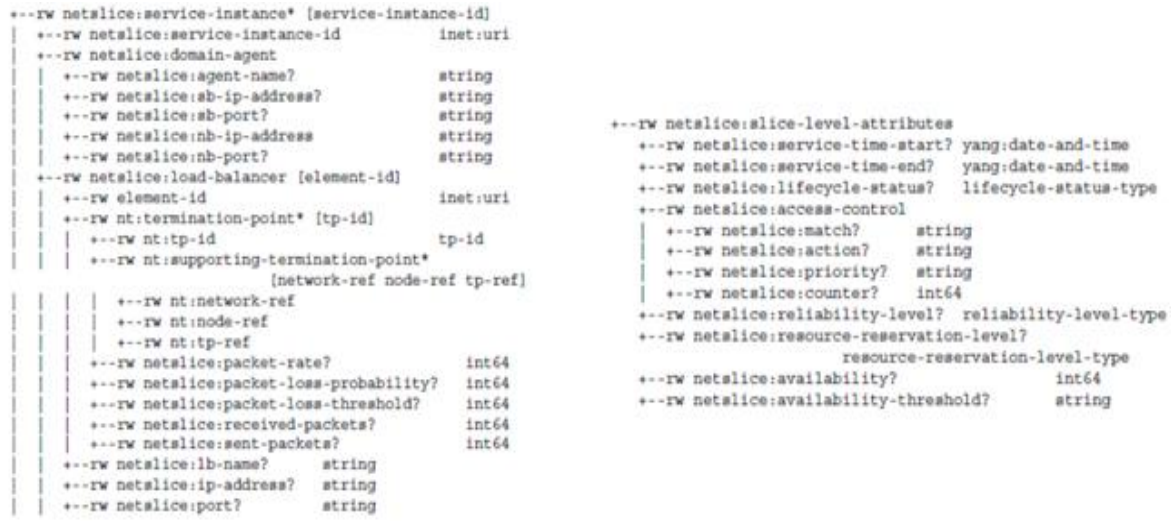


Figure 3 COMS "netslice:service-instance" (left) and "netslice:slice-level-attributes"(right) models

While this IETF approach to network slice information model is very much tied to a network topology view, which might not always be applicable to end-to-end slices offered to verticals, the combination of base resources and service functions and slice level attributes following a YANG principles is very relevant to SliceNet.

2.1.3 Gateway Function for Network Slicing

As mentioned above, COMS tackles network slicing in both single and multiple administrative domains. This means that the proposed technology agnostic management and operation approach needs to cope with the orchestration of network slice subnets and their interconnection and integration into end-to-end network slices.

For this purpose, COMS proposes an approach based on the Slice Gateway Function (SLG), which is a function or a group of functions that are used to connect or disconnect network slice subnets. In particular, SLGs are conceived to interconnect subnets while guaranteeing the required QoS and performances in the end-to-end slices, still applying a technology agnostic model by means of dedicated SLG Control functions that can be orchestrated following the COMS principles. This SLG approach is shown in Figure 4, where multiple SLGs glue network slice subnets at both intra and inter administrative domain level. Moreover, SLG are defined to provide specific functions for identification of user and service traffic and their allocation to the appropriate network slice subnet at each edge of the end-to-end network slice.

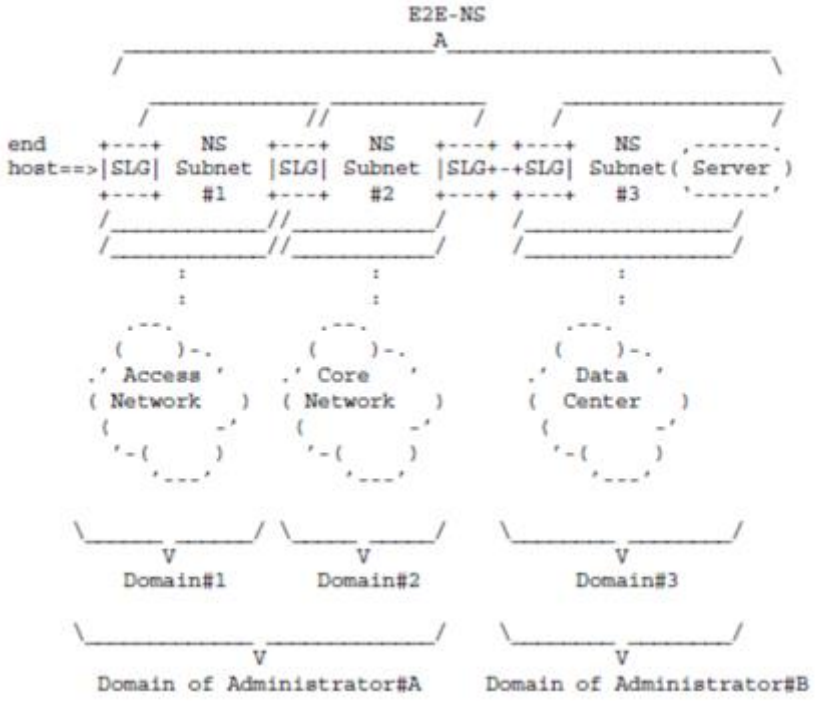


Figure 4 COMS SLG approach for network slice subnets interconnection

With reference to SliceNet, it is relevant to highlight how COMS considers and approaches the usage of SLGs for inter administrative domain scenarios. As shown in Figure 5, inter-domain (ID) SLGs are intended to be used to forward network slice subnets data packets to other ID-SLGs located on different administrative domains and hosting network slice subnets part of the same end-to-end slice. ID-SLGs also support authentication for connecting to opponent SLGs and slice isolation features, while from a control perspective may expose dedicated interfaces to configure policies and collect telemetry information.

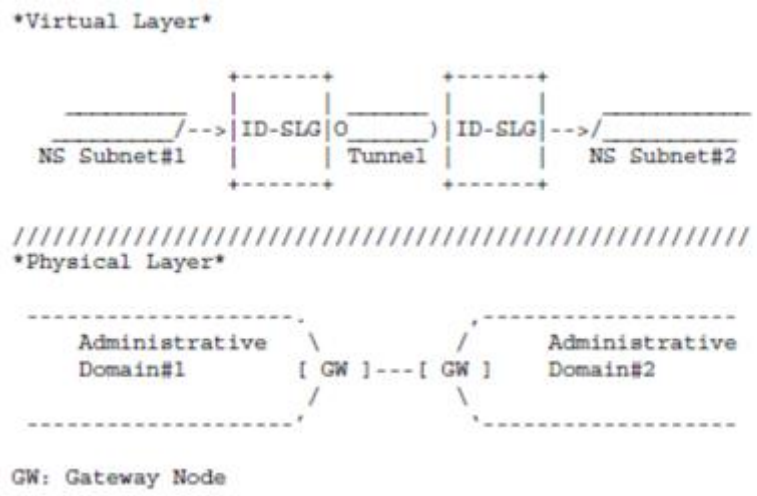


Figure 5 Inter-Domain (ID) SLG for inter administrative domain network slice subnets interconnection

Moreover, SLGs can be deployed in the form of **Virtualized Network Functions (VNFs)** following the ETSI NFV MANO principles, as shown in Figure 6. This is highly relevant in the context of SliceNet where cross provider (or operator) slices may be properly controlled and managed via dedicated SLG VNFs that enforces proper QoS policies as agreed by the involved actors on a per-slice basis.

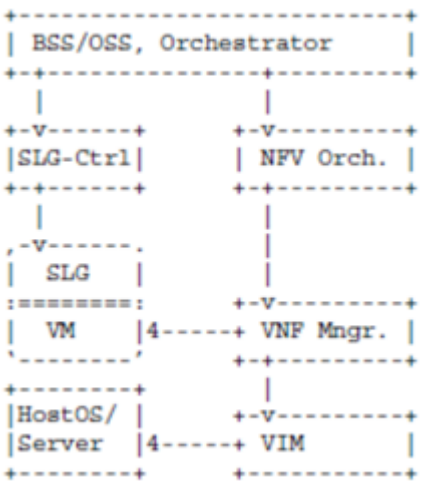


Figure 6 Deployment of SLG functions (and control) in NFV environments.

2.2 ETSI NFV Network Slicing Support

During 2017, ETSI NFV started to analyse and investigate how its principles and architectures could be mapped to network slicing concepts and use cases defined in other standardization bodies. In particular, in the context of the Evolution and Ecosystem (EVE) WG, a dedicated document [9] has been released early 2018 with the aim of reporting how and if network slicing (as defined mostly within NGMN, 3GPP and ONF) could be supported by the ETSI NFV architecture and MANO concepts, Figure 7.

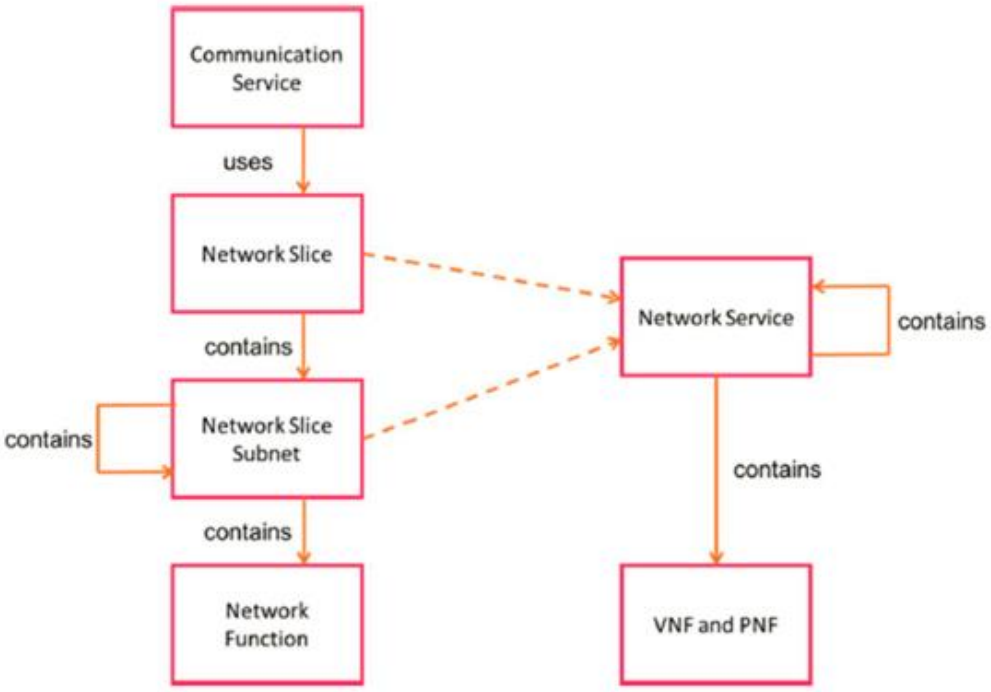


Figure 7 3GPP and NFV information models potential mapping (source ETSI GS NFV-EVE 012)

From a practical perspective, [9] analyses network slicing from three different perspectives:

i) how the network slice information models and architecture components map with ETSI NFV MANO ones,

ii) figure out potential impacts of network slicing use cases (mostly from 3GPP) on ETSI NFV constructs (i.e. VNF and NS descriptors), security and reliability,

iii) provide recommendations in term of potential ETSI NFV MANO evolutions resulting from the analysis the network slicing use cases.

In the context of SliceNet, and this deliverable in particular, the most relevant considerations provided by [9] are those related to information models and architectural aspects specifically targeting 3GPP network slice concepts. Indeed, 3GPP defines a network slice as a combination of zero or more network slice subnets, following a kind of recursive approach where each subnet can contain zero or more other subnets, as well as zero or more network functions.

Network functions in 3GPP are associated to VNFs and PNFs, therefore a direct mapping of an NFV Network Service as a resource-centric view of a network slice is highly appropriate. Moreover, as 3GPP foresee that network slice subnet instances can be shared by multiple network slice instances, virtualized resources for a slice subnet (including compute, network and storage) can be mapped to nested NFV Network Service concept. This way, as shown in Figure7, a correspondence between network slice instances and network slice subnets instances with NFV Network Services exist following the relationship provided by the dotted arrows.

This can be considered as a key starting point and reference baseline for the SliceNet slice modelling exercise. However, this 3GPP network slice to NFV constructs mapping at the information model level translates into further considerations from architectural point of view. In particular, from a management perspective, 3GPP defines a Network Slice Management Function (NSMF) as responsible for the lifecycle management of network slice instances, if applicable NSMF is also linked and delegates to Network Slice Subnet Management Function (NSSMF) the lifecycle management of subnet slice instances. Figure8 shows how [9] considers these network slice management functions positioned with respect to NFV MANO architecture and components. Here, the Os-Ma-Nfvo reference point (that is the interface in ETSI NFV that the NFV Orchestrator exposes towards OSS functions) can be used as placeholder for interactions among NFV MANO components and 3GPP management ones. In practice this means that NSMF and NSSMF functions need to be aware of available NFV Network Services as offered by the NFV MANO to be either instantiated or re-used to fulfill the requirements of network slice and slice subnet instances. In other words, NSMF and NSSMF would need to map network slice templates and NFV Network Service Descriptors, considering the relevant (potentially multiple) Network Service deployment flavours available.

In summary, [9] defines that a network slice instance can be mapped to:

i) an instance of single NFV Network Service instance,

ii) an instance of composite nested NFV Network Service instances,

iii) a concatenation of NFV Network Service instances.

And in general, different network slice instances generated from the same template can make use of NFV Network Service instances of the same type (i.e. from the same Network Service Descriptor) and possibly with different deployment flavors. In this case, the mapping perfectly works when network slice instances share a large common subset of network functions but differ each other in terms of required performances so that NFV deployment flavors can play the role of differentiators among same types of NFV Network Services.

As a main take-away for SliceNet, this initial information model and architecture components mapping and relations/interactions between 3GPP and ETSI NFV are crucial for the definition of management and orchestration principles and concepts. It is worth to mention that it is foreseen in SliceNet that network functions as defined in 3GPP, i.e. constituent functions of network slice instances, to fulfill performance requirements for specific vertical services requiring customized applications running at the edge of the network. Therefore, as an example of gap that SliceNet can

fill to have a coherent and consistent end-to-end slice management and orchestration framework, what [9] defines as mapping between network slice and NFV Network Service would require further extension and enhancement in SliceNet to consider RAN, CORE and MEC applications for example as part of the NFV Network Service Descriptors and instances, at least, Figure 8.

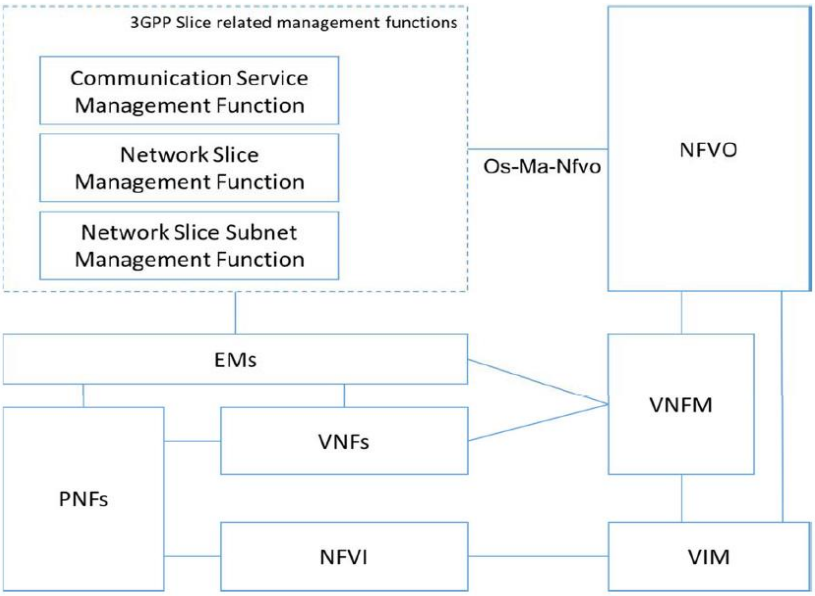


Figure 8 3GPP and NFV management components potential relationship (source ETSI GS NFV-EVE 012)

2.3 3GPP Slicing concepts

A concept of end to end slicing for 4G mobile networks has been identified in [13] and in its enhanced version of [14] under the terms of DECOR and eDECOR respectively. The concept foresees a number of DEdicated CORe networks to be serving UE beyond the RAN part of the network. Each Dedicated Core Network (DCN) is assumed to be serving one type of subscribers that are identified either by extra optional subscription information stored in HSS (DECOR) and/or by UE provide information that is used to assist DCN selection and minimise signalling traffic (eDECOR). A general overview highlighting the (e)DECOR concept is presented in the following figure. While (e)DECOR concept adoption by operators is still pending, its slicing potential can be coupled with the Control User Plane Separation (CUPS) principles as applied on top of ETSI-NFV capabilities which makes it a good candidate for applying slicing aspects in the context of 4G either by passive (DECOR) or active participation of the UE (in case of eDECOR) in slice selection. The latter case is quite aligned with the 5G slicing concept as it is presented in the next paragraph in the context of NSSAI, Figure 9.

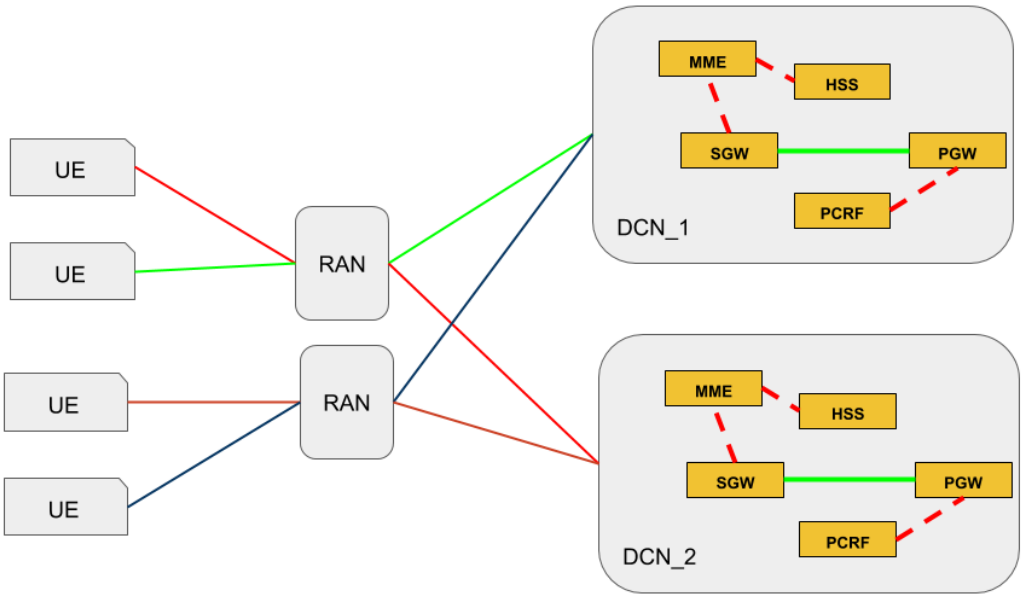


Figure 9 3GPP Dedicated Core

5G Slicing

According to [15] a Network Slice (NS) consists of Physical and/or Virtual Network Functions (NFs, VNFs/PNFs) that can belong to Access (AN) and Core (CN) Network part. The synthesis of an NS serves a particular functional purpose and once instantiated it is used to support certain communication services. Much alike Network Services in NFV-MANO approach, Network Slice Subnets (NSS) constitute Network Slice ingredients that can be used to perform specific tasks within a Slice and allow more flexible management over the NS instantiation process. For example an NSS may be providing the RAN part, while another NSS may provide the Core part of an NS. An NSS is, therefore, a collection of interconnected NFs that provide a clearly identified functionality. NSs are, obviously, higher layer aggregations of the NSSs but cannot span across domain borders.

Typically, all NFs contained in one NSS are interconnected. The interconnection pattern is also maintained for the inclusion of NSSs inside NSs resulting in an overall interconnectivity graph for which each connection is subject to specific FCAPS requirements. All these requirements are reflected onto the network configurations that are required to support these interconnections and are subject to be constantly monitored and adjusted for the overall SLA, QoS and QoE support that is intended to be offered as a communication service to the vertical customer, Figure 10.

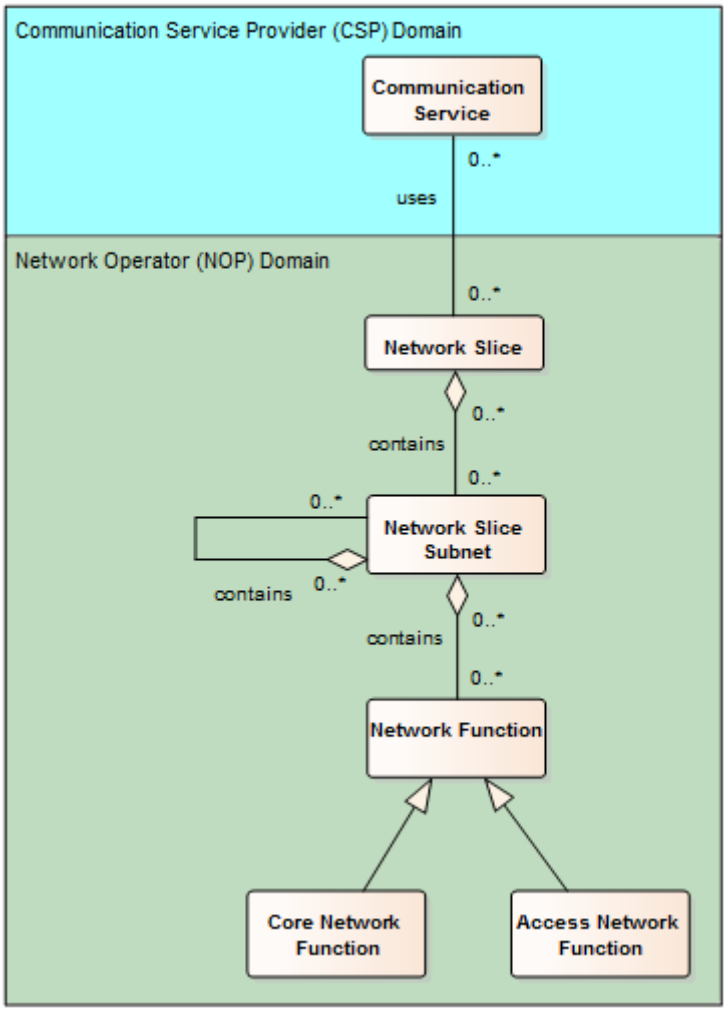


Figure 10 3GPP information modeling of a slice

NSSs and NSs can be designed in the form of templates, NSSTs and NSTs respectively, according to the above information model. Each template can be instantiated by the provision of the instance specific information that is aimed to be supporting the communication services customer according to a set of foreseen SLA; QoS and QoE agreements such as:

- Network characteristics (latency, reliability, etc.)
- Application characteristics (load balancing, packet management/dropping/monitoring)

3GPP foresees that the UE participates in the process of NSI selection by use of the Network Slice Selection Assistance Information (NSSAI). The Single NSSAI (S-NSSAI) contains the Slice/Service Type (SST) that identifies the NSI behaviour in terms of features and services and the Slice Differentiator (SD) that can differentiate an NSI among those of the same SST. The S-NSSAI (up to 8 per NSSAI) identifies one Slice to which the UE is connected and this information is processed to connect the UE session (in contrast to 4G (e)DECOR where the UE belongs to a slice) to the appropriate AMF and consequently to the overall set of NFs of the slice as presented in the typical 5G system architecture below.

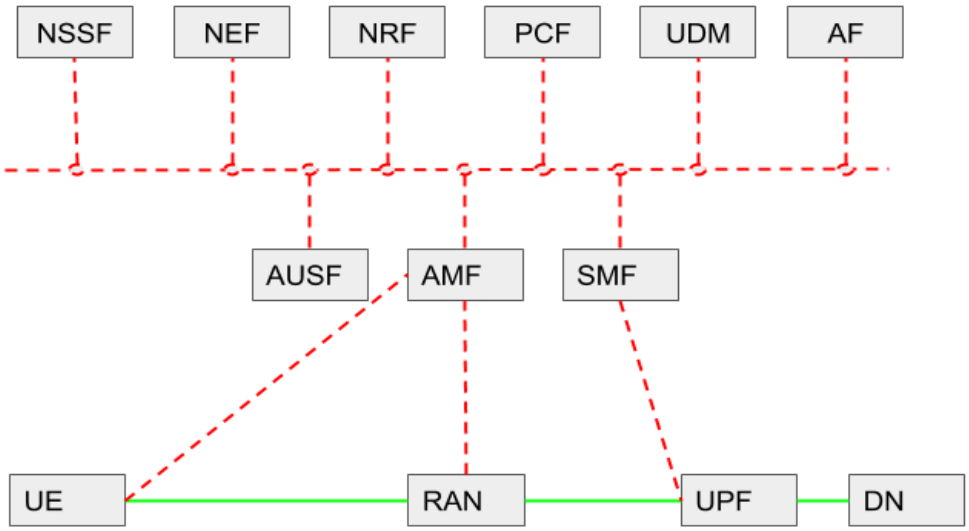


Figure 11 5G Core Network Functions and Service based architecture

5G Architecture, Figure 11, is Service Based and also Control and User Plane is disassociated by design/specification. Therefore ETSI-NFV aspects can be easily applied for dynamic lifecycle management of slices.

Among details that relate to the proper configuration of the contained NFs, security aspects can be also addressed in the form of a number of aspects:

- Data path isolation
- Data path encryption/protection
- NF sharing
- NSS sharing

NSS and NS requirements are not limited only to the above features and the complexity introduced by the combinations of underlying functionality (also pluggable) can allow for higher and more complex requirements to be addressed by the templates and the corresponding instances, since NSSs can be defined not only with respect to contained NFs but also with inclusion of other NSSs. However, the complexity is not a prohibitive factor but an added value feature expected to be supported by the flexibility of the slicing infrastructure and its capability to handle properly the instantiation of the templates both at NS (NSMF functionality) and NSS (NSSMF functionality) level.

3 SliceNet Roles Considerations

In this section, we present and define the considered business roles and their associated responsibility in the SliceNet. Additionally, we also describe how the defined SliceNet roles integrate with each other and how they deliver to the Vertical industries the required network conditions to accelerate their business. In the end, the major objective of each business entity is to monetize their core assets - the Network Operator needs to monetize their network resources, the Service Providers want to maximize the usage and profitability of their services and the Verticals also need to improve their business.

This section also describes the roles model applied in a very specific, but challenging scenario, which is the integration of multiple-administrative domains. In this case, multiple administrative domains are related with the integration of several Network Operators to open and provide their core assets as a service (either “raw” network resources and/or Network Slices) to Service Providers on top. With this model in place, Service Providers will have the opportunity to design new, vertical-oriented service offers distributed across several Network Operators.

The described roles in the following subsections are based on the SliceNet roles model introduced in D2.2. Although based on the roles described in D2.2, some of the presented roles are grouped together to simplify and map to the digital industry evolution in the coming years.

Based on business roles defined on standardization bodies [17][16], we defined the key three roles we are considering in SliceNet:

- Network Service Provider (NSP)
- Digital Service Provider (DSP)
- Digital Service Customer (DSC)

Each of which can be decomposed further, however to ensure a clearer mapping of roles to multi-domain and to the management system definition we keep this compact decomposition of roles.

3.1 SliceNet Roles Definition

3.1.1 Network Service Provider Role

Traditionally, the Network Operator is a static and relatively closed entity. It's not the Network Operators culture to provide their assets (network resources) to third parties. Furthermore, besides operating the network resources, Network Operators usually play the role of Service Providers, or, to be precise, Communication Service Providers (CSP). That is, besides operating the network resources, they also provide services to end-customers. Good examples of this business approach is the High Speed Mobile Internet Service and/or IPTV service offers, which are most of the time provided by the same entity – the traditional, incumbent, Network Operator. This is typically, the Network Operators business strategy to occupy also the business space of Service Providers. In the next years, it is expected that Network Operators significantly increase their service offer to monetize the investment that they do on the network resources.

However, in parallel, Network Operators should also be prepared to open and provide/expose their network assets to other Service Providers. A typical example, that is already pressuring Network Operators, is the need to expose their network assets to Mobile Virtual Network Operators (MVNOs). The latter want to provide High Speed Mobile Internet Service to customers but do not want to invest in network resources – they prefer to use them following the Cloud paradigm, that is, as a Service. More generically, besides the MVNOs, independent IPTV service providers are also raising – for example, Netflix, Google, Amazon, etc. These Service Providers are looking for network availability in different worldwide geographies to deliver their contents with the required quality.

This trend is here to stay and Network Operators are adapting themselves to this reality by becoming Network Service Providers, which are able to open and expose their network assets as a Service to third-party Service Providers. Figure 12 illustrates the new business positioning for Network Operators - become Network Service Provides, which are able to manage their network resources, including Network Slices, and expose them as Network Infrastructure Services to other business entities, e.g. Service Providers. In a very simple way, being the Network Slice materialized in an organized, isolated and shared collection of network resources, it is under the responsibility of the Network Service Provider to manage and abstract the exposition of the Network Slice to the top business entities.

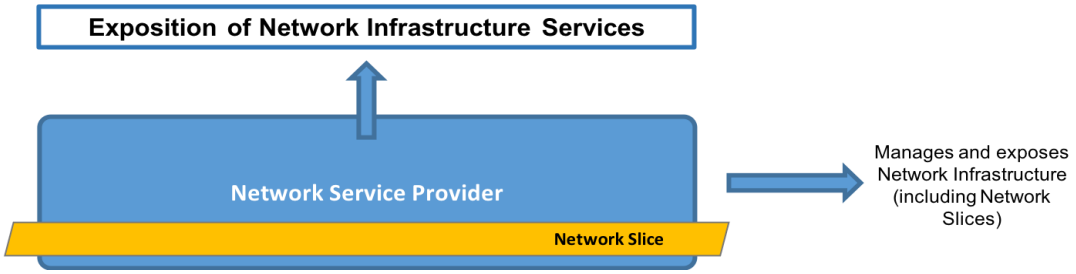


Figure 12 Network Service Provider Role - High-Level Perspective

Figure 13, illustrates in more details the internals of a Network Service Provider. In summary, this entity must be able to manage, expose and monetize the network infrastructure resources (and slices) as a service. Therefore, the NSP plays the role of providing the infrastructure as a service, (close to an IaaS approach), or better to say that the NSP plays the role of a Network Slice Provider, (NSEP), where the slice spans the end-to-end architecture. The slice includes details with regards to authentication, billing, monitoring etc.

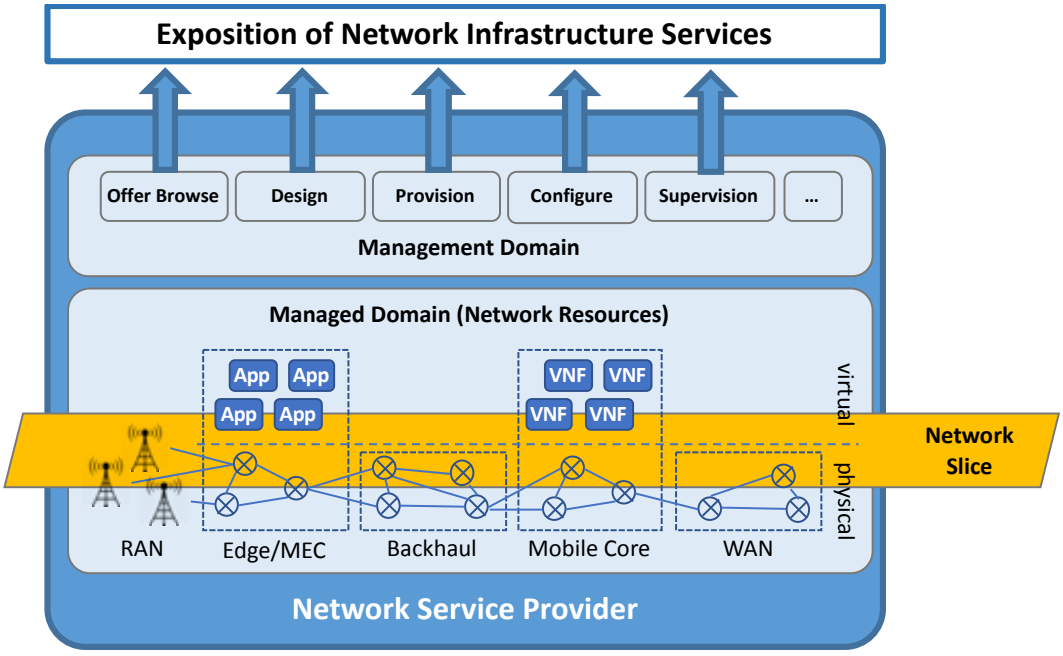


Figure 13 Network Service Provider Role - Detailed Perspective

There are three key responsibilities within the Network Service Provider:

- Managed Domain
  - Heterogeneous network infrastructure resources (e.g. VNF, MEC Apps, PNFs, SDN-Apps, ...);
  - Groups of resources, also known as Network Slices and Sub-slices;
- Management Domain

- Heterogeneous network infrastructure resources lifecycle management (e.g. design, onboard, deploy, provision, monitor, account, …)
- Slices lifecycle management (e.g. design, onboard, deploy, provision, monitor, account, …)

- Capabilities Exposition: the High-level APIs to enable Communication/Digital Service Providers to manage their service offers over the network infrastructure & slices. For example:
  - Offer browsing: enable Service Providers to select and subscribe for a particular Network Infrastructure Service offer;
  - Design: enable Service Providers to request new Network Infrastructure Service offers (not yet available in the Network Service Provider portfolio);
  - Provision: enable Service Providers to provision new customers (e.g. mobile customers/SIM cards in the 4G/5G mobile access network);
  - Configure: enable Service Providers to configure their Network Infrastructure services (e.g. it could be a simple reconfiguration of a traffic shaping service, or a more complex instantiation of a specific network function in a specific region of the network);
  - Monitor: enable Service Providers to monitor and supervise their network infrastructure services;
  - Account: enable Service Providers to account the usage of the network infrastructure service that was subscribed (e.g. network slice).

3.1.2 Digital Service Provider Role

On top of the above described Network Service Provider is the Digital Service Provider, which leverages on the services exposed by the former to create digital services. This could go from "simple" communication services (e.g. IPTV, voice, Internet) to more customized service offers towards the vertical industries (e.g. ultra-low latency communication service). Figure 14 provides a high-level perspective of the Digital Service Provider.

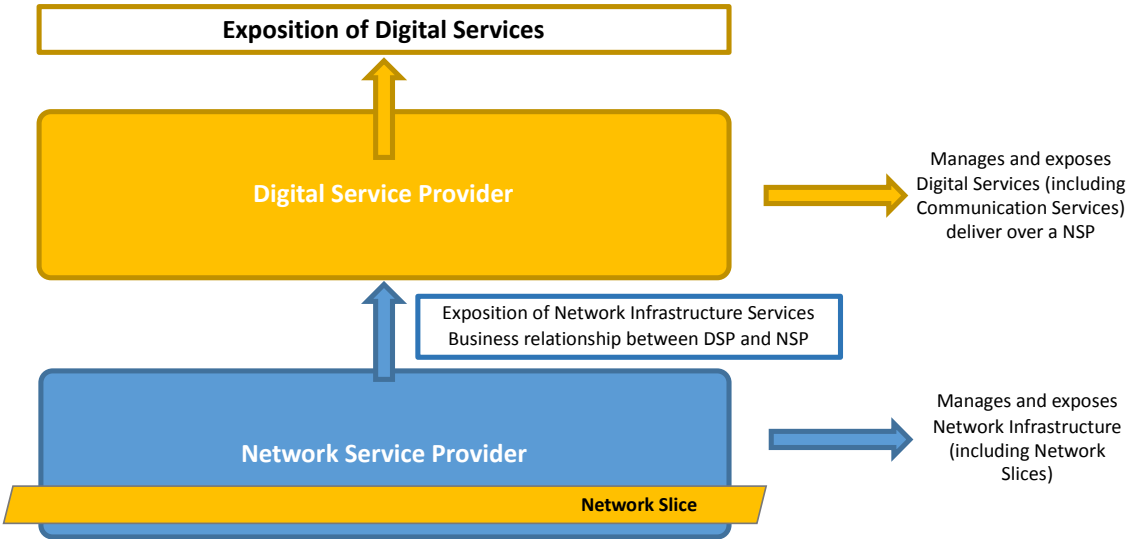


Figure 14 Digital Service Provider Role - High-Level Perspective

Figure 15 illustrates in more detail the internals of a Digital Service Provider. In summary, this entity must be able to manage, expose and monetize digital services running on top of a sliced network infrastructure provided by the Network Service Provider. In this model, the Digital Service Provider is unaware of whether the network infrastructure is sliced or not. The responsibility to deal with the network infrastructure details is of the Network Service Provider.

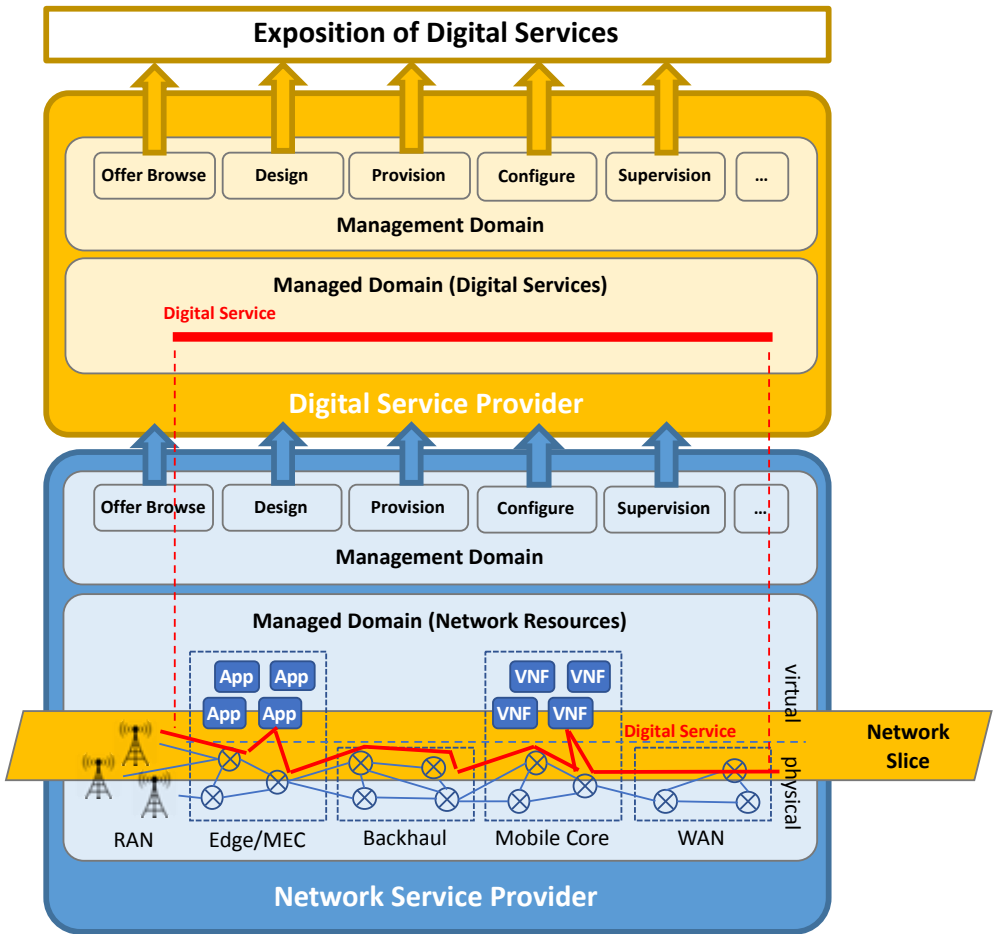


Figure 15 Digital Service Provider Role – Detailed Perspective

There are three key responsibilities within the Digital Service Provider:

- Managed Domain

  Heterogeneous digital services (running on top of the Network Service Provider) (e.g. traditional communication services – IPTV, HSI, VoIP or digital services);

- Management Domain

  Digital services lifecycle management (e.g. design, onboard, deploy, provision, monitor, account, …);

- Capabilities Exposition

  High-level APIs to enable Customers to consume and manage the subscribed service offers (browse, design, provision, monitor, account, etc.).

3.1.3 Digital Service Customer Role

Finally, the third business role is the Digital Service Customer (e.g. Vertical). Figure 16 illustrates the Digital Service Customer and how it relates with the Digital Service Provider and with the Network Service Providers. The Digital Service Customer will relate with the Digital Service Provider to consume digital services and will relate with the Network Service Provider to, for example, attach to the 4G/5G RAN mobile network.

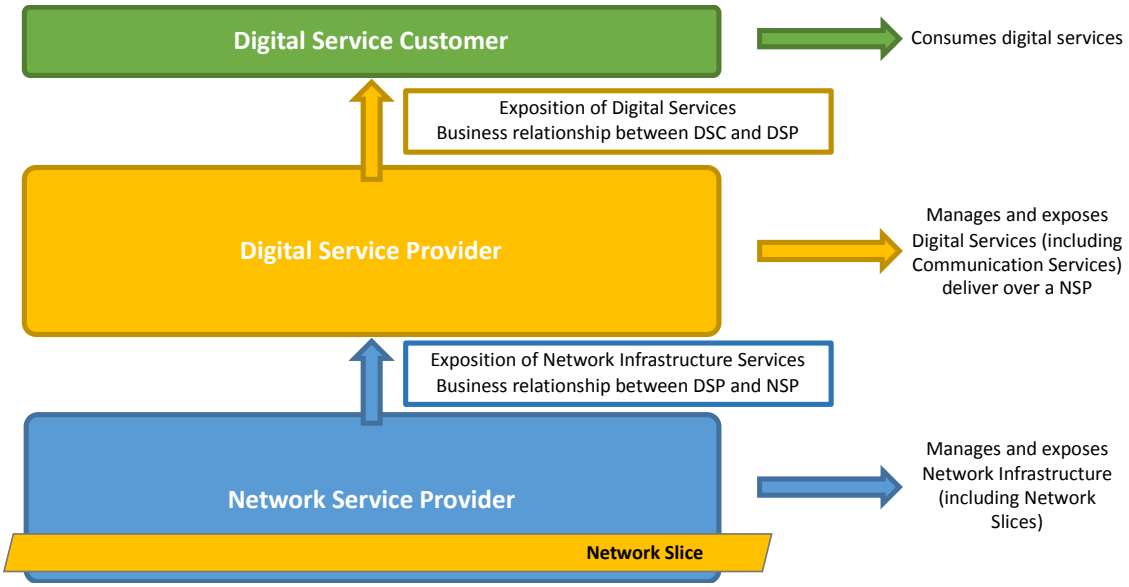


Figure 16 Digital Service Customer Role - High-Level Perspective

Figure 17 illustrates the Digital Service Customer interactions with the Digital Service Provider. Again, as described for the Digital Service Provider, the Network Slice is "hidden" from the Digital Service Customer. The latter is unaware of the technical procedures that the Network Service Provider uses to provide the required network infrastructure service capabilities.

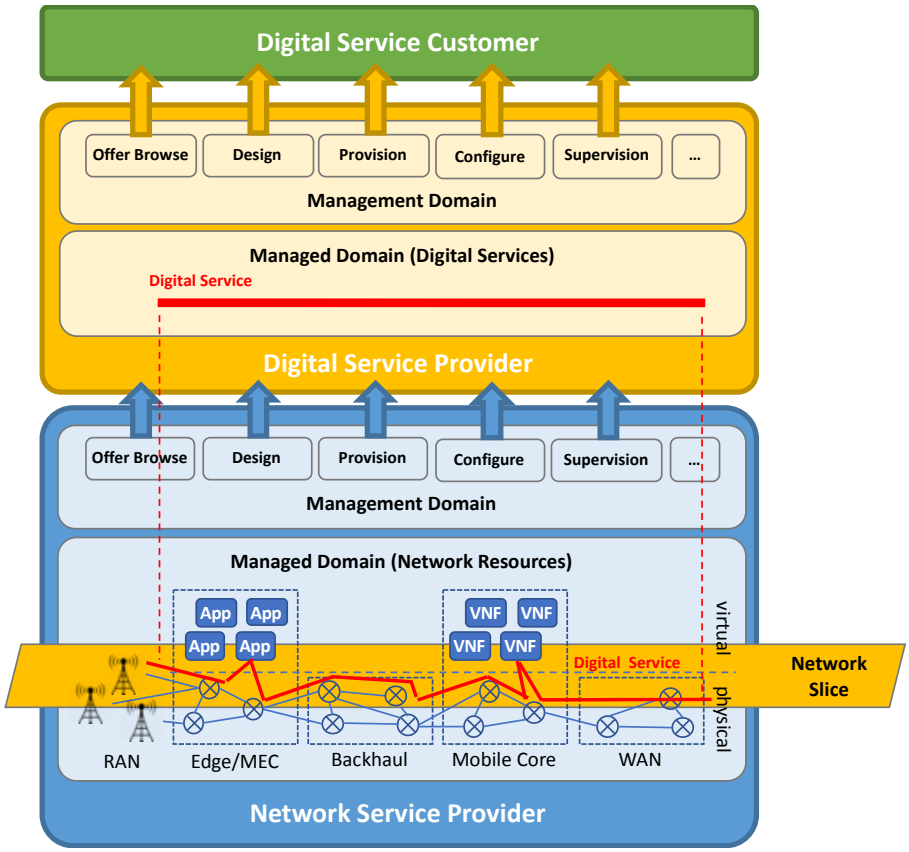


Figure 17 Digital Service Customer Role - Detailed Perspective

3.2 Overview of Multi-domain considerations

There are different perspectives to classify multi-domain scenarios, as expressed by different industry alliances and standardisation bodies. In particular, the views from NGMN are considered representative and have been largely adopted by 3GPP and other stakeholders.

Firstly, in [18] NGMN defines two general categories of scenarios where network services need to be provided across multiple service providers with an existing SLA:

- Roaming scenario: Individual users move from one provider (i.e. Home network provider) to a network managed by another provider (i.e. Visited network provider). The services that a user requires while roaming needs to be specified in the SLA between the two providers. In this case the two providers, with an SLA, would be the P-Hosted (Home network provider), and the P-Hosting (Visited network provider), with the corresponding behaviours required to support the inbound roamers (e.g. using a service instance or network slice instance) by P-Hosting.
- Business verticals scenario: When a business vertical service user's request cannot be met by the capabilities of a single provider, the provider may harness the necessary capabilities from another provider, based on an SLA between the two providers. In this case the two providers, with an SLA, would be the P-Hosted (Home service provider), and the P-Hosting (Third-party service provider), with the corresponding capabilities required by the P-Hosted from the P-Hosting.

Secondly, NGMN has further defined the categories of administrative domain configurations in the context of "5G End-to-End Architecture Framework" [19]

- Inter-domain configuration: This refers to two different administrative domains that are required to cooperate to provide the necessary resources and functions to support any given service. The network slice required to support the service is established through a cooperation of the domain specific orchestrators, based on policies and agreements that are applicable across the two different participating administrative domains.
- Multi-domain configuration: This refers to more than two different administrative domains that are required to cooperate to provide the necessary resources and functions to support any given service. The network slice required to support the service is established through a cooperation of the domain specific orchestrators, based on policies and agreements that are applicable across all the different participating administrative domains.

It is noted that these two classification methods are complementary and thus a specific use case scenario may fall into one or more of the categories, e.g., a use case scenario can be both of the roaming scenario and multi-domain configuration. Moreover, naturally, the multi-domain configuration is an evolution or expansion from its inter-domain counterpart, and thus for design, prototyping and deployment purposes, a progressive approach is recommended to follow this evolution.

3.3 SliceNet Roles applied to Multi-Domains

Figure 18 describes (an example among other possible approaches) the instantiation of the SliceNet roles in a multi-domain scenario. In this case, the Digital Service Customer requests a digital service (from the Digital Service Provider) that requires network infrastructure services from two Network Service Providers (A and B). Each Network Service Provider manages and exposes their network infrastructure services to the Digital Service Provider.

In this approach it's under the responsibility of the Digital Service Provider to browse, select, manage and orchestrate, based on the service needs of the Digital Service Customer, the required network infrastructure services from different Network Service Providers in order to create a **composed digital service offer** to the Vertical customer. In the end, the Digital Service Customer will consume

the provided composed digital service offer without knowing that it is a composed offer and therefore without knowing the underneath involved Network Service Providers. Additionally, from the Digital Service Provider perspective, it will subscribe to a network infrastructure service A_1 from Network Service Provider A and a network infrastructure service B_1 from Network Service Provider B, totally unaware about the Network Slices that are used within the Network Service Provider domain to deliver the network infrastructure services.

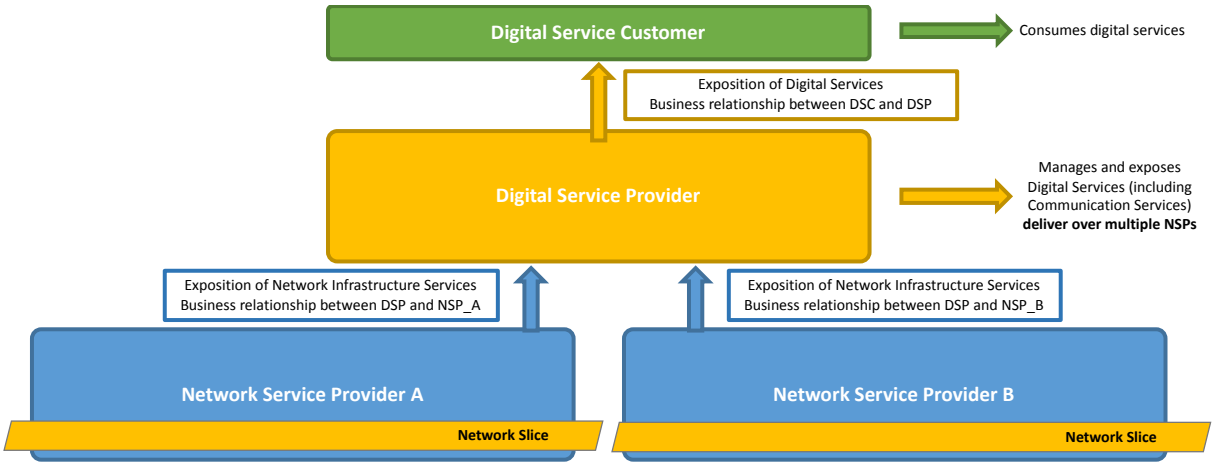


Figure 18 SliceNet Roles Applied to Multi-Domain - High-Level Perspective

Figure 19 provides a detailed perspective, "opening" each one of the entities involved, of the multi-domain scenario.

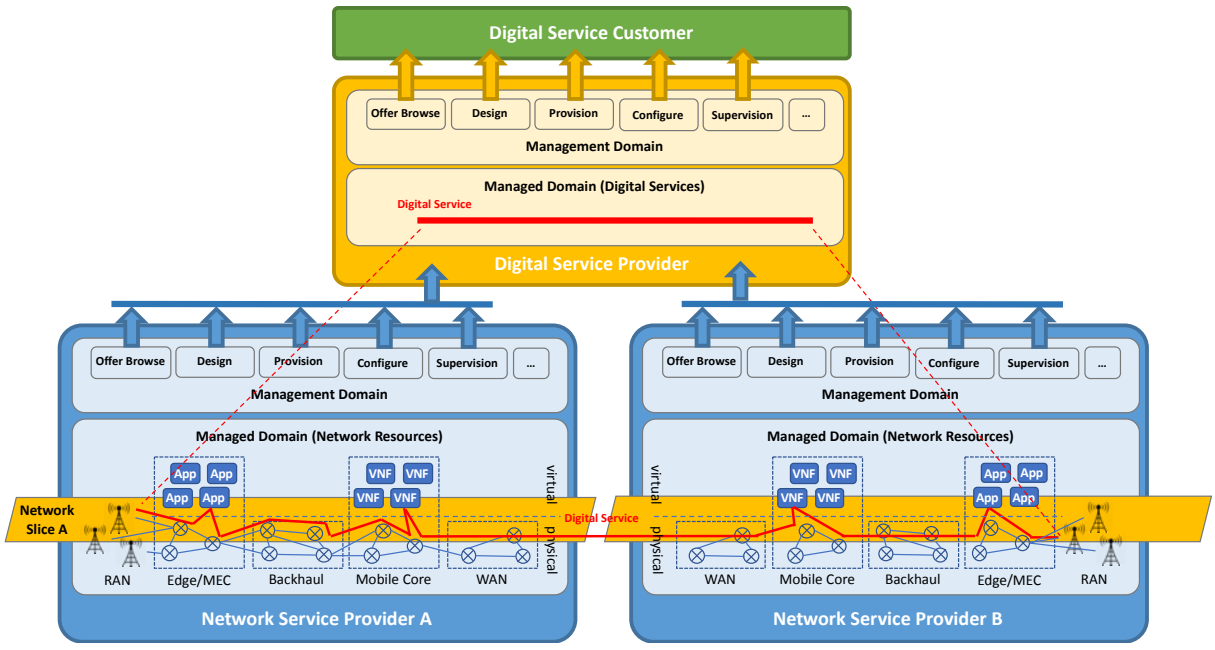


Figure 19 SliceNet Roles Applied to Multi-Domain – Detailed Perspective

3.4 Considerations about the SliceNet Management Architecture and Roles

The SliceNet roles model depicted in the previous sections allow the same actor to occupy several business roles. For example, a Service Provider can occupy the role of an NSP "Standalone Actor", the role of a DSP "Standalone Actor" or combine the functionalities of a DSP and an NSP – this combination of roles is from now on called "Combined Actor".

In terms of management, depending on the type of actor (Standalone vs Combined), the set of responsibilities is also different.

3.4.1 DSP & NSP Standalone Actors

Figure 20 illustrates the "Standalone Actor" scenario and the macro-management functionalities of each actor. Herein the NSPs encompass the "**SliceNet Slice-level Management Plane**", which has the following macro management responsibilities:

- Network infrastructure resources management;
- Network slices management;
- Network slices as a service management.

The NSP management responsibilities are tied to a particular administrative domain.

On the DSP side, it includes the "**SliceNet E2E Service-level Management Plane**", which has the following macro management responsibilities:

- E2E vertical services management;
- Orchestration and management of multi-domain network slices as a service.

Opposed to the NSP, the DSP has an inter-domain scope since it is the one responsible for composing the several network slices into a single E2E slice that is exposed to the vertical/customer.

Within this business roles/actors approach, since different business entities are responsible for the resources & slices management (NSP) and for the E2E service/slice (DSP), access to information across providers will be limited. Therefore, limited management interactions across the DSP "**SliceNet E2E Service-level Management Plane**" and the NSPs "**SliceNet Slice-level Management Plane**" are expected, blocking many cognition and supervision activities that could be important for the overall E2E slice optimization.

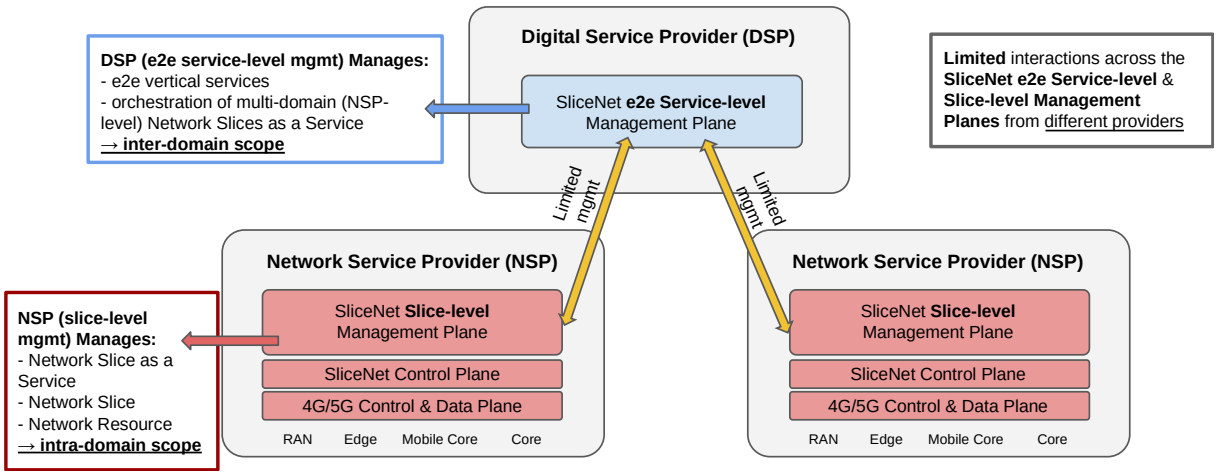


Figure 20 Management Responsibilities vs SliceNet Roles (DSP & NSP Standalone)

From an architecture perspective, within the DSP, the management architecture components will be related with E2E service-level management capabilities (as illustrated in Figure 21) – E2E Service Orchestration, E2E Service Monitoring, E2E Service Aggregation, E2E Service Cognition, etc. The network slices and resources management components are not required in the DSP domain (since it is not its management responsibility).

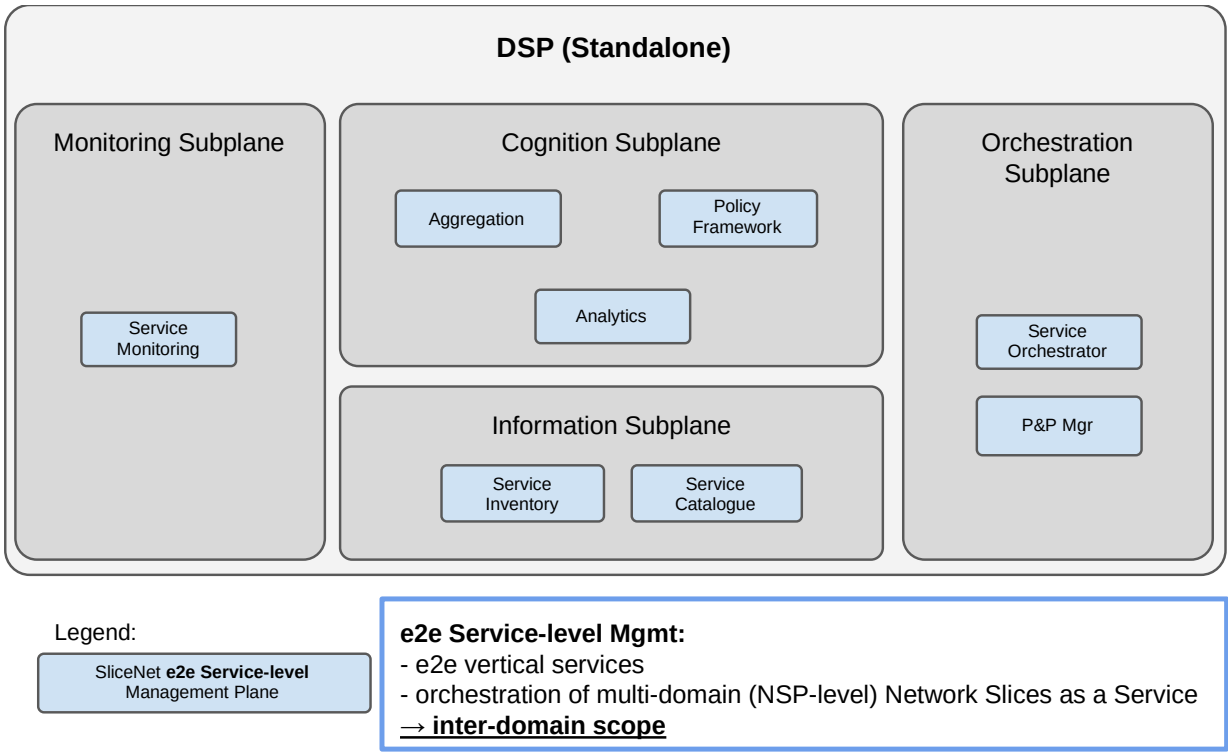


Figure 21 Management Architecture Components – DSP Standalone Perspective

On the other hand, from the NSP Standalone perspective, the required architecture components are related with resources, network slices and network slices as a service exposition management – Resource/Slice/Service (NSaaS) Orchestrator, Resource/Slice/Service (NSaaS) Monitoring, etc. – illustrated in Figure 22.

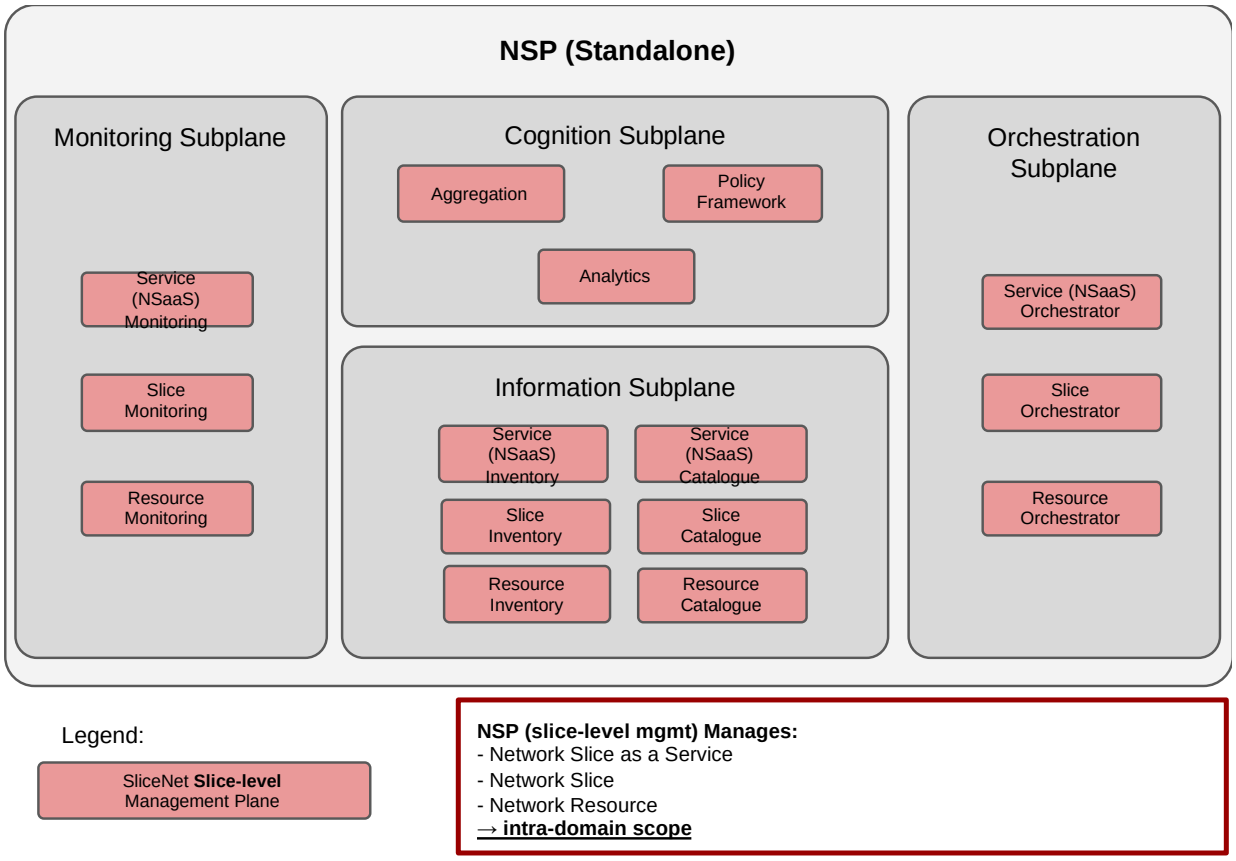


Figure 22 Management Architecture Components – NSP Standalone Perspective

3.4.2 DSP & NSP Combined Actor

Figure 23 illustrates a mixed scenario composed by a "Combined Actor" (NSP + DSP) and a standalone actor (NSP), as well as the related macro-management functionalities. Herein the "Combined Actor" includes both the "**SliceNet Slice-level Management Plane**" and the "**SliceNet E2E Service-level Management Plane**", combining the following macro-management responsibilities:

- Network infrastructure resources management;
- Network slices management;
- Network slices as a service management;
- E2E vertical services management;
- Orchestration and management of multi-domain network slices as a service.

As illustrated in Figure 23, with this approach, the interactions between the resources/slice level and the E2E/vertical service level are unlimited since it all happens within the same service provider. This provides total flexibility to process, analyze and actuate over the data, stimulating advanced cognition procedures (due to the unlimited access to information and procedures). Since this actor encompasses the DSP business role, it is also responsible for the interactions with peer NSP administrative domains to create E2E network slices/services that span across multiple NSPs.

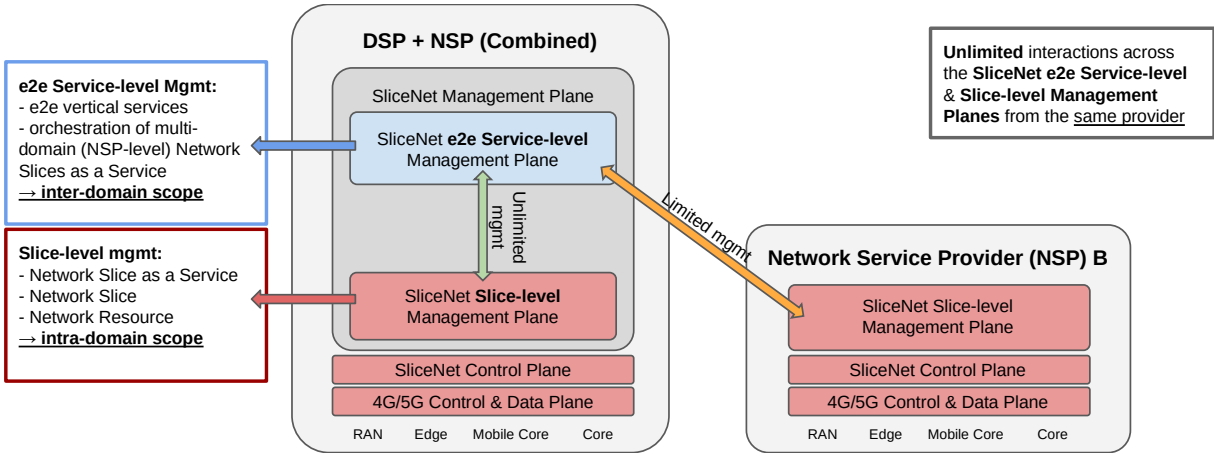


Figure 23 Management Responsibilities vs SliceNet Roles (DSP & NSP Combined)

From an architecture perspective, the combined "DSP + NSP" actor includes management components related with the E2E service – e.g. (E2E, NSaaS) Service Orchestration, (E2E, NSaaS) Service Monitoring, (E2E, NSaaS) Service Aggregation, (E2E, NSaaS) Service Cognition, etc., as well as management components related with slices and resources management capabilities – e.g. Slice/Resource Orchestration, Slice/Resource Monitoring, Slice/Resource Aggregation, Slice/Resource Cognition, etc. This approach is depicted in Figure 24:

- Red components are related with Slice/Resources management (NSP scope) – e.g. Slice/Resource Orchestration, Slice/Resource Monitoring, etc.;
- Blue components are related with Service management (DSP scope) – e.g. P&P Manager;
- Red/blue mixed components are related with functionalities that can be combined together (DSP and NSP scope) – e.g. service-level orchestration functionalities combined in a single Service Orchestration component (e.g. E2E Service Orchestration and NSaaS Service Orchestration), aggregation-level functionalities combined in a single Aggregation component (e.g. aggregate slice-level aggregation, E2E service-level aggregation, NSaaS service-level aggregation), etc.

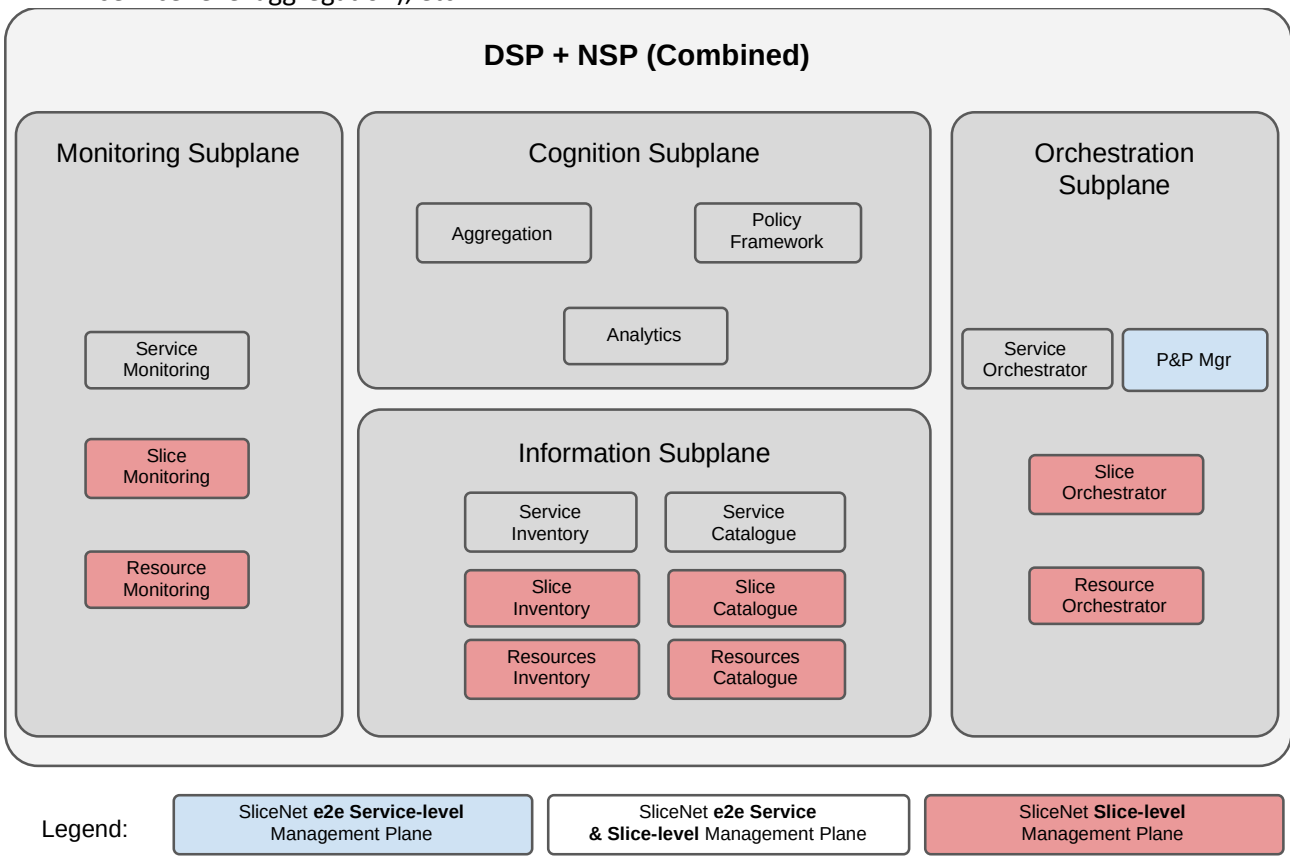


Figure 24 Management Architecture Components – DSP & NSP Combined Perspective

Finally, Figure 25 provides an instantiation example in a multi-domain environment, including the inner components relationships. In this case, two actors are involved:

- Combined DSP + NSP Actor;
- Standalone NSP Actor.

A mixed scenario, such as the one presented in Figure 25, in which a combined actor (DSP + NSP) and a standalone actor (NSP) are in place, is a suitable approach for SliceNet since it allows (i) to replicate real-life/production scenarios (mixed scenarios), (ii) unlimited management capabilities (in the combined actor) and (iii) limited management capabilities (in the interaction between the combined and the standalone actor).

Since network slices are exposed as a service (NSaaS) towards the DSPs, interactions between the combined and the standalone actors are expected to take place at the service-level. For example:

- Service Catalogue-level interactions to exchange NSaaS templates among the administrative domains;
- Service Orchestration-level interactions to exchange instantiation-related information;
- Service Monitoring level-interactions to exchange supervision-related information.

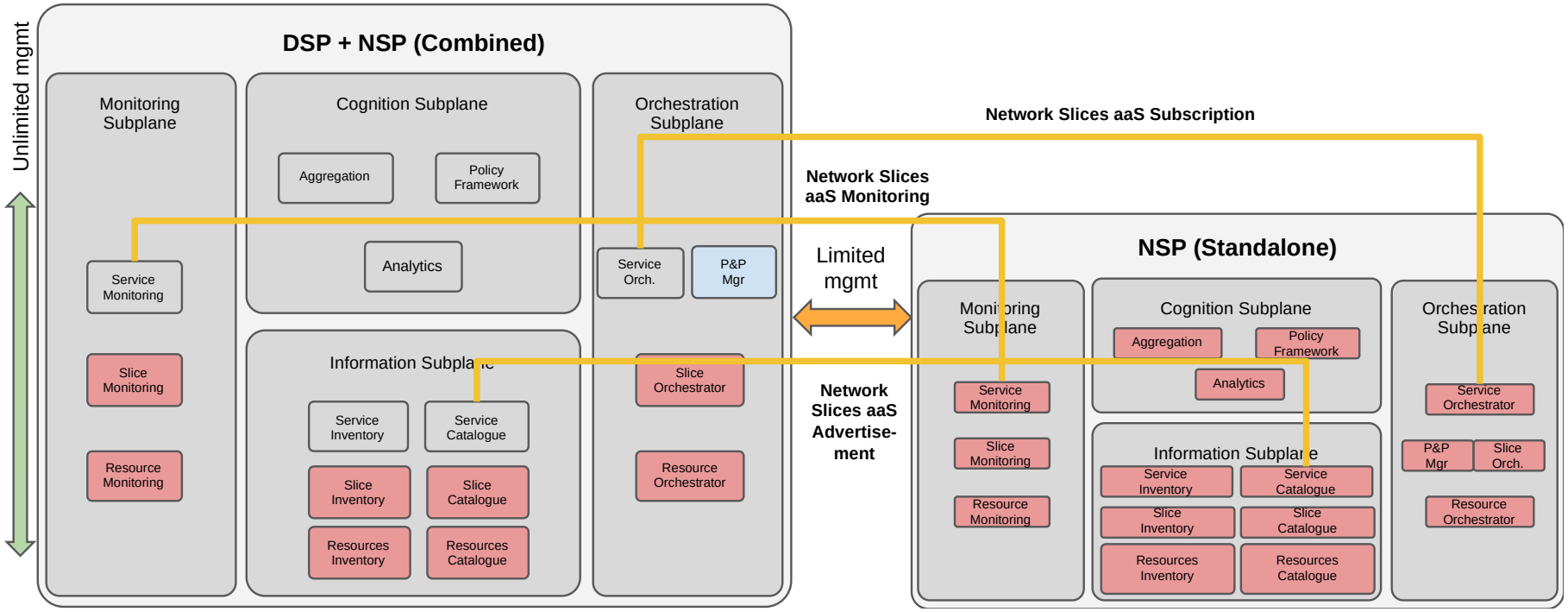


Figure 25 Management Architecture Components – Instantiation Example (Combined Actor & Standalone Actor)

These interactions will be further detailed in sections 5 and 6 of this document.

4 SliceNet Information Model for Slices

An Information Model provides a system conceptualization; several definitions have been provided by standardization fora and initiatives. According to IETF, an Information Model is "an abstraction and representation of the entities in a managed environment including definition of their properties, operations and relationships. It is independent of any specific type of repository, software usage, platform, or access protocol." [20]. TMF states that " an Information Model is a representation of business concepts, their characteristics and relationships, described in an implementation independent manner " [21]. In 3GPP " Information Model denotes an abstract, formal representation of entity types, including their properties and relationships, the operations that can be performed on them, and related rules and constrains ." [22]

The SliceNet information model is elaborated based on the analysis of the ongoing initiatives and standardization. It has several roles: it aims to bring a consensus on the Networking Slice paradigms and its related concepts by defining them, proposing relationships between the concepts.

In addition the concepts of the information model help to define the objects that the management modules will manipulate and exchange through the interfaces and this by instantiating the information into one or several data models that will be specific to technologies and/or implementations in the coming project work package (for example WP4, WP5, WP6).

4.1 Service-Slice-Resource concepts definitions

The concepts definitions in Table 1 and Table 2 are based on the TMF, 3GPP and ETSI definitions [23][24][25].

Table 1 Slice related Concepts

Concept	Definition
URLLC	Slice suitable for the handling of ultra- reliable low latency communications.
eMBB	Slice suitable for the handling of 5G enhanced Mobile broadband, useful, but not limited to the general consumer space mobile broadband applications including streaming of High Quality Video, Fast large file transfers etc.
mMTC	Slice suitable for the handling of massive IoT.
Slice Service Type(SST)	refers to the expected Network Slice behaviour in terms of features and services;
Customer Facing Service (CFS)	A CustomerFacingService defines the properties of a particular related specification (i.e. know-how) that represents a realization of a vertical request within an organization's infrastructure;
Customer Facing Service Instance (CFSI)	The vertical may require several instances for its service running in different geographical areas for example.
Customer Facing Service Template (CFST)	CFS template captures the vertical request w.r.t. the demanded service, its business constraints, etc
Network Slice(NS)	A Network Slice (NS) consists of Physical and/or Virtual Network Functions (NFs, VNFs/PNFs) that can belong to Access (AN) and Core (CN) Network part. The synthesis of an NS serves a particular functional purpose and once instantiated it is used to support certain communication services.

	It is a concept describing a system behaviour which is implemented via Network Slice Instance(s).
Network Slice Template(NST)	description of the structure (and contained components) and configuration of a network slice
Network Slice Instance (NSI)	a set of network functions and the resources for these network functions which are arranged and configured, forming a complete logical network to meet certain network characteristics. It is an instance created from a Network Slice Template (NST)
Network Slice Subnet (NSS)	is a set of subnet and or a set of network function. NS and NSS is a recursive approach where NS is a set of NSS and NSS is also a set of NSSs and Network functions.
Network Slice Subnet Instance (NSSI)	A set of network functions and the resources for these network functions which are arranged and configured to form a logical network.
Network Slice Subnet Template (NSST)	Description of the structure (and contained components) and configuration of the network slice subnet.
Network Function (NF)	Network function is a 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behaviour and 3GPP defined interfaces. A network function can be implemented either as a network element on a dedicated hardware, or as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure.

Table 2 associations between main concepts

Concept name	Association name	Concept name
Customer Facing Service Template(CFST)	describes	CFS
Customer Facing Service(CFS)	corresponds to a	SST
Customer Facing Service(CFS)	is assigned to (or “is supported by”), via the SST of the associated	NST
Customer Facing Service Instance (CFSI)	is supported by	NSI
Network Slice Instance(NSI)	deployed using	NST
Network Slice Template (NST)	has	SST
Network Slice Template (NST)	refers to 1 or multiple	NSST
Network Slice Instance(NSI)	contains 0 or multiple	NSSI
Network Slice Subnet Instance (NSSI)	contains 0 or multiple	NSSI
Network Slice Subnet Instance (NSSI)	contains 0 or multiple	NF
Network Slice Subnet Instance (NSSI)	deployed using	NSST
Network Slice Instance(NSI)	deployed using	NST

Network Slice Template (NST)	has	SST
Network Slice Template (NST)	refers to 1 or multiple	NSST
Network Slice Instance(NSI)	contains 0 or multiple	NSSI
Network Slice Subnet Instance (NSSI)	contains 0 or multiple	NSSI
Network Slice Subnet Instance (NSSI)	contains 0 or multiple	NF
Network Slice Subnet Instance (NSSI)	is deployed using	NSST
Network Function (NF)	is deployed as	VNF
Network Function (NF)	is deployed as	PNF
Network Slice Subnet Template (NSST)	is mapped to 1 or multiple	NSD
Network Slice Subnet Template (NSST)	realized by 1or multiple	NSD
Network Slice Subnet Template (NSST)	is realized by 1 or multiple	NFV-NS
NFV-Network Service (NFV NS)	is deployed using	NSD
Network Service Descriptor (NSD)	refers to 0..N	VNFD
Network Service Descriptor (NSD)	refers to 0..N	PNFD
Network Service Descriptor (NSD)	refers to 0..N	
Virtual Network Function (VNF)	deployed using	VNFD
Virtual Link (VL)	deployed using	VL
NFV-Network Service (NFV NS)	includes	PNF
NFV-Network Service (NFV NS)	includes VNF	VNF
NFV-Network Service (NFV NS)	includes	NFV-NS

4.2 Information Model Diagrams

In the diagrams below we present different levels of concept following the hierarchy of Service-Slice-Network Service-Resources as depicted in Figure 26.

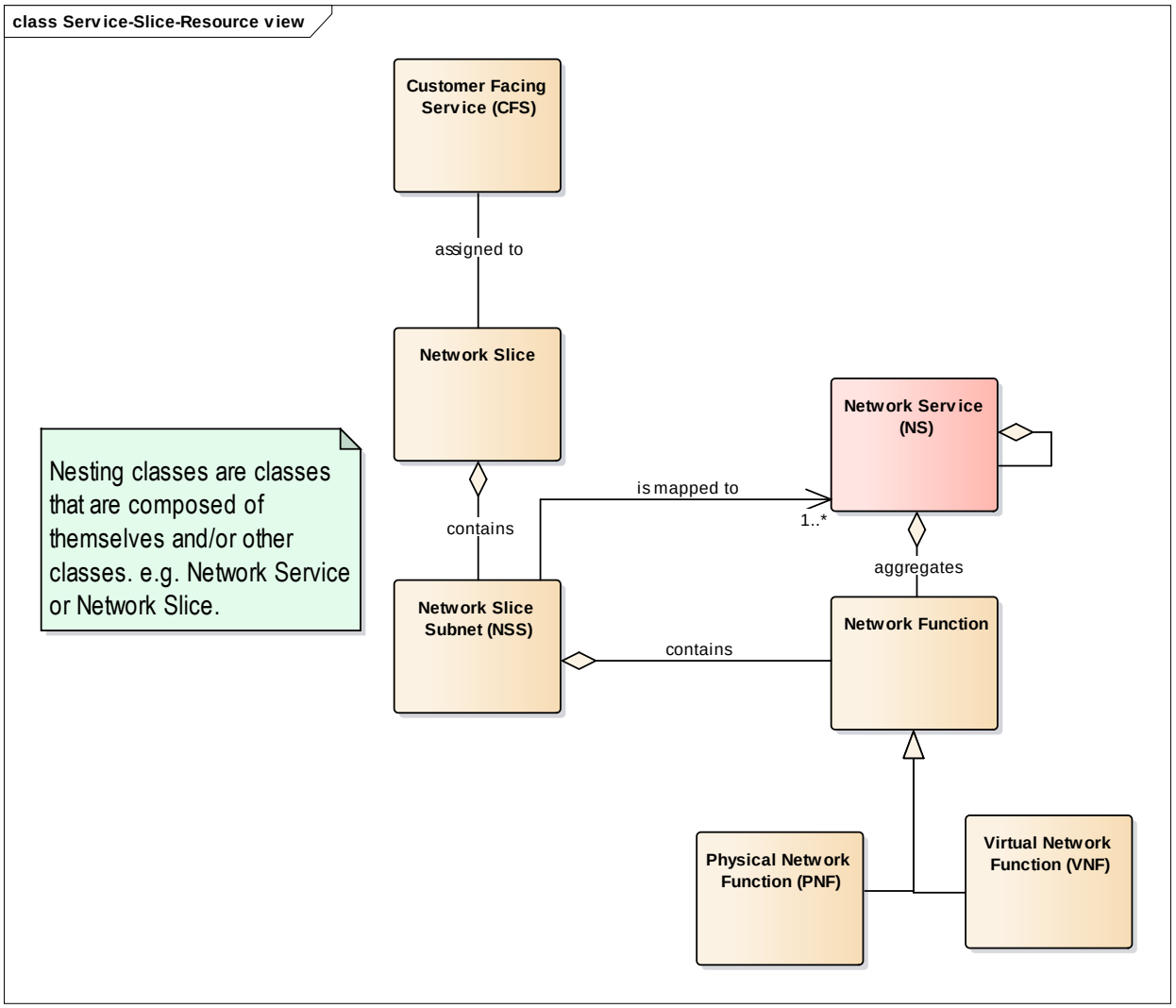


Figure 26 Service-Slice-Resource view

In the service level concepts diagram in Figure 27, the service is referred to as the “Customer Facing Service” as defined in the previous subsection.

In SliceNet those Customer Facing Service could be the Smart Grid, Smart City and eHealth. Each service has a Customer Facing Template in which the requirements of vertical and its request are captured. Each Service or CFS corresponds to a Slice Service Type that could be one of the three types as standardized by 3GPP.

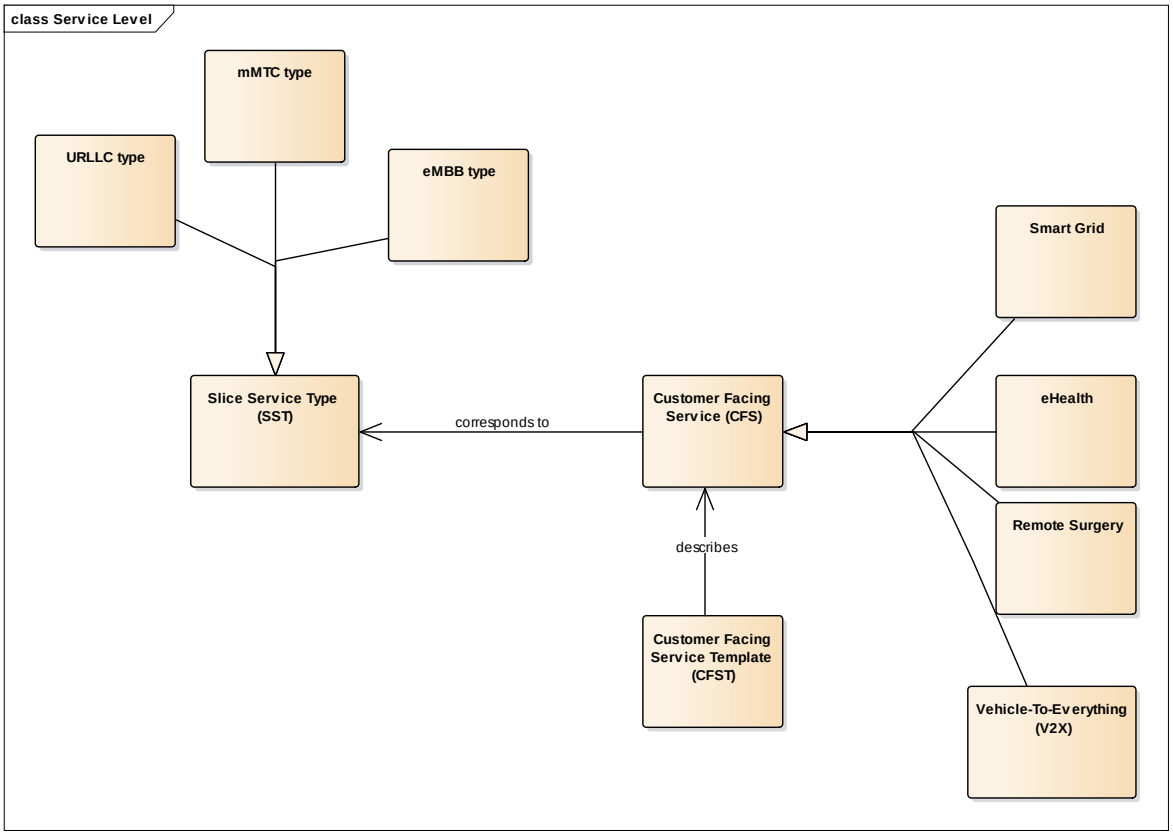


Figure 27 Service Level

The Service-Slice level, Figure 28, presents the how the service is related to the slices. Each CFS is assigned to a Network Slice. Each Network Slice is realized with instances, NSI. The NSI uses one or multiple Network Slice Subnet Instances NSSI. The template of a given Network Slice has the role of enabling the deployment as it encompasses technical details intended to meet the service fulfillment to the vertical.

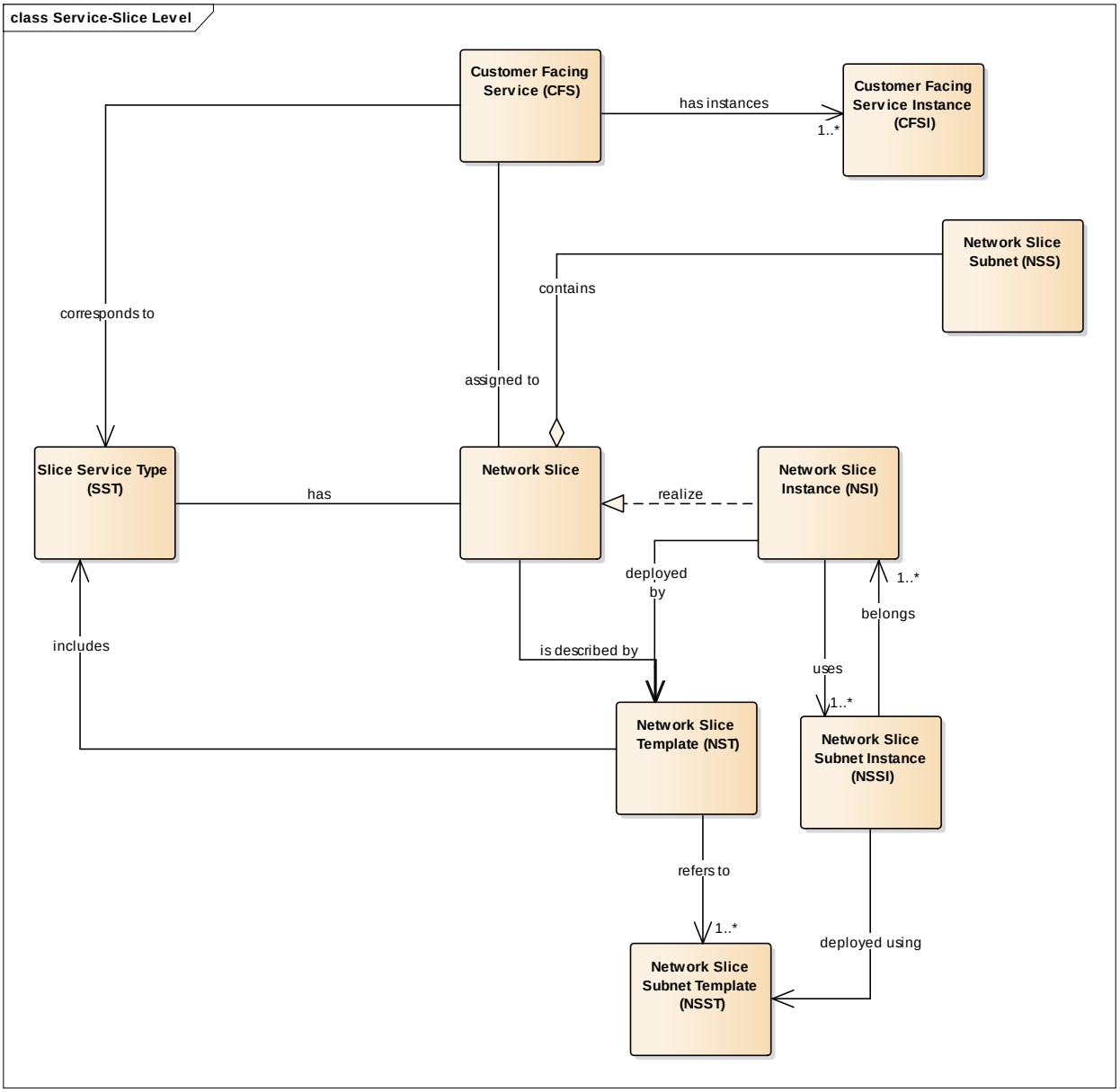


Figure 28 Service Slice-Level

In Slice-Resource level diagram, Figure 29, we present how the slice concepts are related to the resource concepts. Basically it shows the relationships between instances of Slices and instances of physical and virtual resources.

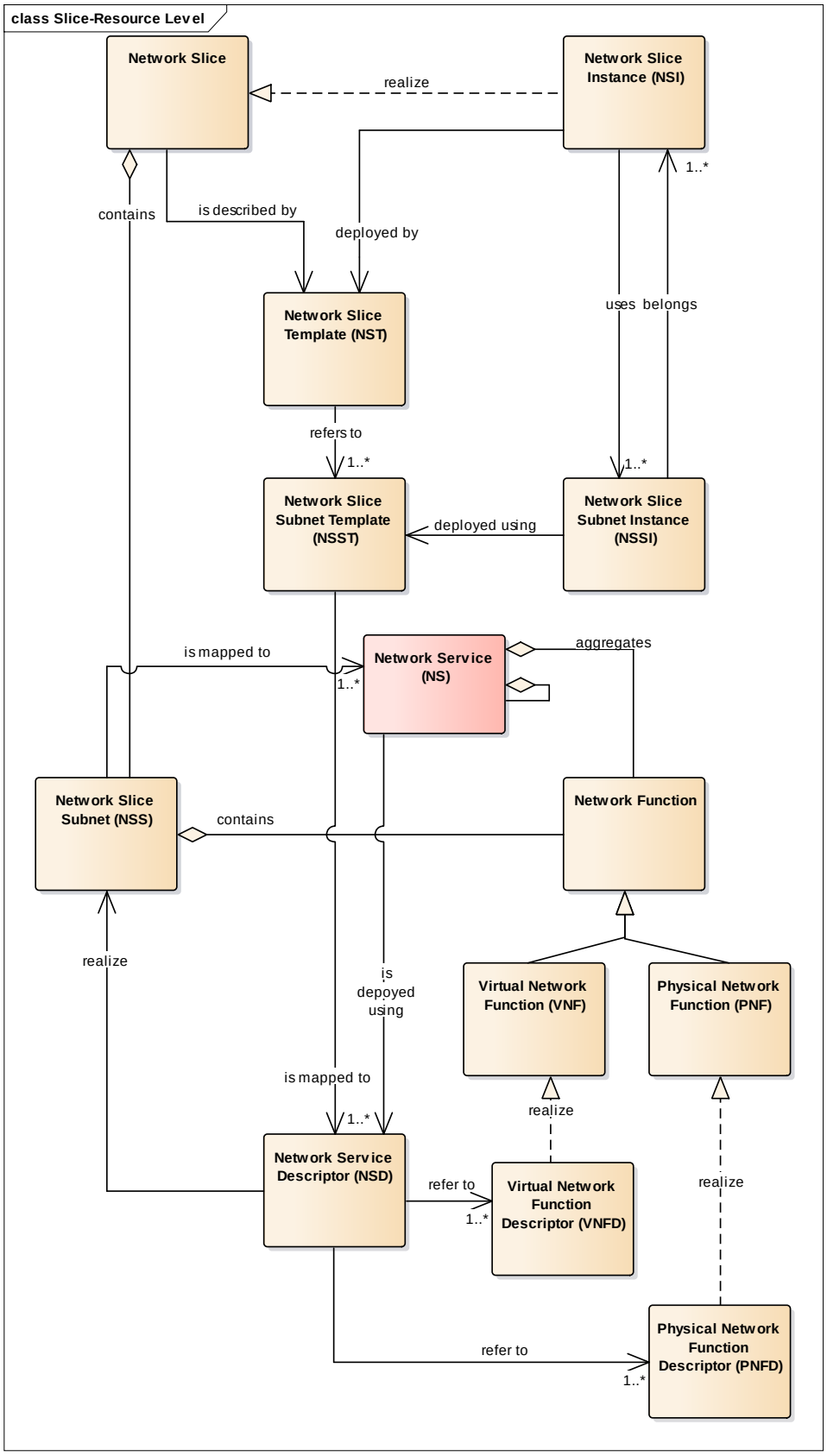


Figure 29 Slice-Resource Level

4.3 SliceNet Slice Template

In this section we zoom on the Network Slice template to define a set of parameters that we will follow in the SliceNet use cases. In addition to the information model concepts, the template complement with specific parameters that should be part of a given Network Slice template class.

Table 3 Slice template

Class name		Use case Smart City
Slice Type		eMBB
Network Topology	P2P P2MP MP2P Mesh	P2MP
Endpoints	Max number of configured endpoints Max number of attached endpoints Max number of active endpoints	thousands
mobility and networking features	Dynamic Session support Nomadicity support In-country Roaming support Seamless handover (session continuity) Max end-point speed - intra-cell Max end-point speed - inter-cell Max end-point speed - inter-domain International Roaming support Multicast support	No-mobility
Security features	Authentication Encryption	N/A
VAS	Firewalling NAT Parental control	N/A
Network Performance	Commited Bandwith per endpoint - DS Commited Bandwith per endpoint – US Total Slice Bandwidth – DS Total Slice Bandwidth – US	50kbps 50kbps the number of endpoints multiplied by the committed bandwidth per endpoint(endpoints communicate simultaneously)
Priority levels	Latency – peak Latency – mean Jitter – peak Jitter – mean Packet loss - without	<1000ms <500ms 300ms 100ms <1%
Plug & Play feature	Monitoring only	Monitoring only

	NFs configuration QoS/QoE control SDN forwarding NFs lifecycle Slice lifecycle	
Plug & Play view	Service level Slice level NF level	Service level view

5 Management System Definition

In deliverable D2.2 the high-level SliceNet Management & Orchestration architecture was defined. In this deliverable, a deeper level of details is provided for each one of the architecture components previously identified.

According to the SliceNet architecture-related terminology, this section provides a Level-2 (L2) perspective of the architecture, whereas D2.2 provided Level-0 (L0) and Level-1 (L1) perspectives. Among other aspects, this includes the description of

- the inner modules of each system component,
- the several closed-loops of the architecture and how they are coordinated/governed,
- the role of cognition and the
- Heterogeneous (MEC, RAN, NFV, PNF) resources management.

The SliceNet management and orchestration architecture is built as the composition and integration of four main subplanes, as specified in deliverable D2.2. Figure 30 presents the macro functional split of the management and orchestration architecture in line with D2.2, where the four subplanes are shown:

- Orchestration Subplane,
- Information Subplane,
- Monitoring Subplane,
- Cognition Subplane.

Those subplanes aim together to go beyond the classical FCAPS (Fault, Configuration, Accounting, performance, Security) management functions and the silos OSSs. Hence the inner management modules interactions ensure anticipation of fault and attacks to ensure SLA compliancy, availability and security of the slices as well as decision-making operations.

The **Orchestration Subplane** provides a set of coordination functions required to onboard, provision and maintain of vertical services and network slices as the combination of different network functions including virtualized and non-virtualized functions including MEC applications and RAN/CORE VNFs resources. It provides functionalities to make the whole SliceNet management and orchestration subplane work in a coherent way. The orchestration subplane also keeps the ownership of the information subplane that basically provides a heterogeneous set of catalogues and inventories. While the catalogues maintain the information related to the SliceNet platform capabilities and offerings in terms of NFV/MEC/RAN network functions and service descriptors, as well as network slice descriptors and vertical service templates, the inventories keep track of all provisioned instances of vertical services, mapping and correlating all the components in terms of network slice instances and NFV/MEC/RAN running functions and service instances. It also encompasses the P&P manager entity to manage to ensure lifecycle of the customization of the control plane to the verticals. In addition the recommendation of the QoE/SLA indicators is maintained with the QoE/SLA manager with the other components of the orchestration subplane.

The **Monitoring Subplane** provides a cross-layer platform for collecting metrics and counters from virtual and physical infrastructure components, NFV/MEC/RAN network functions, dedicated and specialized QoE and QoS sensors. The main goal of the monitoring subplane is to integrate and combine heterogeneous sources of metrics and counters information in a common way, where applicable providing preliminary aggregation of data at network slice and vertical service level, exposing the collected and pre-processed data towards the cognition subplane for further aggregation and analysis purposes.

The **Cognitive Subplane** uses artificial intelligence technique to ensure the operational aspects for services, slices and the underlying resources. It is elaborated based on state of the art and in

particular the research collaborative project within the H2020 program, namely the 5G CogNet. Hence it extends the latest results of cognitive-based network management for the slices.

It represents a logically centralized point in the SliceNet management and orchestration architecture. The intelligence it provides is distributed among its inner modules. We cite here the main roles of the cognition as the following:

- Cognitive or IA techniques could be used for the extraction of the main features or indicators to capture the behavior of resources when the services are activated within a given slice. For example the use of machine learning to identify the main thresholds for some key indicators based on the analysis of raw data. In addition several basic techniques like PCA (Principal component analysis) may be used to reduce the dimensionality of the data and get it ready to the machine learning algorithm.
- Cognition will also be used to select the IA model and how to configure it with respect to a given problem, for example fault management problem or security attach detection, etc. Obviously this takes into account the data types and the system constraints for the training process.
- Cognitive or IA techniques could be used for classical machine learning operations like the classification, prediction or clustering, etc. helping to predict anomalies, faults, malwares, degradation, etc. that may happen during the lifetime of the services running upon a given slice.
- The cognitive management fully embraces then the slice concept and is aware of slice contexts.
- Cognitive or IA techniques could be used within the policy management. This is coupled to the vertical-oriented approach to capture the vertical request, interpret it, generate the required templates and descriptors to ensure effective deployment and run time of the services running upon the slices. The One-Stop-API allows the vertical to provide QoE feedback and P&P allows pushing the vertical context into the control plane and into the sensors. This enables vertical-informed data processing and is integrated into the cognitive analysis in support of QoE optimization.
- Cognitive or IA techniques, in particular optimization algorithms and heuristics could be used for the slice dynamic resources allocation and network function deployment while respecting the energy constraints, as well as the slice type w.r.t latency for example. Cognitive analytic methods are simultaneously applied per (sub-) slice instance, per slice type (class) and per end-to-end composite slices. Thus, for example, parameter optimization from one slice instance can be readily applied to new instances of the same or similar type; as another example, this awareness allow simultaneous optimization of multiple slice instances over shared resource.

Moreover, SliceNet foresees cognitive analytics applied by multiple owners and multiple roles; some of which may not even be managed by SliceNet. The SliceNet cognitive process can feed off data sources created by external analytic processes; and it turn, it feeds back some analytic results as new data sources to be consumed by other management and control components, as well as by external consumers. Slice (topology) awareness together with policy-controlled information exchange allows end-to-end cognitive management across roles and across domains.

The SliceNet management and orchestration architecture components and building blocks, arranged in the four subplanes introduced above, can be deployed and glued together in different flavors and options depending on the business role (i.e. Digital Service Provider or Network Service Provider) provided by a given actor.

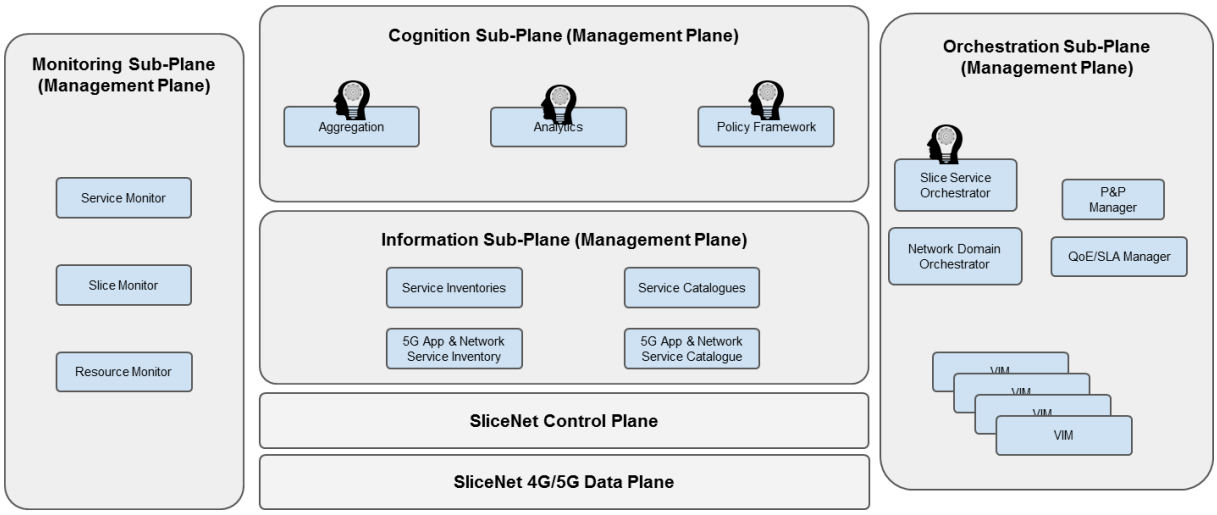


Figure 30 SliceNet management and orchestration overall view

5.1 Orchestration and Information components

The SliceNet Orchestration system is built around two major components:

- Slice Service Orchestrator (SS-O)
- Resource and multi network segment Orchestrator (NMR-O), as depicted in Figure 30.

The SS-O is the entry point of the Orchestration system and of the SliceNet platform at large, and it handles the association of services offered to verticals and other service providers with network slices and their correspondent management functions. The SS-O also takes care of the end-to-end orchestration of services across multiple domains. On the other hand, one or more NMR-Os are responsible for orchestrating per-administrative-domain network slices and network slice subnets implemented, following the ETSI GS NFV EVE 012 [9] principles presented in section 2.2, as a composition and combination of NFV Network Services (NFV-NSs) spanning the multi-network segments NFV (e.g. CORE, RAN including MEC applications) as well as the geographically distributed NFVI-PoP domains.

As depicted in Figure 30, the SliceNet Orchestration system follow and approach where the SS-O can consume the services offered by one or more NMR-Os in the same administrative domain.

Moreover, following the multi-domain NFV orchestration principles and procedures defined in [26] and [27], the SliceNet Orchestration system does not prevent multi-domain NFV-NSs interactions among peering NMR-Os (i.e. belonging to different administrative domains) aiming to fulfill end-to-end slice requirements and performance constraints. This option of NMR-O to NMR-O communication between different provide has to be considered as an optional feature in SliceNet, as the primary choice is to keep multi-domain interactions at the service and slice orchestration level only.

In addition to these components, the SliceNet Orchestration system also includes the Plug&Play Manager, as the lifecycle manager of the SliceNet Plug&Play Control functions described in deliverable D2.3 and offering to verticals and service (or slice) consumers at large the possibility to customize the runtime control of their services and slices, including access to monitored service, slice and resource metrics and KPIs. In the same line, the QoE/SLA Manager is responsible for managing the life-cycle of the per-slice QoE Optimizer instances (described in D2.3), which assure that the QoE requirements of the services running in the slice are fulfilled.

Following the different options available for the SliceNet business roles, the SliceNet Orchestration system includes either all or a subset of the above mentioned components, as detailed in section 3.

Indeed, in the case of combined DSP and NSP actor, as well as in the case of standalone NSP, both the SS-O and NMR-O are deployed in the SliceNet Orchestration system.

On the other hand, in the case of standalone DSP actor, the SS-O is envisioned to be required to manage service level lifecycles, Figure 31.

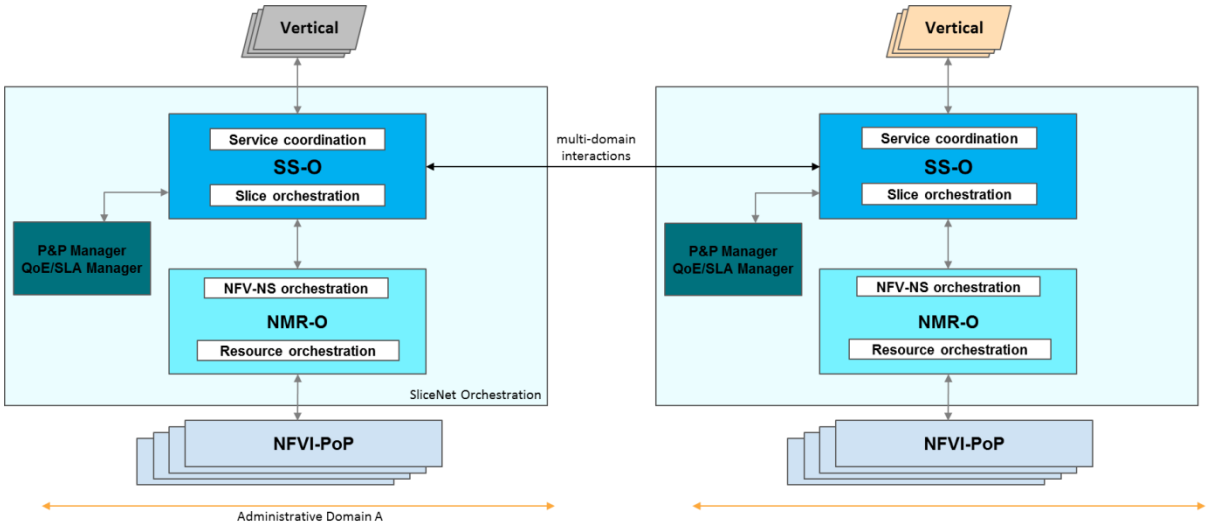


Figure 31 SliceNet Orchestration overview

5.1.1 Slice Service Orchestrator overview

The SS-O is the common entry point for all service related functionalities within the SliceNet platform. From an SS-O perspective, a service can be declined in two complementary ways:

- a vertical service, being it the ultimate end-to-end service offer of a DSP (or a combined DSP+NSP) to a vertical,
- NSaaS (Network Slice as a Service), being it the network slice service offer of an NSP to a DSP (or to a combined DSP+NSP) to implement multi-domain and cross-provider services and slices.

The SS-O coordinates the on-boarding and provisioning of customized services for verticals and other service providers. The SS-O offers the possibility to define customized services from a set of service-oriented templates, which aims at capturing the service requirements to be specified by the vertical or service consumer in general (e.g. DSP or combined DSP+NSP in another administrative domain).

The Service Template (ST) therefore represents a pre-determined service offer in the form of a blueprint version of the Service Descriptor (SD), where subsets of attributes have to be specialized by the vertical (or service consumer). Following the Customer Facing Service Template (CFST) information model defined in section 4.

The ST describes the structure of the corresponding service offer, including service components and additional capabilities to express, among the others, SLA, QoE/QoS and Plug&Play (in terms of control exposure required) requirements.

The ST follows a service-oriented language and semantic, and describes the service offer in terms of service components rather than resource components.

Starting from a ST, verticals or service consumer's at large request a customized service by specializing the template attributes. This request is processed by the SS-O which translates it into a Service Descriptor (SD), that identifies and characterizes the given customized service offer.

In particular, the SD is obtained after the vertical or the peering service provider enforces the missing attributes and information in the ST, and therefore its structure is derived from the corresponding

ST, possibly including additional service description information not exposed to the vertical or service consumer, e.g. for multi-domain interconnection and combination purposes, reference to constituent network slices, etc.

During this translation process, the SS-O composes the SD as a combination of one or more network slices, offered either by its own administrative domain or by peering domains (as NSaaS services).

In practice this translation maps a SD into a Network Slice Template (NST), which follows the SliceNet modeling principles defined in section 4 and provides a more resource centric description and composition of offered service, that can be used from the SS-O slice orchestration functions to coordinate network slice and network slice subnets provisioning. The NST is intended to be dynamically built and composed by the SS-O during the SD translation process, as a customized resource centric view of the service offer.

Following the approach proposed in [9] (and reported in section 2.2) the SS-O practically implements a network slice with extended NFV Network Service Descriptors (NSD), thus as a set of VNFs, PNFs and MEC applications (still modeled and implemented as specialized VNFs according to [28] to interconnected following a forwarding graph structure by means of Virtual Links with several options for fine-grained instantiation parameters (i.e. deployment flavours) related to QoS attributes and scaling schemes [32]. Therefore, a given service offered by the SS-O, translated into the correspondent NST, can be seen as the combination NFV-NSDs provided by the NMR-Os in the same administrative domain and possibly NSaaSs offered by SS-Os in peering domains. And during service provisioning phase, the SS-O is responsible to request the selected NMR-O to create or update the NFV-NSs that implement the slices associated to a customized service offer (i.e. to an SD), as well as to request peering SS-Os to instantiate any NSaaS service in other domains required to implement the end-to-end vertical service.

Figure 32 shows a high level functional split of the SS-O, where the main service and slice orchestration and coordination functions are highlighted along with their interactions with other SliceNet platform components. This split also identifies and highlights service and slice catalogues and inventories under the ownership of the SS-O.

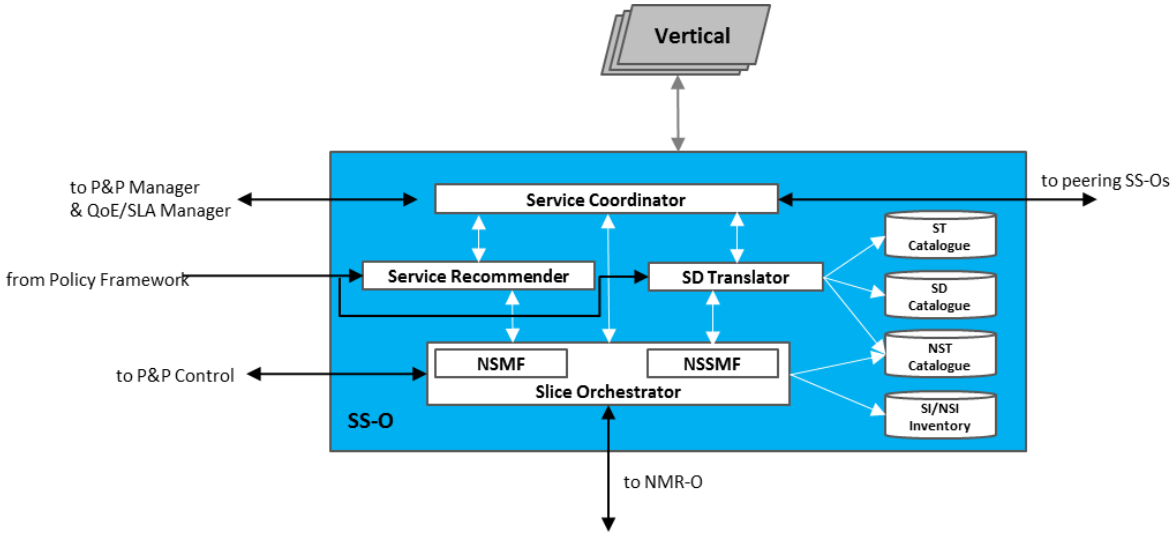


Figure 32 SS-O high level functional split

The **Service Coordinator** is the overall orchestrator of the service-related logic, operations and mechanisms within the SS-O. It is the entry point of the SS-O and it is in charge of coordinating the multi-domain interactions with peering SS-Os in other domains. It manages the ST, SD and NST catalogues, and it takes care to map the business needs of verticals and service consumers, in terms of SLA requirements, to slice capabilities. The Service Coordinator is also responsible to interact with

the Plug & Play Manager to coordinate the lifecycle of Plug & Play control instances offering customized runtime control and management of services and slice instances to verticals and service consumers.

Similarly, the Service Coordinator contacts the QoE/SLA Manager to instantiate and coordinate the life cycle of the QoE optimization associated to the slice that will support the requested service.

The **SD Translator** translates SD requirements at service level into requirements at network slice and NST level with the aim of fulfill incoming service requests from vertical and other service providers.

It supports the Service Coordinator in the mapping of SDs into NSTs, as combination of NSaaS services from other domains and NFV-NSDs exposed by the NMR-O to implement end-to-end vertical customized services.

The **Service Recommender** supports the Service Coordinator for what concerns the resolution of races and contentions in the service to network slice mappings. Indeed, it provides a decision engine for mapping service offers to existing network slices and NFV-NSs, allowing for slice and NFV-NSs sharing across services (and across verticals if applicable) depending on SLA requirements. For this, it receives dynamic instructions from the Policy Framework in the SliceNet Cognition Subplane to enforce specific mapping policies in light of services and slices monitoring and analysis. In this way, the Service Recommender takes advantage of the previous experience of the cognition sub-plane to provide more accurate service configuration. It also interacts with the Slice Orchestrator to collect required information about available slices and NFV-NSs instances and descriptors (i.e. NSTs and NSDs). All possible combinations between services and network slices are supported by the Service Recommender, including: i) a network slice shared by different vertical services, ii) a given vertical service mapped to multiple network slices.

The **Slice Orchestrator** is the overall coordinator of the slice-related logic, operations and mechanisms within the SS-O and thus it is the gluing functionality between the SS-0 and the NMR-O, taking care to relate service logics with NST and NFV-NS logics. Following the 3GPP terminology, it provides the Network Slice Management Function (NSMF) and Network Slice Subnet Management Function (NSSMF) capabilities.

In particular, it is in charge of lifecycle management of network slice instances modeled as NSTs and implemented as combination of NFV-NSs by offering the client side of the northbound interface exposed by the NMR-O. When applicable, the Slice Orchestrator also exposes to the Plug & Play control instances (dedicated per vertical) access to well defined set of slice orchestration and runtime adaptation primitives and APIs.

The **Service Template Catalogue** stores and handles the whole set of STs the given SS-O can offer to either verticals or peering SS-Os in other domains, following the service-level information model described in section 4. Service offers for peering SS-Os (e.g. modeling NSaaS services) and service offers for verticals are clearly separated and managed with independent procedures. Indeed, the STs related to peering SS-Os offers can be either exchanged with on-line (e.g. on-demand queries) or off-line procedures (e.g. continuous advertisement), but not exposed in any case directly to the vertical. On the other hand, STs related to vertical offers are fully exposed as main repository of vertical slice offers.

The **Service Descriptor Catalogue** maintains and handles the customized service offers for either verticals or other service providers. SDs for customized services required by peering SS-Os and those for customized vertical services are also managed separately as for STs, mostly to avoid verticals to access and view end-to-end SDs only. In general, SDs stored in this catalogue contain full information required by the Service Manager to trigger the service and slice instantiation process according to the model described in section 4, thus including information required to map service components into NFV-NSs offered by the NMR-O and NSaaS offered by peering SS-Os.

The **Network Slice Template Catalogue** stores the network slice deployment templates, describing the characteristics of network slices and their constituent components at a slice resource level, i.e. NSTs. NSTs are produced dynamically by the SS-O, in particular by the combination of Service Coordinator, SD Translator and Slice Orchestrator functions and workflows, when a new service offer (either for a vertical or for a peering SS-O) is built in the form of a SD. This catalogue maintains slice resource level information following the NST model described in section 4 and required by the Slice Orchestrator to manage the lifecycle of network slices, including the mapping with NFV-NSDs offered by the NMR-O.

The **Service Instance (SI) and Network Slice Instance (NSI) Inventory** maintains the information related to provisioned end-to-end vertical services, as well NSaaS service instances offered to peering SS-Os in other domains, including full information of service components (e.g. service access points). It also stores full information of instantiated and running network slice instances, in terms of slice level resources provisioned, including the mapping to NFV-NSs (for relating entities maintained by the NMR-O). All the information stored in the SI/NSI inventory follow the SliceNet information model specified in section 4 and can be accessed by the Service Recommender for applying proper network slice and NFV-NSs sharing schemes.

5.1.2 Network Domain Orchestrator

The Network Domain Orchestrator that corresponds to the NFV/MEC/RAN Orchestrator (NMR-O) acts as a NFV NS and resource orchestrator, taking care of coordinating the lifecycle management of NFV NS instances composed by the combination of VNFs, PNFs, MEC applications (still implemented as specialized VNFs) interconnected by means of forwarding graphs. The NMR-O is also responsible to orchestrate the RAN slicing and configurations leveraging on the SliceNet Control Plane capabilities as described in deliverable D2.3.

The NMR-O targets a combined and integrated orchestration of NFV and MEC infrastructures and environments, following the principles defined in the [28]. In particular, as depicted in Figure 33, the NMR-O combined orchestration of NFV and MEC segments considers the Mobile Edge Hosts as specialized NFV Infrastructures (NFVIs) that follows [31] architecture but deployed in an NFV environment. For this, the MEC architecture components are deployed and managed as follows by the NMR-O:

- The Mobile Edge (ME) platform is deployed as a VNF and therefore the procedures defined by ETSI NFV MANO specifications for its lifecycle management by means of dedicated VNF Managers (VNFM) applies
- MEC applications are implemented as regular VNFs, allowing for reuse of ETSI NFV MANO information models for NS and VNF descriptors with proper enhancements and extensions to integrate the AppD model defined in the [29]
- The Mobile Edge Host virtualization infrastructure is deployed as a NFVI and its virtualized resources are managed by the VIM. For this purpose, the procedures and principles defined by ETSI NFV for VIM interfaces and models can be applied.

In this context, the NFV and ME NS orchestration features within the NMR-O (as depicted in Figure 33) takes care of the lifecycle management of the various types VNFs, including the Mobile Edge platform and the MEC Applications. On the other hand, the resource orchestration features allow to allocate required resources in the different NFV virtualized infrastructures (NFVIs), including those part of the Mobile Edge Hosts, by means of dedicated VIMs.

In summary, the NMR-O can be considered as an NFV and MEC combined orchestrator that supports the deployment and lifecycle management of MEC Apps and Mobile Edge Platforms as VNFs in the MEC segment. Following [30][28] orchestration principles, the NMR-O is split into three main functional components, as depicted in Figure 34: the Network Service Orchestrator, the Mobile Edge Application Orchestrator and the Resource Orchestrator.

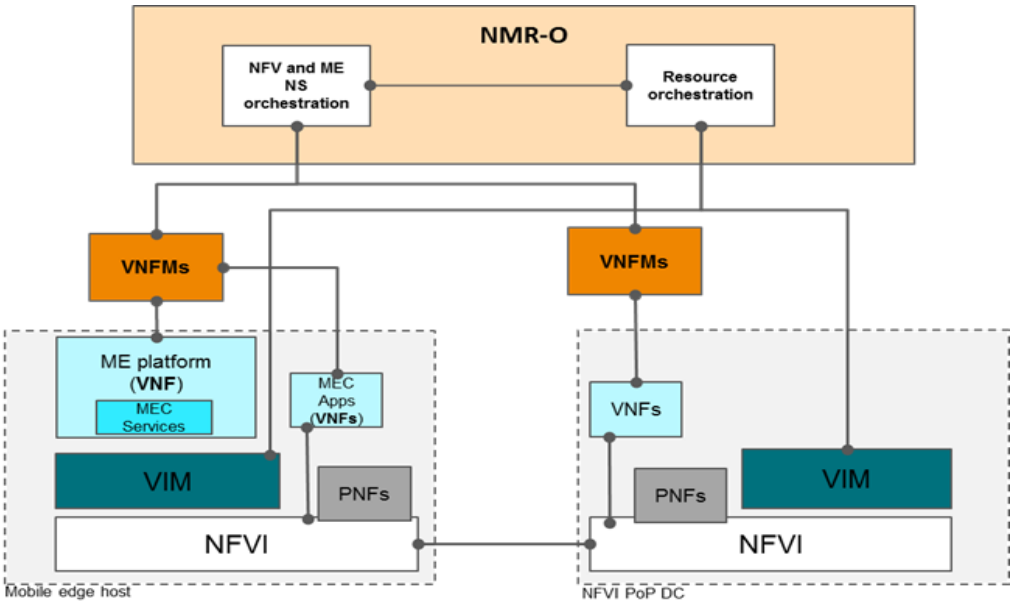


Figure 33 MEC in NFV approach and NMR-O NFV and MEC combined orchestration

The **Network Service Orchestrator (NSO)** is an enhanced NFV NSO that takes care to manage the lifecycle of NFV NSs, interacting with generic or specialized VNFMs for lifecycle management of regular VNFs and specialized VNFs implementing MEC Apps and MEC platform.

The NSO owns and manages the 5G App and NFV NS catalogue depicted in Figure 34, thus taking care to offer dedicated interfaces to onboard VNFs (including MEC Apps), PNFs (in general grouped as 5G Apps) packages and NFV NSDs. The NSO decomposes NFV NSs into VNFs and PNFs and provides the management of their instantiation in coordination with dedicated VNFMs. In this context, it takes care to establish the connectivity between VNFs and PNFs parts of a NFV NS, i.e. to enforce forwarding graphs and virtual links with NS specific and customized QoS requirements by interacting with the Resource Orchestrator. The NSO is also in charge of granting VNF (including those implementing MEC applications) lifecycle management operations from VNFMs, as those may impact NFV NSs. It is unaware of fine-granular resources status and availability in its own administrative domain, i.e. at NFVI-PoP, Mobile Edge Host NFVIs and RAN level, while it is only aware of the resource capacity as exposed by the Resource Orchestrator.

The NSO is the main entry point of the NMR-O for NFV and ME NS lifecycle management, for which it offer to SS-O and other SliceNet management components an interface aligned with ETSI GS NFV IFA 013 [33]. It leverages on the coordination and orchestration features exposed by the MEAO for what concern the MEC Applications implemented as VNFs in the context of a given NFV NS.

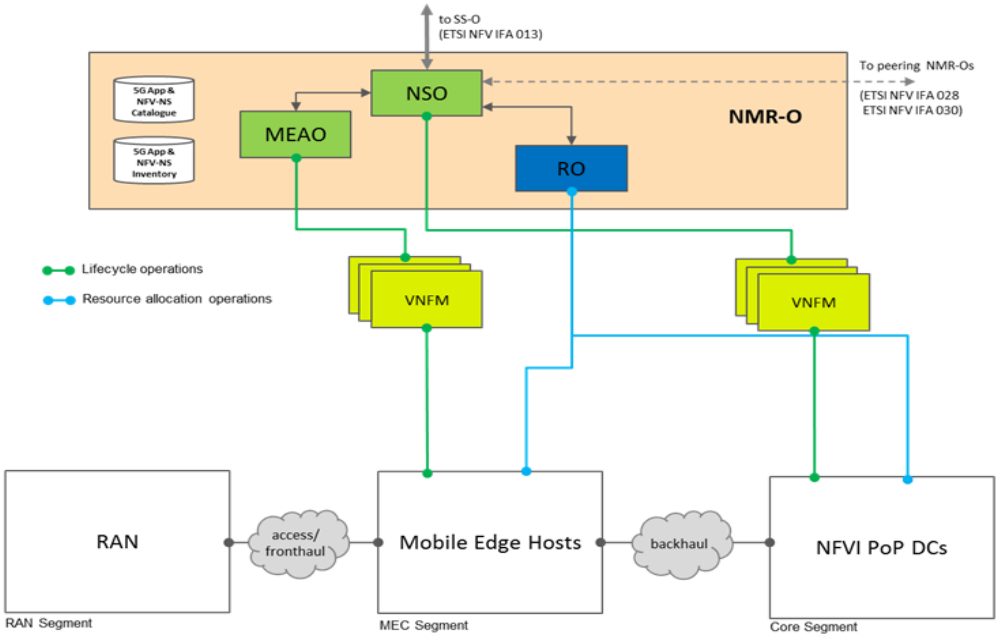


Figure 34 NMR-O high level functional split

The Mobile Edge Application Orchestrator (MEAO) is a Mobile Edge Orchestrator (MEO) as defined in the ETSI MEC architecture that augments the NSO and RO for service and resource orchestration of the set of MEC applications (implemented as VNFs) as one or more NFV NSs. Therefore, the combination of MEAO and NSO implements within the NMR-O the full set of NFV and ME NS coordination and orchestration functions, taking care to manage the lifecycle of NFV NSs spanning across MEC and NFV segments.

The MEAO selects appropriate Mobile Edge Host NFVI location for MEC Apps instantiation based on constraints such as latency, available resources, and available services, leveraging on the RO functions for allocating the required resources in the NFVI. Moreover, the MEAO manages the lifecycle of MEC Applications and ME platforms leveraging on their specialized VNFMs, mostly for triggering MEC Application instantiation and termination, as well as relocation when supported.

SliceNet considers the NSO as the unique entry point for NFV NS lifecycle operations towards the SS-O, and therefore as the responsible for the coordination with the MEAO for those NFV NSs composed by MEC Application VNFs. This can be achieved and implemented within the NSO (and the 5G App and NFV NS Catalogue) by modelling and managing the NFV NSs (i.e. those composed by regular VNFs and those composed by MEC Application VNFs) following the NSD nesting principles.

The **Resource Orchestrator (RO)** is an enhanced NFV RO, that takes care to allocate and configure resources in the end-to-end single-administrative domain infrastructure (from RAN segments to Mobile Edge Host NFVIs and NFVI-PoPs virtual infrastructures) for deploying VNFs (including those implementing MEC Applications) in proper locations to fulfill end-to-end NFV-NS (and network slice) requirements. As a generic feature, the RO keeps and provides an overall view of network, compute and storage resources available in the RAN, MEC and NFVI-PoP domains. The RO therefore provides a proxy gateway functionality towards the VIMs and acts as a bridge for some networking primitives for routing and QoS enforcement depending on the capabilities exposed by the VIMs. Indeed, the RO access the 5G App and NFV-NS catalogue to retrieve the deployment requirements in terms needed resources and expected performance constraints for each VNF, MEC Application and Virtual Link modelling a given NFV-NS to be provisioned upon NSO request, and then map them to the actual availabilities and capabilities of the underlying NFV and MEC infrastructures. In particular, for what concerns performance and QoS constraints, RO fully supports the ETSI NFV information models [9] for Virtual Link Descriptors (VLDs), VNF Forwarding Graphs (VNFFG.s), VNF Descriptors (VNFDs) and

NSDs, where QoS attributes are well defined and related to Deployment Flavors (DFs). A DF at the NFV-NS refers to the combination of the DFs for the NFV-NS components, i.e. mostly VNFs, Virtual Links and VNFFGs. Indeed each NFV-NS component can have several flavors (i.e. options in terms of performance, QoS and resource combinations) to choose at the time of instantiation and scaling operations. For example, for Virtual Links and VNFFGs, DFs can model several alternatives and options for QoS attributes in terms of bandwidth and latency constraints that can be used for mapping to end-to-end service and network slice QoS requirements.

The RO maintains an abstract resource view and is aware of the resource usage and availability in the NFVIs and RAN segments (when applicable). For this, it is constantly updated with the latest infrastructure resources organization (e.g. in terms of geographical and logic distribution in availability zones), availability and utilization from the various VIMs in its administrative domain. The RO is not aware of the logical grouping of the resource requirements into VNFs, and it is relevant to highlight that it cannot take lifecycle decisions based on VNF and MEC application instances or on NFV NSs instances, as it needs to be instructed by the NSO or the MEAO.

As depicted in Figure 35, the RO leverages on the SliceNet Control Plane to fulfill end-to-end resource allocations and configurations, spanning from RAN segments to MEC and NFV virtual infrastructures, and complement what it is not directly offered or controlled by the VIMs in the NFV and MEC segments. In particular, the RO exploits the SliceNet Control Plane Technology and Implementation Agnostic APIs [3] to provide actual end-to-end resource allocations and slice control configurations in those network segments not covered by the NFV and MEC VIMs. This translates, following the SliceNet Control Plane abstraction principles defined in D2.3, into enforcing proper configurations for: i) RAN slicing, ii) fronthaul and backhaul network connectivity provisioning with isolation across NFV-NSs and network slices, iii) WAN network connectivity provisioning in support of multi-domain (i.e. cross-provider) services. With reference to Figure35, the RO combines resource allocation operations (in blue lines) through the respective VIMs, with control plane slicing operations (in grey lines) through the SliceNet Control Plane. As an example, the VNFFGs requirements expressed in the NFV-NSDs are translated by the RO into proper operations and actions to be applied through the SliceNet Control Plane on (at least) fronthaul and backhaul network segments for ensuring that VNFFGs spanning different domain and segments are properly provisioned and guaranteed.

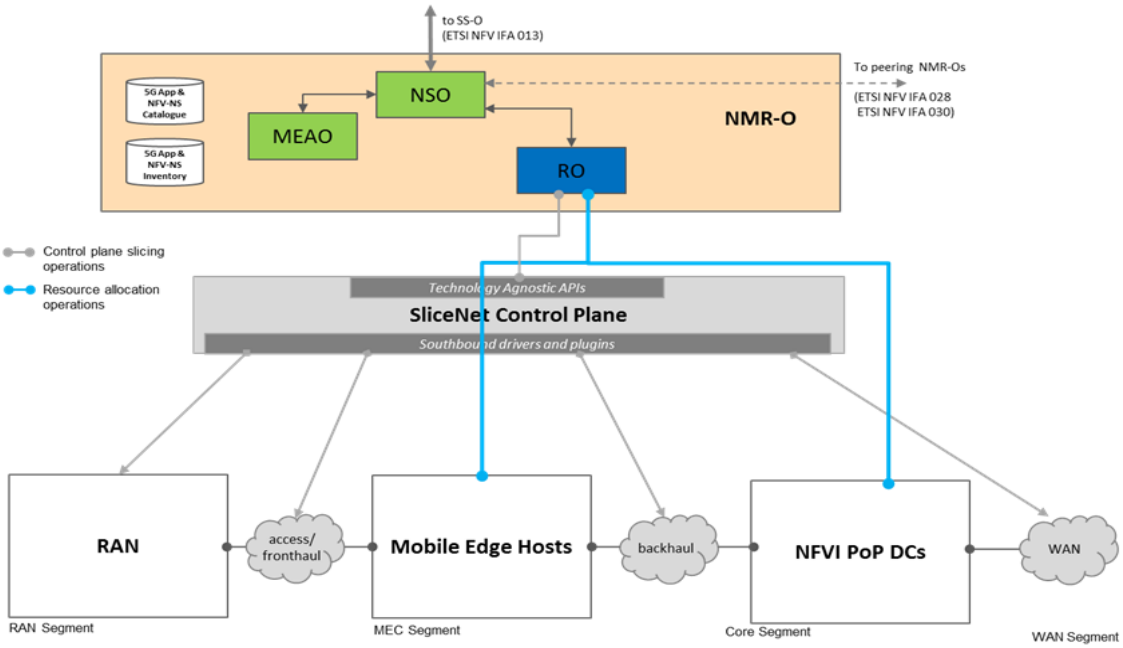


Figure 35 NMR-O high level functional split and positioning with respect to SliceNet CP

As already mentioned above and depicted in Figure 35, the NMR-O maintains a **5G App and NFV-NS Catalogue** where all the VNFs (including those implementing MEC Applications) and PNFs (being them together called 5G Apps) and NFV-NS are onboarded and modelled in terms of deployment templates and constraints, from resource and performance/QoS requirements to software images and lifecycle management information.

This 5G App and NFV-NS Catalogue is intended to offer more than a simple catalogue listing applications, network functions and NFV-NSs registered in the SliceNet orchestration platform. It is indeed conceived to provide a full onboarding service, managing a set of operations including 5G Apps and NFV-NSs onboard, enable, disable, update and offboard, including management of software images and binaries upload where applicable. The 5G App and NFV-NS Catalogue adopts generalized standard formats and contents for VNFs, MEC Apps, PNFs and NFV-NSs descriptors, following ETSI NFV and MEC [9] information models, thus allowing to decouple the onboarding process and NFV-NS design phase from the specific NSO, MEAO and RO technology and implementation choices (e.g. based on open source platforms like ONAP [37] Open Source MANO [34], OpenBaton [35] or on proprietary NFV MANO tools). Therefore, this 5G App and NFV-NS catalogue service is responsible to translate and map its unified models into tech-specific formats required by the specific NSO, MEAO and RO targets.

Moreover, in support of the SliceNet cognitive driven and QoE enabled on-demand sensing and actuation principles, the 5G Apps in the catalogue should include description of additional application-level characteristics not strictly related to their lifecycle management, like: i) configuration schemes to be applied after instantiation (e.g. Day1 and Day2 configurations), ii) monitoring metrics exposed.

As an additional onboarding principle, the idea of this generalized 5G App and NFV-NS Catalogue is to allow verticals to bring their own VNFs (including MEC Applications) to augment the SliceNet orchestration platform with vertical specific and customized functions, to be either deployed by default for their end-to-end services (i.e. as part of their default NFV-NS deployment flavor) or as a result of Plug & Play and QoE optimization procedures driven by cognitive loops.

As a complement of the above described catalogue, the NMR-O also maintains the **5G App and NFV-NS Inventory**, as depicted in Figure 35. This inventory stores the information related to instantiated VNFs, MEC Apps and PNFs and provisioned NFV-NSs, thus keeping track of the actual resources allocated for each entity and their relationships. All the information stored in the 5G App and NFV-NS inventory follow (and enhance where required) the ETSI NFV and MEC models and can be accessed by the NSO, MEAO and RO for applying their lifecycle and resource allocation logics, as well as from other SliceNet components (external to the NMR-O) for querying specific NFV-NS instances (and related components) information.

5.1.3 QoE/SLA Manager

One of the goals of the SliceNet project is to provide cognition-based QoE optimization on the services deployed over the slice. In this context, The **QoE/SLA Manager** module is responsible for managing the per-slice QoE optimization process. To do this, the QoE/SLA Manager takes care of the creation and life cycle maintenance of the QoE-Optimizer module instances that run in the SliceNet control plane in D2.3.

Figure 36 depicts the high level functional split that has been defined for the QoE/SLA Manager. During the service provisioning, the SS-O contacts the QoE Coordinator to request the QoE environment set-up (e.g. initial deployment of QoE sensors and actuators). The QoE Coordinator, in turn, contacts the QoE Life Cycle Manager (**QoE LCM**) which is the responsible entity for managing the life cycle of the QoE optimization instance (**QoE-I**) for each slice. The QoE/SLA Manager takes advantage of the cognition sub-plane inputs to provide the most appropriated QoE configurations and metrics according to the service/s to be offered over the slice based on the system previous

experience. In addition, the QoE Coordinator forwards the SLA/SLO inputs received from the SS-O so the QoE optimization system takes them into account. During the slice operation, the inputs provided by the cognition to the QoE/SLA Manager can be used to modify or reconfigure settings of the slice in order to improve such QoE. In this case the QoE LCM is responsible for updating the QoE Optimizer which, in turn, will operate over the lower layers of the SliceNet control plane.

Finally, the **QoE CP API** provides a unified set of operations to create and manage the QoE Optimizer instances in the SliceNet control plane.

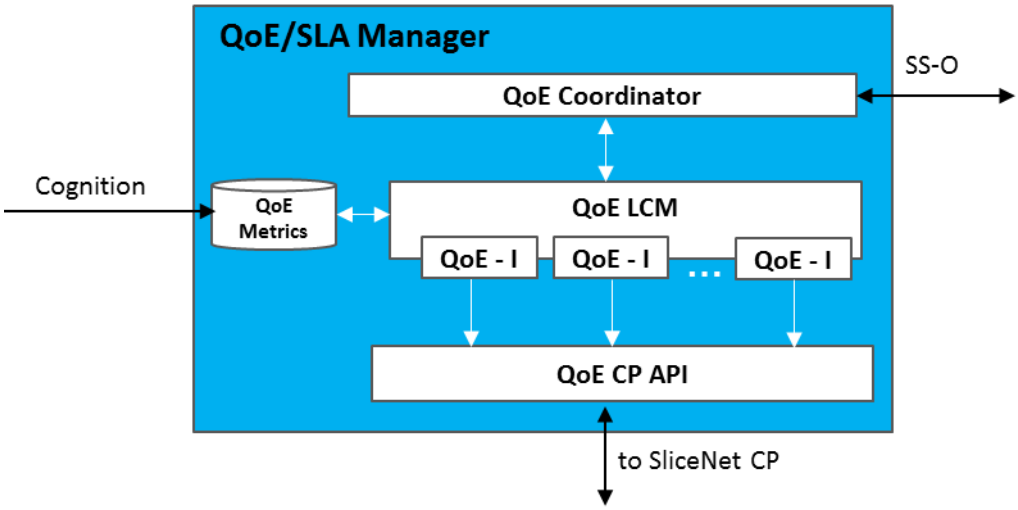


Figure 36 QoE/SLA Manager high level functional view

5.1.4 P&P Manager

Plug & Play is one of the key concepts in SliceNet as it aims at providing a truly customized environment for offering vertical runtime control and operation of their end-to-end slice instances. The ultimate goal of the SliceNet Plug & Play control is to offer vertical-tailored services and enable a high degree of slice customization, allowing verticals to plug their own control logics on top of provisioned slices and customize their services.

The Plug & Play has been presented in its high level approach and functional decomposition components in deliverable D2.3, where it is defined as an isolated control environment, specific per slice instance that can be activated on-demand upon provisioning of end-to-end slices. In practice, each Plug & Play control instance can provide verticals a mediated (and abstracted) access to a limited set of SliceNet platform control and management primitives, according to the specific the Plug & Play requirements specified by the vertical when customizing its Service Template and then reflected as specific vertical-tailored level of slice control exposure in the Service Descriptor and the Network Slice Template.

The Plug & Play Manager is the lifecycle manager of the whole set of Plug & Play control instances under the ownership of the SliceNet platform. It basically takes care to activate new Plug & Play control environments for each new slice instance, either they are offered to a vertical or to a peering service provider, and to specialize them with a customized slice view and control exposure. Of course, it is also responsible for keeping the Plug & Play control instance aligned and synchronized with the actual status of the related slice instance, in terms of constituent network functions and other generic attributes (e.g. related to QoS) with the aim of offering to the vertical (or slice consumer) and up-to-date view of its slice.

As described in D2.3, each Plug & Play control instance is built around three main layers leveraging on a generic, common and technology agnostic vertical slice view information model: i) pluggable plugins and drivers, to provide the required adaptation between the Plug & Play generic slice model

and the SliceNet monitoring, control plane and orchestration platform primitives, ii) abstraction and slice-specific model, to specialize of the generic slice information model into the customized vertical (or slice consumer) view of a given slice instance, iii) vertical oriented APIs, offering a set of APIs for tailored control operations over the slice-specific model and view, following the slice control exposure set in the Service Descriptor and Network Slice Template.

At slice provisioning and instantiation time, the Plug & Play Manager is invoked by the SS-O to trigger the activation of a new dedicated Plug & Play control instance, and it takes care to apply a customized configuration of above three layers according to control exposure information specified in the Service Descriptor and the Network Slice Template. In particular, the Plug & Play Manager is responsible to:

- activate the proper set of plugins and drivers towards specific SliceNet platform control and management components, according to the control logics to be exposed to the slice consumer for the given slice instance
- customize the generic slice model into the specialized vertical view of the slice, according to the level of control exposure information set into the Network Slice Template
- customize the vertical oriented APIs to limit the exposed control operations on top the customized slice model, again according to the level of control exposure described in the Network Slice Template

Moreover, at runtime, i.e. during the lifecycle of each given slice instance, the Plug & Play Manager is responsible for maintaining the slice view offered as synchronized and coherent with the slice status recorded in the service and slice inventories (maintained by the SS-O) as well as in the NFV NS inventories (maintained by the NMR-O).

Figure 37 shows an insight of the Plug & Play Manager high level functional split. The main entry point is the **P&P Coordinator,** which basically offers to the SS-O a set of lifecycle management primitives to activate new dedicated and isolated Plug & Play control environment when a new slice has been provisioned, and to deactivate it as soon as the related slice instance is decommissioned. If applicable, the P&P Coordinator is also responsible to coordinate dynamic adaptations of Plug & Play instances at runtime, e.g. by enforcing the plugging of new plugins and drivers in support of slice instance upgrades in terms of level of control exposure (validated and accepted by the slice provider) from the vertical.

The **P&P Lifecycle Manager (P&P LCM)** is responsible to coordinate the individual Plug & Play lifecycle managers to be dynamically created to manage each Plug & Play control environment. It is triggered by the P&P Coordinator which is in charge to allocate a dedicated new lifecycle manager for each new slice instance. Indeed, it is the **P&P Instance Manager (P&P IM)** that provides the actual logic to manage the lifecycle of each Plug & Play control instance, thus coordinating all the actions to be performed for their creation, configuration and deletion. For each slice-dedicated Plug & Play control environment, it can be therefore considered as the core engine of the Plug & Play Manager for the related lifecycle management operations. The P&P LCM takes care to create a new P&P IM for each Plug & Play control instance. In particular, the P&P LCM provides access to service, slice and NFV-NS catalogues and inventories owned by the SS-O and the NMR-Os to allow each P&P IM to customize the Plug & Play control instance under its ownership according to levels of control exposure expressed in Network Slice Template, as well as to the actual NFV, MEC and RAN resources allocated to given slice instance.

The **P&P configuration driver** offers to each P&P IM a common interface to create and configure new Plug & Play control instances in their deployment environment. The approach envisaged, as currently under definition in WP4, is to implement the Plug & Play control instances following a micro-services approach based on loosely coupled Docker containers managed by open source orchestration tools like Kubernetes [36]. This allow to have for each Plug & Play control an isolated

and controlled environment, that if required can be fully offered to the vertical or the slice consumer. Therefore, in this context, the P&P configuration driver provides a kind of wrapper to the APIs offered by Kubernetes for managing containerized applications.

In support of this micro-services and containerized applications approach, the Plug & Play Manager owns a **P&P Drivers Catalogue**, where the diverse Plug & Play southbound plugins and drivers as defined in D2.3 are stored and accessible to the P&P IMs for being integrated and configured in the Plug & Play control instances as part of the plugin activation function described above.

Moreover, to keep track of the diverse Plug & Play control instances deployed and available, a **P&P Inventory** is also owned and maintained by the Plug & Play Manager and accessed by the P&P IMs to retrieve any required information about running instances.

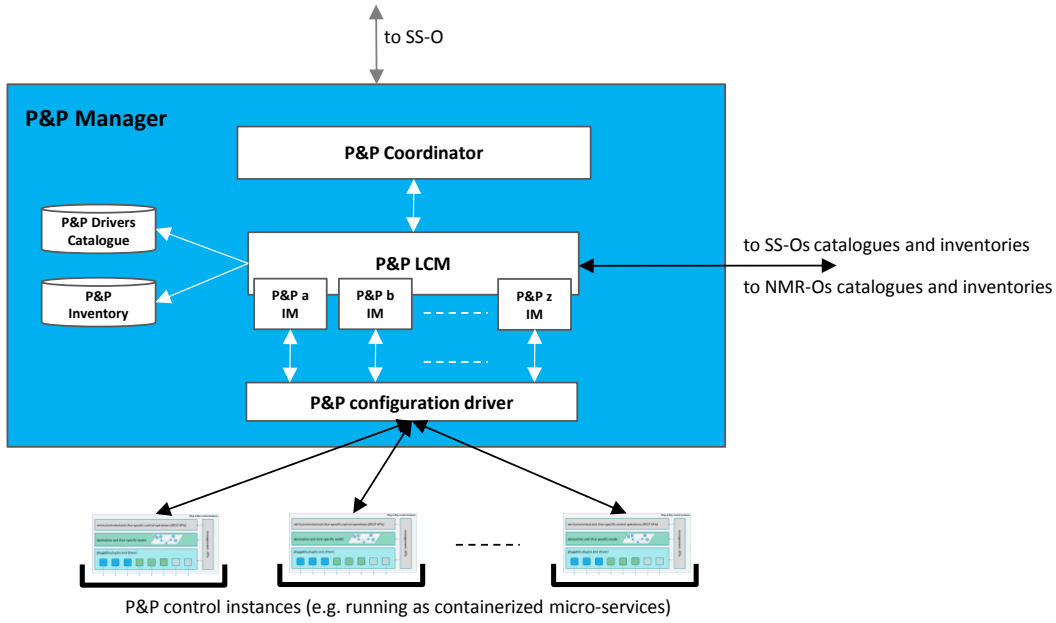


Figure 37 P&P Manager high level functional split

It is relevant to highlight that the SliceNet Plug & Play has to be considered agnostic of the specific provider-to-consumer interaction. This way it can be applied to any service provider to vertical or service provider to service provider case in support of either single-domain or multi-domain end-to-end slices. This way, Plug & Play control functions can be exposed to verticals for their customized slices operation, and to other customers in general (like other service providers) in the context of end-to-end slices spanning across multiple administrative domains. In other words, for what concern the Plug & Play Manager component described in this section, different deployment options are envisaged depending on the SliceNet business roles: i) single Plug & Play Manager in the case of combined DSP and NSP with full access to catalogues and inventories of both SS-O (slice/service level) and NMR-O (NFV-NS level), ii) dedicated DSP Plug & Play Manager having access to only service/slice level SS-O catalogues and inventories, and dedicated NSP Plug & Play Manager with access to catalogues and inventories of NMR-O (NFV NS level).

5.2 Monitoring components

The main goal of the monitoring sub-plane and components of the SliceNet architecture is the collection of both structured and unstructured data from various sources and at multiple layers in a flexible way, either to support current management requirements or to expose desired KPIs towards vertical customers. This is achieved thanks to monitoring capabilities exposure at lower infrastructure levels and pluggable software sensors at higher levels to filter and aggregate the information so it can be consumed by other management functions (e.g. cognition sub-plane) or

vertical users. Given this, the monitoring components can mainly be divided onto resource, topology, traffic, slice and service monitoring, as depicted in Figure 38, where the main functionalities and scope of each monitoring layer are also summarized.

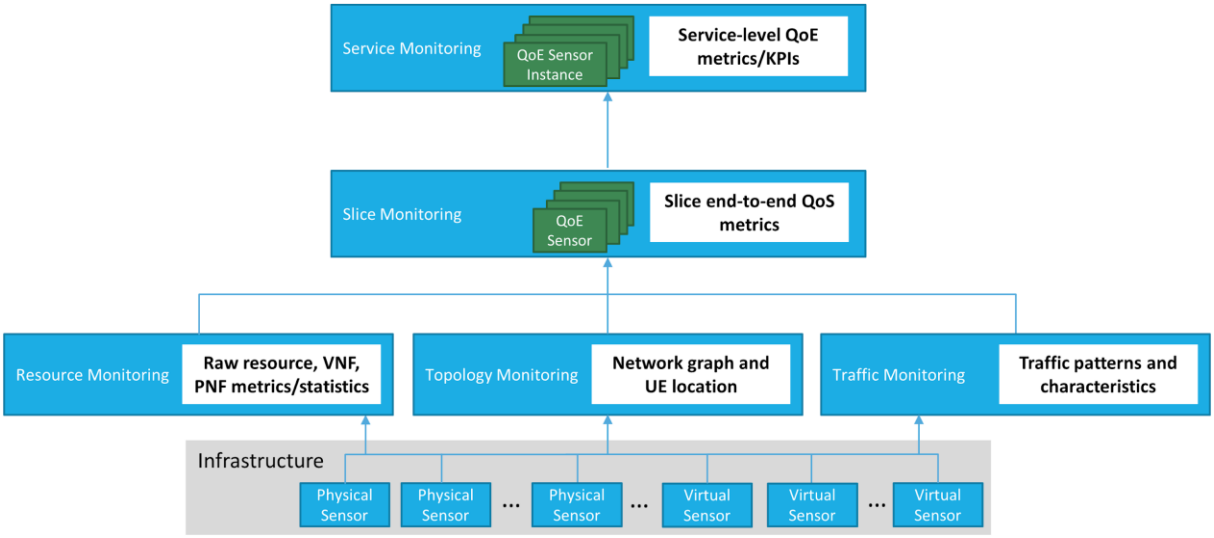


Figure 38 Summary of monitoring sub-plane components

The **Resource Monitoring** is based on an extendable set of probes supporting monitoring of entities belonging to various technologies, which constitute the data plane (either physical or virtual). The component implements interfaces used by technology agnostic cognitive management layer to collect infrastructure performance metrics. Examples of the monitored resources are VNFs, SDN-based elements or PNFs. VNF states detected using such techniques as pinging via management IP, CPU utilization, failure events, timers, other performance KPIs can be collected on-demand through resource monitoring probes and saved into a Data Storage. The data collected, along with topological and aggregated traffic information, serves as foundation for higher level monitoring capabilities (slice and service) as well as main input for the cognitive/machine learning loops found at the cognition sub-plane.

The **Topology Monitoring** enables the collection in a close to real-time manner the current topology of the layered (physical and virtual) network as well as to to track UE mobility. This data will enable more efficient preparation to such states as handover and assist in place-based allocation of resources to minimize traffic latencies and delays. It is also important to emphasize that one of the roles of the component will be enriching the layered topology presentation with links correlating entities from virtual and physical layers. The links will help with allocation/decomposition of different higher level elements and further resource utilization.

The **Traffic Monitoring** is aimed at tracking, aggregating and extracting metrics of traffic flows currently instantiated at the infrastructure level racking flows with appropriate level of anonymity will help the cognitive QoE loops to detect slice states, current traffic bottlenecks and failing entities, find traffic patterns and via machine learning techniques define prediction modules and thresholds, and finally generate new policies or update existing ones to be used by the Control Plane actuators. Two kinds of Traffic Monitors will be required: Infrastructure Provider's Traffic Monitor, and Network Operator's Traffic Monitor. An Infrastructure Provider's Traffic Monitor should be able to detect and differentiate traffic flows belonging to multiple tenants (i.e., Network Operators) and thus multi-tenancy awareness is required. Meanwhile, a Network Operator's Traffic Monitor should be tailored to support the traffic monitoring in a particular type of network.

The **Slice Monitoring** is the responsible to collect and generate the data related to slice level performance indicators, for instance, end-to-end bandwidth and latency between deployed VNFs instances among other metrics. To do so, it leverages on the information provided by the lower level

monitoring entities, that is, Resource, Topology and Traffic Monitoring. With such information, it composes the different QoS metrics coming from the different NSSIs to provide the globals QoS metrics of the slice. These performance indicators will then feed both the cognition sub-plane to further derive new policies and QoE models as well as the QoE Optimizer module at the Control Plane to trigger slice actuations to maintain desired QoS/QoE levels (if needed). In this regard, the concept of QoE sensor is introduced. A QoE sensor is a software sensor that its aim is to define and filter the most relevant QoS metrics that impact on the QoE levels of the services supported over the slice. In this way, the information exchange is limited to only the crucial data for proper QoE evaluation. The definition and instantiation of such sensors is performed during the provisioning phase of the slice, while the filtered data by them is employed at runtime by the QoE optimizer, cognition loops and service monitoring capabilities. Additionally, as a result of machine learning, modifications on the information to be filtered or new types of sensors may be derived to keep the QoE evaluation at the most optimal levels. Moreover, thanks to the capabilities exposed through the P&P, new sensors may be defined and instantiated at request from the vertical as a way to customize the exposure of QoE information towards them. (QoS levels that require reaction will be subject to intra-domain or inter-domain resolution and the events will be forwarded to the appropriate intra or inter domain management modules to ensure end-to-end slice QoE/SLA. On the other hand receiving external info will be hold by the Monitor component)

The **Service Monitoring** adds high-level information regarding specific service instance performance/failures/QoE to the already collected slice level and resource level information and exposes it towards cognition loops or vertical users for KPI reporting. This information will assist to correlate QoE markers with the lower layer slice configuration. It will be also valuable for the cases of cross-domain services, where achieving QoE/SLA is even a more challenging task. In this level, the QoE sensor concrete instances materialize, which are parameterized for the specific service instance running at that moment in the slice (e.g. the video session for the eHealth use case). Such QoE sensor instances may be programmable by the vertical through the P&P to customize the QoE information exposure or the way in which QoE information should be aggregated for the service instance at hand.

In addition to the domain specific information, the module is used to receive information in the process of cognition inter-loop data exchange. The exchanged data is sanitized, filtered and transcoded in an appropriate format before being fed to the Monitoring module. The information to be exchanged includes for example cell BW, user link quality, current throughput, and metrics regarding flows such as uplink/downlink usage. This information is especially valuable in the use case of eHealth ambulatory, where the user is mobile and the historical data can be used to build ML models and knowledge base in the receiving cell/domain after handover in a fast and efficient manner using historical records regarding the user in the new administrative domain.

5.3 Cognitive management components

The cognitive management components aim to ensure smart management operations such as fault, performance and security management and go beyond the classical FCAPS (Fault, Configuration, Accounting, Performance and Security) management tools. It encompasses the machine learning operations (prediction, classification, clustering, etc.) to identify faulty network slice components, detect anomalies such network cyber-attack and malwares, predict SLA/SLO violations, etc.

Hence the cognitive management components will ensure smart FCAPS through the use of a variety of algorithms such as

- FFNN (Feed Forward Neural Network) to predict network metrics per slice evolution and identify through decision tree if a violation of network behavior will occur.
- LSTM (long Short Term Memory) to classify network data per slice and point the anomalies within the slice activated sessions

- CNN (Convolutional Neural Network) as a recommended algorithm for data fusion to combine different data sources expected with the cognitive analytics applied by multiple owners and multiple roles.

Besides leveraging the classical FCAPS, the cognitive management component fed the Orchestrator plane with the prediction of the slice PDU sessions status, for example, and in its turn the orchestrator will compute/calculate the needed the resource to be allocated and ensure smart placement of those resources.

In this section we zoom on the main component defined in D2of the cognitive plane

- Aggregation,
- Analytics with two sub-modules (Model Selection and Analytics Engine)
- Policy Framework.

We capitalize on the advanced architecture proposed on the CogNet project [38][39]. In addition, cognitive management will rely fundamentally on the MAPE loop. Its main focus will be in providing management for multiple slices within the same framework (including taking care of sharing resources) and composition of subnet slices to provide optimized end-to-end slices.

In the following sub sections we will details the different modules of those components displayed in the Figure 39:

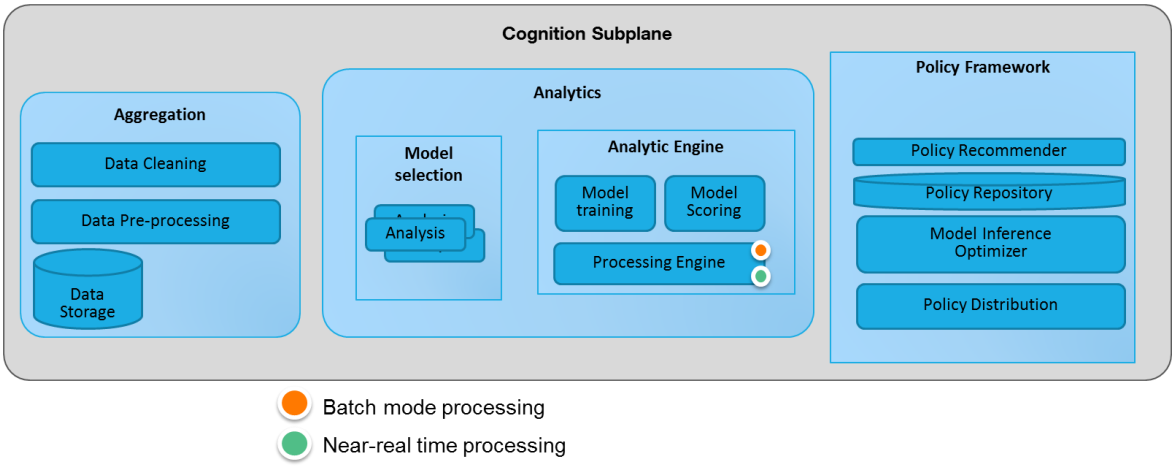


Figure 39 Zoom on the cognitive Subplane

5.3.1 Aggregation modules

The aggregation module, Figure 40, collects data from multiple levels as indicated in the monitoring tool. It encompasses the following services:

Data Cleaning & Filtering: it cleans and refines received data, tags the information with relevant slice identifiers, and then stores it into the local Data Storage.

Data Storage: it stores historical data, and makes them available for multiple components constituting the cognitive framework. In addition, the One-Stop-API should allow the slice user to access exposable per-slice aggregate information. Finally, stored data may include analysis results (from simple aggregates to predictive time series “sensors”) to allow easy consumption by Control Plane, in particular, the QoE Optimizer.

Data Pre-processing: pre-processes collected data stored in the Data Storage of NSP and makes it ready to export only filtered and tagged information to the Cognitive Management loop, where filtered per-slice information will be stored and used by the cognition and analytics module. Such functionality is essential to support the overall flexibility of the architecture and to keep it adjustable to constantly changing environment. It controls the noise and reduces the processing time of analytic works in the big data context.

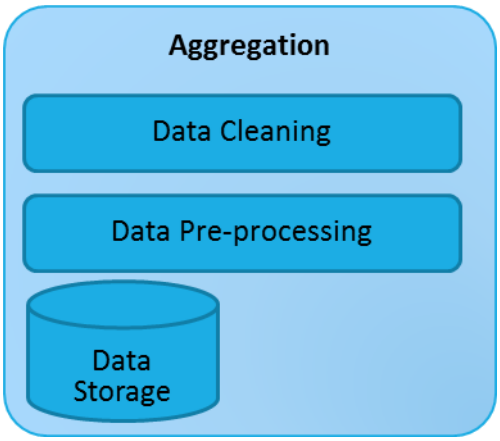


Figure 40 Zoom on the aggregation module

The collected raw data from multiple sources are cleaned by some light-weight approaches that aim to reduce the size of data for storage. The feature extraction could be done based on the domain expertise or with the use of machine learning techniques to identify the main features to use. It could be performed directly on the raw data or on the cleaned data based on the request from the Data Pre-processing if the data is forwarded back from the Analytics module. Afterwards, processed data are stored in the local Data storage or consumed directly by the analytics module and then the policy framework before feeding the QoE optimizer.

The Data Pre-processing will further process the stored data by normalisation and extraction. The former operation refers to adjust values measured on different scales to a notionally common scale, which is essential for certain machine learning algorithms, such as classifiers that calculate the distance between two points by the Euclidean, and can potentially facilitate convergence of given machine learning approaches, such as gradient descent. The latter one covers methods that transform raw data into informative features for machine learning algorithms.

5.3.2 Analytics modules

Model Selection

The model selection module is responsible for applying the desired analytics to the various multi-level data sources. Its objective is to analyze the data type for example and to select the right machine learning method.

This selection is based on *policy*, as prescribed per slice and per customer requirements; *data-set characteristics*, including availability, granularity, and stability; cognition compute *resource availability* and priority; and *strength* of the model. All these selection criteria may be provided as policy, analyzed as a preprocessing, and/or learned by previous cognitive analysis. The same data source may be analyzed by several models to allow finding the best model and to support new models.

Analytics Engine

The Analytics engine, Figure 41, applies the selected models and ML methods to analyze the cleaned data. It runs both model training and model inference tasks. It retrieves data from the data aggregation module and applies these data to train a model. The trained models are fed into the policy framework to be applied in real-time by control-plane components, such as the QoE Optimizer.

The models are also applied in the cognition plane for non-time-critical analysis, such as forecasting and policy refinement. The Analytics Engine continuously scores the models by evaluating changes in data characteristics and by assessing the effectiveness of the models. These scores are fed back to

the model selection module. The main outcome of the analytics processes are slice configuration parameters, which are applied through the policy framework.

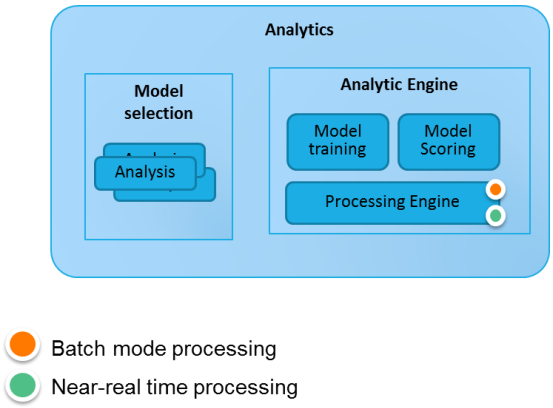


Figure 41 Zoom on Analytics

The objective of the Analytics Engine is to support the various Machine Learning modules that in turn contribute to the delivery of slices with their expected services while ensuring the QoS and QoE expectations.

The Analytics Engine will then provide cognitive functions such as forecasting and prediction services, anomalies and fault recognition and slice configuration recommendation to feed and trigger the policy framework which in its turn will compute the necessary polices to pass to the Control Plane modules.

The Analytics Engine relies on the **Processing Engine.** The Processing Engine retrieves consumption and state data from the Data Storage, and applies these data to train a model or generate scores. The processing engine has two modes of operations the batch mode and the near-real tile mode.

- In the batch mode, the Processing Engine will evaluate the distortion of the actual model. If the model becomes inapplicable, it will compute a new model from scratch and make this model available for execution for the Near Real-time Processing mode.
- In the near-real time mode, the Processing Engine consumes the data from the aggregation module directly, and issues scores within a short period of time. This can be done while applying the models computed in the batch mode, or by using light-weight on-line learning approaches directly, such as some on-line clustering algorithms. In this mode, the Processing Engine computes scores either in real-time if it is implemented and deployed in a distributed real-time computation system, such as Apache Storm, or near real-time if it is powered by a mini-batch system, such as Spark Streaming

Note that the scoring in both modes is not to only apply one machine learning model but may involve a sequence of models associated with post-processing. For example, to detect network anomaly, we may need to score a number of records and then make a conclusion based on a linear combination of generated scores.

5.3.3 Policy Framework Modules

The policy framework, Figure 42, is generic and technology agnostic framework used by Analytics modules and the Orchestration modules.

Its main role is to ensure the interpretation of the scoring generated by the Analytics module in order to feed the modules of the Control Plane or the Orchestration and management modules on how to scale the slice resources, or to enforce an imminent network function migration, to recommend new network and slice configuration (including the recommendation of QoE and SLO metrics), to generate slice template and ensure dynamic mapping with the network service descriptor, etc. One the

policies are generated/computed, optimized and recommended, the policy framework ensures also their distributions thanks to the different points of executions (PDP, PEP, etc), Figure42.

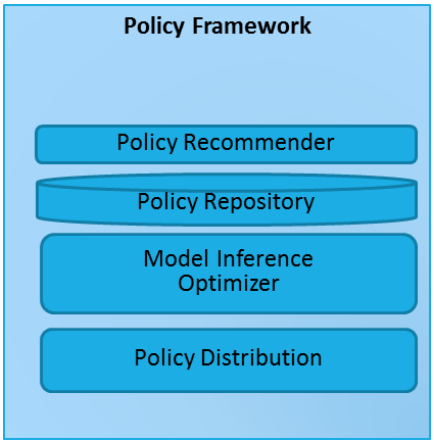


Figure 42 Policy Framework Modules

Policy Recommender

The Policy Recommender is a decision point that combines the scoring computed by the machine learning algorithms with the various information (such as the state of the slice resources, the business objectives, the expected QoE and the business objectives) and then suggests the overall resource management required for network services and the associated slices.

In addition to the above, optionally the recommender can feed the repository with adapted/new policies. The Recommender can be extended to adapt/recommend new policies based on the experience gathered from applying previously existing policies as for example recommending which QoE to associate to a given Service Request from the vertical. This is done through the analysis of historical events and actions and generally by using interactive learning.

Policy Repository

It stores policies related to all network resources. The policy format is the ECA, Event Condition Action.

Optimizer

The Optimizer consumes what is predefined or generated within the repository. It deals with parameters tuning for example how to much the service requests, the slice type, the current resource status. The Policy Optimizer receives policy decision from the Policy Recommender, and then transforms the abstract actions specified in selected polices into concrete ones based on the state and configuration information from the orchestration subplane. This information can be static, such as source or destination addresses or dynamic such as current available network resources.

Importantly the Optimize manages the conflicts between policy actions and priorities before passing them to the policy distribution.

Policy Distribution

The Policy Distribution invokes APIs offered by the components that are hosted in the orchestrators subplane, Control plane, etc. It recommends actions according to the decision of Policy Recommender and current network conditions.

Before diving into the Policy Framework internal modules, a high-level overview of the SliceNet Policy Architecture is described herein. SliceNet will implement a solution in which policies are coherently distributed across several policy subsystems of the overall architecture, guaranteeing the appropriate functioning of the subsystem independently of each other. The following policy-based optimization subsystems are defined within SliceNet:

- Cloud Optimization Subsystem: encompasses the VIM-related policy-based optimization procedures;
- 4G/5G Network Optimization Subsystem: includes the Network-related policy-based optimization procedures; it can include PCC-related networking policies and/or NFVO-related policies;
- Slice Optimization Subsystem: deals with slice-level policy-based optimization procedures;
- Service Optimization Subsystem: responsible for service-level policy-based optimization procedures.

Through this approach the architecture is more flexible and fast to react since each subsystem is able to perform its own activities (e.g. closed loops) independently of the other subsystems. Although subsystems operate independently, they must be coordinated to avoid overlapping decisions. The overall governance and coordination of the policies distributed and applied at each subsystem is made by the Policy Administration Point (PAP) - illustrated in Figure 43.

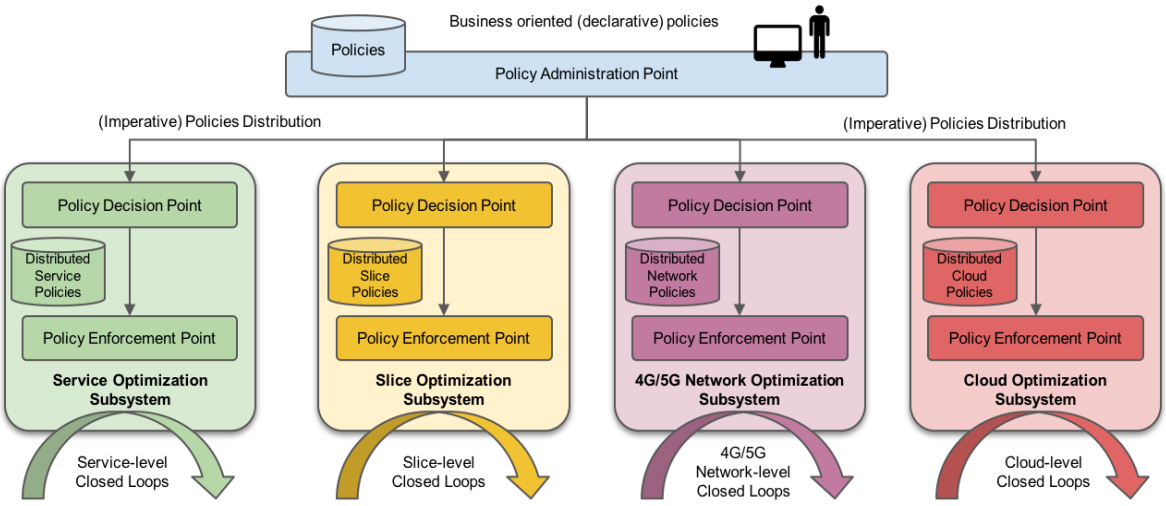


Figure 43 SliceNet Policy Architecture Entities

The PAP is the entry point of policies in the system. Business-oriented policies are designed by a human and onboarded to the SliceNet system through the PAP. At this stage, business policies are designed using a declarative approach, instead of an imperative one. This will enable the user of the system to design and onboard business policies without having to know the technical details of the system.

The PAP is responsible for (i) translating the declarative policy into an imperative policy or policies and (ii) coherently distributes these to the appropriate subsystem or subsystems. Each subsystem will store the distributed imperative policies and decide, at each moment and depending on the situational context, which policy should be enforced. Therefore, at each subsystem, there is a Policy Decision Point (PDP), which decides which policy to use, and a Policy Enforcement Point (PEP), which enforces the selected policy in the subsystem. Figure 43 illustrates the SliceNet policy-based optimization subsystems, which reflect the several closed-loops of the architecture.

Figure 43 illustrates the SliceNet policy architecture entities (PAP, PDP and PEP) mapped to the SliceNet system architecture illustrated in section 5. The Policy Framework component is the “heart” of the policy architecture since it is responsible for the administration, governance and distribution of the architecture policies through the other architecture elements - **Policy Administration Point (PAP).** It contains the business-oriented (declarative) policies provided by the “human”, translates these to imperative policies and coordinates its distribution to the several SliceNet optimization subsystems, which will independently decide (Policy Decision Points) when to apply them (Policy Enforcement Points). Additionally, it also plays the role of a **decision (PDP)** and **enforcement point**

(PEP) for service-level closed loops. As depicted in Figure 43, the following PDPs and/or PEPs are identified in the architecture:

6 Preliminary management view for SliceNet use cases

SliceNet has defined three representative vertical use cases [1]. In this section we will describe how those use case will instantiate the management moduleswhile considering the multi-domain aspects, the SliceNet roles and the SliceNet Information model. In this section we present a preliminary management view for the use cases with the goal to prepare the coming working in the WP4, WP5 and WP6.

6.1 Multi-domain considerations applied to SliceNet use cases

In Table 4 we start by listing a subset of technical requirements that are closely related to the multi-domain scenario consideration in the use cases. Based on these considerations and requirements from the use cases, Table 5 identifies the multi-domain categories for each of the use cases, following the classification approaches from NGMN, as described in the previous subsection.

Table 4 Multi-domain requirements from SliceNet use cases

	Smart Grid	eHealth	Smart City
Alignment to 3GPP UCs	URLLC (Ultra-Reliable and Low Latency Communications)	eMBB (enhanced Mobile Broadband)	mMTC (massive Machine Type Communications)
QoS/performance requirements	High reliability; low delay	High bandwidth; high mobility; low delay	High density
Multi-domain	Yes (static)	Yes (mobile)	No
UE mobility/handover control	No	Yes (ambulance)	No
MEC (Mobile Edge Computing)	No (or partially for low delay or push Core to edge)	Yes	No (but can be extended to leverage MEC)

Table 5 Mapping of NGMN multi-domain categories to SliceNet use cases

	Smart Grid	eHealth	Smart City
Roaming scenario	No	Yes	No
Business vertical scenario	Yes	Yes	No
Inter-domain configuration	Yes	Yes	No
Multi-domain configuration	Yes	Yes	No

6.2 Smart City

6.2.1 Use case description

The services of a Smart City consist in general in the following:

- Metering solution (gas, energy, water, etc.),
- Remote monitoring of city infrastructure (pollution, temperature, humidity, noise),
- Real-time traffic information and control,
- City or building lights management
- Public safety alerts for improved emergency response times,

SmaLi-5G use case is considered in the scope of the 5G Massive machine-type communication slice category where the challenge is to accommodate the massive number of connected lighting sensors/controllers without impacting the service QoS and QoE. The SmaLi-5G use case may be extended to assure ultra-high network reliability and availability, while low-power, context awareness and location awareness requirements for managing the connected actuators/controllers over the access and transport layers can further improve the solution cost efficiency. The smart city use case defines several KPI's requirements as cites in the tables 6 and 7:

Table 6 General Smart City UCs KPIs

Smart city	Experienced user throughouput Traffic volume density	300 Mbis DL; 60 MbPS UL 700 Gbps/km2
	Connection density Latency	200k users/Km2 Seconds to hours
	Mobility	low

Table 7 Smart City KPIs

SliceNet Key Requirements	Smart City
Alignament to 3GPP Ucs	mMTC(mIOT)
QoS/performance requirements	High device density
Multi-domain	No
Mobility/handover Control	No
MEC	No
Enterprise	Yes(extended)
Scalable Slice(resource control/management)	Yes(horizontal/vertical)
Communication pattern/service	unicast/anycast
FCAPS requirements	Yes
Cognition requirements	Yes
Sensors, Actuators, Network functions, Apps	Flow;Resources;Topology;Security
P&P	Yes
Multi-tenancy	Yes

6.2.2 Management modules overview

The use case requires the deployment of physical infrastructure that is enabled to support virtualized network functions as well as physical network functions. It includes Radio access Network (4G/5GNR-New Radio), Core (vEPC-Evolved Packet Core and NGCN-Next Generation Core Networks) as well as the Enterprise that includes IoT platform and Smart Lighting Apps for service controlling. In addition to 5G network segments and technologies, the use case includes also the lighting system information with respect to the applications like the Lighting apps; Dashboard (information related to number of lighting poles, statistics, traffic, service health, presented to the customer and Ticketing).

In the following table 8, we will describe the management operations while referencing the management modules used for the use case:

Table 8 Mapping the management modules and the operations realized for the use case

Management module	Operation instantiated for the use case
One stop API	The order is received for smart city services with a set of parameters. : Number of IoT devices, to be connected, service KPIs(jitter, delay, availability, packet loss), devices location, traffic information(bandwidth).
Orchestrator/SS-O SD/translator	The service template is translated
Orchestrator ND-O	descriptors deployment, resource verification; resource reservation; resource allocation resource configuration (OS and NE deployments) • RAN; vEPC; Enterprise • service chaining
Orchestrator/SS-O/Slice Orchestrator	slice activation (common slice)
Monitoring modules/ Slice, Service and resources levels.	service monitoring and service supervision triggered action: • sensors/actuators QoS and QoE service based • resource based (CPU; RAM; HDD) • network traffic metrics
	• Resource monitoring, physical and virtual (VNFs/PNFs), traffic monitoring (pattern characteristic), topology monitoring (specific use case network graph). • Slice monitoring (QoS metrics) (data related level indicator) performance indicator • Service monitoring (QoE metric) per specific service instance, based on the deployment of QoE sensors and QoE instances. • Based on the system monitoring , the system will be triggered for scaling
Resource catalogue for vertical	Network segments • vEPC: vMME;vS/P-GW;vHSS a. network segments OS b. repository • RAN

	a. RAN Type(4G;LTE-M;Nb-IoT;NR) • Enterprise a. enterprise segments OS b. repository • network segments chain Network Resources • VMs for a(i): CPU; RAM; Storage; Network Interfaces • VMs for a(iii): CPU; RAM; Storage; Network Interface • RAN
Service template	Service template catalogue for vertical • KPIs related information a. jitter [ranges: 100ms] b. delay [ranges: 300-500ms] c. packet loss 0.001] • QoS, SLA, availability • service components, related to end-to-end lighting apps a. IoT platform; Dashboard; Monitoring; Ticketing • service chaining
Slice template	• virtualized resource, independent block, isolated a. vEPC Apps: vMME;vS/P-GW;vHSS b. RAN: Radio c. Enterprise : IoT Apps; Dashboard(sets of VMs with specific functionalities) • slice virtual function chaining • application domain: single domain a. common slice parameters
Monitored metrics	• **Metrics** overview VNF`s vCPU/RAM/disk consumption rate, end to end packet loss, reachability state of the end-devices., Jitter, Latency, etc.
Cognitive modules	Aggregation of metrics to fault management and performance management

6.2.3 Use case considered SliceNet Roles

In the Figure 44, below we present the three main network components identified: (1) RAN; (2) Core; (3) Enterprise. The use case is established by Orange that is combining the NSP and DSP roles.

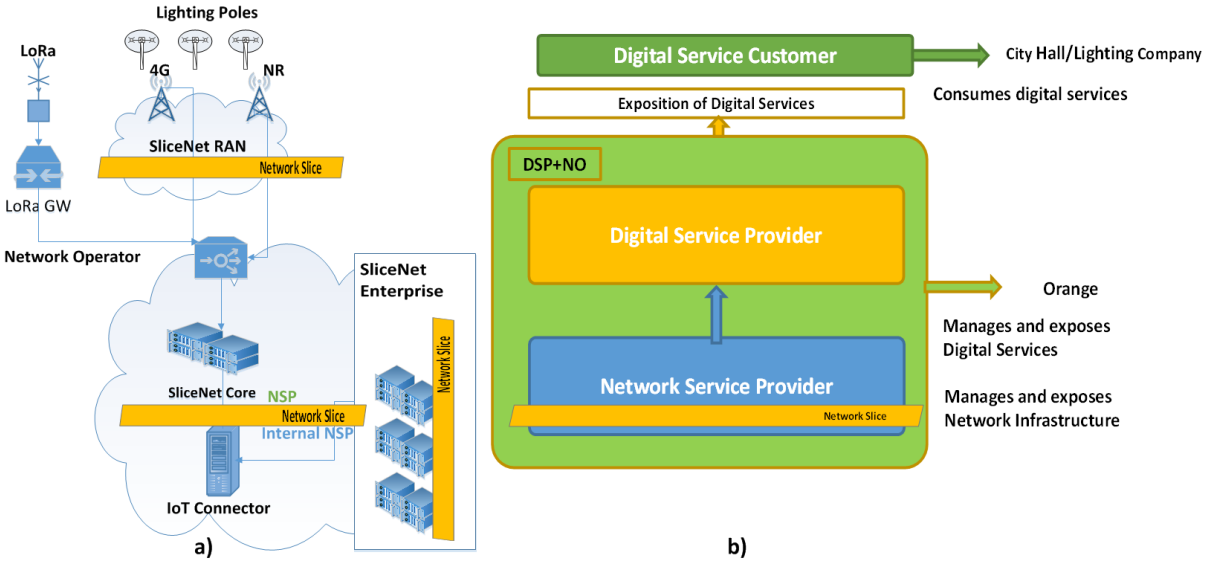


Figure 44 a) high level architecture; b) Roles considered by the Smart City use case

In this use case the Digital Service Customer consumes digital services and provides the city hall with lights hence acting as Lighting Company. The **Digital Service Provider** manages and exposes digital services, composed by the specific communication service for lighting (massive Machine Type Communications) offered to the vertical and lighting applications (enabling visualization, lighting control, statistics). The **Network Service Provider** manages and exposes the communication network infrastructure and performs interoperability with 5G connected virtualized infrastructures that in this scenario is owned by the NSP and deployed as extension of the network, managed by the provider also.

Based on those roles the consumer is the City Hall, that receives from the DSP the service (contract based). The DSP has the capabilities for: Service Offering, Design, Provision, Configure, Supervision, Monitoring, Scaling, within single domain that includes the (RAN, EPC, Enterprise Apps & Infrastructure). The telco Operator, Orange as depicted in the Figure 44, Figure 45, is playing the role of: DSP and NSP (including infrastructure and resources).

The slice is the "virtualized network", established on demand (creation, deletion, configuration, etc), capable of "scaling" of resources, within mIoT KPIs.

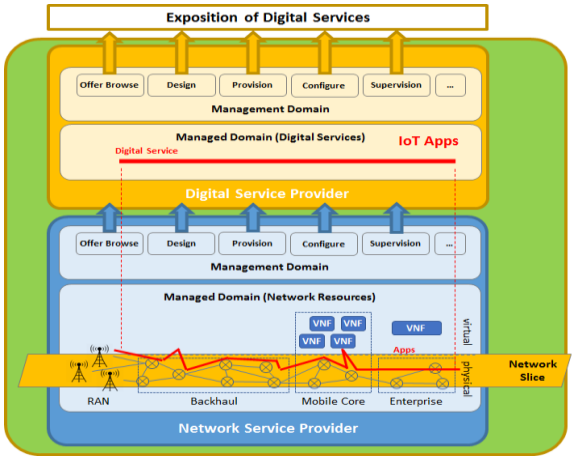


Figure 45 Smart City view

6.3 Smart Grid

6.3.1 Use case description

The increasing demand for power supply Quality of Service (QoS) has motivated utilities to spread out beyond the substation environment, to increase the number of monitoring and protection-capable devices deployed along the energy distribution networks and to use these devices to implement self-healing schemes. The lack of a high-performance, reliable, and cost-effective wireless network with the required geographical coverage has been one of the major drawbacks for high-speed protection and automation schemes implemented outside contained substation environments. Although the latest advances in mobile communications have propelled the implementation of communication-based self-healing schemes, fourth generation technologies are still unable to fully comply with the demanding peer-to-peer communication needs, especially in geographical areas where signal strength and/or quality is not optimal. The need for an ultra-reliable, fault-tolerant, cyber-secure communication infrastructure gains relevance for communication-based fully decentralized self-healing schemes, where a single point failure jeopardizes the entire system.

The Smart Grid self-healing use case presented in the SliceNet project focuses on an IEC 61850-compliant communication-based decentralized solution, in which power system Intelligent Electronic Device (IED) coordination is ensured by machine-to-machine communications over a 5G mobile network. The IEDs that integrate and implement these self-healing schemes are typically sparsely spread out over relatively wide areas. The decentralized solutions approached by the use case require the continuous exchange of time-critical messages between the remotely located IEDs. Figure 46 illustrates the smart-grid self-healing use-case scenario.

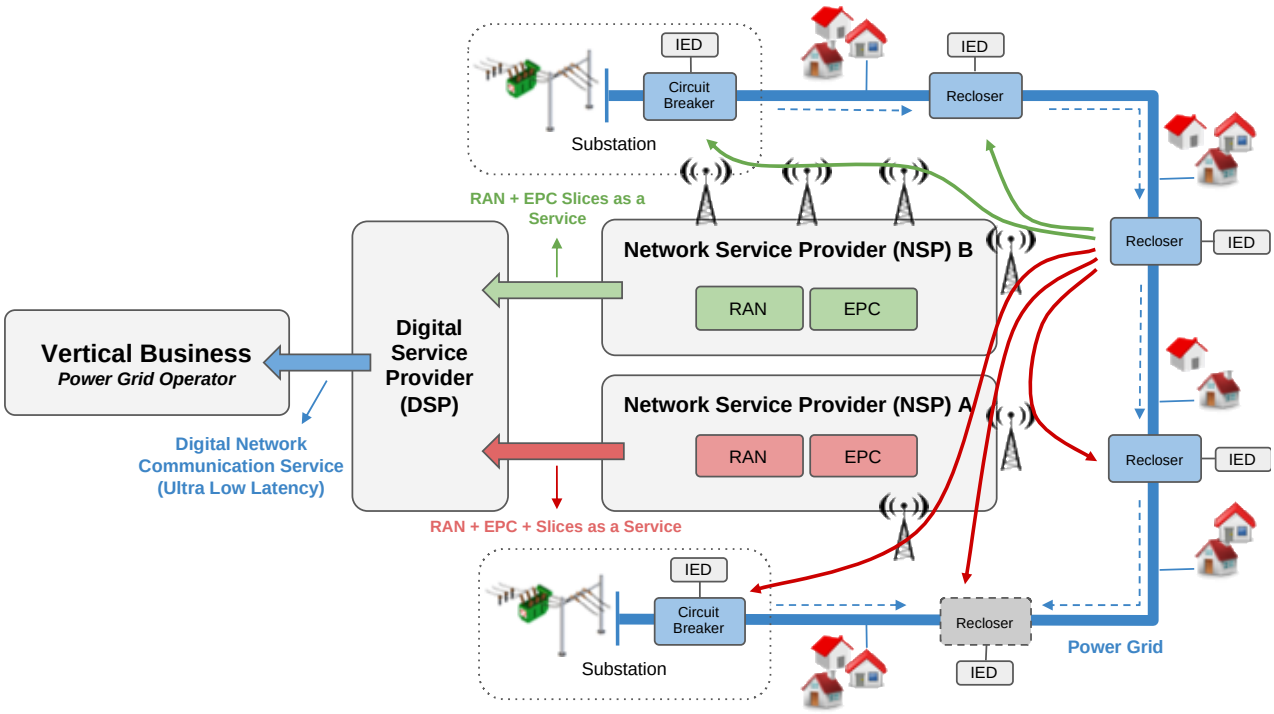


Figure 46 Smart-grid self-healing UC Overview

The applications covered by the use case rely on ultra-reliable low latency communication between power grid sensors and actuators (i.e., protection, automation, and control IEDs), requiring a high density of network communications coverage with a very high quality. Based on these requirements, the most critical aspect of the UC is the RAN coverage. Since it is very difficult for a single Network Service Provider (NSP A) to be able to cover the whole power grid geographies with the desired SLA, a second NSP (B) is involved to provide complimentary RAN connectivity.

In terms of performance requirements, the following are comprised within this scenario (Table9).

Table 9 Use-case performance requirements

Requirements	Minimum	Optimal
Protection Coordination Scenario (further details in D2.1)		
E2E Latency	<10ms	<5ms
BER	<10e-4	<10e-6
Bandwidth (down/up)	10/1 Mbps	20/2 Mbps
Automatic Reconfiguration Scenario (further details in D2.1)		
E2E Latency	<30ms	<10ms
BER	<10e-4	<10e-6
Bandwidth (down/up)	5.9M/600k Mbps	17/1.7 Mbps
Differential Protection Scenario – IEC 61850 SV Communications (further details in D2.1)		
E2E Latency	<5ms	<3ms
BER	<10e-6	<10e-8
Bandwidth (down/up)	1.6M/512k bps	3.2/1 Mbps
Differential Protection Scenario – GOOSE P2P Communications (further details in D2.1)		
E2E Latency	<10ms	<5ms
BER	<10e-4	<10e-6
Bandwidth (down/up)	17/1.7 Mbps	30/3 Mbps

6.3.2 Management modules overview

From the network operator side perspective, the Smart-Grid Self-Healing UC requires RAN access (4G/5G), mobile core (EPC/NC) and an IP/MPLS network. Additionally, it also requires the delivery of these functionalities in more than one administrative domain (to enable the full coverage of the power grid devices in wide geographies). From the vertical (power grid operator) side, it requires the power grid sensors/actuators devices that are interconnected (through a 4G/5G modem) to the network operator RAN, enabling their communication on a peer-to-peer mode.

The following table10 describes, from a high-level perspective, the management components that are used (and how) within this use-case.

Table 10 mapping the management modules and the operations realized for the use case

Management module	Operation instantiated for the use case
One stop API	The One Stop API is used for the interactions between the Vertical and the SliceNet system, in particular, with the Digital Service Provider (DSP) actor. For example: • Ultra-Low Latency Service instantiation during the subscription phase – the vertical should indicate, among other parameters, the geographical area to be covered by the IEDs, required latency, throughput, etc. • Ultra-Low Latency Service reconfigurations during the runtime phase – the vertical can change the service reconfigurations during the service runtime (e.g. add a new IED).

Service Catalogues	Catalogue the Ultra-Low Latency Service template and the Network Slice templates (from the several administrative domains).
Slice Service Orchestrator	Translate the Ultra-Low Latency Service template to the appropriate Network Slice templates. Ultra-Low Latency Service: • Network Slice A (from NSP A) – vEPC & vRAN • Network Slice B (from NSP B) – vEPC & vRAN Instantiate the Ultra-Low Latency Service and the required Network Slice templates (in the several administrative domains)

Network Domain Orchestrator	Instantiate and configure (in a single-administrative domain) the NFV NSs (composed by VNFs, PNFs and/or MEC applications) interconnected by means of forwarding graphs.
	• vEPC
	  • vMME
	  • vHSS
	  • vPGW
	  • vSGW
	• vRAN
	  • vBBU

P&P Manager	Instantiate a P&P instance to deal with the vertical configuration requests (e.g. add new IED) for the slice instance.
Resource Monitor	Collect resource-level counters: • VM – vRAM, vCPU, storage I/O, disk networking usage; • vEPC (vMME, vHSS, vSGW, vPGW) VNFs counters; • vRAN (vBBU) VNFs counters; • Traffic/flow counters: • Number of packets per second;
Slice Monitor	Collect slice-level counters: • Latency; • Jitter; • Throughput; • Packet loss.
Service Monitor	Collect service-level counters: • Latency; • Jitter; • Throughput; • Packet loss.
Aggregator	Aggregate resource, slice and service level counters to produce high-level metrics/KPIs related with the slice and the service performance.
Analytics	Predictive fault management – predict and mitigate service and slice related faults; Predictive performance management – predict performance degradations at service and slice level.

6.3.3 Use case considered roles

The Smart Grid use case requires a multi-domain setting due to the nature of the distributed substations/IEDs deployed over a large geographical area consisting of both urban and rural districts, which is typically beyond one administrative domain's coverage. Consequently, two or more domains need to be involved to fulfil the service coverage requirements, leading to the inter- and multi-domain slicing. As shown in Figure 47, the E2E slice in this use case consists of sub-slices (or subnet network slices) from the various network segments belonging to two or more domains (two domains are depicted for presentation simplicity).

It is noted that no mobility support is required in this use case, and thus the inter- or multi-domain slicing can be controlled and managed in a "static" manner. In particular, the negotiations between/among the domains are typically arranged in the provisioning stage, and the topology of the slice is semi-permanent and thus the control and management of the topological aspects of the slice is of a static fashion in terms of no real-time mobility handling is required. Meanwhile, with the expansion of the business, additional domains can be added although this is not considered as real-time mobility or the focus of this use case. It is further noted that a substation/IED in Domain 1 may need to communicate with its peer in Domain 2 with a delay constraint. In that case, RAN-level slicing between the two involved RANs directly as a "shortcut" may be needed for the delay consideration. Therefore, it is desirable to take this potential case into consideration. For this use case, the focus is to achieve static inter- and multi-domain slicing that spans the segments of the domains as shown in Figure 47.

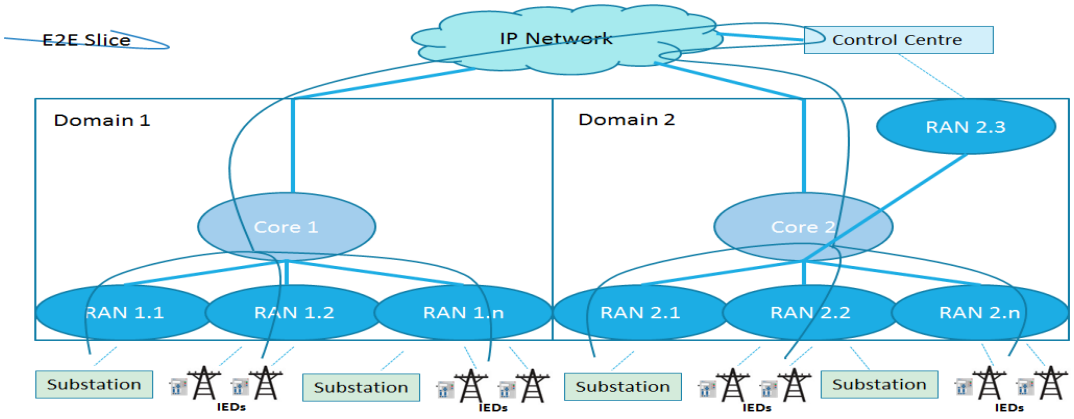


Figure 47 Multi-domain view of the Smart Grid use case

As described above, at least two NSPs (NSP A and NSP B) are required to fulfill the scenario requirements. Both, NSP A and NSP B provide vRAN and vEPC Network Slices (NSs) on their environment/network, and expose these Network Slices as a Service (NSaaS) to be subscribed by other entities. In this case, a Digital Service Provider (DSP) is responsible for subscribing for the NSP A and NSP B NSaaS offers and creating/composing an end-to-end Ultra-low Latency Service for the Vertical. This will allow the Vertical to attach their IEDs to the RANs and guarantee always-on connectivity with very low latencies among them.

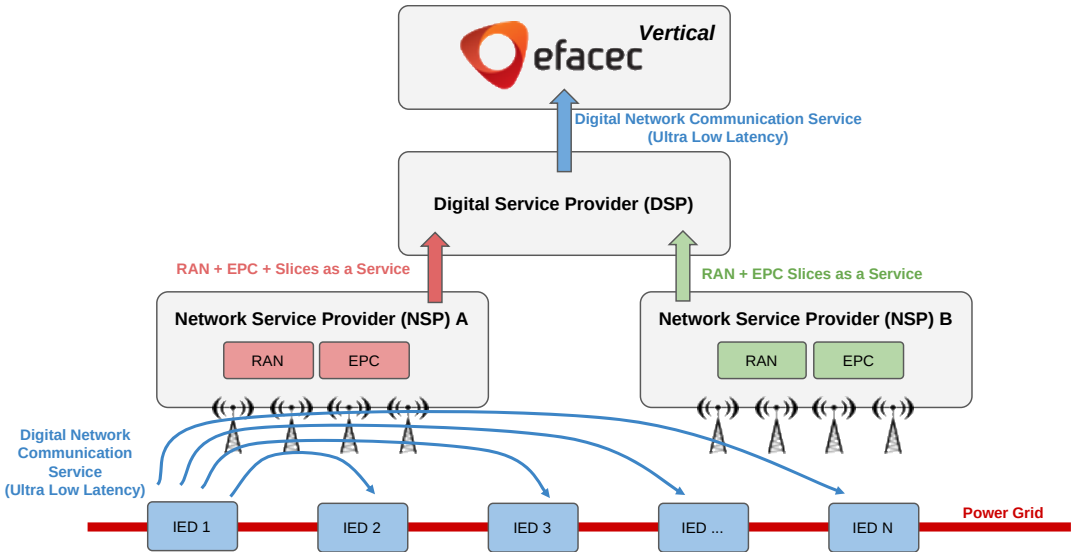


Figure 48 UC Roles Overview

Shortly, in terms of roles and relationships, the following responsibilities are expected as in the Figure 48:

- Network Service Provider A (NSP A)
  - Network Slices (NSs)
    - RAN Network Slice
    - EPC Network Slice
  - Network Slices as a Service (NSaaS)
    - RAN Network Slice as a Service
    - EPC Network Slice as a Service
- Network Service Provider B (NSP B)
  - Network Slices (NSs)
    - RAN Network Slice
    - EPC Network Slice
  - Network Slices as a Service (NSaaS)
    - RAN Network Slice as a Service
    - EPC Network Slice as a Service
- Digital Service Provider (DSP)
  - Ultra-low Latency Digital Service (composed through the combination of the NSaaSs offers provided by NSP A and NSP B).

6.4 eHealth

6.4.1 Use case description

The **eHealth Smart/Connected Ambulance use case** aims to provide a connection hub (or mobile edge) for the emergency medical equipment and wearables, enabling storing and potential real-time streaming of patient data via ambulance/wearable/drone mounted camera to the awaiting emergency department team at the destination hospital. The UC also provides a (MEC-based) Telestroke Assessment which also receives the patient video data and run a ML-based algorithm to provide the consultants some assessment on the patient's stroke condition. To assess the connected ambulance scenario, a set of KPIs, which is shown in Table11, below, is proposed in SliceNet for this particular use case.

Table 11 Proposed SliceNet KPIs for eHealth UC

SliceNet KPIs	eHealth UC
Service reliability	Yes
User Quality of Experience	Yes
Connection density	No
Low latency and critical comm.	Yes
Secure communication	Yes
Service creation time	Yes
Multi-domain coverage	Yes
Plug&play control for verticals	Yes
One-stop service order for verticals	Yes

In SliceNet, an E2E slicing for eHealth will provide a complete network slice connecting all terminals operating at the Ambulance/s, at the Dispatch Centre and at the Hospitals. This eHealth slice provides the services that the NAS (National Ambulance Service) vertical requires, including the National Digital Radio Service (NDRS), (MEC-based) Telestroke Assessment Service (TAS) and the BlueEye Service (BES). These services are provided by the Digital Service Provider (DSP) who is responsible for designing and customizing an overall E2E slice by combining different slice level parts (network slice subnets) by requesting from one or more specific Network Service Provider(s) (NSP).

As in D2.1, eHealth uses the enhanced MBB (eMBB) which requires both extremely high data rates and low-latency communication in some areas, and reliable broadband access over large coverage areas. Also, ultra-reliable and low-latency capabilities are key for eHealth applications due to patient safety requirements.

Due to the mobility of the ambulance/s, the ambulance/s might goes through different RAN segments managed by different operators (i.e. different administrative domains), therefore, the eHealth UC is considered to be a multi-domain UC. Figure 49 shows the multi-domain aspect of the UC.

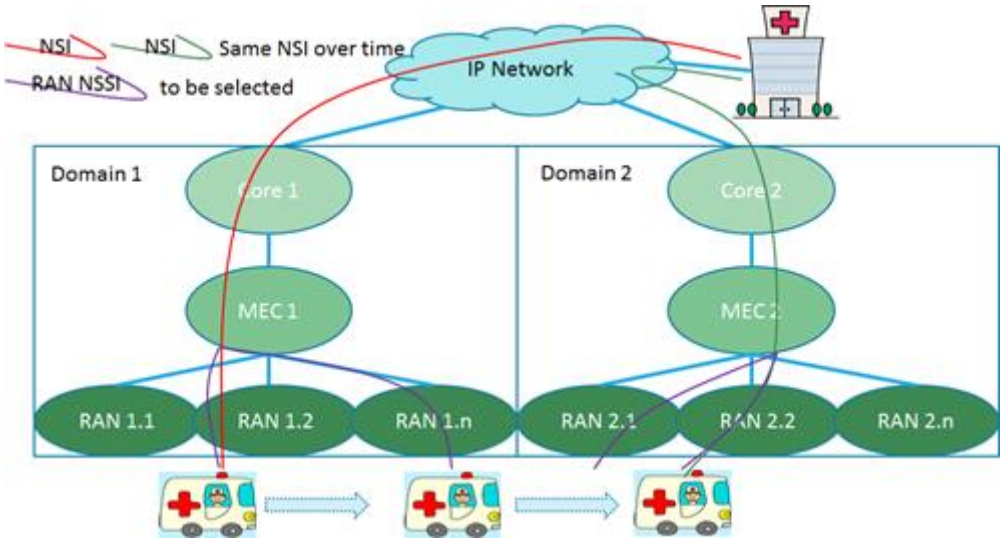


Figure 49 Multi-domain view of the eHealth UC

6.4.2 Management modules overview

Table 12 management modules for the use case

Management module	Operation instantiated for the use case
One stop API	The Vertical interacts with the SliceNet system via this one stop API at two phases: • eHealth Service instantiation during the subscription phase. At this phase, the vertical indicate the requirements in the SLA including classes of QoS, security, network performance, service availability, mobility, etc. • eHealth Service operations during the runtime phase where the vertical can request specific lifecycle management actions for some network functions, e.g., reallocating a VNF instance due to the mobility of the ambulance, or reconfiguring VNF instances, etc.
Service template	• eHealth service template
Slice template	• NDRS NS/NSS template • BlueEye NS/NSS template • Telestroke NS/NSS template
Slice Service Orchestrator	Translate eHealth service template into Slice templates: NDRS, BlueEye, Telestroke NS/NSS templates. Instantiate the eHealth Service and the required NS/NSS instances. The instantiation might involve several administrative domains providing the above NS/NSS.
Network Domain Orchestrator	Received request from SS-O, instantiate the NS/NSS the domain provides accordingly.
P&P Manager	Instantiate P&P instances for the slice instances, including P&P instances for monitoring, orchestration and control services.
Service Monitor	Video quality: • Frame rate;

	• Frame resolution • Bitrate/Encoding Rate Service availability/Coverage level
Slice Monitor	QoS: monitor latency, jitter, packet loss, packet error rate, availability time of each network connectivity link (network availability), and each components. Security: monitor traffics (traffic flows, flash events, traffic patterns, etc.), monitor equipment behaviours (registration, activities, etc.) for anomaly detection, offline data analytics for further breach detection/analysis. Fault and Performance: monitor network performance variations and trends (QoS monitoring targets above), etc.
Resource Monitor	RAN resources: • Radio link quality, signal strength, traffic congestion in current cell where the information is useful to make a decision when to start a handover process (to new Base Station) for better link/traffic. • Channel Quality Indicator (CQI) to enforce a new resource allocation policy or change the content quality to optimise video streaming and QoE. Topology/UE mobility. Coverage: Number of active Base Stations and overall coverage area, in case of events reducing the coverage level, some actions to consider include increasing the number of active BSs or signal strength adjustment for each BS to achieve the required coverage level. Fault and Performance: monitor hardware equipment (detecting faults), interference (corrective actions: frequency reallocations, antenna/radio adjustment, coordination between Base Stations), network capacity (rescheduling algorithms to reduce/avoid congestion, etc.), etc.
Analytics	Fault and Performance: • predict and mitigate faults in service/slice/resource level; • predict the preparation time (time to instantiate relevant NS/NSS with different selection of VNF locations, etc.) to estimate the time to setup/configure the components in the slice; • predict the mobility of the ambulance; • etc.

6.4.3 Use case considered roles

The roles mapping in eHealth UC involves the vertical as the NAS, and the Digital Service Provider (DSP), who designs and customizes the overall eHealth slice provisioning to the NAS vertical. To provide the required services to the NAS vertical, the DSP requests from one or more different Network Service Provider(s) the NSS(s) that they offer.

As the NAS is now requesting the NDRS service, along with video streaming and Telestroke Assessment services, E2E slice for eHealth must include three basic sub-slices:

- National Digital Radio Service (NDRS) NSS
- Video Streaming/BlueEye NSS
- Telestroke Assessment NSS

Depending on the DSP and the NSP(s), these services could be provided by one or many different NSP(s). Without loss of generality, Figure 50 assumes, the three services are provided by three different NSPs.

The Services are, National Digital Radio Service (NDRS), Video Streaming, Telestroke Assessment

The E2E slice provided by the DSP combines three different slice level parts, provided by one or more NSP(s), spanning from terminals in the Ambulance/s through the network to the Dispatch Centre and to the terminals in the Hospital/s, the entire network is operated by one or more NSP(s) that the DSP has requested.

Resource: all the resources/managed elements operate in RAN/MEC/CORE segments contributing to the above services.

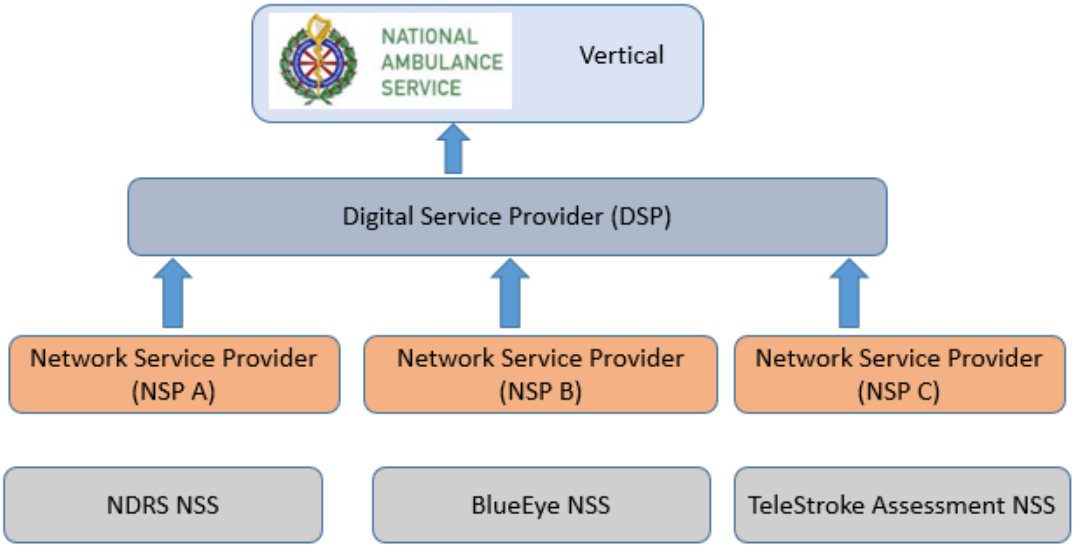


Figure 50 Roles mapping in eHealth UC

The E2E slice is spanning across multiple domains where the DSP is responsible for the service management level (slice provisioning and monitoring) and the NSP is responsible for its own NSS (slice and resource management level).

One example to clarify the roles mapping in existing eHealth scenario in Ireland is in Figure 51, where the NAS vertical (National Ambulance Service) subscribes to TETRA IRELAND (NSP) the NDRS service. In this model, the NAS acts as the vertical where TETRA IRELAND is the Network Service Provider who is operating its TETRA network resources and offering the NDRS service to the NAS vertical.

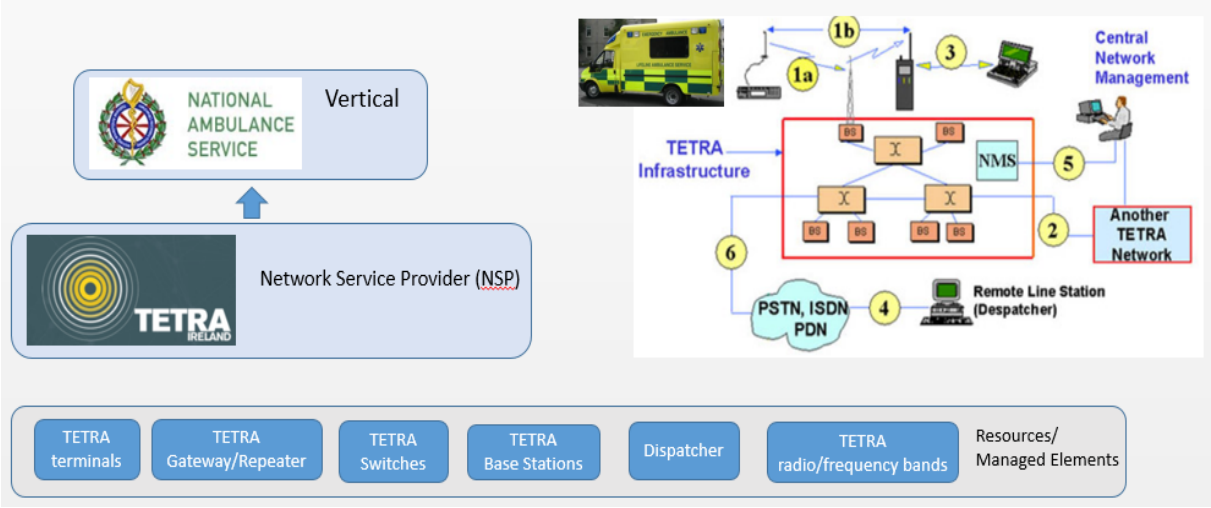


Figure 51 Roles mapping in National Ambulance Service in Ireland

- **Service**: National Digital Radio Service (NDRS).
- **Slice**: TETRA slice spanning from terminals in the Ambulance/s through the TETRA network (one or more) to the Dispatch Centre to the terminals in the Hospital/s, the network connectivity is operated on one of the TETRA radio/frequency bands that the NAS has subscribed to TETRA Ireland.
- **Resource**: all the resources/managed elements in the above figure.
- **Domain Aspect**: as TETRA Ireland has 98% coverage and is the only NSP providing this NDRS service to the NAS, it is operated in a single domain.

eHealth Showcasing

For eHealth Showcasing, SliceNet focuses to provide a demonstration an eHealth network slice composed of the two NSSs:

- BlueEye NSS
- Telestroke Assessment NSS

There are some considerations regarding the deployment for this demo, including the infrastructure, software and service stack. Figure 52 shows the abstraction of the eHealth UC demo.

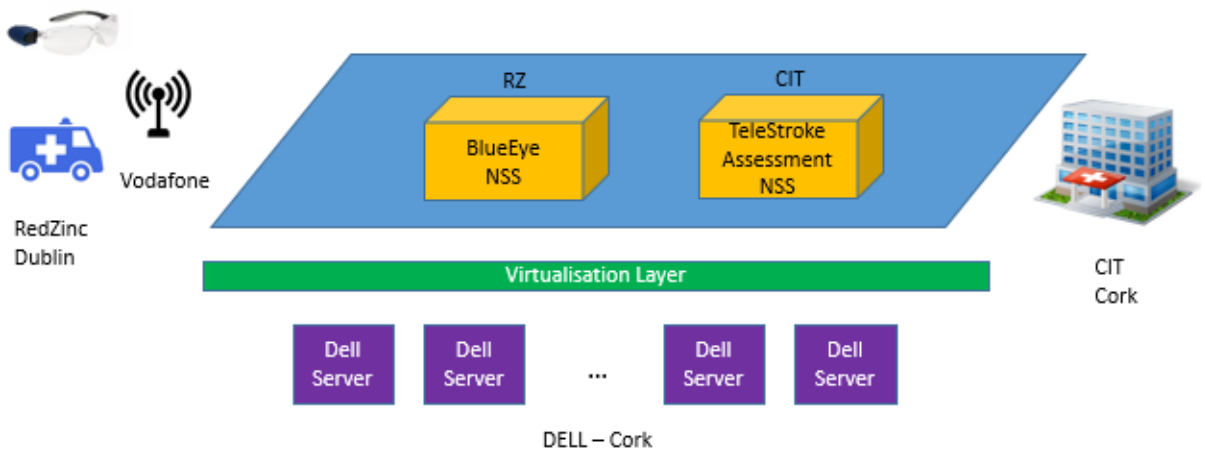


Figure 52 Demo Plan for eHealth UC

7 Conclusion

In this deliverable, we defined the management system for 5G networks with respect to 1) how to manage vertical requests, 2) set up and deploy the needed slices, 3) which scenarios and considerations for the multi-domains, 4) what are the new managed objects and elements, 5) what are the inner modules to consider for the management plane, monitoring plane and orchestration plane (including inventories and catalogues).

In fact, we analysed the latest management architectures proposed by standardizations and widely referenced in the academic research and other collaborative projects. The goals were to bring a consensus about how to manage the 5G network slicing for research and SDOs and ensure effective contributions from the project to those standards bodies. For that, we adopted a twofold approach to specify the management system:

Within the top down approach, we analyzed the state of the art with the focus on the SDO architectures for slice management in the 5G context. Based on that, we leveraged our previous deliverable, D2.2, by defining the inner modules of the management planes: this encompasses multi-layer monitoring (traffic, topology, resources, services and slices); cognition plane with modules spanning from the data preparation and cleaning to model setup and recommendation of which policies to set up or which QoE indicators to assign to a given Slice request; and the orchestration plane with several functions ensuring slice, service and resource operations while guaranteeing the required QoE.

The intelligence by means of cognitive operations is distributed to cover the Slice design time and the slice run time (life time).

On the one hand, during the design time, we foresee the smart translation of vertical request into the required QoE/QoS as well as the use of optimization techniques and heuristics to allocate resources and optimize the placement of the network functions within the slice. On the other hand, during the slice life time, we foresee the usage of analytics modules based on deep learning techniques for slice sessions supervisions and anticipations of degradation as well as to recommend actuations on the network slices to avoid the predicted faults.

In addition, we defined an information model to define the concepts related to the slices and that need to be managed by the inner management modules as well as to serve as basis for the instantiation later on the project within the use cases.

Within the bottom up approach, we collected the KPIs per use case; we analyzed the scenarios for multi-domain considerations per use case as well as the managed elements. This analysis was iterative so to converge both approaches. This resulted on the mapping of the management modules to the architecture of eHealth, Smart City and Smart Grid; the slice template is described for each each use case. Hence, this will serve as basis for the WP4, WP5, WP6.

References

[1] SliceNet Project deliverable, D21; SliceNet project; Report on Vertical Sector Requirements Analysis and Use Case Definition

[2] SliceNet Project deliverable, D2.2; SliceNet project; Overall Architecture and Interface Definition

[3] SliceNet Project deliverable, D23; SliceNet project; Control Plane System Definition, APIs and Interfaces

[4] IETF Network Slicing; https://www.ietf.org/archive/id/draft-geng-netslices-architecture-02.txt

[5] IETF COMS; https://tools.ietf.org/html/draft-geng-coms-architecture-02

[6] IETF COMS and Network Slicing Information Model; https://tools.ietf.org/html/draft-qiang-coms-netslicing-information-model-02

[7] IETF YANG Information Model; https://tools.ietf.org/html/draft-ietf-i2rs-yang-network-topo-20

[8] IETF YANG Information Model; https://tools.ietf.org/html/draft-ietf-i2rs-yang-network-topo-20

[9] Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework, Network Slicing report: http://www.etsi.org/deliver/etsi_gr/NFV-EVE/001_099/012/03.01.01_60/gr_nfv-eve012v030101p.pdf

[10] NGMN Alliance: "Description of Network Slicing Concept", January 2016.

[11] 3GPP; 3GPP TS 23.501: "System Architecture for the 5G System".

[12] ONF; ONF TR-526: "Applying SDN architecture to 5G slicing", Issue 1, April 2016.

[13] 3GPP TR 23.707-Rel.13; Architecture enhancements for dedicated core networks; Stage 2

[14] 3GPP 23.711-Rel.14; Enhancements of Dedicated Core Networks selection mechanism

[15] 3GPP 28801; Telecommunication management; Study on management and orchestration of network slicing for next generation network

[16] ETSI Network Functions Virtualisation (NFV);Accountability; Report on Quality Accountability Framework http://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/005/01.01.01_60/gs_nfv-rel005v010101p.pdf,

[17] 3GPP TS 28.530; Telecommunication management; Management of 5G networks and network slicing; Concepts, use cases and requirements v0.5.0

[18] NGMN, Description of Network Slicing Concept, V1.0.8, Sept 2016

[19] NGMN, 5G End-to-End Architecture Framework, V2.0.0, Feb. 2018

[20] Telemanagement Forum; Information Framework, https://www.tmforum.org/information-framework-sid/

[21] A YANG Data Model for Routing Information Base (RIB); draft-ietf-i2rs-rib-data-model-10https://tools.ietf.org/html/draft-ietf-i2rs-rib-data-model-10

[22] 3GPP (Telecommunication management; Configuration Management (CM); Part 5: Basic CM Integration Reference Point (IRP): Information model (including Network Resource Model (NRM)

[23] 3GPP 23.501; System Architecture for the 5G System

[24] 3GPP 28.530; Management and orchestration of networks and network slicing; Concepts, use cases and requirements

[25] 3GPP 28801; Telecommunication management; Study on management and orchestration of network slicing for next generation network

[26] ETSI GS NFV IFA 028; Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on architecture options to support multiple administrative domains; Multi admin domain support -report

[27] ETSI GS NFV IFA 030

[28] ETSI MEC017; Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment; http://www.etsi.org/deliver/etsi_gr/MEC/001_099/017/01.01.01_60/gr_MEC017v010101p.pdf

[29] ETSI MEC 010-2; ETSI Multi-access Edge Computing group releases a first package of APIs. http://www.etsi.org/news-events/news/1204-2017-07-news-etsi-multi-access-edge-computing-group-releases-a-first-package-of-apis

[30] ETSI IFA 009; Network Functions Virtualisation (NFV);Management and Orchestration; Report on Architectural Options

[31] ETSI GS MEC 003: Mobile Edge Computing (MEC); Framework and Reference Architecture Network Functions Virtualisation (NFV) Release 2; Management and Orchestration;

[32] Network Service Templates Specification; http://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/014/02.04.01_60/gs_NFV-IFA014v020401p.pdf

[33] ETSI IFA 011; Network Functions Virtualisation (NFV);Management and Orchestration; VNF Packaging Specification https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=44577

[34] Opensource MANO; https://osm.etsi.org/

[35] OpenBaton, http://openbaton.github.io/

[36] www.kubernetes.io

[37] ONAP; https://www.onap.org/

[38] Building an Intelligent System of Insight and Action for 5G Network Management: http://www.cognet.5g-ppp.eu/

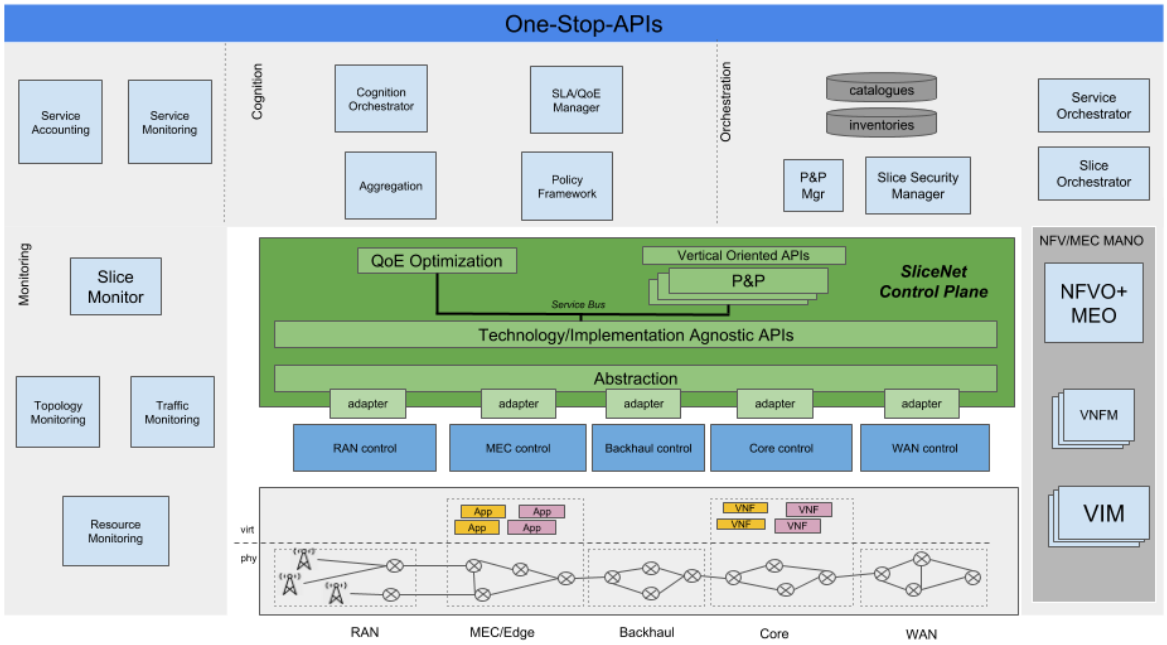
[39] CogNet final requirements, scenarios and architecture; http://www.cognet.5g-ppp.eu/public-deliverables/

Annex A

A.1 Control Plane and APIs

SliceNet Control Plane is designed (D2.3) to operate on top of an infrastructure spanning across several PoPs per administrative domain with each PoP being allocated to one of the three main network segments of a 5G network: RAN, MEC, Core. Additionally, a backhaul segment and an inter-domain segment are foreseen in the context of the inter-PoP and inter-domain connectivity requirements. These five segments are identified as the five control infrastructure pillars of SliceNet and their role is:

- RAN Control: exposes control functionality over Access Network resources
- MEC Control: exposes control functionality over MEC resources
- Core Control: exposes control functionality over Core resources
- Backhaul Control: exposes control functionality over connections among Single Domain PoPs
- WAN Control: exposes control functionality over infrastructure responsible for Inter-Domain connections



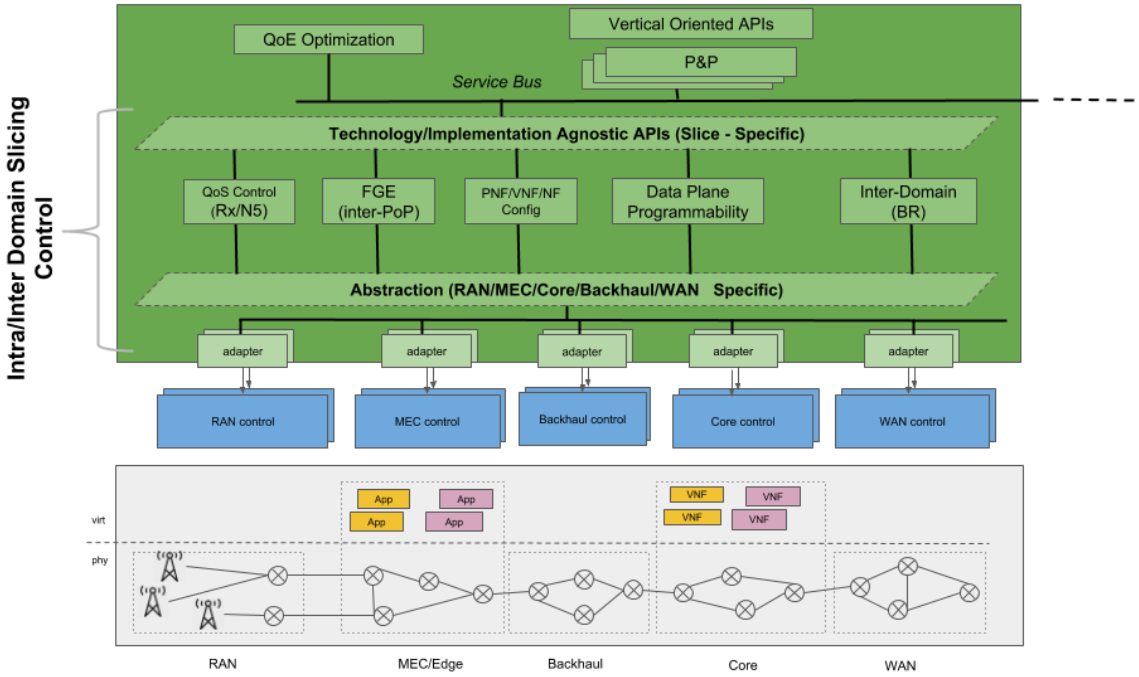
Aiming at retaining a level of granularity that is adequate enough to cater for a variety of requirements stemming from verticals and also flexible enough to accommodate future technologies, SliceNet CP assumes that control pillars are not bound to specific vendor or technology specific implementations and additionally the same pillar within a single domain may consist of several instances of the same or different implementations activated in parallel. For this purpose the adaptation concept is defined in order to allow control pillar instances to be easily integrated under the command of the SliceNet CP and furthermore in the context of management and orchestration of end to end vertical slices. The functionalities exposed at that level constitute a first level of abstraction that can allow SliceNet CP workflows executed in a common way over the available CP resources. Each implementation requires an adapter (one per implementation instance) that at its SBI supports the interaction with specific technology/implementation details whereas provides an NBI according to the model of the common set of functionalities. The provision of the related adapter on top of a control pillar entity belongs to the responsibilities of the related vendor. All implementations for a single pillar are providing the functionalities of a common set and there is a

minimum subset of the functionalities that is mandatory so that an implementation can be integrated.

In D2.3 the following operations have been identified as a minimum set of supported functionality provided per pillar through registered adapters:

- (Radio) Access Network
    - Collect Cell/Slice/User Monitoring Metrics
    - (Re)configure Cell/Slice/UE
    - Allocate access resources to slice
    - Configure basic RAN and CORE services
    - Apply QoS constraints
    - Configure MEC Breakout
- MEC
    - Allocate MEC Resources
    - Instantiate MEC Applications
    - (Re)configure MEC Applications
- Backhaul
    - Provision SDN intent
    - Remove SDN intent
    - Provision QoS-enabled SDN Forwarding Rules
    - Update QoS-enabled SDN Forwarding Rules
    - Remove QoS-enabled SDN Forwarding Rules
    - SDN Topology Exposure
- Core
    - Add Core Function Instance to Slice
    - Configure UE Set for Slice
    - Configure Traffic Classification per Slice
    - Apply UE Addressing scheme for Slice
    - Enable broadcasting support for a Slice
    - Enable direct point to point communications support for a Slice
    - Get Sessions per Slice
    - Get Flows per Slice Session
    - Apply QoS via AF Rules
    - Create MEC Breakout (UPF level)
- WAN
    - Provision Border QoS-enabled SDN Forwarding Rules
    - Update Border QoS-enabled SDN Forwarding Rules
    - Remove Border QoS-enabled SDN Forwarding Rules
    - Inter-domain SDN Topology Exposure

On top of the pillar abstractions a number of CP services are foreseen.



These services are exposing underlying pillar capabilities through the slice technology and implementation agnostic APIs which represent the set of slice configuration endpoints that can be accessed by other SliceNet platform components (from P&P and QoE optimization to management and orchestration tools), thus providing the control context of a slice in terms of the following operations per CP service:

- Inter-PoP forward graph configuration
  - Provision Forwarding Graph
  - Add nodes to forwarding graph
  - Remove nodes from forwarding graph
  - Provision link in forwarding graph
  - Remove link in forwarding graph
- Configure routing scheme
  - Delete forwarding graph
- PNF, VNF and 4G/5G (either user or control) NF configuration
  - Add VNF/PNF/NF Configuration
  - Update VNF/PNF/NF Configuration
  - Rollback VNF/PNF/NF configuration
- Inter-domain connectivity
  - Interconnect Slice to Peering Domain(s)
  - Modify Slice Interconnection to Peering Domain(s)
  - Remove Slice Interconnection to Peering Domain(s)
- UE Session QoS Control
  - Configure Session QoS Parameter
  - Configure Session Priority
- Data Plane Programmability for quality based user traffic management
  - Set flow priority
  - Set session priority
  - Set flow acceleration
  - Set session acceleration

CP components and interfacing to the MP

The CP is interfaced to the management plane through dedicated plugins to allow the slice instances to be customised and managed appropriately by the vertical through the One Stop box. The logical instance exposed to the vertical contains APIs with extra information of how the end user should be authenticated and what type of access and level of capability has over the management of the slice instance. One of the main components of the Slicenet CP is the P&P component that communicates with the management plane through a P&P agents residing inside the MP. This management API has the capability to:

- activate the required plugins and drivers which are required for the specific logical slice
- translate the slice modeling view into a view that the end user can understand
- activate specific APIs in the form of control logics to the vertical
- translates slice instance optimizations controlled by the QoE optimizer into control logics

Another important component in the CP that communicates with the MP through dedicated APIs is the QoE optimizer that communicates with the MP through two components. These are the monitoring component in the MP plane that communicates with a local decision engine in the CP that examines the trigger that receives from the management plane and provides the proper trigger to another component of the CP, the slice policer that communicates with dedicated API to the policy engine in the MP.

The above two components of the CP are communicating with the MP, while there three more components, the intra-domain, the intra-domain 5G-RAN core slicing components that communicate through dedicated APIs to the data plane. These three components have proper adapters and local controllers to communicate with the data plane and control the slice instance respectively. The inter-domain slice component can be thought to be one that connects intra-domain components.

