5G Exchange

Deliverable 2.1

5GEx Initial System Requirements and Architecture

Revision information: December 5, 2016
(Approval from the European Commission pending)

Dissemination level:

- **Public version (some sections removed)**

This project is funded by the European Union

Document Information

Editors

Carlos J. Bernardos (UC3M)

Authors/Contributors

Balázs Péter Gerö (ETH), Manos Dramitinos (AUEB), Carlos J. Bernardos (UC3M), Aurora Ramos (ATOS), Luis M. Contreras (TID), Róbert Szabó (ETH), Riccardo Guerzoni (HWDU), Balazs Sonkoly (BME), Alex Galis (UCL), Donal Morris (REDZINC), Barbara Martini (KTH), Javier Melián (ATOS), Hakon Lonsethagen (TNO), Diego Daino (TI), Gergely Biczók (BME), Marco Di Girolamo (HPE), Francesco Tusa (UCL), George Darzanos (AUEB), Ioanna Papafili (AUEB), Andrea Sgambelluri (KTH), Olivier Dugeon (ORANGE), George D. Stamoulis (AUEB), Miguel Á. Carnero (TID), Rafael Cantó (TID), Francisco Valera (UC3M), Alberto García (UC3M), Hagen Woesner (BISDN), Juhoon Kim (DT), Fabio Ubaldi (TEI).

Document History

Version	Date	Comment
D2.1 v1.1 PUBLIC	05/12/2016	Public version (some sections removed)
D2.1 v1.1	02/12/2016	Updated version addressing reviewers comments
D2.1 v1.0	30/09/2016	Final version of D2.1 at M12
D2.1 v0.9	05/08/2016	Snapshot of D2.1 at M10
IR2.1	31/03/2016	Snapshot of D2.1 (as per MS1)

Coordinator

Robert Szabo
Ericsson Research, Hungary

Partners

Ericsson (Hungary and Italy), ATOS, AUEB, BISDN, BME, Deutsche Telekom, Hewlett Packard Enterprise, Huawei, KTH, Orange, RedZinc, Telecom Italia, Telefonica I+D, Telenor, UC3M, UCL, Media Network Services.

Project Funding

ICT-2014/H2020-ICT-2014-2, Innovation action
Grant Agreement No. 671636 – 5G Exchange (5GEx)

Legal Disclaimer

Executive Summary

D2.1 is the first WP2 document and it has as one of its main goals to **present a first version of the 5Gex architecture**. In order to do so, the document first overviews the business ecosystem, including use cases of interest to 5Gex. It also provides an initial set of **requirements for the 5Gex architecture and business-layer functionality** that needs to be integrated to support the 5Gex orchestration and market. This initial 5Gex architecture will be further refined in subsequent iterations, considering feedback from the implementation and experimentation of the different prototypes of WP3, the integration and testing in the Sandbox of WP4 and other external initiatives.

The overall **architecture design methodology is based on converging two different approaches:** (i) **a top-down approach providing a green field architectural vision** from the identified requirements, (ii) **bottom-up approach based on existing orchestration components architecture that 5Gex can leverage on**, adding the missing pieces required for the enablement of multi-domain orchestration. In order to achieve this convergent design, we have conducted a review of the state of the art, including related efforts at different standardisation bodies. This analysis benefitted from the analysis of the overall business ecosystem and roles, which was also considered when identifying the main use cases of interest for the project. Initial pricing schemes for 5Gex resources and services are also presented, though the main conclusion of this work will not be available until D2.3 is released at the end of M28.

The main outcome of WP2 during the first part of the project, reported in this deliverable, is the initial definition of the 5Gex architecture, which was provided to WP3, which further developed it into an implementation architecture, as described in D3.1. It was also provided for the integration in the Sandox of WP4.

This document also includes a first analysis on **how to apply the functional architecture blocks to set up example services** across multiple administrative domains in specific network scenarios, to verify the applicability of the functional architecture in these deployment scenarios and **identify improvement areas.**

The main innovations (findings) reported in this document are:

1) The definition of the main architecture multi-domain building blocks of 5Gex and their interfaces, considering not only the technology gaps but also the business considerations. This architecture vision is based on a **revised vision of the ETSI NFV** ISG framework, which is being **contributed to relevant standards,** namely ETSI and IETF. It is also anchored in the emerging **overall 5G networking architecture** focussing on the Infrastructure Softwarisation,

Control and Integrated Management Planes, which is being contributed to **ITU-T IMT 2010** standard group.

2) A novel analysis of **business roles in a multi-domain environment, looking at the 5GEx framework, 5GEx services definition as well as describing possible coordination models that can apply to the 5GEx framework.** A main conclusion is that distributed coordination models scale better and build upon existing business relationships, resulting in lower deployment costs, less trust issues and easier bootstrapping of the 5Gex solution. Centralised coordination on the other hand can increase both the multi-domain service orchestration probability and the overall system efficiency. On-demand service composition can be used to discover the 5G market needs, which is useful in early markets, serving as a feedback loop for the specification of service catalogues that can significantly reduce the amount of on-demand customer requests and promote automated and fast service orchestration and trading.

This document has identified the main use cases of interest for the project, deriving the main requirements for the architectural work. These requirements, together with a deep analysis of the state of the art, and an analysis of the business eco-system, have been used in the design of a first 5GEx architecture. This design has not only considered the identified requirements, but also the different software components that were available at the beginning of the project, to maximise the re-use of existing tools and synergies with ongoing efforts. It was not in scope to provide a final architecture definition, as this is an interative process that requires from implementation and operational feedback to be refined. An analysis of the business cases relevant to 5GEx is also included in this deliverable. A more complete pricing model will also be part of **our next steps,** which also include looking into more detail into security and scalability aspects, which have not being the main focus of the work reported in this deliverable.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS

5Gex	5G Exchange
ALTO	Application-Layer Traffic Optimisation (ALTO) Protocol
API	Application Programming Interface
ASQ	Assured Service Quality
B2B	Business-to-Business
BGP-LS	Border Gateway Protocol – Link State
BRG	Bridged Residential Gateway
BSS	Business Support System
C2B	Customer-to-Business
CA	Controller Adapter
CDN	Content Delivery Network
CLI	Command Line Interface
COP	Control Orchestration Protocol
DoA	Description of Action
E2E	End-to-End
EM	Element Management
EM	Equipment Manager
EoF	Exchange of Functions
EoIC	Exchange of Information and Control
EoR	Exchange of Resources
EPC	Evolved Packet Core
ESCAPE	Extensible Service ChAin Prototyping Environment
ETICS	Economics and Technologies for Inter-Carrier Services
ETSI	European Telecommunications Standards Institute
EVE	Evolution and Ecosystem
FCAPS	Fault, Configuration, Accounting, Performance, Security
FE	Functional Entity
HOT	Heat Orchestration Template
IFA	Interfaces and Architecture
IoT	Internet of Things
IP	Internet Protocol
IPNP	Initiating Party Network Pays
ISG	Industry Specification Group
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KPI	Key Performance Indicators
KQI	Key Quality Indicators
LTE	Long Term Evolution
M2M	Machine-to-Machine
MANO	MANagement and Orchestration
MdIaaS	Multi-domain Infrastructure as a Service
MdO	Multi-domain Orchestrator
MPLS	Multiprotocol Label Switching
NaaS	Network as a Service
NERG	Network Enhanced Residential Gateway
NF-FG	Network Function Forwarding Graphs

NFIB	NF Information Base
NF-IB	Network Function Information Base
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NFVIaaS	Network Function Infrastructure as a Service
NFVI-PoPs	Network Function Virtualisation Infrastructure Point of Presence
NGMN	Next Generation Mobile Networks
NGSON	Next Generation Service Overlay Network
NS	Network Services
NSD	Name Server Daemon
OH	OpenStack Heat
OL	Orchestration Layer
OSS	Operation Support System
PCEP	Path Computation Element Communication Protocol
PoC	Proof of Concept
PoP	Point of Presence
QoE	Quality of Experience
QoS	Quality of Service
RACF	Resource Access Control Facility
RG	Residential Gateway
RO	Resource Orchestrator
RPC	Remote Procedure Call
SC	Service Composition
SDK	Software Development Kit
SDN	Software Defined Network
SDO	Standards Development Organisation
SDP	Service Delivery Platforms
SDX	Software Defined X
SFC	Service Function Chaining
SG	Service Graph
SIP	Session Initiation Protocol
SL	Service Layer
SLA	Service Level Agreements
SlaaS	Slice-as-a-Service
SLS	Service Level Specification
SOA	Service Oriented Architecture
SON	Service Overlay Network
SP	Service Provider
SPNP	Sending Party Network Pays
SR	Service Routing
Sreg	Service registry
SWA	Software Architectures
SWOT	Strengths, Weaknesses Opportunities, Threats
TLV	Type Length Value
TMF	TM Forum
vCDN	Virtual CDN

vG	Virtual Gateway
VIM	Virtualised Infrastructure Manager
VM	Virtual Machine
VNF	Virtualised Network Function
XaaS	X-as-a-Service

1 Introduction

This document describes the first design out of the versions planned of the 5GEx architecture. It includes an overview of the business ecosystem, including use cases of interest to 5GEx.

The initial version of the 5GEx architecture, introduced in this document will be further developed in subsequent iterations, considering feedback gathered during the implementation and experimentation of the different prototypes. This architecture design will be finally updated in D2.2.

This deliverable is structured as follows. Section 2 reviews the state of the art from different angles, including, but not limited to, related EU projects, relevant standardisation activities, existing orchestration frameworks and commercial products. Section 3 analyses the business ecosystem and the roles that are related to the goals and ambition of the project.

Section 4 identifies and describes the most interesting use cases to the project. We then identify the main requirements, taking into consideration the identified use cases, the business ecosystem and the general 5G environment. Section 5 provides a high-level overview of pricing schemes for 5GEx resources and services. Section 6 provides a SWOT analysis applied to the three types of 5GEx solutions envisioned in 5GEx (described in Section 3.3).

Section 7 describes the overall 5GEx architecture, including the definition of the different entities as well as the interfaces that exist among them. Section 8 describes how to apply the functional architecture blocks to set up example services across multiple administrative domains in specific network scenarios. Section 9 provides an overview of initial business cases of interest for 5GEx and its stakeholders. Finally, Section 10 summarises and concludes this deliverable.

We include as annexes additional information, either providing more detailed background information, going deeper into some specifics or providing extra examples.

1.1 5G network architecture context

The 5GEx project addresses some of the challenges that future 5G networks are expected to tackle. As such, it is important to provide some general context to the project work. D3.1 [69] provides a detailed walkthrough of the current 5G network architecture context. Since this is important, we have extracted some of this input and included it in Annex B.

5G networks are conceived as extremely flexible and highly programmable E2E connect-and-compute infrastructures that are application- and service-aware, as well as time-, location- and context-aware. They represent:

- an evolution in terms of capacity, performance and spectrum access in radio network segments; and
- an evolution of native flexibility and programmability conversion in all non-radio 5G network segments: Fronthaul and Backhaul Networks, Access Networks, Aggregation Networks, Core Networks, Mobile Edge Networks, Software Networks, Software-Defined Cloud Networks, Satellite Networks and Edge IoT Networks.

The currently proposed 5G framework can be specified as separate planes of functionality. Although separately defined, the planes are not completely independent: key items in each are related to items in the other planes. However, the planes are sufficiently independent to simplify reasoning about the complete system requirements. The interworking between planes is manifested by groups of interfaces (i.e., reference points) that would be used for exchange of information and/or controls between separate (sub)systems sharing boundaries. The projected separation of concerns in distinct planes are: Application and Business Service Plane, Multi-Service Management Plane, Integrated Network Management & Operations Plane, Infrastructure Softwarisation Plane, Control Plane and Forwarding/Data Plane.

The 5GEx project position itself and it is focusing on the Infrastructure Softwarisation, Control and Integrated Management Planes of the above presented 5G Framework.

2 Review of the state of the art

In this section, we provide a review of the state of the art regarding to technologies and efforts relevant to 5GEx. This is done following a multi-folded approach, by looking first at different exchange environments, then to several proposed software network architectures, mainly proposed within the main standards developing organisations. We also identify and describe other major projects working on related areas, noting that in some cases we will re-use some of their outcomes as input for 5GEx. Some key areas for the project (orchestration, SLA design, service catalogue and multi-domain service delivery) are also analysed, identifying some important open aspects for 5GEx to explore and further develop.

2.1 Exchange environments

We next review the concepts of Internet Exchanges and Federations, as they are relevant related architectural aspects for the 5G-Exchange.

2.1.1 Internet Exchanges

The success of Internet data based services over the last decades has a fundamental driver in the full reachability of contents accessed by the end-users and served by content providers, which is facilitated by the interconnection of networks.

Service providers have for long time focused on delivering the best possible connectivity to their retail and enterprise customers, remarking the fact that traffic routing and exchange, and access to remote content, have been at the core of the networking business during the last decades. Value added services have typically been offered by the same service providers using manual configuration of static infrastructure for tailoring services according to the specific customer needs. This is difficult to maintain, adapt, port and rollback when the demand varies, the underlying infrastructure needs to be changed (e.g., because of equipment obsolescence) or errors occur during the service provisioning phase.

Traditional interconnection services have been merely based on pure delivery of IP traffic between interconnected parties, even without direct connection of the parties. Advertisement of IP prefixes with the usage of the BGP protocol allows knowing how to reach a remote destination just identifying the next hop for traffic delivery. This peer model enables full connectivity as far as the participants' networks announce their own prefixes.

There are several interconnection models in place [35]. The most obvious is the direct, private interconnection between networks. A more sophisticated approach is the constitution of interchange points (Internet eXchange Points, IXPs) where several operators and service providers meet in order to interconnect, typically through the usage of common switching infrastructure pertaining to the interchange point entity, and operated by it.

As an example of the infrastructure present in one of such exchange points, Figure 2-1 shows the infrastructure of AMS-IX[1], a Dutch IXP.

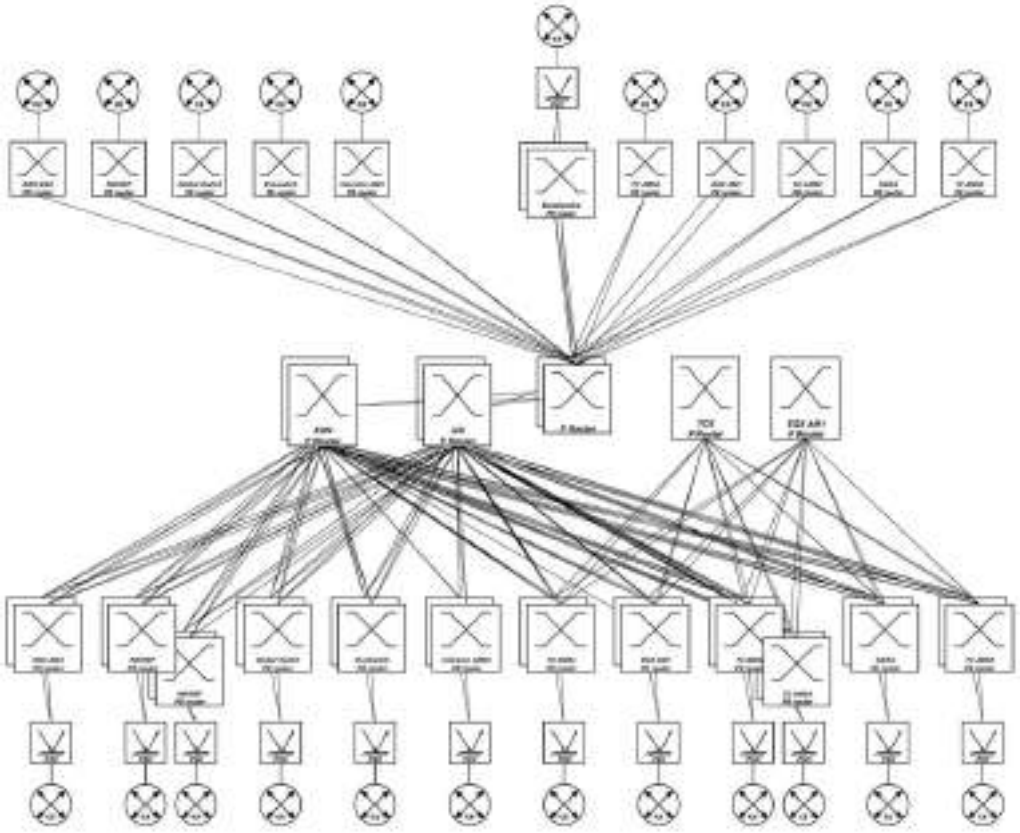


Figure 2-1: AMS-IX layout

AMS-IX is a distributed exchange, currently present at multiple independent colocation facilities in Amsterdam. Each site is equipped with one or more access devices to enable connections to the AMS-IX infrastructure.

The current implementation of the AMS-IX peering platform uses an MPLS/VPLS infrastructure. This setup allows for a resilient and highly scalable infrastructure inherent to MPLS, while at the same time the interface towards the members and customers is still the common shared Layer 2 Ethernet platform.

Networks connect with either Gigabit Ethernet (GE), 10 Gigabit Ethernet (10GE), 100 Gigabit Ethernet (100GE) or multiples of these on the access

[1] https://ams-ix.net/

devices which are PE routers. To provide more resilience in the connection of 10GE & 100GE connections to the platform, these are terminated on photonic cross-connect (PXC). The PXC connects the member router (at Layer 1) to one of the local PE routers and if necessary moves this connection to a backup router. The core of the network is built around P routers.

As an example of connectivity, two customer routers at the top of the diagram in Figure 2-2 are connected through a photonic cross-connect (PXC) to a set of PE routers (PE-1-red, PE-1-blue) with 10GE & 100GE connections. At the bottom, a customer router connects to a PE router (PE-3) with a 1GE connection directly. Each PE router is connected to each of the core (P) routers with one or multiple 10GE & 100GE connections. The P routers are located in two different physical locations (core-location-1 and core-location-2). There are two P routers per core location.

The logical connections between the PE routers are implemented as label switched paths (LSPs). Between each pair of PE routers, we define four LSPs, one for each core. The diagram shows the set of LSPs for each pair of PE routers in a different colour (for example, green for the LSPs between PE-1-blue and PE-3, orange for the LSPs between PE-1-red and PE-1-blue). Traffic between each pair of PE routers is load-balanced over the four LSPs. When any of the physical components in an LSP fails, the LSP will move over to an alternative physical path.

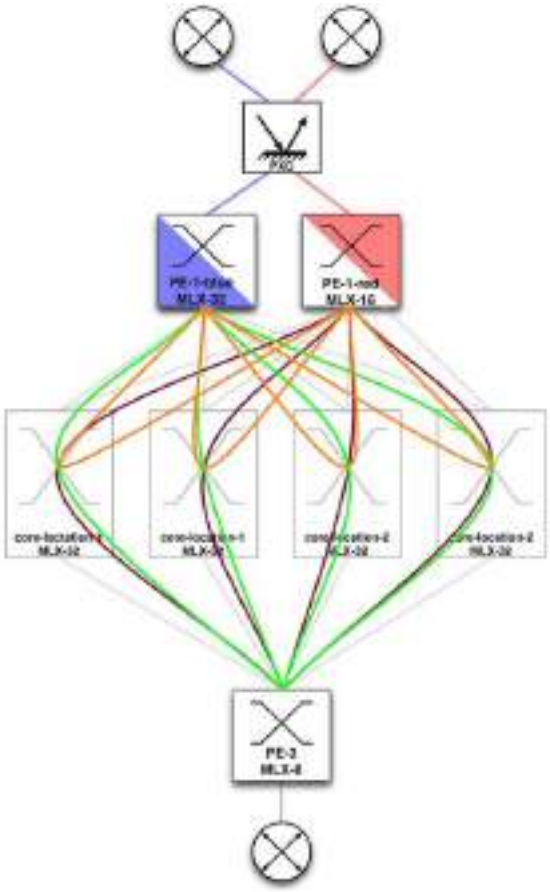


Figure 2-2: LSPs and load distribution for typical customer connection in AMS-IX

In a general manner, the BGP sessions remain to be established in a peer-to-peer fashion, while sharing the switching infrastructure to optimise the number of ports in use for maintaining multiple simultaneous interconnections in these environments. It is also common, at the same time, to find private interconnections for some of the members of the interchange point in the same premises, according to the volume of traffic delivered between peers.

Having such IP connectivity substrate ready, services exceeding one administrative network domain are constructed through the application of complex, manual configurations enabling transport mechanisms just providing end-to-end connectivity. The service on top of such connectivity requires further configuration, sometimes needing mediation of other providers for configuring the infrastructure participating to the service provisioning.

The offering of connectivity has so far relied upon exchanges conceived for pure transmission and forwarding of IP traffic [36][37], pure roaming of mobile users (like in the case of GPRS roaming exchange, GRX) or interworking and roaming interconnection arrangements for IP services with committed QoS (like in IP exchange, IPX) [38]. All these environments are also static, requiring long interactions for setting up any inter-provider connection. The IPX is an inter-Service Provider IP

backbone which comprises the interconnected networks of IPX Providers and General Packet Radio Service (GPRS) Roaming eXchange (GRX) Providers. The IPX Network was originally conceived as an inter-Service Provider IP backbone created to carry GTP-tunnels (GPRS Tunnelling Protocol) via the Gp interface between the GPRS Support Nodes (GSNs) at different GSM Operators (i.e., data roaming). The Gp interface allowed mobile end-users to make use of the GPRS/3G services of their home network while roaming in a visited network. Later, Multimedia Messaging Service (MMS) interworking and Wireless Local Area Network (WLAN) authentication data roaming were added as supported services. The original GRX model has been enhanced by adding new requirements like end-to-end Quality of Service and the introduction of the IPX Proxy which facilitates interconnect cascade billing and multi-lateral interconnect agreements. Figure 2-3 presents the generic IPX model.

In addition to the *classic* Internet Exchange Points, it is worth mentioning here the efforts around the so-called SDN exchange points. The SDX[2] (SDN exchange point) project proposes to deploy SDN-capable switches at IXPs in order to make a step forward from conventional hop-by-hop, destination-based forwarding and hence to solve long standing problems in interdomain routing. Since SDN allows direct expression of flexible policies, the participating ISPs can execute many different network applications on their packets traveling through the IXP, such as inbound traffic engineering, redirection of traffic to middleboxes, wide-area server load balancing, and blocking of unwanted traffic. The project participants have developed a controller that provides each ISP with the abstraction of its own virtual switch and sequentially composes the policies of different ISPs into a single set of rules in the physical switches to support these applications. The main features of SDX include providing a virtual topology for each operator, ensuring that participants' policies do not interfere or conflict with one another, and of course scalability [22].

[2] http://noise-lab.net/projects/software-defined-networking/sdx/

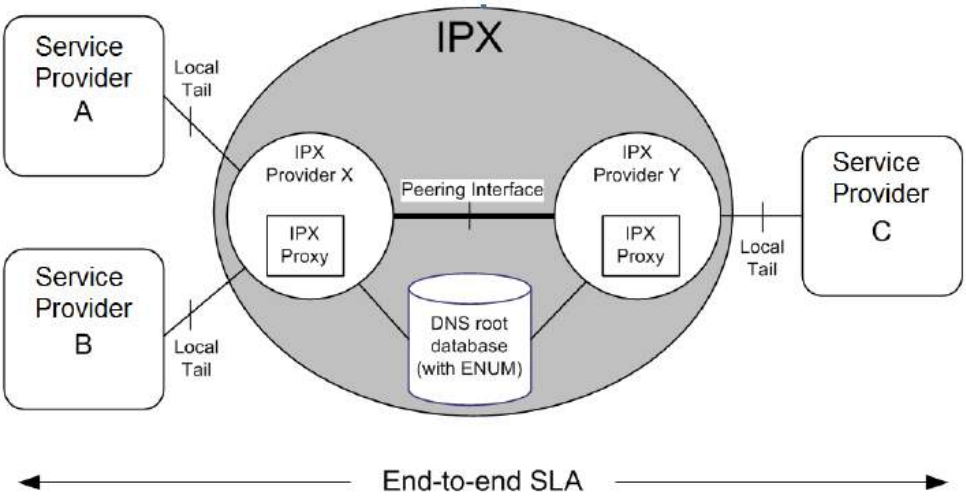


Figure 2-3: IPX model

2.1.2 Federations

We now provide a brief overview of federation models most relevant to 5GEx.

Federations have recently attracted attention in the networking world, for IP interconnection where the current business models are based on peering or transit agreements between providers for best effort connectivity (the current Internet is just a federation of interconnected Autonomous Systems). Concerning the collaborative approaches, an important initiative has been carried out in the ETICS project [3] where the ETICS *community* concept is proposed as a novel three-stage collaborative service provisioning paradigm. The ETICS community is formed by Network Service Providers that support the ETICS approach for provisioning additional interconnection goods, the Assured Service Quality goods over inter-domain paths and regions. ETICS introduces three main types of interconnection communities, each reflecting different amount of trust and cooperation among its participants, information sharing and level of business constraints, namely: i) *Open Association* (solely technical specifications and best practice directives), ii) *Federation* (an additional level of information dissemination and common objectives, potentially common technical facilities for supporting functions), and iii) *Alliance* (common and strict business policy rules directed by a defined market objective and revenue sharing). For each variant, a set of business policy rules have been specified in an attempt to "regulate" the community environment and attain efficiency. Though the ETICS community is interesting, ETICS has not been materialised in the market, mostly due to the outdated interconnection technology it relied on and the scalability and cost – in terms of technical alignment and business coordination – issues of its approach.

Another interesting research approach is the one explored in the VITAL [4] and BATS [5] projects, focusing on federation and coupling between

satellite and terrestrial systems for hybrid access, including either fixed and/or mobile networks. The motivation is the combination of satellite and terrestrial components to form a single/integrated telecom network as a promising approach to significantly improve the delivery of communications services. The project defines interesting use cases, including 4G/5G backhauling. The adoption of SDN and NFV technologies into the satellite domain is seen as a key facilitator for satellite communications to become a well-integrated constituent part within an anticipated multi-layer/heterogeneous 5G network architecture.

Federations have also been envisioned in the content delivery business and in particular Content Delivery Networks. Though the CDN business has been traditionally dominated by large players such as Akamai, the rise of smaller and even telco-owned CDNs has raised interest on CDNi, a technical federation of CDNs supporting various use cases and business models, both bilateral seller-buyer and federated ones. The idea behind CDNi and its multiple forms, as envisioned by vendors like Cisco [8], standardisation bodies like IETF [6], and research projects [7], is that CDNs combine their infrastructure and services to aggregate content and users or lease infrastructure and presence at certain geographic regions strictly on-demand basis.

Federations/exchanges are gaining momentum in the cloud world, including Data Center interconnection over federated infrastructure. A typical example is OnApp [9], a federation of cloud providers with cloud IaaS and CDN product offerings of fine geospatial granularity world-wide. Each member of the federation can buy and sell capacity through the OnApp market.

Cloud28+ [10] is a similar European initiative to create an open federated community of Cloud Service Providers, Cloud Resellers, Independent Software Vendors, System Integrators and government entities. It allows a fair comparison of available services versus customer requirements and uses a single catalogue of available federation services, with homogenous semantic description of services and search-and-rank algorithms for best service selection. It also integrates a brokering model and enforces rules about workload portability/interoperability.

Another case is Arjuna [11], a dynamic federated cloud computing platform that is created for IT resources offered by autonomous, cooperating business parties within and beyond an enterprise, and under certain policies. *Arjuna Agility* creates a dynamic pool of IT resources that are offered from different administration departments, and under certain policies and relies on SLAs. The administrator of each set of resources can add or remove resources to/from Agility. Each administrator defines his policies with respect to Agility's use of those offered resources, namely the conditions under which, and by whom, the resources may be utilised. Agility seamlessly extends the internal computing utility across organisations, thus create a federation across multiple enterprises and organisations.

Additional cases are the Deutsche Börse Cloud Exchange [12] supporting advanced economic mechanisms, namely spot and futures markets, and the UK-based CloudStore [13], supporting public, private and hybrid clouds and IaaS, SaaS, PaaS and Specialist Cloud Services.

Related work on federations also provides useful lessons learned for the 5GEx project, regarding the multi-operator collaboration, the required business coordination and technical alignment of services and business processes, SLAs, value propositions, business models and charging principles. A brief overview on how 5GEx could leverage on the previous initiatives is provided here below.

Since the ETICS community is focused on interconnection, the community concept, variants and rules from the *Open Association*, *Federation*, and *Alliance* interconnection community types are valuable lessons for 5GEx. Moreover, the ETICS Sending Party Network Pays principle as the cornerstone for inter-operator compensation for multi-domain services, should also be assessed and potentially adapted by 5GEx.

CDNi also contributes interesting use cases and collaboration models among the CDNi members, including the bilateral agreement and the exchange model, as depicted in Figure 2-4. The recommendation that CDN exchanges must be provided by a neutral party can also be adapted by 5GEx regarding the actor-role model. Additional lessons learned concern:

- Pricing of wholesale services, which must be clearly articulated with the additional value created (e.g., quality of experience, reporting, scalability).
- SLA measurements and monitoring, critical to the creation of retail contracts.
- Federation architecture must be developed with openness in mind, since participants will come to the table with their own legacy architectures and network technologies.
- The observation that multiple federations will exist to serve a variety of international and country-specific needs is of high value to 5GEx architecture and actor-role model.
- Technologies and functions that simplify and help automate operation processes such as discovery and dynamic content acquisition will be key success factors.

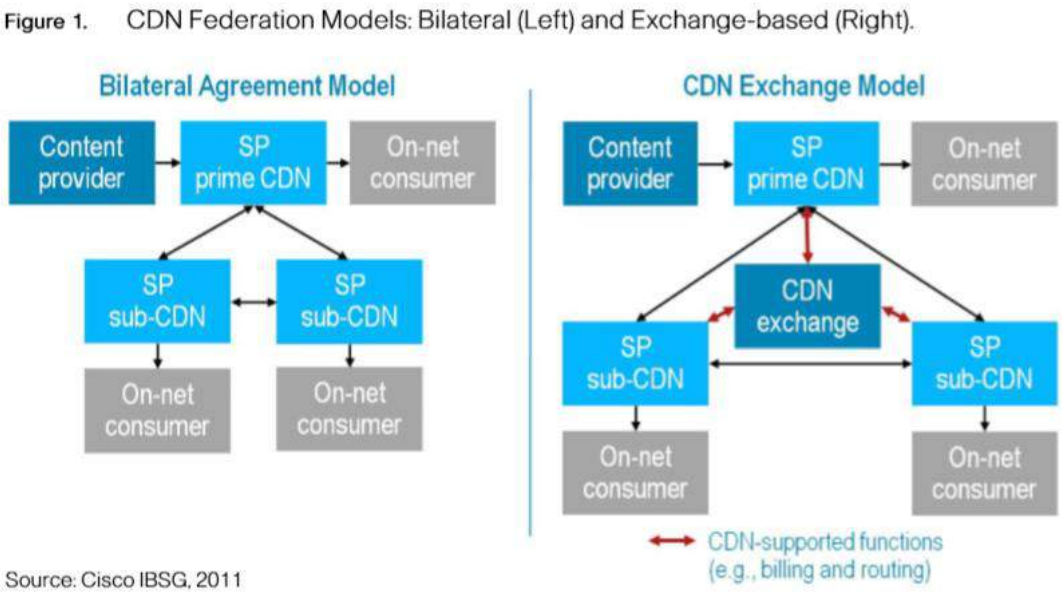


Figure 2-4: The CDN Federation coordination models envisioned by [8]

Cloud federations such as OnApp [9], also provide useful lessons learned, in particular:

- Interoperability of different (cloud) platforms is the key factor for a global infrastructure federation.
- Additional revenues are the main incentive of collaboration and participation in a federation.
- Finally, the federation could be transparent to customers.

The same last lesson learned also comes from Arjuna [11], which additionally stresses as, in the federation of Infrastructure providers, each provider can share resources according to self-defined flexible policies. An additional lesson is that dynamic monitoring of applications performance is required, in order to manage resources for avoiding violation of SLAs in the Service layer, and here as well it's prominent that the federation could be transparent to its customers.

Similarly, Cloud28+ [10] emphasises the need for fair comparison of available services versus customer requirements and proposes a unified catalogue of available federation services. Furthermore, an additional lesson learned is the potential of the brokering model and the importance of enforcing rules for portability/interoperability.

Finally, additional cases such as the Deutsche Börse Cloud Exchange [12] and the UK-based CloudStore [13], emphasise the importance of efficient allocation/trading mechanisms, including advanced economic mechanisms such as spot and futures.

2.2 Commercial solutions

There are available several commercial solutions in line with 5GEx scope[3]. For simplicity, few of them will be described here (based on public information) as examples of solutions that could be extended to cover 5GEx solution.

All these commercial solutions are intrinsically conceived for single administrative domain scenarios. Up to our knowledge, multiple administrative domain scenario has not been yet addressed by any commercial solutions in place. 5GEx can result in a guidance for any commercial solutions towards targeting the multiple administrative domain problem, following the architectural principles and the interface specifications developed in the project.

There is a continuous evolution in the comercial offerings and the Solutions provided by vendors. Both NDA constraints and multiplicity of options prevent 5GEx partners to provide and extensive list of alternatives here. We have chosen probably the most relevant ones at the time of writing, to the best of our knowledge. However we acknowledge the dynamicity of the market, so we refer the reader to the periodic reports and surveys made available by specialized media[4] for an up-to-date overview of existing commercial solutions. These kind of reports and surveys are made free and public but requiring a registration for accessing them. Recent examples of these reports are the LightReading's "SDN/NFV: Market Update" report of the SDxCentral's "Mega NFV Report", "Future of Network Virtualization and SDN Controllers", or "Lifecycle Service Orchestration Market Overview" reports.

2.2.1 Netcracker

Netcraker portfolio offers solutions for both Service Orchestration and Network Orchestration.

The Service Orchestration component is intended to enable cross-domain service lifecycle management across all kind of networks, including legacy networks, SDN-enabled networks, and cloud and NFVI environments. This provides a consolidated view of service processes and service inventory across such domains. Through this capabilities it is in principle possible to enable closed-loop control, unifying service fulfilment and assurance for physical and virtual networks. The following figure presents the framework of the Service Orchestration proposed by Netcracker.

[3] A broad and concise collection of solutions can be found in the 2016 Mega NFV Report Part I, from SDX Central, available at https://www.sdxcentral.com/wp-content/uploads/2016/04/SDxCentral-Mega-NFV-Report-Part-1-MANO-and-NFVI-2016-B.pdf. Solutions falling under the category of Orchestration are those in line with 5GEx project matters.

[4] LightReading: http://www.lightreading.com/, and SDxCentral: https://www.sdxcentral.com/

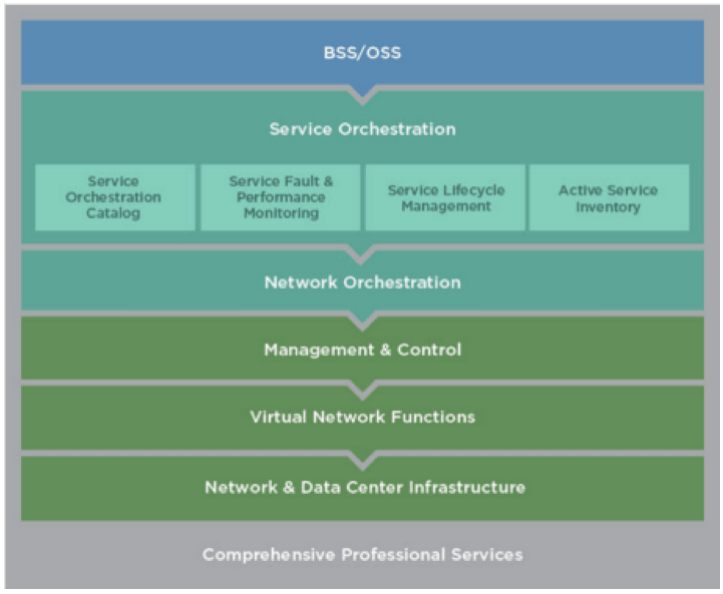


Figure 2-5: Netcracker's Service Orchestration components

In addition to that, Netcracker complements its offer with Network Orchestration capabilities. In this case the objective is to offer means for on-boarding multivendor virtual network functions (VNFs), unify policy-based service fulfilment and assurance for virtual networks and control network service and VNF lifecycles. It is claimed to optimise VNF performance by intelligently deploying them based on security, performance and latency requirements.

Netcracker offering fully complies with ETSI MANO architecture with the idea of seamlessly managing and operating multi-vendor VNF ecosystems. It provides an automated import of YANG service and resource models, and OASIS TOSCA deployment templates for simplified VNF on-boarding. The following figure presents this framework.

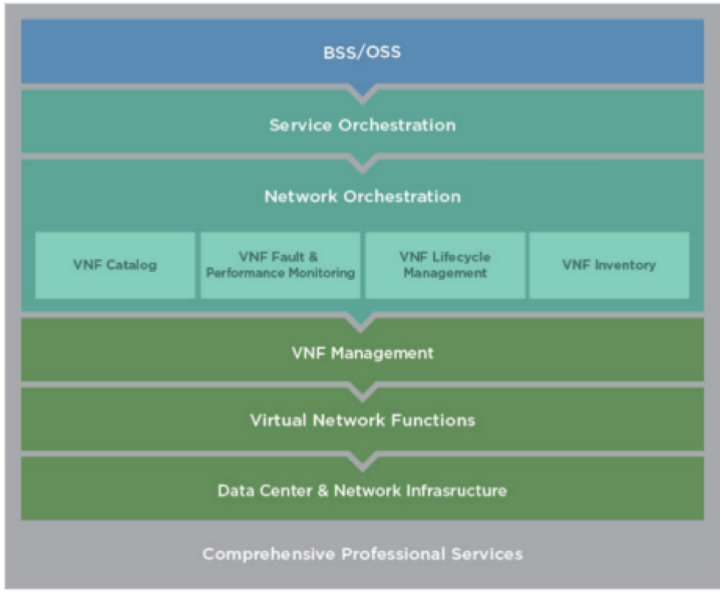


Figure 2-6: Netcracker's Network Orchestration components

2.2.2 CENX

CENX commercialises a solution named Exanova built on an open, vendor-agnostic, and network agnostic architecture, leveraging a wide range of existing OSS and IT data sources. Exanova offers capabilities for workflow orchestration and policy-driven capacity planning.

Focusing on the former, Workflow Orchestration is developed in order to unify and automate workflow activity and service orchestration capabilities across traditionally disparate, siloed systems, multi-vendor infrastructure, and inter-provider networks.

The aim is to decompose existing business processes breaking them down into consistent, well-defined tasks that can be scheduled in sequences, for later on being assigned to resources. APIs are used to send and receive notifications and alerts from northbound and southbound systems interacting with workflows, ensuring interoperability across systems.

The main modules of Exanova solution are shown in the following figure.

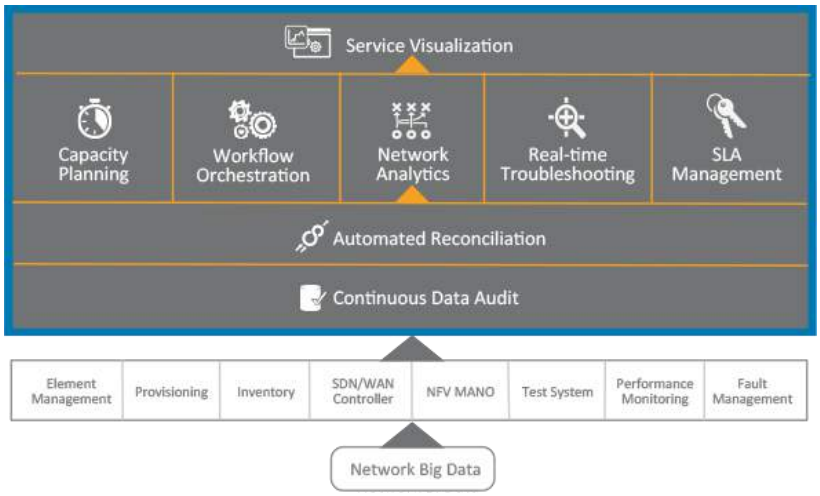


Figure 2-7: CENX' Exanova framework

2.2.3 Ciena's Blue Planet

Ciena offers Blue Planet as orchestrator. This product was developed by an acquisition of Ciena, a company named Cyan.

Blue Planet aims to allow the creation and deployment of services end-to-end. A network operator's infrastructure is comprised of multiple technology layers and specialised domains such as cloud, metro, access, and core networks. This environment entails updating multiple vendor- and domain-specific element managers and/or SDN controllers.

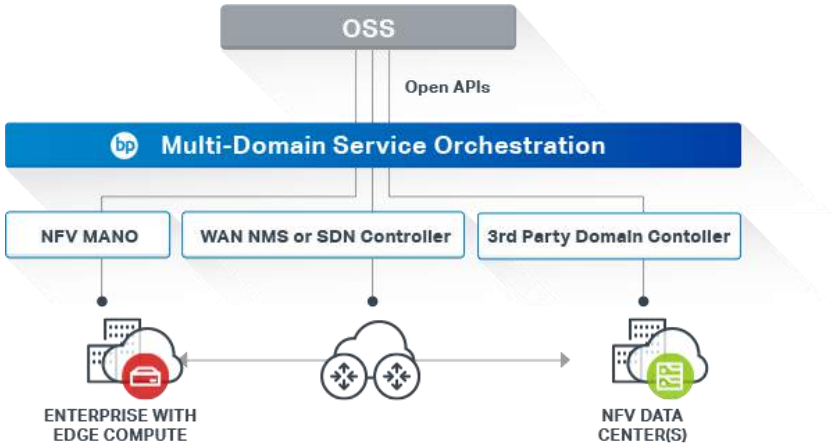


Figure 2-8: Blue Plane scope

Blue Planet claims to support Multi-Domain Service Orchestration (MDSO) capabilities, providing an open software layer with the intention of eliminating management silos and enabling network operators to automate end-to-end service provisioning and orchestration. Leveraging open APIs and model-driven templates, Blue Planet integrates with third-party SDN controllers, element/network management systems, and orchestration platforms to manage and orchestrate services comprised of physical and virtual resources across multiple technology and vendor domains.

2.3 Software networks architectures

Due to software nature of the 5GEx architecture, it is relevant to analyse related software networks architectures, as defined by the main standardisation bodies.

Many organisms are focusing their efforts on the creation of new specifications and the revision of their current architectural frameworks and models in order to integrate SDN and NFV technologies, and this work represents a valuable and important landmark for the development of 5GEx activities.

The following sections reports a summary of the main activities being developed at the standardisation bodies with reference to Software Network Architectures. For every organisation an analysis of general principles, aspects and current results is reported.

2.3.1 ETSI Network Function Virtualisation (NFV) ISG

The ETSI NFV ISG (Industry Specification Group) is probably the most relevant standardisation initiative so far arisen in the Network Function Virtualisation domain. It was incepted at the end of 2012 by a group of top telecommunication operators, and has rapidly grown up incorporating other operators, network vendors, ICT vendors and service providers. To date, the ETSI NFV ISG can count on over 270 member companies. It represents a significant case of joint collaboration among heterogeneous

and complementary kinds of expertise, in order to seek a common foundation for a multi-facet problem like NFV towards a solution as open and scalable as possible.

The ETSI NFV roadmap foresaw two major phases. The first one was completed at the end of 2014, where a number of specification documents were issued[5], covering functional specification, data models, PoC description, etc. The second and final phase is closing in the current timeframe, and will release the expected final version of the ETSI NFV specification documents. The work of the ISG is further articulated into dedicated working groups. In phase 1 three WGs have been created, dealing with Network Function Virtualisation Infrastructure (NFVI), Management and Orchestration (MANO) and Software Architectures (SWA). In phase 2, two additional WGs were spawned, IFA (Interfaces and Architecture) and EVE (Evolution and Ecosystem).

The currently acting specification of the ETSI NFV architecture has been released in December 2014, and its high level picture is shown in Figure 2-9.

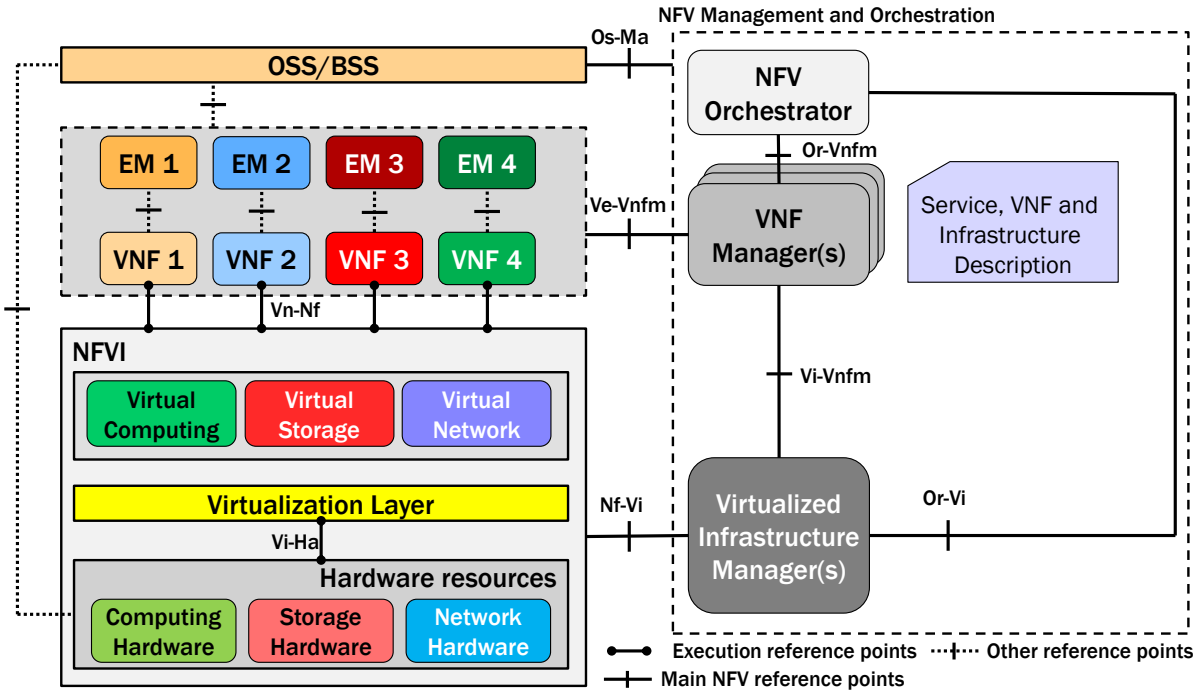


Figure 2-9: ETSI NFV architecture

The ETSI NFV specification defines the functional characteristics of each module, their respective interfaces, and the underlying data model. The data model is basically made up by static and dynamic descriptors for both VNFs (Virtual Network Functions) and Network Services. These latter are defined as compositions of individual VNFs, interconnected by a specified network forwarding graph, and wrapped inside a service.

[5] Available at http://www.etsi.org/technologies-clusters/technologies/nfv

The ETSI NFV framework specifies the architectural characteristics common to all the VNFs. It does not instead rule out which specific network functions can or should be virtualised, leaving this decision up to the network function provider (apart from the use cases advised for the proofs of concept).

The ETSI NFV architecture supports multi-PoP configurations, where a PoP is defined as the physical location where a network function is instantiated. A PoP can be mapped to a datacentre or a datacentre segmentation isolated from the rest of world. Thus, supporting multi-PoP configurations pertaining to different administrative domains means supporting the multi-domain concept at the foundation of 5GEx.

A summary description of the modules in the ETSI NFV architecture is as follows:

Virtualised Network Function (VNF)	Virtualised instance of a network function traditionally implemented on a physical network appliance.
Element Management (EM)	Component performing the typical network management functions (FCAPS) requested by the running VNFs.
NFV Infrastructure (NFVI)	Totality of hardware/software components building up the environment in which VNFs are deployed, managed and executed. Can span across several locations (physical places where NFVI-PoPs are operated). Include the network providing connectivity between such locations.
VIM (Virtualised Infrastructure Manager)	Provides the functionalities to control and manage the interaction of a VNF with hardware resources under its authority, as well as their virtualisation. Typical examples are cloud platforms (e.g., OpenStack) and SDN Controllers (e.g., OpenDaylight).
Resources	• Physical resources (computing, storage, network). • Virtualisation layer.
NFV Orchestrator	Component in charge of orchestration and management of NFVI and software resources, and provisioning of network services on the NFVI.
VNF Manager	Component responsible for VNF lifecycle management (e.g., instantiation, update, query, scaling, termination). Can be 1-1 or 1-multi with VNFs.

The ETSI NFV framework assumes the existence of an outside OSS/BSS layer in charge of the basic datacentre/service management functions.

The list of documents authored by the ETSI NFV ISG specifies, among the others:

- General VNF architecture.
- MANO (MANagement and Orchestration) layer architecture.

- NFVI infrastructure architectural guidelines.
- SDN usage and interfacing within an NFV system.
- Different specifications concerning privacy, security and resilience.
- Quality metrics.
- Detailed interface specifications.

2.3.2 ETSI Open Source MANO (OSM)

During 2016 ETSI has launched the Open Source Mano (OSM) initiative. OSM intends to develop an Open Source NFV Management and Orchestration (MANO) software stack aligned with ETSI NFV specifications. This kind of Open Source software initiative can facilitate the implementation of NFV architectures aligned to ETSI NFV specifications, increasing and ensuring the interoperability among NFV implementations.

2.3.3 TM Forum

The TM Forum (TMF) has rolled out the ZOOM program – Zero-touch Orchestration, Operations and Management – to develop Virtualisation and NFV & SDN best practices and standards. The goal is to create a living blueprint for a new generation of service provider support systems, to deliver true business agility and new digital services and revenue opportunities[6].

The following topics (among others) are addressed:

- Specification updates on the Information Model to manage and correlate diverse and disparate data from managed systems addressing the out-of-scope management areas for ETSI MANO.
- Specification updates on Policy Management rules, to manage Access Control and the integration of the Policy model fragment into the ZOOM model.
- Security: Linking Access Control Policies to the Privacy initiative.
- API Requirements.
- Future OSS Architecture.
- Definition of the concept of Orchestration and how it relates to Policies and architectural entities.

The most recent documents produced are part of Framework release 15 or 15.5, and all are of TMF Maturity Level 3 (Team Approved). A brief overview including document purpose and scope is provided hereafter (the text is borrowed from the TMForum web site). These documents are considered of relevance to 5GEx. Other TMForum documents from other

[6] For more information, see: https://www.tmforum.org/zoom/frameworx-15-0-foundational-studies/#form

programs or projects might also be relevant to 5GEx. Consider for instance the following: Open Digital Ecosystem / Open Digital Project, APIs and Developers, and Smart City.

- TR224 Identity and Naming
    - Designing a name and identifier scheme for network management is difficult and has many subtle traps. The existing identity and naming schemes used for TM Forum management interfaces were designed to support traditional network elements, not software functions that can traverse a network.

      This document aims to provide an identity and naming scheme that supports traditional network elements, virtual network elements and movable software functions, giving us a complete and robust solution for the future. We will also provide a migration path that can be applied to existing models.
- TR225 Logical Resource: Network Function Model
    - This Technical Report combines the work done in TR215 on Forwarding Relationships with earlier work on Termination Points and Connection-oriented Connectionless Convergence. It starts with a framework model proposal, defines the terms in the framework model and then builds on the framework to provide functionality equivalent to the existing MTOSI and SID models. We can think of this as defining the skeleton model which provides the core support, and then fleshing out the details using that supporting structure. This document will focus on 'moving forward' and will only include earlier work when it is needed to help in understanding as we build up the new model. The new model is designed for the future; it must support data centre, virtualisation, SDN, NFV and other current initiatives – as well as supporting the existing legacy network.
- TR227 TM Forum Specifications relevant for MANO Work
    - This TM Forum ZOOM deliverable identifies the potential applicability of TM Forum specifications to areas of work of MANO.
    - The document addresses areas where TM Forum specifications can help to standardize the information presented and interfaces of the MANO reference points. These areas refer to the Information, Integration and Business Process Frameworks.
    - As result a contribution was provided to ETSI NFV for its consideration.

- TR228 TM Forum GAP Analysis related to MANO Work
  - This report provides an initial ETSI NFV MANO Gap Analysis (based on MANO GS V0.3.9) with respect of TM Forum specifications for MANO Interfaces and Information Elements. The analysis compares TM Forum specifications to MANO in order to determine the set of features and functionality described in ETSI NFV MANO that cannot be met by the TM Forum specifications.
  - The gap analysis covers both the NFV orchestration and management architecture interfaces, and the NFV orchestration and management descriptors.
  - The resulted gap analysis was contributed to ETSI NFV.
- TR244 TM Forum Information Framework enhancements to support ZOOM
  - This document describes a portion of the ZOOM information model, which has been integrated into the Information Framework. It defines four concepts fundamental to modelling NFV-based systems (VirtualResource, NetworkFunction, NetworkService, and Graph), as well as two general-purpose concepts (Catalogue and Event) that have been used by existing Catalysts, and are also generally critical for realizing SDN and NFV systems.

2.3.4 Open Networking Foundation (ONF)

The ONF is a member-driven organisation aiming to promote the adoption of SDN through the development of the well-known OpenFlow protocol as open standard for the communication between the controller and the data forwarding network elements. Ultimately, ONF is also transforming into an organisation promoting Open Source developments as a way of consolidating impact in the Industry.

Apart from OpenFlow specifications development, ONF is very active in the definition of architectures around SDN, independently of the protocol to be used for accessing and configuring the equipment (the so called South Bound Interface from the controller perspective).

ONF is structured in several working groups (WGs). Some WGs are focused on defining extensions to the OpenFlow protocol tailored for enabling SDN capabilities in specific technological areas like the Open Transport (OT) WG, the Mobile (W&M) WG, and the Northbound Interfaces (NBI) WG. On the other hand, some other WGs focus their activity on providing new protocol capabilities which can enhance the protocol itself, like the Architecture WG or the Migration WG.

A number of initiatives in ONF are relevant to 5GEx, listed as follows:

- Architecture definition. The Architecture WG releases architectural specifications for SDN. The two main specifications are [39] and [40]. Both specifications provide insight on SDN architectural matters, with emphasis on the controller capabilities and the interfaces with the other elements in the architecture (applications on top, devices below). Relevant to 5GEx, the latest report, SDN Architecture - Issue 1.1 introduces an initial idea about the interaction of Peer Controllers, as reflected in Figure 2-10, where basically each of the controllers may act as client to invoke services from the other as server (being A-CPI the Application-Controller Plane Interface, and D-CPI the Data-Controller Plane Interface). The relationship among controllers is then proposed to be equivalent to the hierarchical provider/customer relationship that we are evaluating in the 5GEx architecture (see Section C.1.3).

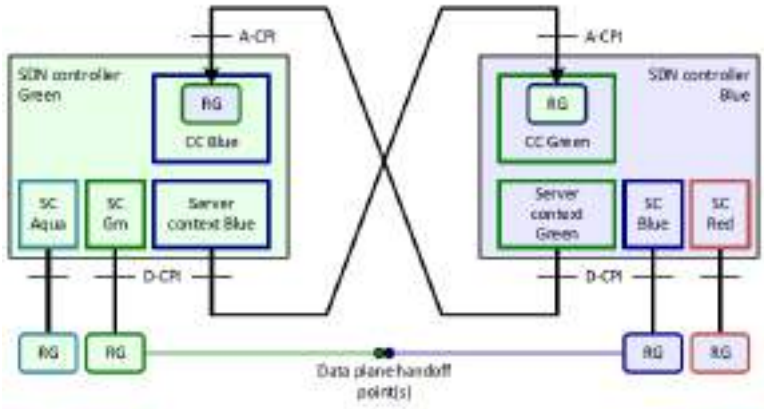


Figure 2-10: Peer controllers in the ONF architecture

- APIs between layers. The APIs are defined at interface boundaries for interaction between layers in the SDN architecture. There are a number of initiatives in ONF exploring APIs between layers. From 5GEx perspective, two of them are of special interest. The Transport API (publication pending) specifies an API for the following transport network controller services:
  - Topology Service.
  - Connectivity Service.
  - Path Computation Service.
  - Virtual Network Service.
  - Notification Service.

  These APIs are defined to be applicable on the interface between a Transport SDN controller (with a Black Box approach) and its client application (i.e., transport network application systems).

  The functional architecture of the T-API is depicted in Figure 2-11.

  On the other hand, the North Bound Interface (NBI) group is working on Intent based NBIs. This work defines the principles governing Intent

NBIs between Application Plane systems and Controller Plane systems (i.e., Intent NBI is an A-CPI). Intent NBI is a service, or service-oriented, interface. An Intent NBI expresses what a network service-consuming agent (i.e., an application or operator) requires from a network (i.e., it defines a requested network service) but it does not specify or constrain how that service may or should be delivered by the network.

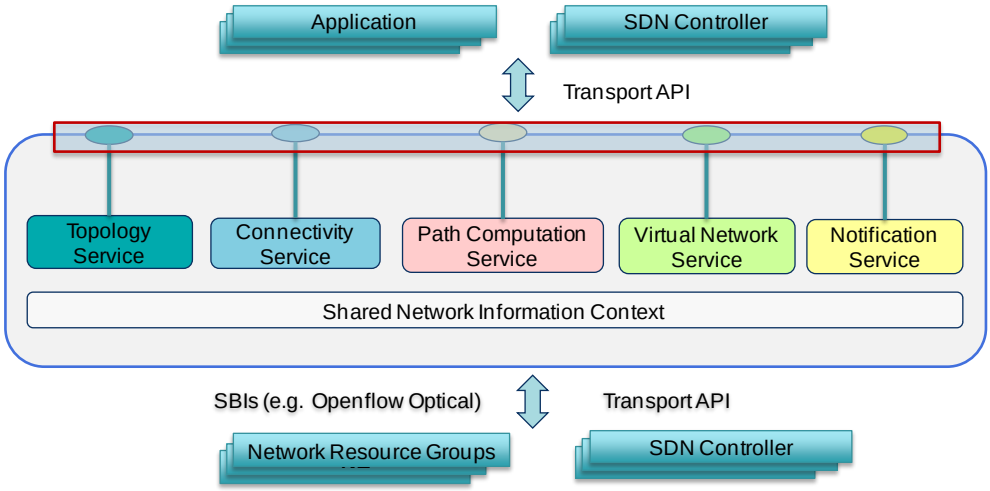


Figure 2-11: ONF T-API functional architecture

- Carrier Grade SDN. The Carrier Grade SDN WG is working on a framework document (publication pending) where a number of requirements are identified to accomplish a truly operational SDN from the perspective of network operators and service providers. Aspects like the ability to deliver managed services end-to-end, SLA compliance, Service Operations and Maintenance capabilities, etc. are highlighted as core of an SDN Carrier Design. These topics are for sure relevant in single domain environments, but they become much more critical in multi-domain environments. The Carrier Grade SDN framework document also describes some of these issues considering Inter-Carrier interoperability and Interoperability/co-existence between SDN and Legacy networks. Figure 2-12 presents a schema of the multi-carrier approach being considered in the document. 5GEx project is cited in such document as exemplary project analysing the multi-domain aspects.
- Slicing for 5G. The Mobile WG is producing a report for the application of SDN to 5G slicing. This document is in its preliminary steps. The idea is to describe how key functional aspects of the SDN architecture apply for 5G enablement, including the business-driven concept of network slicing. In particular, the SDN architecture supports the ability of defining network slices created on demand on dynamically determined endpoints and resources. Ideas like the one proposed in [41] are also being considered in this group.

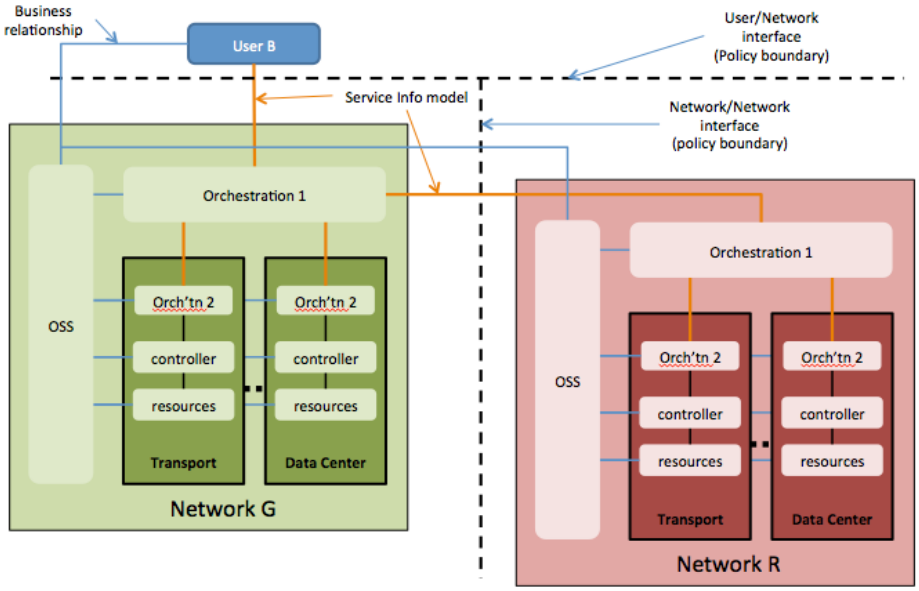


Figure 2-12: Multi-carrier approach in the ONF Carrier Grade SDN framework document

2.3.5 Metro Ethernet Forum (MEF)

The MEF LSO (Lifecycle Service Orchestration) Reference Architecture [42] proposes a multi-domain orchestration model (see Figure 2-13).

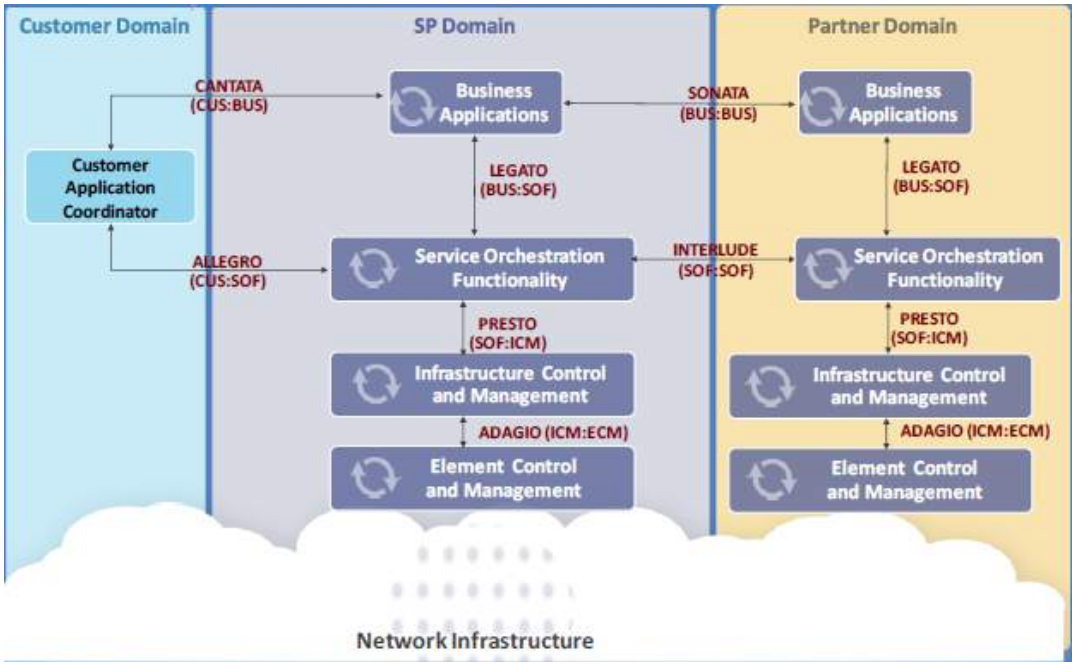


Figure 2-13: MEF LSO architecture

LSO proposes an open and interoperable automation of control and management operations over the entire lifecycle of Layer 2 and Layer 3 Connectivity Services. This includes design, fulfilment, control, testing, problem management, quality management, billing & usage, security, analytics and policy capabilities, over all the network domains that require coordinated management and control in order to deliver the service.

LSO intends to define both information and data models for a later definition of open and interoperable APIs (including virtualised functions, e.g., SDN and NFV).

The following functional management capabilities are considered in LSO, as documented in [42]:

- Business Applications (BUS): The Service Provider functionality supporting Business Management Layer functionality (e.g., product catalog, ordering, billing, relationship management, etc.).
- Service Orchestration Functionality (SOF): The set of service management layer functionality supporting an agile framework to streamline and automate the service lifecycle in a sustainable fashion for coordinated management supporting design, fulfilment, control, testing, problem management, quality management, usage measurements, security management, analytics, and policy-based management capabilities providing coordinated end-to-end management and control of Layer 2 and Layer 3 Connectivity Services.
- Infrastructure Control and Management (ICM): The set of functionality providing domain specific network and topology view resource management capabilities including configuration, control and supervision of the network infrastructure. ICM is responsible for providing coordinated management across the network resources within a specific management and control domain. For example, a system supporting ICM capabilities provides connection management across a specific subnetwork domain. Such capabilities may be provided within systems such as subnetwork managers, SDN controllers, etc.
- Element Control and Management (ECM): The set of functionality supporting element management layer capabilities for individual network elements. While a system supporting ECM capabilities provides for the abstraction of individual infrastructure elements, it may reflect the element view for multiple elements, but not provide coordinated management across the set of elements.
- Customer Application Coordinator (CUS): A functional management entity in the Customer domain that is responsible for coordinating the management of the various service needs (e.g., compute, storage, network, etc.) of specific applications. The AC may be responsible for the harmonisation of cloud services on behalf of multiple applications. The AC supports Customer interactions with the Service Provider to request, modify, manage, control, and terminate Products or Services.

These functional management capabilities are considered for the LSO interface reference points as reflected in Figure 2-13.

Co-operation between Carriers takes place at the higher level through the Inter-Carrier orchestration API that exchanges information, functions and control ("Sonata" and "Interlude" in LSO). These interfaces serve for

the Business-to-Business and Operations-to-Operations relations between Carriers to complement the Business-to-Customer relations. Domain orchestrators ("Presto" in LSO) and controllers ("Adagio" in LSO) operate during the orchestration, control, and enforcement of domain policies required for multi-domain orchestration. This approach allows for a clear demarcation between the inter-domain elements and the intra-domain elements, while still ensuring the flexibility to handle both and keeping local infrastructure details confidential and hidden from neighbours. The multi-domain orchestrator is in charge of abstracting the underlying infrastructure before it announces what utilities and functions the operator is capable of to its neighbouring Carriers.

2.3.6 Broadband Forum (BBF)

The Broadband Forum (BBF) is focused on engineering smarter and faster broadband networks. Its work defines best practices for global networks, enables new revenue-generating service and content delivery, establishes technology migration strategies, engineer's critical device, service & development management tools, in the home and business IP networking infrastructure. It develops multi-service broadband packet networking specifications addressing architecture, device and service management, software data models interoperability and certification in the Broadband market.

SDN and NFV are currently under study and development in the BBF mainly in the "SDN and NFV" and "Architecture and Migration" Work Areas.

With reference to "SDN and NFV" Work Area, and more specifically to Virtualisation technology, the working text WT-359 "A Framework for Virtualisation" is being developed. The purpose of this working text is to revisit the current Reference Architecture in order to establish a framework to effectively reference and specify systems in order to facilitate the deployment of NFV (as defined by the ETSI NFV ISG) to BBF specified networks. The objective is to combine the BBF and ETSI NFV reference models in order to have the respective functional components and reference points together for the management and control of services along with the interworking of the user/data plane.

Moreover, a couple of working texts (WT-328 Virtual Business Gateway and WT-317 Network Enhanced Residential Gateway) are in an advanced state and almost in phase of completion. The first, WT-328, specifies architecture and requirements for the virtual business gateway. The work is related to the migration of functionalities running on a business gateway to the network service provider infrastructure for enabling network-based features and services. Such migration is expected to simplify the deployment and management of the network and business services. The second, WT-317, specifies the Network Enhanced Residential Gateway (NERG) architecture. NERG consists in shifting some of the functionalities of a residential gateway (RG) to the operator's

network. In this way the functions traditionally provided by the RG are now distributed between the on-site device called BRG (Bridged Residential Gateway) and a network based component, called vG (virtual Gateway). The vG is a flexible hosting environment that can benefit both from network equipment and network virtualisation technology.

With reference to the SDN technology, the Study Document SD-365 is being developed. This document is related to the definition of a new BBF SDN Architecture Reference Model, and once completed it should be inserted in the issue 2 of the document WT-359 "A Framework for Virtualisation", described above. Several contributions from partners of the FP7 Research Project "Unify" and related to the "Unify" project have been proposed and accepted to be part of this document, with the aim to create a section related to the ecosystem of already existing architectural frameworks.

On the other hand, in the "Architecture and Migration" Work Area, the WT-345 (Broadband Network Gateway and Network Function Virtualisation), almost in phase of completion, represents a first attempt to define a framework for the introduction of Network Function Virtualisation into the BBF Architecture models, based upon enhancements to the hierarchical BNG model and providing migration paths to the deployment of NFV infrastructure in existing BBF networks as well. It has to be considered as an augmentation of the work previously done with the hierarchical BNG model definition, examining all the implications of introducing virtualisation with regard to aspects like traffic management and QoS, data plane OAM, resilience, basic service chaining and steering of selected flows from a subscriber IP session into the NFV infrastructure. On the other hand, other aspects like VNF definition, Service & Cloud orchestration and system reliability beyond that of the network infrastructure are out of scope for this work. The Working Text also introduces a new element: the NFVI GW, whose role is to interwork the WAN transport with the NFVI.

Finally, a new project relative to 5G has been initiated in BBF. The name of this project is "5G Requirements and Enablers" and it is related to the exploration of 5G use cases, architectures and requirements, in order to identify relevant components and aspects to be addressed and provided as enablers by BBF. The new initiative aims to lay the motivations, analyse the use cases for 5G discussed in the industry, and identify components and aspects to be addressed by BBF, with the objective to:

- Extend the principle of 5G to wireline accesses.
- Provide a service oriented programmable network, customizing network functions and applications instead of a single physical network infrastructure for all the services.
- Go beyond simple improvement of bandwidth for mobile broadband, delivering on the promise for consumers expecting to

be ubiquitously connected, no longer having to care whether they are served through wireless or wireline access.

- Make the aggregation segment agnostic to access technologies.

2.3.7 IEEE Next Generation Service Overlay Network (NGSON)

With the proliferation of services and the need to provide richer experience to users offered by the blending of services from various service providers, the complexity of service control and delivery operations grows significantly. In order to allow network and computing service providers, content providers and end-users to offer and consume collaborative services, there is a need for an efficient way of service and application delivery that at the same time is customer-centric. This is a challenge that has not been sufficiently addressed by the prior Service Delivery Platforms (SDPs) that ended up managing service delivery and QoS support only within the same administrative domain (i.e., silos approach) [24]. Therefore, there has been a motivation to organise the services/applications offered by various networks on an overlay allowing service providers to offer richer services [29]. According to this approach, the Service Overlay Network (SON) was developed to provide a common infrastructure for delivery of different value-added Internet services over heterogeneous networks. However, the SON initiative proved to have an intrinsic limitation to handle diverse and dynamic environments of users, services and networks characteristics of recent service scenarios, such as those enabled by 5G technologies [24]. With the current trend of pervasive and ubiquitous computing technology and services, user requirements and expectations are highly diverse in terms of users, devices, service and networks. Indeed, users expect different service configurations even for the same service if accessed through different devices or in different user situations (i.e., location, network access). The heterogeneous and dynamic characteristic of service control and delivery affect not only the user environment but also the service and network environments.

To address such requirements, the Next Generation Service Overlay Network (NGSON) standard was developed in IEEE [23]. The NGSON standard specifies a framework for control and delivery of composite services over diverse IP-based networks (e.g., Internet, P2P overlay, IMS, PSTN, Mobile) with context-aware, dynamically adaptive, and self-organizing networking capabilities including advanced routing and forwarding schemes, that are independent from underlying networks. As result, a better quality of experience can be assured to users by customizing and adapting composite services to the dynamic context of users, devices, services, and networks, at the same time optimizing network and computing resources consumption. Ultimately, the NGSON standard establishes a reference framework for an open service ecosystem where different stakeholders (e.g., network and computing service providers, content providers, third party) may cooperate to utilise

and dynamically compose each other's services in a highly distributed environment to satisfy users' ever changing requirements.

Context-awareness is a distinguishing feature of NGSON. Context-aware capability allows to monitor any information that can be used to characterise the circumstances or situations under which the services operate. According to collected context information, NGSON automatically adapts its behaviour to react to any significant context changes. In this sense, context awareness is ultimately related with both dynamic adaptation and self-organisation. Notions of dynamic adaptation and self-organisation are correlated at service level but each has its own unique features. Self-organisation focuses on maintaining integrity and optimising the performance of service overlay network. Dynamic adaptation focuses on delivering advanced services in which the service execution adapts its operations to the context changes in order to keep continuing the service delivery without any service disruption or quality deterioration [23].

The implementation of context-aware policies in NGSONs is empowered by the fact that the NGSON capability of interworking with different network operators and service providers allows acquiring context information from a plenty of sources. In NGSON, four classes of context have been defined:

- *Service context* includes information that characterises a service, such as service QoS (i.e., execution cost, response time, availability, reputation), service category, service roaming state, service network endpoints, etc.
- *User context* includes information that characterises the status of a user, such as location, presence, environment constraint, current activity, social relations and preferences.
- *Network context* includes information characterizing underlying networks, such as overlay network topology, bandwidth and traffic performance (e.g., delay, packet loss rate).
- *Device context* includes device hardware configuration (e.g., device model, display), software configuration (e.g., operating system, mobile platform) and dynamic status information (e.g., battery power, memory consumption, received signal strength of available access networks).

Context-aware adaptation may be enforced at different levels, as shown in Figure 2-14. At the application and service level, context parameters may be used for driving the dynamic discovery, composition and selection of services. For instance, this may include discovery mechanisms for retrieving those service profiles that match with context information (e.g., user's preferences and current activity), runtime selection and invocation of the service instances closer to user's location (context-aware routing), dynamic substitution of a basic service with another one due to faults or requirement changes (adaptive service composition), as well as selection of content caches or sources according to user location and guaranteed

Quality of Service (QoS) (context-aware content routing). At the network level, NGSON tries to optimise data delivery between an end user and a service endpoint or among service endpoints by negotiating QoS requirements in the underlying networks, while enforcing the proper service data forwarding across the network according to the current context (e.g., user' current activity and location and device capabilities) and required QoS [28].

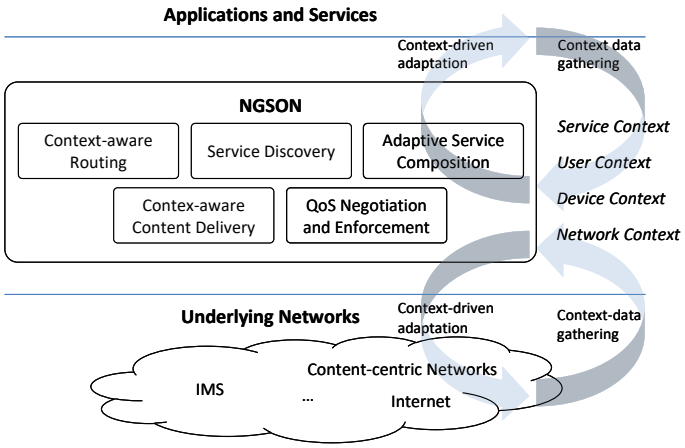


Figure 2-14: Context Awareness in NGSON

Figure 2-15 illustrates a high-level overview of NGSON's functional architecture and shows various supporting functions and external reference points for interacting with external components.

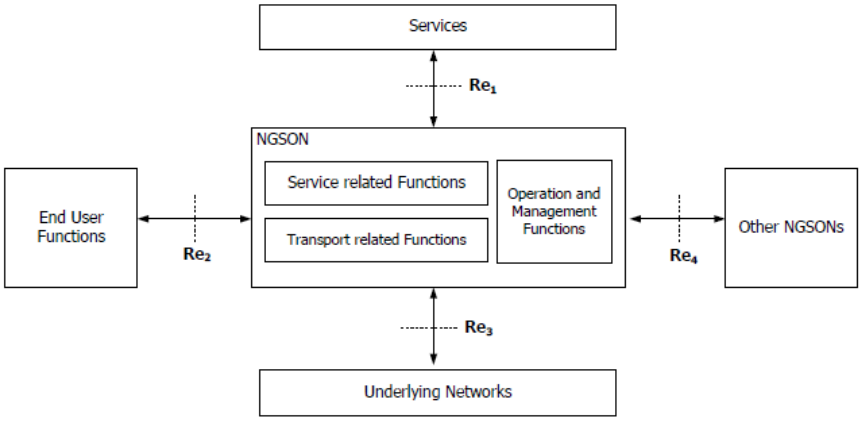


Figure 2-15: Overview of NGSON functional architecture [23]

The NGSON functional architecture includes service-related functions, transport-related functions, and operation and management functions. The service-related functions include functions relating to service control operations, i.e., *service registry*, *service discovery and negotiation*, *service composition*, and *service routing*. The transport-related functions support the delivery of service data between end-users and services or among services by interworking with underlying networks to negotiate and enforce the QoS required in the transport of service data across networks. Operation and management functions are also foreseen such as service management, lifecycle management, and service assurance [24].

The NGSON architecture also specifies four reference points, i.e., Re1, Re2, Re3 and Re4, for interacting with external systems. Specifically, Re1 allows providers to publish their services to NGSON and Re2 enables End User Functions to access NGSON service and content delivery capabilities. NGSON should support existing protocols (e.g., SIP, Diameter and ALTO protocols) to interwork with underlying heterogeneous networks (Re3). A federation of NGSONs can be established through the Re4 reference point.

At the service level, the essential function of NGSON is to route a service request received from an end-user or a service, i.e., service requester, to an appropriate service instance along the overlay network. A service request contains the functional requirements of the target service used during the selection of service instance as well as input data to be delivered to the selected service for interactions. In case of a composite service NGSON also takes a role of aggregating, i.e., orchestrating, the interactions among multiple component services for a single composite service. For example, a "Travel Planner "composite service may aggregate multiple services for flight booking, travel insurance, accommodation booking, car rental, itinerary planning, etc., which are executed sequentially or concurrently. The orchestration of service component interactions is carried out according to service composition specifications defining the service logic to coordinate the invocation of services, i.e., order of service chaining, thereby addressing the provision of a single composite service. To the purpose of orchestration, NGSON integrates service-aware technologies typical of Service Oriented Architectures (SOA) [25] to integrate service components deployed in heterogeneous systems while exploiting context information and adaptation features to dynamically (re-)accommodate service components and their interactions.

Three related standard projects are active around NGSON specifications:

- P1903.1 - Standard for Content Delivery Protocols of Next Generation Service Overlay Network (NGSON) [30].
- P1903.2 - Standard for Service Composition Protocols of Next Generation Service Overlay Network (NGSON) [31].
- P1903.3 - Standard for Self-Organizing Management Protocols of Next Generation Service Overlay Network (NGSON) [32].

NFV and SDN can significantly contribute to achieve greater elasticity in network service deployments and accelerate a prominent innovation in NGSON service provisioning and delivery functions. In particular, SDN and NFV allows service providers to create a more powerful service logics based on NGSON, including virtualised network functions handled as service components and participating to the service composition and orchestration process [28]. In this regard, a liason has been recently established between the IEEE SDN Initiative [33] and the NGSON WG to identify potential new standards in SDN/NFV areas to be developed in IEEE. The goals are to accelerate the proliferation of SDN services and applications and to offer a more efficient way of providing them through a

service-architecture ecosystem of one-stop shopping for service-specific challenges [34].

2.3.8 Internet Engineering Task Force (IETF)

In the Internet Engineering Task Force (IETF) – and also in the sibling organisation, the Internet Research Task Force (IRTF) – there are distinct working groups addressing topics of interest for 5GEx, both from the research perspective (IRTF) and from the normalisation perspective (IRTF). Some of the activities of interest are the following:

- IRTF SDN Research Group. This group has recently adopted a draft document exploring the separation between Service and Transport concerns in SDN [41]. The motivation for this approach is substantiated in a number of problems identified in current architectures:
    - No clear responsibility for service provision and delivery.
    - Complicated reutilisation of components for delivering different services.
    - Monolithic control architectures, driving to lock-in.
    - Difficult interoperability, then difficult interchange of some modules.
    - No clear business boundaries.
    - Complex service/network diagnosis and troubleshooting.

  In order to address such problems, two different strata are defined, one called Service Stratum, the other call Transport Stratum. The scope of the former is to focus on (final) service aspects, leaving to the latter the connectivity concerns for connecting the service end nodes building the end-to-end service requested by applications on top. The architecture is summarised in the figure below.

  This draft also considers multi-domain, for the different strata. Future versions of the document will develop such scenario.
- IRTF NFV RG. The NFV Research group explores issues around NFV. A recent contribution [43] has been released to analyse the gaps about handling of multiple administrative domains in NFV environments.

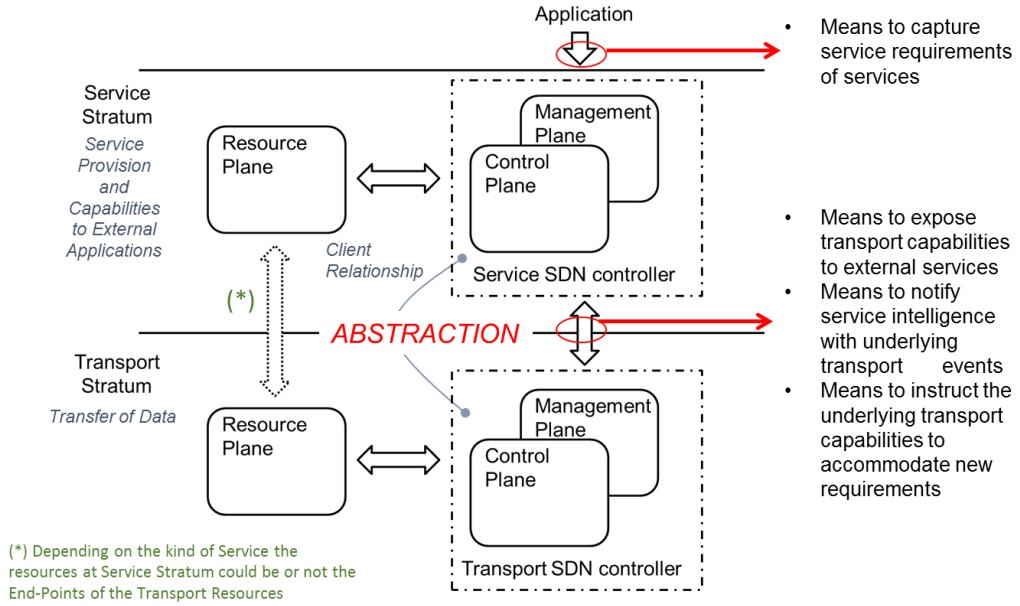


Figure 2-16: Cooperating Layered Architecture for SDN (CLAS)

- IETF TEAS. The Traffic Engineering Architecture and Signaling WG is elaborating a number of specifications around the interchange of traffic engineering information between interconnected networks [44]. Some concepts can be applicable to 5GEx, especially regarding abstraction, as shown in Figure 2-17.

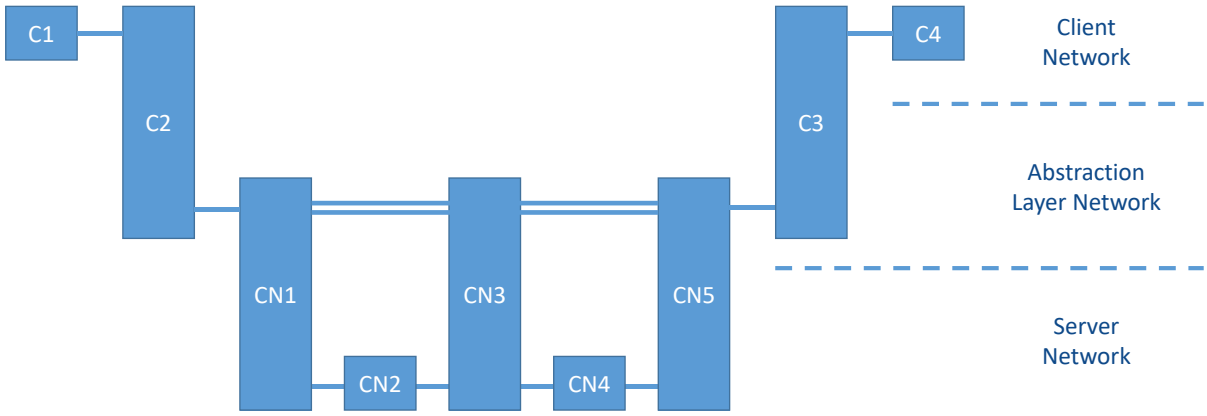


Figure 2-17: Layered Network Abstraction

2.3.9 Network Service Interface (NSI)

The Open Grid Forum (OGF) have been working on the definition of a solution to allow dynamic circuit services in inter-domain scenarios [45]. The aim is to directly provide such circuits to applications that require bandwidth and service quality guarantees through automated management systems provisioning circuits dynamically based on user requests.

The work has been carried out within the OGF's Network Services Interface Working Group (NSI-WG) defining an interface to request such circuits. Both a user-to-network provider interface and a provider-to-provider interface have been specified.

The NSI-WG has published a Network Service Framework document that defines the scope of the Network Service Interface (NSI) protocol [46], over which many network services can be offered. NSI delivers an enabling technology in accordance with the SDN approach. NSI can be used as a north-bound API that supports multi-domain network service delivery and management. It defines several architectural elements:

- The Network Service Interface for the request of services from either an application or from a network provider.
- The NSI Protocol.
- The Network Service Agent (NSA) [47].
- The Network Services, where each service has an associated Service Definition (SD).
- An abstracted inter-network Topology.

Each service is managed by an exchange of NSI Messages between agents. These messages operate using a set of service primitives. Service primitives are the set of instructions that allow the requester to set up and manage a service. Each service request will result in the allocation of a service id for the new service instance.

The Connection Service document [48] describes a service architecture and the protocol for end-to-end circuit provisioning interface. Complementary services, such as a Topology Service and a Discovery Service are not yet specified.

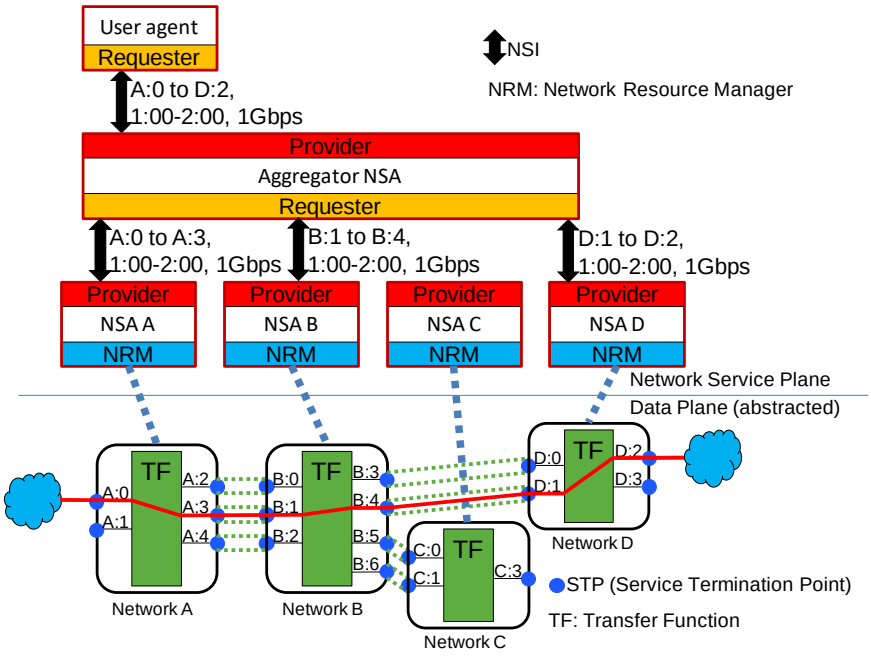


Figure 2-18: NSI Connection Services overview [45]

In the NSI architecture, each provider's network is managed by an NSA, and the NSI Connection Service protocol is the service interface between NSAs. An NSA can take on the role of a requester, a provider, or both. Multiple NSAs can be used to build up a hierarchy of requesters and providers. Requests can be propagated through this hierarchy of NSAs

using a tree or chain workflow. Figure 2-18 graphically shows the chaining capabilities of NSI.

The NSI framework identifies a circuit end point with a Service Termination Point (STP) identifier. STPs are conceptual entities, and by combining the concepts of NSAs and STPs, a mapping between a "service topology" and an abstract representation of physical topology can be realised.

A Network is divided into Service Domains. A Service Domain groups a set of STP that has a common Service Definition. A Network can include one or more Service Domains. Each STP within a Service Domain will be able to be connected to every other STP in the same service domain. Each Service Domain has an associated Service Definition that describes the service offered by the domain. A common Service Definition can be defined for more than one Service Domain, however, each of these Service Domains will offer the described service. Figure 2-19 presents the concept of Service Domain and STP in NSI.

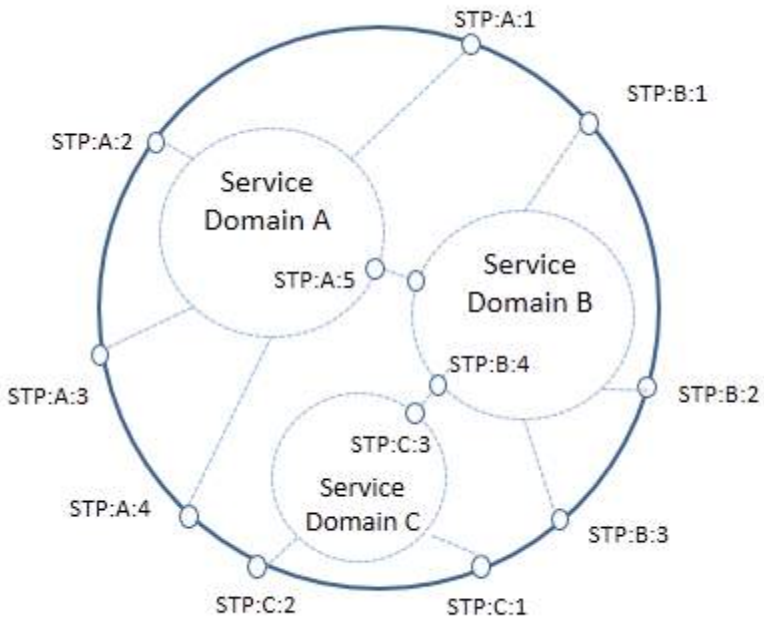


Figure 2-19: Service Domain in NSI [48]

The network topology is used for finding paths. The signaling for that is specified in [49]. Two different ideas of topology are handled in NSI. The Intra-Network Topology refers to the topology of the resources within a Network, where a Network is defined as the group of network resources managed by a single network provider and a single NSA. The Inter-Network Topology refers to the topology of interconnected Networks. Here a Network is a topology object.

The Inter-Network Topology is concerned with describing the way in which Networks are statically interconnected. It treats each Network as

an aggregated set of Network capabilities with Edge Points. Inter-network topology is described using NSI Topology definitions consisting of Networks and STPs. Figure 2-20 depicts the Inter-Network and Intra-Network topology representations.

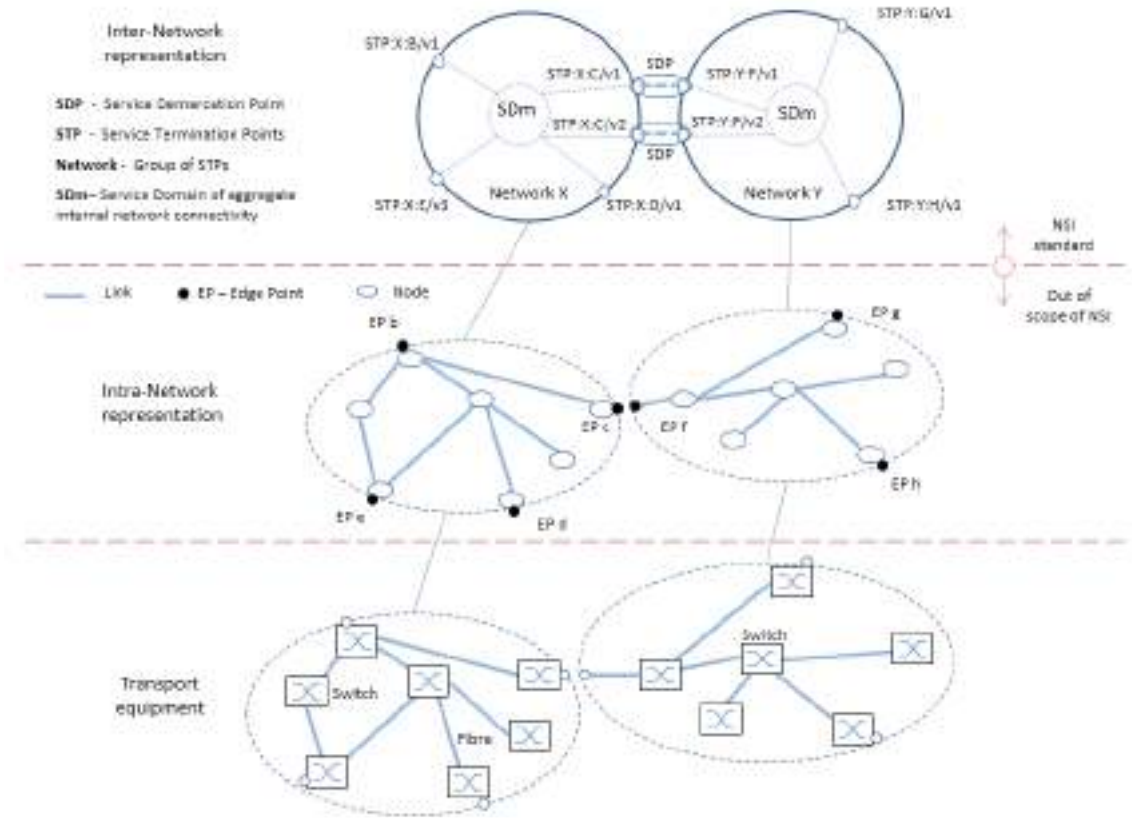


Figure 2-20: Inter-Network and Intra-Network topologies

Using the NSI Connection Service (NSI-CS), a reservation of an end-to-end connection can be requested with a designated start-time and end-time, two end points and certain parameters such as bandwidth.

2.4 Other projects

We next identify and briefly describe other projects related to 5GEx, focusing on the aspects that they have in common and/or are of interest for 5GEx. Note that 5GEx plans to leverage on several outcomes of these projects.

2.4.1 UNIFY

UNIFY is an EU-funded FP7 project, which aims at unifying cloud technologies and carrier networks in a common orchestration framework. This involves a novel service function chaining control plane on top of "arbitrary" domains including different Network Function (NF) execution environments, SDN networks or legacy data centres. By this means, UNIFY fills the gap between the high level orchestration components of ETSI's MANO framework and the available infrastructure domains. The UNIFY architecture supports automated, dynamic service creation based

on a dynamic fine-granular service chaining model leveraging NFV, SDN and cloud's virtualisation techniques.

The main objectives of UNIFY design are the following:

- Establish a general narrow waist SFC control plane for flexible service creation.
- Support joint programming and virtualisation of cloud and network resources.
- Enable recursive orchestration of different types of resources.
- Support different (even legacy) technologies and migration between them.
- Give a future-proof solution by providing an easily extendable architecture.

The overarching view of UNIFY architecture comprises the Service Layer (SL), the Orchestration Layer (OL) and the Infrastructure Layer (IL) with reference points between major components (see Figure 2-21).

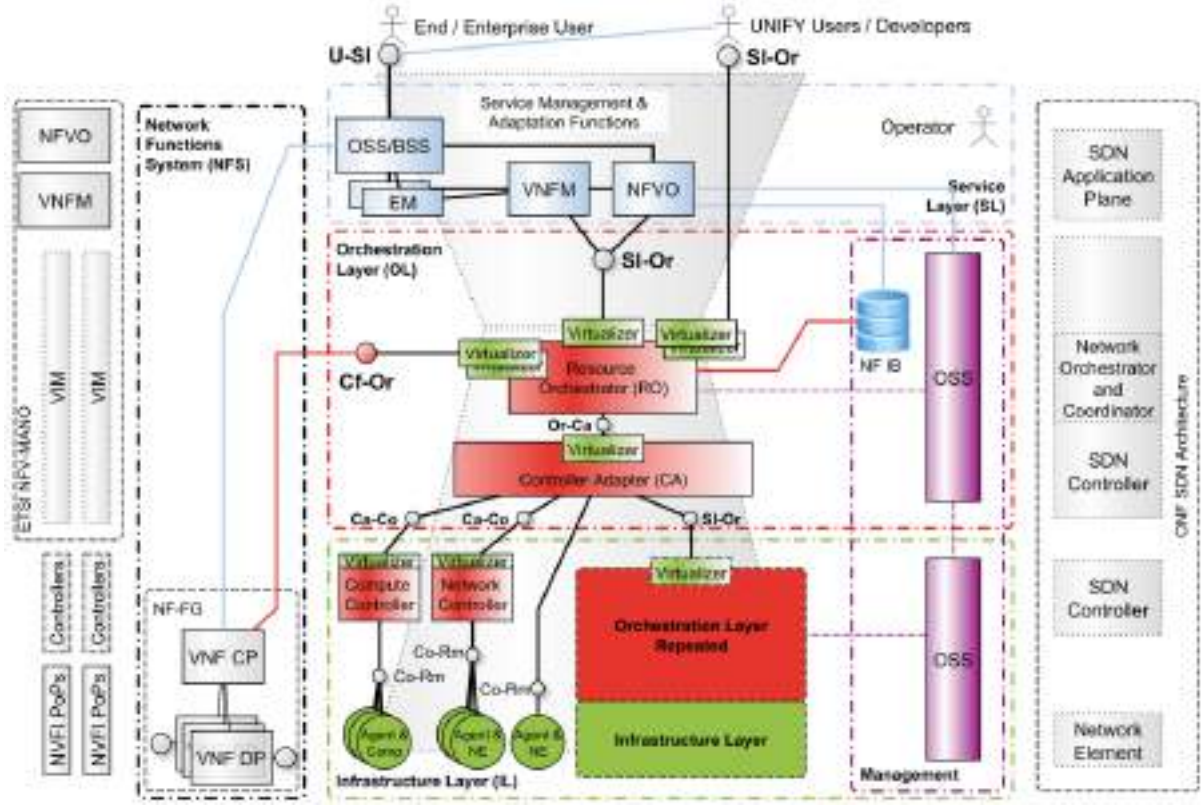


Figure 2-21: UNIFY architecture

The SL comprises "traditional" and virtualisation-related management and business functions concerned with service lifecycle collectively denoted as "Service Management and Adaptation Functions". Traditional lifecycle management functions include Element Management, Operation Support System (OSS) and Business Support System (BSS) related to service and business management environments associated with Service Providers (SPs). Virtualisation-related management functions include

lifecycle management for virtualised network services, lifecycle management for VNFs and orchestration over the resources presented by the lower layer. Management functions within the SL should be infrastructure-agnostic and should deal with the management of the offered services.

The OL encompasses two major functional components: *i)* Resource Orchestrator (RO), which is responsible for exposing virtual resource views, policy enforcement and resource orchestration between virtualisers and the underlying resources; *ii)* Controller Adapter (CA) which provides domain-wide resource abstraction functions and virtualisation for different resource types, technologies, vendors or even administrations. The CA can be considered as a multi-technology, multi-vendor or multi-domain controller. The interface between SL or external consumers and the RO, which is denoted by Sl-Or, is a key element of the framework. It is UNIFY's proposal for a new, joint software and network control programmatic reference point as a narrow waist. The RO and CA are managed by a corresponding management system including, for example, an OSS shown in the right-hand side of Figure 2-21. A Network Function Information Base (NF-IB), which is used by the RO and is also part of the management system, stores resource descriptions for NFs to support orchestration.

The Infrastructure Layer contains resources, local resource agents and/or Controllers. Controllers inherently implement virtualisation functions corresponding to a single domain. Physical resources comprising all possible resource options (compute, storage and network) together with their corresponding local agents, e.g., OpenFlow switch agent or Open-Stack Nova compute interface, and Controllers are managed by a corresponding management system (OSS).

2.4.2 T-NOVA

T-NOVA is a FP7 project aimed at designing and implementing a prototypal end-to-end NFV platform, enabling creation and provisioning of Network Services composed by Virtual Network Functions. The architecture is based on the ETSI NFV model, enhanced by a marketplace layer, providing a business-level interaction with the end users willing to select and activate network service instances. The general T-NOVA architecture is shown in Figure 2-22.

The layers more relevant to 5GEx are the *Marketplace* and the *Orchestration*. The Infrastructure Management and NFVI layers map respectively on 5GEx Controllers layer and 5GEx Resources layer. Mapping to the general 5GEx model, the Marketplace can implement 5GEx interface 1 as some management multi-domain orchestration features.

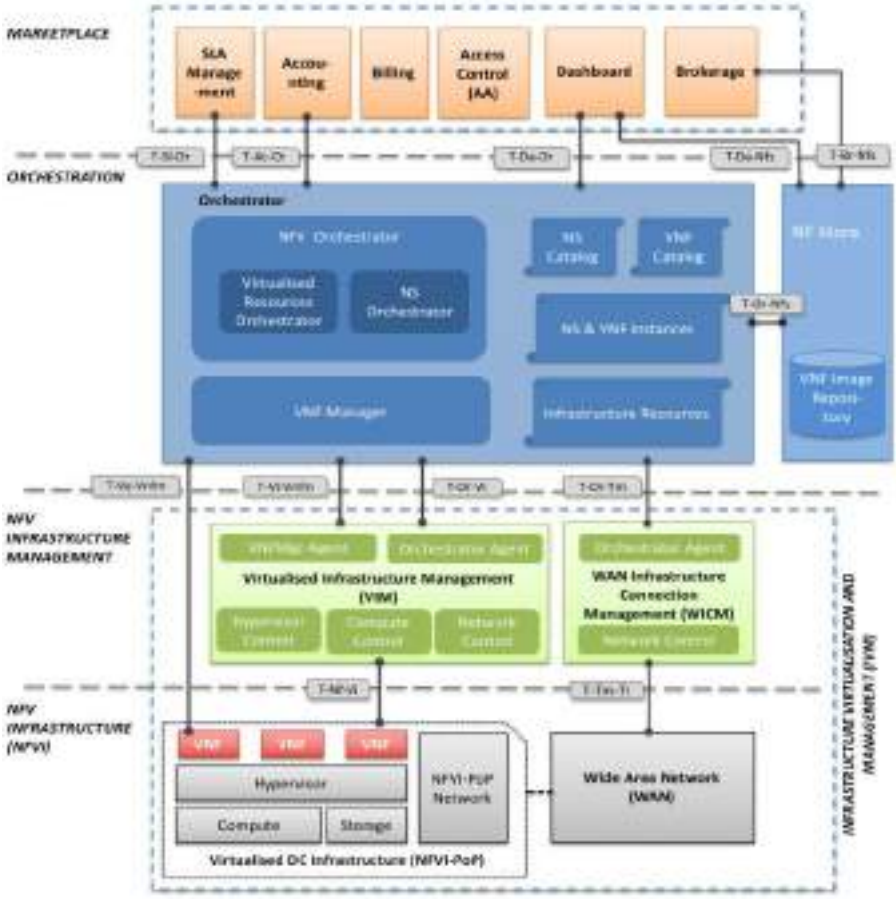


Figure 2-22: T-NOVA Architecture

A more detailed breakup of T-NOVA marketplace internal structure is in Figure 2-23. The main capabilities provided by T-NOVA marketplace relevant to 5GEx are:

- Service specification via an interface based on the ETSI NSD information model;
- Structures to manage service instantiation and monitoring (in dotted line in the figure as further documentation is needed to clarify which capabilities are supported);
- SLA evaluation, supported by the component "SLA Manager", which receives inputs in WS-Agreement format and generates penalties on violations caused by unmet SLAs. This function needs enhancement to support interaction with SLA Manager in other domains through interface 2.
- A business service catalogue.

The T-NOVA Orchestration layer includes the core NFV Orchestrator, plus the additional components needed for provisioning and operational management of VNFs and Network Services. It is designed on a micro-service based internal architecture, allowing to individually deploy each component, hence also omitting or replacing some of the components with alternative ones compliant with T-NOVA interface specification.

The functional components in the T-NOVA Orchestration are:

- SLA enforcement
- Identity management
- Management GUI
- VNF descriptor validator
- HEAT template generator
- Network Service catalogue
- Network Service manager
- Network Service active instance repository
- Service Mapping
- Network Service monitoring
- Network Service provisioning
- VNF Catalogue
- VNF Manager
- VNF provisioning

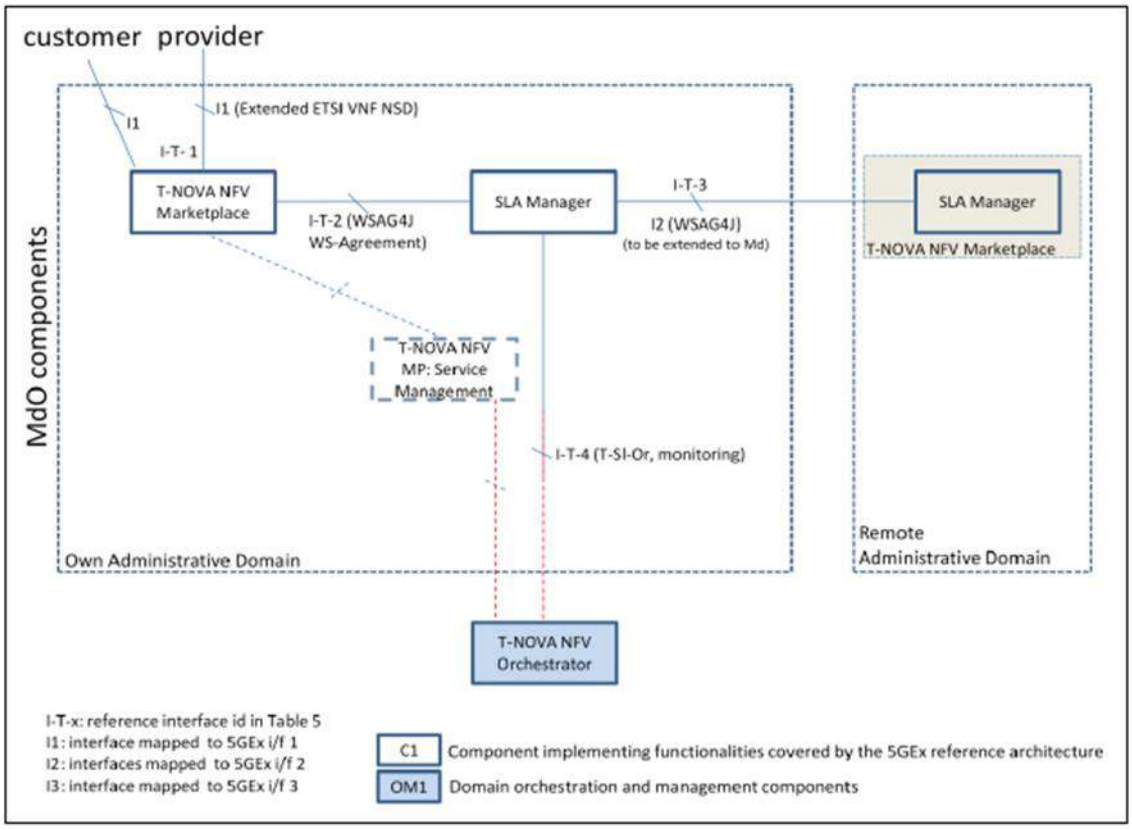


Figure 2-23: Extending T-NOVA Marketplace to Multidomain scenario

The prototype implementation of T-NOVA is based on OpenStack (cloud resources controller) and OpenDaylight (SDN Control Plane) as VIM layer modules. The whole API implements the ETSI NFV interface specification. The Orchestrator southbound API is hence based on OpenStack and OpenDaylight standard APIs, whereas the northbound one is a REST-based interface with JSON data exchange.

2.4.3 ETICS

ETICS [3] supports the emerging Internet QoS-sensitive high-performance services (e.g., HD video streaming, tele-presence, e-health)

through network interconnections of assured quality. Technically, ETICS automates the support of end-to-end (e2e) QoS guarantees across multiple networks. Economically, it serves as a market enabler for services that require QoS assurance. In particular, ETICS supports premium inter-domain connectivity services by stitching or nesting connectivity agreements - called Assured Service Quality (ASQ) agreements - from several ETICS providers. The ETICS ASQ products are a family of novel interconnection products that support paths of predefined assured performance in terms of business and technical attributes, described in an SLA. There can be several variants of ASQ goods, depending on those parameters, as depicted in Figure 2-24.

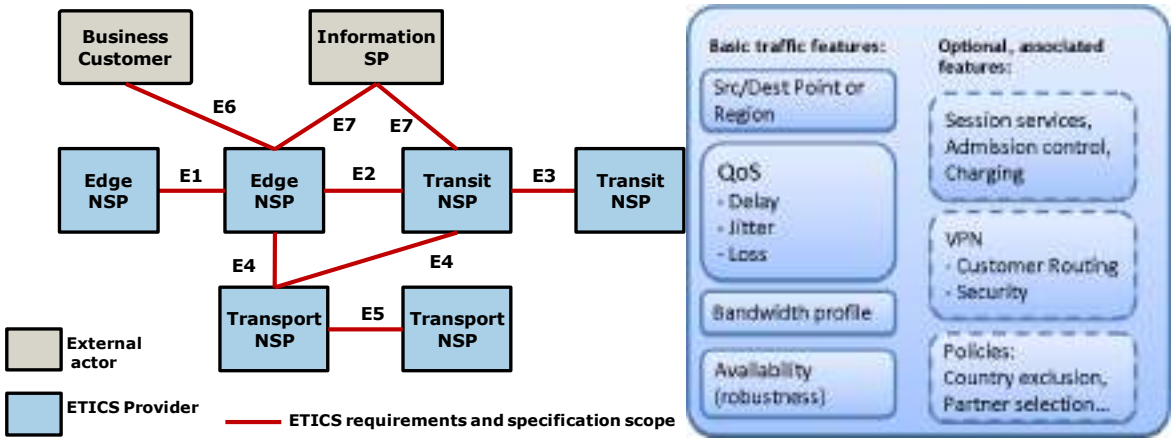


Figure 2-24: The ETICS actor role model and the definition of the ASQ product

Internet Best Effort service is enabled by two interconnection market products: peering and transit. Each NSP accepts only BGP information from its neighbours and classifies all incoming packets to low priority, ignoring any Type of Service information in packet headers and RSVP signalling. This reflects both the lack of trust among NSPs and the lack of compensation for the extra effort of the NSP to provide a premium service. On the other hand, ASQ products provide tangible QoS assurance in terms of reliability, bandwidth, delay, jitter, etc. over a certain ASQ path; this path is selected independently of the BGP in order to meet the QoS constraints demanded by the customer. Furthermore, multiple ASQ products can be offered for the same destination, e.g., one per service.

In the ETICS context, service composition is the process of establishing the e2e path based on the technical parameters of the associated Service Level Agreements (SLAs) over a chain of ETICS network operators. In order to do so, participants must be aware of the available services/products and all the necessary information (prices, availability, etc.), which takes place through a service discovery and PCE-based establishment mechanism. Other types of functionality involved are admission control for service establishment and SLA monitoring during service provisioning in order to validate SLA conformance.

2.4.4 CityFlow

CityFlow project [50] was an OpenFlow City Experiment – Linking Infrastructure and Applications. CityFlow provided a proposal for the introduction of a dynamic OpenFlow capability in public networks by looking at the commercial challenge to the growth of the internet and describing a new operational model for the internet to address this challenge. The CityFlow experiments were focused on the large scale emulation of an OpenFlow network. CityFlow considered a city of 1 million users, setting a target of Busy Hour Flow Invocations of 75,000 for the baseline case and 450,000 for the expansions case. The project conducted a range of experiments and an analysis of the virtual path slice engine in an Amazon cloud.

The CityFlow project[7] proposed a differentiated connection model for multiple autonomous systems. A high level view of the operational model is shown in Figure 2-25. The essential idea is to segment the network capacity (e.g., on a 50:50 basis) into a best effort domain and an OpenFlow Domain. This can be implemented by using an aggregated queue in a gateway network element dimensioned for 50% of the capacity for traffic painted as BE - best effort - using Diffserv code points. The other 50% in the OpenFlow domain can be painted EF or AF – expedited forwarding or assured forwarding - using Diffserv code points. This OF domain can be sliced in a flow core and connection admission control techniques can be used to guarantee the traffic performance. This is especially important for inelastic traffic such as live video which is sensitive to TCP back-off. TCP back-off is common in well loaded best effort networks. Application providers (Appcos) with multiple applications in the area of Internet of Things (IoT), eHealth, Consumer, Cloud, Media Social can use the slicing mechanism to obtain a slice of bandwidth across multiple autonomous systems and to the consumer, connected via optic fibre access or 4G/5G radio access network. Of course, in exchange for obtaining guaranteed bandwidth to the user, the application provider who will be able to drive new business models (e.g., 4K webTV) can expect to receive a charge for conveying the guaranteed traffic. This can be implemented using cascade charging on a wholesale basis, from access to core up to application provider.

[7] This text is an extract from the CityFlow white paper (D3.1: CityFlow White Paper August 2014): http://www.onesource.pt/cityflow/site/index.php?process=download&id=315&code=s7QnH7eI

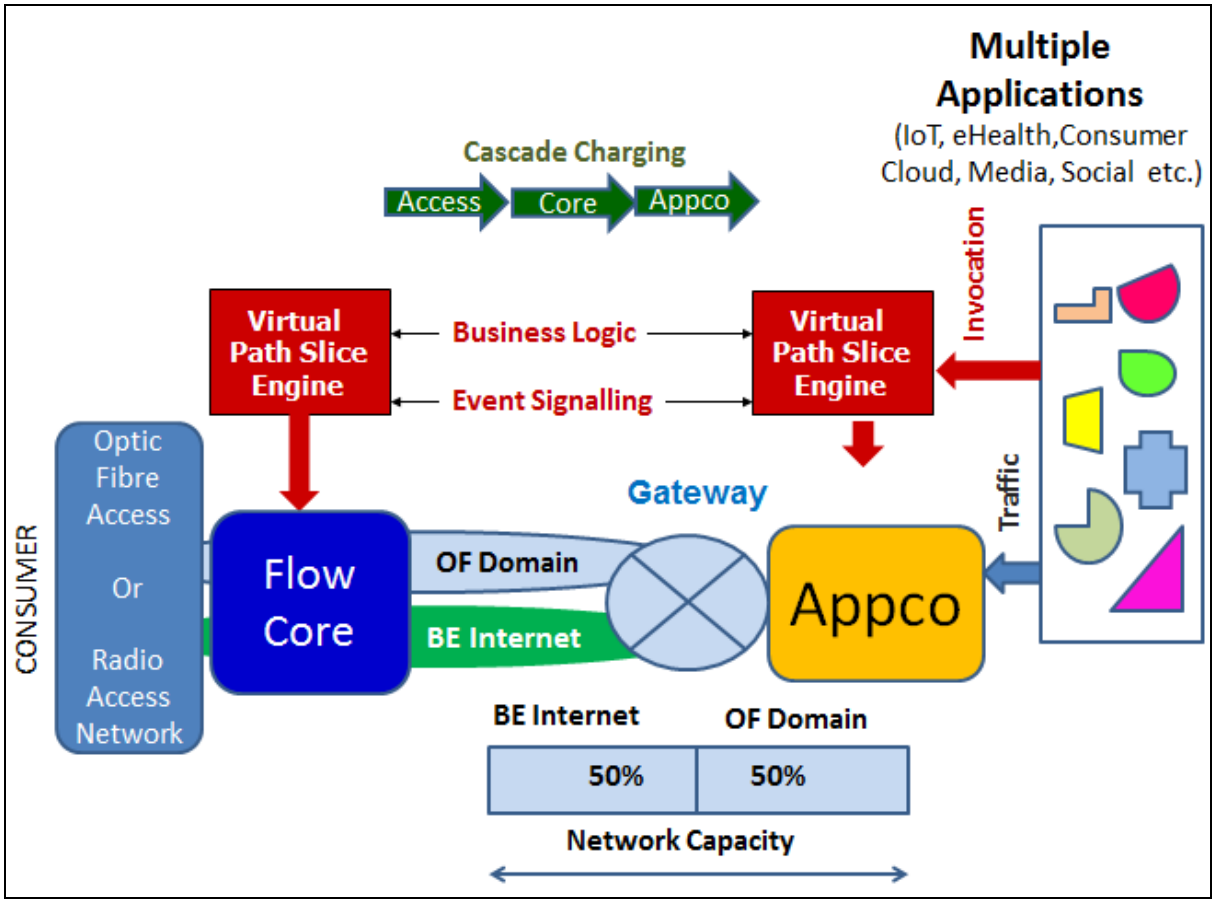


Figure 2-25: Future Internet Implementation Model

2.4.5 H2020 Endeavour

The Endeavour project [51] (started in January 2015) works on the application of SDN paradigm to existing Internet interconnection models as a way of enabling novel services and new economic models. As objectives of the project we can find:

- Inter-domain SDN control plane, with research and evaluation of an SDN architecture for large IXPs, considering distributed SDN Control Plane and SDN Programming Abstractions.
- Scalable fine-grained monitoring, developing a monitoring platform for the SDN-enabled IXP.
- Network services offered to IXP ecosystem, through the analysis of a set of use cases showcasing the types of novel inter-domain network services that can be offered to the IXP ecosystem, like multi-homing, application-level traffic engineering, and flow anomaly detection.

There are not yet public outcomes from the project with regards to architectural topics. However, some requirements and challenges for monitoring have reported in Deliverable 3.1, with a review of existing monitoring techniques for SDN, Cloud and overlay monitoring.

2.5 Orchestration

The definition of a standard interoperable interface among Multi-Domain Orchestrators and/or between Multi-Domain Orchestrator and Domain Orchestrator(s) is of crucial importance to allow the extension of service provisioning beyond a single administrative domain (i.e., inter-operators). This is one of the key aspects to be tackled by 5GEx. Some areas and/or topics are not yet sufficiently covered and/or represent areas where the project can significantly innovate. One of them is the joint orchestration of compute, storage and network resources across administrative domain boundaries, in a common service offering. For effectively implementing that, an interface equivalent as the one proposed by 5GEx connecting (multi-domain) orchestrators from different administrative domains (interface 2) is required. Then full specification of such interface will enable such kind of scenarios. In order to do that, the intended APIs should convey information about the deployment of slices and network functions to be interchanged among administrative domains. Apart from that, a more clear detail on the boundaries and differences between Control and Management seems to be necessary in order to properly interchange information among domains, and between providers and customers.

That control relationship between domains can present different models, like peer-to-peer or hierarchical. These control relationships imply a different location of the administrative boundaries (East-West, North-South), and it is yet to be investigated if this can motivate differences on that relation (the analysis and design of control interface, for instance NetConf, could be similar or not in both cases). The same applies to the relation between Multi-Domain orchestrators from different providers, with respect to the relation between a Multi-Domain orchestrator and the Domain orchestrators internal to a single administrative domain. An assessment of whether the 5GEx interfaces for orchestration can be implemented as two instances of the same interface is required.

In order to build on stable basis, a mapping between 5GEx multi-domain orchestrator and ETSI NFV MANO is needed, including the mapping of the MANO interfaces to the 5GEx interfaces. This can ensure rapid adoption and fast standardisation and interoperability of the innovative outcomes of the project.

Some additional points that present gaps in actual solutions, and that have clear impact on 5GEx project, are topics like autonomous behaviour and self-healing. When dealing with interconnected environments, problems or failures in one of the participating domains can be propagated to the other domains if not proper countermeasures are taken to protect and harnessing the system.

Furthermore, this interconnected system requires from a common understanding of the information exchanged, a common semantic of what is being shared between the participants in the 5GEx environment. Then

proper definition and analysis of common Information Models, as well as agreed level of information exposition (push / pull, subscribe model, etc) are areas of work not yet explored in single domain environments.

Last but not least, orchestration reclusiveness is of interest in order to explore more complex interactions either in the internals of a given domain, but also in the interaction between multiple administrative domains in the exchange ecosystem.

2.6 SLA design and negotiation

The SLA structure should be flexible and descriptive, allowing for network and cloud-specific metrics, as well. Current SLAs are either network or cloud specific, and often contain insufficient details. Also, negotiation is done via humans as of now, which have a critical impact on the overall service creation time. This should be automated to reach 90 s/min service setup time. Some areas and/or topics are not yet sufficiently covered. One case is the management of responsibility resolution. For instance, in the event of a failure or SLA incompliance of a running service, a multi-domain environment like 5GEx requires the ability to detect the specific domain for service breach and in sequence the responsible operator. A basic piece for that is to accomplish an adequate resource monitoring and SLA assurance, where also appropriate time-scale applicable for those SLAs (months vs. days) have to be defined.

Considering that a majority of services will leverage on NFV capabilities, revisiting SLAs for cloud and network availability for sustaining carrier-grade service (99,999% of availability) is also a goal. Services on remote domains are expected to accomplish same levels of service as those implemented locally, then accurate definition of SLAs, and carrier-like behaviour is imposed.

Finally, the reduction of set-up provisioning time and automation enhancements that could assist on such reduction are also areas of work since existing solutions are not sufficient to achieve expected KPIs for 5G.

2.7 Service Catalogue

In order to make the multi-domain orchestrated services accessible and consumable by Customers, services must be stored in some catalogues where they can be traded and purchased. A sample service library is needed for 5GEx so that we can validate that the exchange functions for a realistic and possible set of enterprise, consumer and wholesale services.

As foundation for that service catalogue, it is needed a common taxonomy to associate elements to resources to be instantiated in the different domains. Also, compilation of packages (unified base of objects) that could be commonly understood by the participants in the 5GEx

ecosystem will assist on the common understanding of services. By the way, this will serve as baseline for negotiating SLAs

Because of the tight relation with NFV environments, it is required an analysis of the relation with the concept of ETSI NS/NF descriptors and how to extend it to multi-domain environments.

The service catalogues at the end will support a marketplace complemented with economic mechanisms for the trading of bundles of services and resources enabled by 5GEx. On that marketplace, accounting emerge as one of the pillars for ecosystem sustainability.

2.8 Multi-domain service delivery

Multi-domain orchestrated services are assigned a set of resources which are both heterogeneous (physical/virtual; computational/network) and spread over multiple domains. The 5GEx system must cope with this augmented complexity.

Key for such multi-domain orchestration is to have a common abstraction of resource description across domains. Information exchange and handling (information flows) with mechanisms for operators to share information respect to resources repositories, pricing, SLA, service catalogues, etc. needs to be defined within the project for the multi-domain environment.

A facilitator for that can be the existence of some repository of resource descriptors in 5GEx. For instance, some specialisation on the participant administrative domains could be expected, with some participating as service domains vs. some other participating solely as infrastructure domains.

Also, a description of the min/max functionality/primitives of the 5GEx orchestration with real-time/non-real time characteristics seems to be necessary.

2.9 Industry whitepapers

There is a variety of industry whitepapers on 5G [14]-[21], from vendors like Ericsson, Huawei, Nokia, Alcatel-Lucent and Samsung, and the operators members of the Next Generation Mobile Networks (NGMN) alliance, that present the vision, specify use cases and define architectural requirements of 5G.

5G is a revolutionary technology promising to enable a fully connected and highly mobile society. Furthermore, 5G should provide the capability of control over heterogeneous wireless and wired networks, be flexible enough to support the demanding application with highly diverse characteristics and to accommodate the creation of business and cooperation models [14].

In the next few years, the number of connected devices is going to explode due to the increasing popularity of IoT (Internet of Things). It is expected to reach the number 50 Billions of connected devices in 2020 [19]. The huge number of devices will drive the connection density to the extreme of 200,000 connections per km² [18]. By 2020, small cells are expected to carry a majority of traffic with overall data volume expected to grow up to 1,000 times [16]. Concepts like tactile internet, immersive multimedia, M2M (machine to machine) communication and augment reality will require a virtually "zero latency" [16].

The business context beyond 2020 will be notably different from today with the emergence of new use cases and business models driven by customers' and operators' needs. A number of whitepapers provide a clear categorisation of the 5G use cases. In each whitepaper is followed a different approach for defining these use cases, however most of the outcomes are overlapping, which can be grouped as follows: *i)* Mobile broadband access everywhere, even in areas with high connection density [14], [20] including rural areas with minimum available network infrastructure to support e.g., open-air festivals [20]; *ii)* Higher user mobility, including vehicles moving with speed higher than 500 Km/h; *iii)* Massive IoT, including sensor networks at home, office, stores, streets and also wearables [17][14][20]; *iv)* Ultra-reliable communication for critical service such as e-health, or lifeline communication in disaster situations; *v)* Extreme real-time communication, for QoE-demanding applications like tactile internet and augment reality, in both entertainment and work environments [14][19].

Based on these use cases, the whitepapers provide principles and architectural requirements for 5G, stressing flexibility and reliability: Flexibility to support very diverse applications and services over different link characteristics [17], [18]; also, extensibility and being able to adopt any new technology [18], embracing flexible solutions like NFV and SDN [14]. Reliability is an important aspect of 5G related to the consistency of network performance (e.g., perception of infinite capacity and ubiquitous connection), but becomes even more critical for network communications for control and safety [17].

In whitepapers [14]-[19] the authors identify 5G requirements regarding:

(i) User experience: 5G should deliver a consistent user experience over time for a given service in any location or device that the service is offered. Peak data rates of a 5G system will be higher than 10 Gbit/s but more importantly the cell-edge data rate (for 95% of users) should be 100 Mbit/s. Further, on demand user mobility and E2E (End-to-end) latency of 1ms should be supported.

(ii) System performance: Rates of several tens of Mb/s should be supported for tens of thousands of users in crowded areas.

Spectral efficiency should be significantly enhanced compared to 4G.

(iii) Devices requirements: 5G devices should be programmable, supporting M2M commination and multiple radio technologies, having significantly increased battery life up to 3 days for a smartphone and 15 years for low-cost sensors.

(iv) Service enhancement: 5G should provide the experience of seamless and consistent connection by unifying radio technologies. Security and user privacy should be assured over different heterogeneous networks. Ultra-high reliability should be provided for critical services.

(v) Business models: 5G should enable creation of new business models in a programmable manner without having architectural impact. The modularity of network is a requirement that should be met. Taking advantage of NFV/SDN, network operators will be able to optimise their operational and management costs. Further, creation of open API layer is required in order to allow service providers to configure their own policies and the way its data packets are processed in the network. Finally, 5G should enable synergies and flexible business models that can change dynamically over time.

Following up on these requirements, [14] proposes an architecture that leverages the structural separation of hardware and software, as well as the programmability offered by SDN and NFV. The proposed architecture comprises of three layers E2E management and orchestration function: Infrastructure resource layer, comprising both network and cloud virtualised resources; Business enablement layer, a library of functions required within the virtualised and converged wired-wireless network, and a set of configuration parameters; Business application layer, of specific applications and services of the operator, enterprise, verticals, or third parties that utilise the 5G network. End-to-end orchestration and management provides the capability to manage such a virtualised network end-to-end. A similar approach is presented in [20], where a logical abstraction of networks into slices, i.e., networks-on-demand defined by a number of customizable software-defined functions that will be adapted to the specific demands of each scenario, is introduced. For such abstractions, the proliferation of Cloud technologies together with SDN and NFV are crucial.

This revision of relevant industry whitepapers also provides useful insights for the 5GEx architecture (those related to use cases are discussed in Section 4). An important takeaway is that the 5GEx architecture should enable the modularity and programmability of network resources, utilising the innovative virtualisation technologies of Cloud, NFV and SDN. Both [14] and [20] propose a 5G architecture that abstracts the physical network into customizable software-defined

network functions capable of meeting the requirements of highly diverse use cases by defining appropriate network slices. The presence of a business layer framework and a service catalogue are also crucial. Another valuable lesson learnt from [14] is that the 5GEx architecture should provide end-to-end orchestration and management of these virtual networks that may cross multiple administration domains. SLAs, monitoring and properly designed charging schemes are very important. Another lesson learnt from [14] is also the creation of an open API layer that will allow Service providers to dynamically configure their services and policies in the 5GEx ecosystem. Finally, according to [18], the 5GEx architecture must be easily extensible to allow further innovation.

2.10 Existing orchestration frameworks

This section provides an overview of existing single-domain and multi-domains orchestration frameworks. The choice aims at covering heterogeneous cloud and networking domains, each provided by a technology specific orchestration framework. Note that several of the orchestration frameworks come from past and ongoing projects (analysed in Section 2.4) 5GEx leverages on. While reporting on the available orchestrator frameworks we also perform a gap analysis based on the requirements of the 5GEx architecture.

2.10.1 Resource Domains and single-domain Orchestrators

We provide below a brief description of a set of single-domain orchestrators and their respective resource domains.

1) *OpenStack Heat (OH)* orchestrates cloud resources in the OpenStack framework, managing infrastructure object aggregations (i.e., stacks). The orchestration is performed considering creation, modification, and deletion of aggregates of infrastructure objects like virtual machines (VMs), virtual volumes, and virtual network elements. The infrastructure objects are described in template files, written using the Heat Orchestration Template (HOT) language, a declarative language in JavaScript Object Notation (JSON) format describing all the objects in the aggregate and the relationships among them. Both the orchestration and the provisioning of infrastructure objects are performed by OH collaborating with other specific components, i.e., Nova (for compute resources); Swift and Cinder (for storage resources); and Neutron (for connectivity resources). The interface *I3* of OH is based on REST API and it is used for the management of the stacks. The API, that is available through HTTP(S) protocol, implements both JSON data serialisation formats. Software Development Kits (SDKs) are available for several programming language bindings like Java, Node.js, Python, Ruby, .NET, etc. OH collaborates with Keystone (OpenStack project providing Identity, Token, Catalogue, and Policy services) for authenticating and authorizing cloud users.

2) *ESCAPE* (Extensible Service ChAin Prototyping Environment) is a general prototyping framework which supports the development of the main functionalities of a service chaining architecture (i.e., VNF implementation, traffic steering, virtual network embedding, etc.). EU FP7 *UNIFY* project has proposed a novel SFC (Service Function Chaining) control plane architecture providing unified resource orchestration with joint network and software (compute, storage) virtualisation and programming. In the context of UNIFY, ESCAPE is a proof of concept prototype implementing the relevant parts of this architecture. In particular, it is a realisation of the UNIFY service programming and orchestration framework for both cloud and networking resources. ESCAPE can orchestrate *i)* different technology resources directly using domain managers and adapters, *ii)* abstract resources exposed by lower level UNIFY compatible domains. Domain managers and technology dependent adapters can be added in a modular way. In particular the current version supports an SDN domain manager with POX adapter; a local Mininet (emulated network) domain manager with Mininet adapter, POX adapter and NETCONF adapter; an OpenStack domain manager with POX adapter and NETCONF adapter; and a UNIFY domain manager with REST adapter. On the one hand, the former domains are controlled via multiple control channels (e.g., OpenFlow for the networking resources and NETCONF for the compute resources). By this means, minimal (if any) extension is needed from the infrastructure side. On the other hand, the later UNIFY domain manager implements interface *I3* via the UNIFY Sl-Or interface, which provides the capability of aggregating and managing resources in the form of NF-FG (Network Function Forwarding Graphs). This is the joint control API of UNIFY based on a novel resource abstraction combining cloud and networking resources. This approach requires additional components in the infrastructure domain to be able to *speak the UNIFY language*. For this purpose, a dedicated library has been implemented which enables the extension in several domains. Considering that Sl-Or interface has been designed to be recursively chainable, ESCAPE can act as a multi-domain orchestrator as well, as explained hereby in Section 2.10.2.

3) *Ericsson Harmonizer* aims at providing data center interconnections crossing heterogeneous networking domains, that differ in terms of switching technology (e.g., packet, optical), control system (e.g., SDN, legacy GMPLS), and vendors. The Ericsson Harmonizer provides dynamic and carrier grade end to end (E2E) transport connectivity combining heterogeneity, elasticity, and traffic engineering capabilities in each domain. The solution is based on a hierarchical architecture that guarantees transport resource optimisation minimizing the interworking among the domains. An efficient method for abstraction of the resources allows to expose the E2E connectivity in terms of the service parameters while, at the same time, hiding technology specific details. The Harmonizer supports both standard and proprietary protocols as interface to communicate with the resource domains. The supported standard

interfaces are OpenFlow [2], Path Computation Element Communication Protocol (PCEP), and Border Gateway Protocol - Link State (BGP-LS). The orchestrator supports both the basic version of the protocols and the related extensions proposed in the standardisation bodies. More specifically, considering the PCEP, the Harmonizer can manage the following extensions: hierarchical PCEP, and statefull/instantiated PCEP. As interface to communicate with the upper layer, e.g., a Multi domain Orchestrator (interface *I3*), the Harmonizer supports a proprietary Remote Procedure Call (RPC)-based interface, but the migration to a NETCONF/YANG interface is planned. Possible candidates that can be used are the Control Orchestration Protocol (COP) interface defined in the Strauss project, and the UNIFY interface.

4) *Redzinc VELOX Equipment Manager (EM)* is a component of the VELOX framework that enables the reservation of (abstract) resources for the deployment of Virtual Path slices. It supports heterogeneous networking resources (i.e., IP/MPLS, SDN, EPC networks) by means of VELOX drivers. The interface *I3* of VELOX is based on a TLV-based proprietary northbound API towards the VELOX multi-domain orchestrator.

Table 1 summarises the resource domains considered so far in the 5GEx framework. The information in the table is organised as follows: resource domain; resource type; resource domain orchestrator(s) options; a brief description of the domain functionalities; and the options currently available for the implementation of the interface between the domain orchestrator and the resource domains.

Cloud resources can be managed by REST API through HTTP(S) or by ESCAPE through the OpenStack adapter.

In the case of networking resources, a first implementation option of the interface between the domain orchestrator and the networking resources relies on both (1) BGP-LS to expose network resource abstraction to domain orchestrator and (2) PCEP to enable the orchestrator to issue network provisioning requests to the domain controllers. In particular, BGP-LS provides a distribution mechanism for exchanging link-state data either representing the real physical topology retrieved from routing protocol databases, or an abstracted topology including specifically created virtual paths. PCEP, originally designed to provide communication in support of path computations, has been recently extended (i.e., active functionality) to allow the establishment of new network services.

ESCAPE is an additional candidate interface for enabling the orchestrator to issue network provisioning commands to SDN packet domains. Moreover, given its flexible XML-based architecture exploiting the NETCONF protocol, it can be used to also handle monitoring information. A further implementation option for networking resources, also available as *I3*, consists of the VELOX interface. It relies on a TLV-

based proprietary solution enabling, among other functionalities, operations like bandwidth slice event invocation and service chain in the data plane of IP/MPLS, SDN and EPC Networks.

The interfaces between the resource domains and the domain orchestrators will be used to validate the concepts of resource and service slicing on the 5GEx *Sandbox* network, a pan-European test bed whose data plane includes domains provided by 13 different 5GEx Project Partners from Industry and Academia. Network domains include both cloud and networking resources. In particular, cloud domains, typically implemented with OpenStack technology, are located at the Sandbox network edges. In the 5GEx Sandbox, cloud domains are interconnected by networking domains reproducing Tier1/2/3 heterogeneous transport resources, including SDN and Segment Routing packet domains as well as legacy and flexi-grid optical networks.

2.10.2 Multi-domain Orchestration candidates

1) *T-NOVA* FP7 project, implements a NFV orchestration framework compliant with ETSI NFV MANO, on top of which the T-NOVA system builds a business layer or marketplace that facilitates commercial interactions among NFV business stakeholders, such as NF software developers, Service Providers (SP) and customers. The T-NOVA system architecture was already shown in Figure 2-22. T-NOVA Marketplace allows SPs to purchase VNFs from software developers in order to compose network services (NS) and offer them to their customers, including SLA management, accounting and billing features and the corresponding interfaces with T-NOVA NFV service orchestrator.

The T-NOVA Marketplace capabilities relevant to the realisation of the 5GEx reference architectural framework in Figure 7-2 are:

- A B2C interface based on the ETSI Network Service Descriptor (NSD) information model, which can be mapped to interface *I1* in Figure 7-2 for dispatching service requests to the MdO;
- Service and VNF catalogue that can be directly browsed by the customer;
- Structures to manage service instantiation and monitoring;
- SLA management by means of a component that facilitates SLA specification including definition of penalties or rewards and SLA evaluation.

TABLE 1
RESOURCE DOMAINS AND DOMAIN ORCHESTRATORS

Resource domain		Managed resource type	Reference domain orchestrator	Domain properties and functionalities	Interface between domain orchestrators and resource domains
Cloud domain	OpenStack Compute (Nova)	Computing	OpenStack Heat, ESCAPE	It manages the lifecycle of computing resources (i.e., Virtual Machines-VSs) implementing functions for spawning, scheduling, and terminating VMs on demand	OH: REST API through HTTP(S) protocol ESCAPE: Unify using OpenStack adapter
	OpenStack Block Storage (Cinder)	Block storage	OpenStack Heat, ESCAPE	It provides persistent block storage (i.e., Virtual Volumes) to VMs running in the cloud, managing the lifecycle of block storage objects (i.e., creating, attaching, detaching, and deleting virtual volumes)	OH: REST API through HTTP(S) protocol ESCAPE: Unify using OpenStack adapter
	OpenStack Networking (Neutron)	Cloud networking	OpenStack Heat, ESCAPE	It provides network connectivity to the VMs running in the cloud, managing the entire lifecycle (creation, deletion, use, and control) of all the involved networking objects (e.g. network trunks, subnets, virtual routers, etc.)	OH: REST API through HTTP(S) protocol ESCAPE: Unify using OpenStack adapter
Legacy Packet Domain		Networking	Harmonizer, VELOX EM	IP/MPLS domain composed of commercially available routers and Linux boxes. Support of Segment Routing, GMPLS control plane or Command Line Interface (CLI)	Harmonizer: PCEP and BGP-LS VELOX:TLV based proprietary Interface
SDN packet domain		Networking	ESCAPE, Harmonizer, VELOX EM	OpenFlow based network controllable by different OF controllers (i.e., Floodlight, POX, ODL, ONOS) and different OF versions (i.e., 1.0 and 1.3)	ESCAPE: Unify using POX/NETCONF adapters Harmonizer: OpenFlow1.3 VELOX: TLV based proprietary Interface
Optical Domain		Networking	Harmonizer	Optical domain composed of commercially available ROADMs and optical nodes controlled by Linux-based adapters. Supports flexi-grid	Harmonizer: PCEP and BGP-LS
EPC Network Domain		Networking	VELOX EM	EPC networks with Policy and Charging Rule Function (PCRF) exposed via Rx interface	VELOX:TLV based proprietary Interface

The T-NOVA orchestration layer main capabilities are:

- NS/VNF management and NS/VNF Catalogues management, exposing the Catalogues to the Marketplace;
- Management of networking and cloud resources for NS/VNF hosting;
- Service mapping: resources allocation to NSs;
- NS/VNF instantiation requests management: the T-NOVA orchestrator receives NS/VNF instantiation requests from the Marketplace, executes the instantiation and manages the NS/VNF instances repository;
- NS/VNF monitoring: Virtual Machine (VM) based monitoring data from the lower virtualised infrastructure and management (VIM) layer and maps it to the corresponding NS/VNF instances.

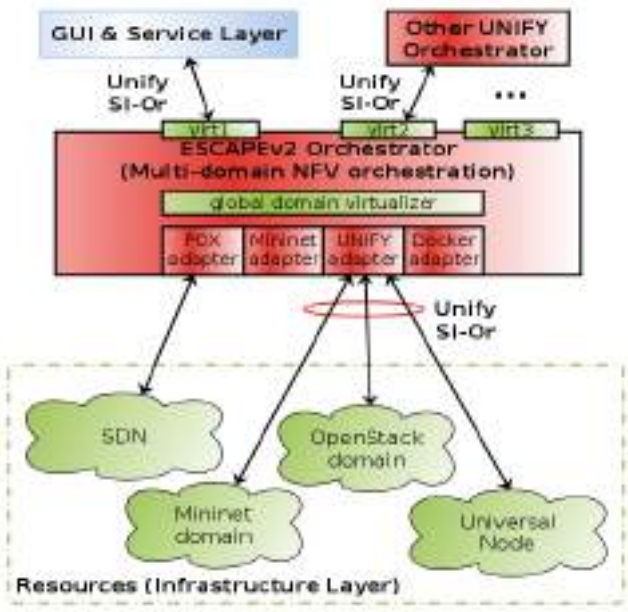


Figure 2-26: ESCAPE architecture

2) ESCAPE, as we have seen in Section 2.10.1, is a proof of concept prototype of the *UNIFY* FP7 project. On the one hand, it can operate as a single-domain Orchestrator for different technological domains. On the other hand, it is a multi-domain orchestrator, thus strictly speaking, it implements the Orchestration Layer of the UNIFY architecture. However, a simple Service Layer interacting with clients, and an Infrastructure Layer based on Mininet were also added. The high-level components and their relations are shown in Figure 2-26. ESCAPE implements the main interface of UNIFY, namely the Sl-Or, both at north and south. This enables multiple higher-level orchestrators on top of ESCAPE with corresponding virtual infrastructure views provided by virtualisers. Virtualisers implement the joint resource abstraction for cloud and networking resources proposed by UNIFY. ESCAPE itself constructs and works on a global domain view. The higher-level virtualiser configurations and VNF deployments are multiplexed in this element. The connection towards different infrastructure domains based on legacy or novel technologies are realised via dedicated adapter modules of ESCAPE. The most important one called UNIFY adapter implements the Sl-Or interface that is a candidate for 5GEx interface *I3*.

The most relevant capabilities provided by ESCAPE relevant to the realisation of the 5GEx reference architectural framework in Figure 7-2 are:

- A Service layer, which receives service requests in form of service graphs according to ESCAPE interface U-Sl;
- Service mapping into domains based on Abstract Virtualiser/NFFG splitting;
- Network Functions configuration and monitoring;
- Resource control and monitoring for the resource domains supported in the UNIFY framework.

2.11 Gap analysis

In this section we have just conducted a review of the state of the art, covering the main and most relevant efforts for 5GEx. Out of this analysis we can pinpoint gaps, which can be taken by the project to look at and tackle:

- There are no proposals regarding NFV exchange points. While there have been some SDN exchange point architecture, none are looking yet at exchanging and trading software resources (not only networking, but also compute and storage). Same comment applies to federation, where work exists related in the networking world, as well as in the cloud environment, but no widely adopted schema exists covering both.
- Existing commercial solutions are intrinsically conceived for single administrative domain scenarios. Up to our knowledge, multiple administrative domain scenario has not been yet addressed, and therefore this highlight the potential commercial value of 5GEx solutions.
- On the standardisation side, almost no work has been done yet in terms of supporting orchestration of multiple administrative domains. The ETSI NVF ISG has just started to look into how to add multiple domains into its architecture, but they are still at a very early stage.
- Many EU projects are working in the area of orchestration, software networks, NFV/SDN and inter-domain interactions. None of them is properly tackling the multi-domain related aspects. While doing so, 5GEx is leveraging on the results of many of these identified projects.
- Joint orchestration of compute, storage and network resources across administrative domain boundaries, in a common service offering, is clearly not yet solved by any orchestration framework. This is of course, one of the main targets of 5GEx. This requires work in many areas, such as interchange information among domains, control relationship between domains, autonomous behaviour and self-healing, just to cite a few.
- Additional flexibility and automation is required in the area of SLA negotiation and assurance. Current SLAs are either network or cloud specific, and often contain insufficient details.
- In order to make the multi-domain orchestrated services accessible and consumable by Customers, services must be stored in some catalogues where they can be traded and purchased. Because of the tight relation with NFV environments, it is required an analysis of the relation with the concept of ETSI NS/NF descriptors and how to extend it to multi-domain environments.
- A common abstraction of resource description across domains. Information exchange and handling (information flows) with mechanisms for operators to share information respect to resources

repositories, pricing, SLA, service catalogues, etc. needs to be defined within the project for the multi-domain environment.

- There is no existing orchestration framework supporting automated multi-provider multi-domain orchestration. 5GEx will provide one, leveraging on existing single domain ones.

3 Ecosystem overview

This section contains an overview of the 5G and 5GEx ecosystem, including the analysis of business roles, 5GEx framework, 5GEx services definition as well as the description of possible different coordination models that can apply to 5GEx framework. The findings of our analysis of these different coordination models are also included.

3.1 5GEx Actor roles

In this section we introduce the main actor roles addressed by the *5GEx Framework*. Actors can take on multiple roles when specific deployments of the 5GEx Framework into *5GEx Solutions* are considered. The 5GEx Framework and actors are illustrated in Figure 3-1 below depicting the various business roles they can implement.

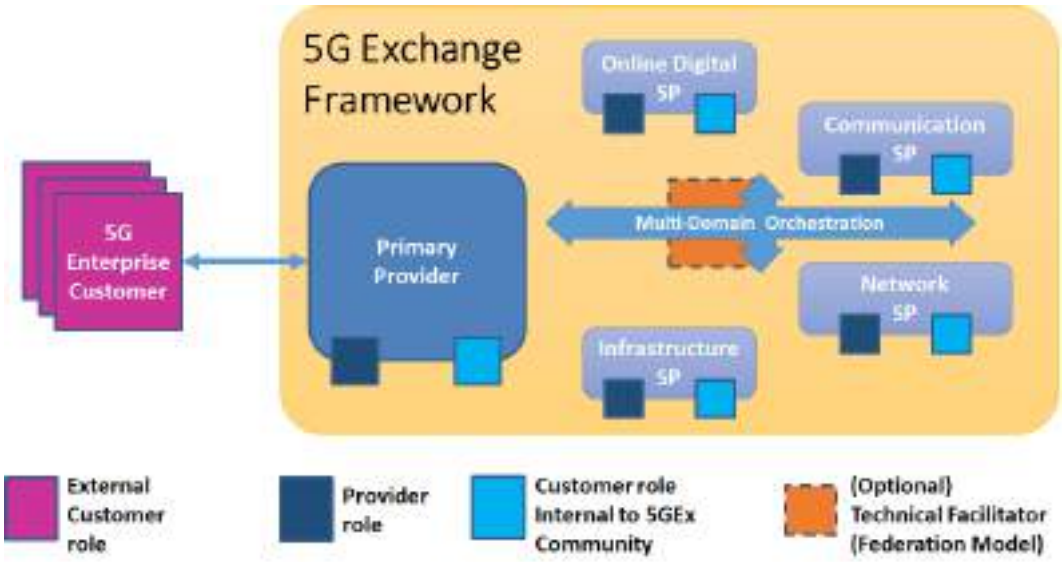


Figure 3-1: 5GEx Framework and actor roles

3.1.1 Actors

We define actors of the 5GEx ecosystem by the set of roles they implement. As it is depicted on the Figure above, an actor can be a 5GEx service provider of any kind (infrastructure, network, communication, online) while a customer of another 5GEx provider at the same time. Similarly, an actor might implement the primary provider role, facing external customers and directly selling services to them, while being a customer to another 5GEx service provider to buy the service to be resold externally. We present the various business roles in the following subsection.

3.1.2 Business roles

Here we provide a short description for all the 5GEx-related business roles.

3.1.2.1 External customer role

The 5G customer as considered by 5GEx is an enterprise customer (the *5G Enterprise Customer*) which can range from an SME or a large enterprise customer from a specific industry vertical to a digital service provider (DSP) offering a specific online application service to their own end-customers over both mobile and fixed access lines. These 5G enterprise customer services can be based on basic best-effort Internet access service, can be based on VPN or even on anticipated evolved Internet access services where differentiated and value added connectivity services (VACS) are supported [52]. This connectivity layer is the communication fabric upon which additional 5GEx services can be offered, potentially incorporating VNFaaS and SlaaS service elements. For instance, a media digital service provider is a 5G enterprise customer for a configurable multi-domain vCDN service, consisting of (own or managed) VNFs such as vCache, transcoding, firewall as well as storage and cloud resources, interconnected by means of 5GEx connectivity services; SlaaS container and management API allow the dynamic adaptation of the service based on the real-time demand exhibited for content by end-users.

The 5G Enterprise Customer buys the 5G enterprise service from the *Primary Provider*, which can be in any of the provider roles illustrated by the 5GEx Framework.

3.1.2.2 Primary/customer-facing provider role

This role is needed for a 5GEx actor in order to be able to directly deal with external customers. This role is not necessarily implemented at all 5GEx participant actors, but those who do implement this role offer an I1 interface to external parties for describing the available service and for negotiating and selling those services.

3.1.2.3 5GEx service provider and customer roles

Within the 5GEx framework we distinguish the type or level of services to be provided and consumed among the 5GEx actors as follows:

- *(5G) Infrastructure Service Provider (IfSP).* This actor role offers 5G-enabled IaaS and can provide services directly also to the 5G Enterprise Customer (5GEC).
- *(5G) Network Service Provider (NSP).* Offering 5G compatible network services, either Layer 2 or Layer 3 services. The network service can be scoped according to private addressing as well as according to public addressing such as the Internet address space.

- *(5G) Communication Service Provider (CSP).* Offering 5G compatible communication services. Typical example services are voice and video communication services. More advanced services also fall into this category such as unified communication and collaboration services, or live event real-time content delivery.
- *Online Service Provider (aka. Digital SP, DSP).* Offering online digital application services that do not fall in the category of communication services. Large OTT SPs (such as Facebook, Google, Microsoft, Apple and Akamai) fall in this category. The notion of Cloud Service Provider (CdSP) belongs to this category. Moreover, we anticipate that the 5G solutions and platform capabilities that can offer a range of 5G infrastructure, value added connectivity services as well as communication service will allow and enable a whole new range of OSPs/DSPs that can now innovate and create new business and value for their own customers, across new market segments ranging across consumer, business and public sectors.

Note however, that these categories are defined from a business perspective. In the next section we make the case for a functional distinction among the services to be offered, and in the meantime a direct mapping to the general 5GEx architecture is made.

3.1.2.4 Aggregator role

The last business role in this list is the aggregator role that aggregates over many supplier partners (5GEx service providers) in order to make a viable (wholesale) product, and the basic service production is performed by the suppliers below the aggregator. This role can also be called as broker or alliance facilitator, and it will be further elaborated in Section 3.4 below.

3.1.3 Mapping 5GEx actor role model to NGMN ecosystem

In this subsection we cross-compare the Generic Actor Role Model of the previous subsection with the ecosystem analysis performed by NGMN[8]. In particular, in the remainder of this subsection we present the NGMN actor-role model, which has striking similarities to the one presented in the previous subsection.

We take MGNM Alliance as a relevant reference for the business analysis in 5GEx, since MGNM aims to provide a real integrated and cohesively managed delivery platform in order to bring affordable mobile broadband

[8] Next Generation Mobile Networks (NGMN) Alliance: https://www.ngmn.org/

services with a particular focus on 5G. The NGMN Actor-roles and envisioned business models are illustrated below:

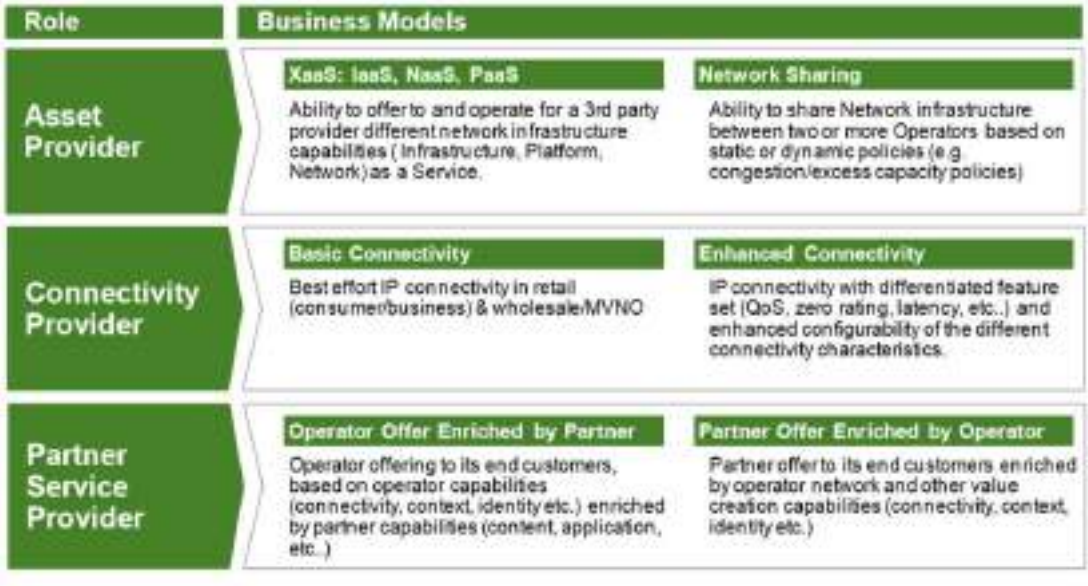


Figure 3-2: NGMN roles and business models

NGMN clearly separates between connectivity, either basic or enhanced and network as a service. To this end, the *Connectivity Provider* role is identified as providing IP connectivity with either basic Best Effort or enhanced-differentiated features. Basic connectivity for wholesale and retail customers is considered so as to include the existing business models while enhanced connectivity, in terms of performance, differentiation and configurability, is an outlook to the future and the 5G emerging connectivity services.

The *Asset Provider* is basically an Infrastructure Service Provider, capable of provisioning and operating Infrastructure, Platform and Network as a Service. This role actually supports XaaS (Anything as a Service), which is one of the core services envisioned by 5GEx as well. This role opens the door to business models where infrastructure is transformed from a siloed resource bundle to assets and services that are to be traded and orchestrated dynamically, based on dynamic and context dependent policies.

The *Partner Service Provider* role goes beyond the Core services provided by the two aforementioned roles and explicitly considers the offerings towards the customer, which may be an end user or an enterprise customer. Two variants are envisioned: The first variant directly addresses the *end customers* where the operator provides integrated service offerings based on operator capabilities (connectivity, context, identity etc.) enriched by partner (3rd party / OTT) content and specific applications. Video streaming services are an example of this variant. The second variant empowers partners (*3rd parties / OTTs*) to make offers to the end customers enriched by the operator network or

other value creation capabilities. An example of such services is remote health monitoring.

This taxonomy of roles is well in line with the 5GEx Generic Actor Role Model of the previous section. The NGMN *Connectivity Provider* role corresponds to the *5G Communication Service Provider (CSP)*. The NGMN Asset Provider covers the roles of the (5G) Infrastructure Service Provider (IfSP) and *(5G) Network Service Provider (NSP)*: In 5GEx we need both these roles in order to clearly mark the different infrastructure service offerings and the interaction with the *5G Enterprise Customer*. Finally, the NGMN *Asset Provider* maps to the *Online Service Provider (Digital SP)*.

The 5GEx Framework enables solutions for 5G enabled and 5G compatible SP-to-SP wholesale service trading where the above mentioned actors (actor roles) can meet and interact according to the 5GEx defined principles and interfaces. The 5GEx actors meet and interact either privately at their agreed private point of interaction or at what we call 5G eXchange points (5GX) where multiple such 5GEx actors meet and can trade 5GEx wholesale services according to 5GEx service specifications[9].

The core of the 5GEx Framework and such wholesale service trading is the multi-domain service and resource orchestration as defined by 5GEx. These capabilities and mechanisms will be further addressed below in subsequent main sections. Moreover, the below subsections will elaborate on the 5G and 5GEx (wholesale) Services and 5G Ecosystem characteristics (Section 3.1.3), as well as specific roles in relation to advanced collaboration models such as federations and alliances (Section 3.4), while Section 3.6 addresses at a high level the key 5GEx collaboration and coordination models.

3.2 5G and 5GEx Services and business models

Based on the analysis done in the previous section, this section focuses on the specifics of 5GEx in terms of wholesale services and a respective classification, also highlighting some key attributes.

The respective service offerings and envisioned business models have also been considered in 5GEx, which jointly address the needs of the wholesale, i.e. market among providers, and the retail, i.e. towards the end user, markets. 5G and Internet services pertain to two different layers and corresponding markets with different stakeholders and business relationships:

- The *Core Assured Service Quality Interconnection Services* (ASQ paths, ASQ traffic exchange), which are set up and traded among

[9] We anticipate that 5GEx Service Specifications will not only be those specified by the 5GEx project but also services as specified in the future according to the 5GEx defined principles.

Network Service Providers, over a multi-operator backbone network supporting 5G/Internet. These are the core infrastructure services that pertain to aggregate data flows, possibly crossing multiple administrative and technological domains.[10]

- The *Value Added Connectivity Services (VACS)* that are the customer-facing connectivity services (on-demand session level) where the network performance is either assured (absolute performance objectives) or improved (relative performance objectives). These services involve the end user and QoS must be taken care of, even at per-flow level, as opposed to the Core services where due to scalability and cost efficiency reasons only large traffic aggregates are managed.

The 5GEx Framework should prepare for the setting where the on-demand and real-time end-to-end quality management of the end-user connectivity (VACS) can be satisfactorily handled, by coordinating the policy control and enforcement at the service nodes of the edge NSPs that serve the end-points that take part in the VACS. By these policies, the VACS traffic is steered onto the Assured Service Quality (ASQ) paths for carrying the traffic across network domains.

The Core and VACS services, their scope and reach in the network for an IPTV "vertical" is depicted below, with the internal darker cloud highlighting the reach of Core services, while the external lighter cloud towards end users' end points and flows are in the scope of VACS. This separation has also been accepted by multiple 5G and Internet related initiatives in the communities, such as [52]).

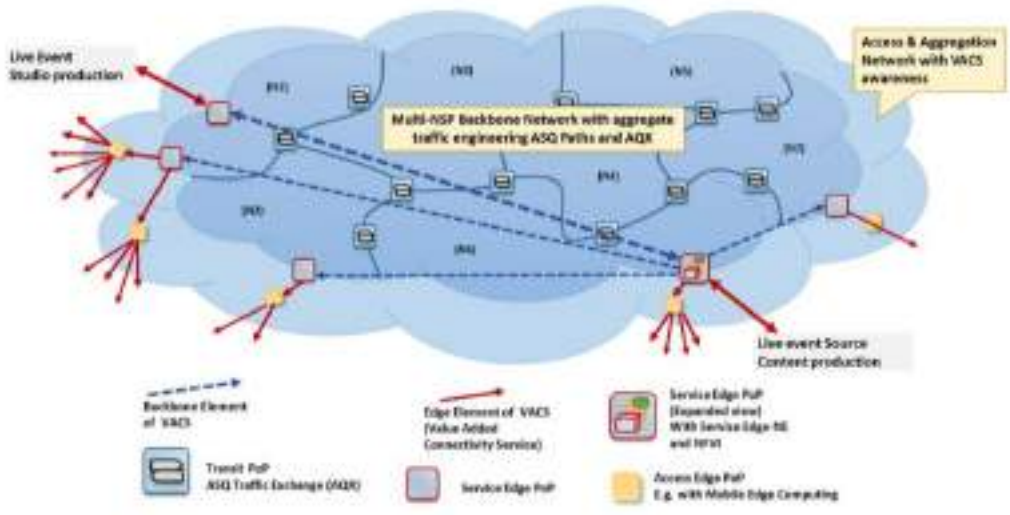


Figure 3-3: Core and VACS services for IPTV vertical

[10] In a similar way, dealing with aggregate level traffic, we also anticipate Enterprise ASQ Interconnection (service) offered by NSPs to Enterprise customers like DC service providers, Online (Digital) Service Providers or in relation to Enterprise VPN Customers.

As also discussed in Section 4 and in the next subsection, the Core and VACS services can be supported by 5GEx by relying on lower-level, less complex commodity infrastructure services built around the notion of *slice*. A slice is a managed set of 5G resources and (potentially) network functions tailored to support a particular type of user or service.

Slices are instantiated on demand using APIs exposed by the management plane, providing dynamic orchestration for multi-layer and multi-domain networks. Virtual resources and Network Functions (VNFs) are composed into slices. To that end, 5G slices lever on the Network Function Virtualisation Infrastructure as a Service (NFVIaaS) paradigm; slices make up infrastructure services, by the concept of Slice-as-a-Service (SlaaS); finally, infrastructure services enable custom VACS and customer specific VNFs.

This way, any high-level services can be decomposed and supported by ASQ connectivity services delivered to a specific Point of Interconnect on top of which service-specific VNFs, also providing control and management over the underlying infrastructure and traffic, can be chained and deployed. These 5GEx-specific roles and services are specified in the next subsection. In Section 4 we discuss the various layers of 5GEx services also from a business point of view, depicting the different value they generate, ranging from low-level low-margin commodity infrastructure services building blocks to high-margin differentiated customer-specific services.

In the remainder of this subsection we provide an overview of the Catalogue of the 5GEx Wholesale Service types offered over Interface 2 or Interface 1. This is an initial listing of the 5GEx wholesale service offerings foreseen to be facilitated by the 5GEx framework, which are also aligned with the layers of 5GEx services elaborated in Section 4. A detailed specification of these services, including their parameters, semantics and data model is to be reported in Deliverable D2.2.

In particular, in this document we mostly focus on 5GEx NSP-to-NSP services (over Interface 2), as well as some initial proposals regarding NSP-to-5GEx Enterprise Customer, e.g. NSP-to-Online Digital Service Provider (over Interface 1). As also explained previously in this subsection, the notion of ***Assured Service Quality (ASQ) connectivity*** is the general term covering all granularity levels of connectivity, from Core ASQ paths, through VPN and Enterprise ASQ interconnection paths to Value Added Connectivity Session services (VACS) level. To this end, the main categories of 5GEx wholesale service types are the following:

A. Core ASQ Connectivity Infrastructure services (NSP-to-NSP): These are the multi-provider wholesale connectivity services that comprise the wholesale communication layer upon which all 5GEx services can be instantiated.

B. Core ASQ Path Information services (NSP-to-NSP): These are the ASQ capabilities "publication"/"directory" services addressing the general ASQ path capabilities from one PoP to another PoP.
C. Enterprise ASQ Connectivity Infrastructure services (NSP-to-Enterprise): These are the wholesale connectivity services towards the 5GEx Enterprise Customers. The granularity and scope of these services, as well as their control and management API is different than those of A, while adapting many of the same capabilities.
D. Value Added Connectivity Session (VACS) services: As explained above, these can be instantiated over Interface 2 or 1, depending on the business relationship and API type in focus, whether that of 5GEx Enterprise Customer (e.g. Online Digital Service Provider) or the NSP-to-NSP relationship.
E. ASQ Connectivity Supporting Information services: Information services providing forecast or monitoring information on the quality anticipated or experienced over multi-domain paths, regions and specific VACS flows.
F. Telco[11] Cloud Infrastructure services: These are NFV Infrastructure as a Service service offerings (aka. SlaaS), potentially bundled with ASQ connectivity.
G. Virtual Network Function services: These are VNFaaS service offerings. As for the resource slice as a service (item F) this service can be bundled with ASQ connectivity

This Catalogue of 5GEx Service types is elaborated to contain a listing of the main services envisioned, i.e. the entries of the 5GEx Service Catalogue whose initial draft can be found in Appendix F. The service catalogue is relevant for all the coordination models and 5GEx service deployment options documented in this deliverable. It comprises a major value offering of 5GEx upon which the business models of the actors can build upon. Business models are also to be reported in Deliverable D2.2.

[11] The notion of Telco is used here as the typical scope of this actor goes beyond that of purely being an NSP.

3.3 5GEx Solutions

The proposed 5GEx Framework allows and supports a variety of specific deployment models referred to as 5GEx Solutions.

First, "direct peering" at an already established local or remote IXP or IPX exchange point, but evolved towards compatibility with the 5GEx Framework, thereby operating as a 5GX.

Second, a new type of dedicated (for-profit) Exchange Point. This instance of 5GX infrastructure is operated by a standalone entity called 5GX Provider (5GXP); 5GXP is somewhat similar to the AMS-IX example in section 3. In addition, the 5G Exchange Framework also supports higher level abstractions and advanced models covering views, resources and services across several 5GXs and other, private PoPs.

Third, the 5GEx Framework can be realised via distributed multi-party collaboration, where the operators implement the exchange functionality in a distributed manner inside their own infrastructure. This Solution option ensures that there is no dependence on other actors in realizing 5GEx. This could be a fallback operation mode, should any persistent error or business dispute arise at a 5GX.

An optional, but potentially important role in the 5GEx ecosystem is that of the customer-facing 3rd Party Providers (3PPs). These entities do not necessarily own infrastructure, but they do implement the multi-domain orchestrator functionality, so they can facilitate service trading (at an abstract level, this role is analogous to a Mobile Virtual Network Operator in today's mobile market). 3PPs can be present at a 5GX or private PoP, where the 5G Enterprise Customer and the Primary Provider meet for service negotiation and setup.

3.4 5GEx collaboration variants

Depending on the respective *collaboration model* the 5GEx community chooses to adopt (this collaboration model is expected to evolve during time), a 3PP can implement different functionalities. The initial collaboration model is expected to be an *open community*, where only technical compatibility cooperation between neighbouring operators are foreseen. In such a context, a 3PP *Broker* could provide a value added service by collecting individual offerings, forming a link between Enterprise Customers and suppliers, thereby catalysing service trading.

As 5GEx evolves toward a more integrated operation and collaboration mode of *Federation* (expected to happen quickly to take advantage of EU-wide footprint), a standardised way of information sharing among participating providers emerges. This enables the creation of service catalogues, potentially covering all service offerings of the 5GEx community. In such an environment, besides the Broker, 3PPs able to present an aggregated view of these distributed service catalogues

towards the Enterprise Customers (and potentially towards operators inside the 5GEx community), are foreseen to emerge: this role can be referred to as *Aggregator*. Aggregators are vital for customers who look for services requiring large geographical footprint (coverage), which can be realised by composing a complex service from the aggregated catalogue.

When the 5GEx community reaches a certain level of maturity, and multilateral trust has been formed among participants, the *Alliance* collaboration model may become feasible. In an alliance, more technical details and also some level of business information are shared among members. In such a deeply cooperative environment, a 3PP instantiation of *Alliance Facilitator* is needed. Such a facilitator is usually jointly owned and by alliance members, while the technical implementation of the role could be centralised (as a separate entity) or distributed (facilitator logic implemented at several alliance members). The main purpose and advantage of a facilitator lies in efficient cost and revenue sharing, boosting the profitability of both the alliance and individual members.

3.5 Service and resource trading

Services trading can take place both between Enterprise Customer and 5GEx, and internally between different providers inside the 5GEx community. In the first case, the Enterprise Customer can request a service from a Primary Provider (which can be a real provider or a 3rd Party Provider Broker/Aggregator) by means of a B2C interface to the customer (referred to as Interface 1 in the 5GEx baseline architecture shown in Figure 7-2). Service offerings are described in catalogues. After the service request is accepted, it is the responsibility of the Primary Provider to create the service; this potentially includes establishing the required "subcontracts" with other providers implementing parts of the requested service through a B2B interface between providers (referred to as Interface 2 in the 5GEx baseline architecture). In the second case, the operational process is similar, but IfSPs (and NSPs) are more likely to be involved in such services, as CSP and DSPs are expected to request lower-level infrastructural resources. Resources from the connectivity, storage and compute domain are expected to be virtualised based on predefined ontologies and can be requested on-demand or traded via catalogues in a similar way with the Amazon standard VMs that can be either purchased on-demand via a fixed catalogue or even through spot markets. Virtualised resources are essentially the lowest-level 5GEx building blocks, to be incorporated in slices and used for service orchestration, instantiation, scaling and management.

Slice trading takes place inside 5GEx in order to combine resources and services of multiple providers so as to orchestrate services. In this case, the "internal" customer role is with a provider within the 5GEx Community, who can purchase by means of Interface 2 resources and VNFs from other providers. Interface 3 (see Figure 7-2) can be used to

provide the 5GEx API for managing those leased resources and services, which can be combined with provider's own in order to build proper slices for the support of customer services. This internal trading is not visible from the external 5GEx enterprise customers who should not be bothered with the details and specifics of the mechanics of service orchestration, as long as the desired quality and performance requirements are met by the service provisioning. Details on how slice trading, control and management are performed are provided both in Section 4, under the XaaS use case, and in the remainder of this deliverable where the architecture details and functions are elaborated.

3.6 5GEx coordination models

An important aspect of the 5GEx Framework is to specify the 5GEx coordination models that are relevant for interfaces 1 and 2, i.e. how 5GEx providers and customers can interact in order to request, offer or trade services. Going into the specific properties of specific services, such as the different kinds of the connectivity ASQ path services there will be additional details to consider. However, from a business and economic framework point of view there are six generic models that capture what are believed to be the major coordination models.

These six models are derived from the basic options in the inter-provider coordination:

Push vs. Pull: Services may be either: (1) requested on-demand by the customers submitting a service request specifying in detail what is to be delivered and for what price or alternatively (2) Providers may advertise their service offerings in a catalogue and customers can browse, buy off-the-shelf and customise the service that meets their needs. Furthermore, a topic for further study is a service catalogue with price labels or categories, not explicit tags. The Provider-specific price labels can be the basis of further price negotiation among the Service/Business Planes of the Provider and the Customer so that the final price can be agreed, also based on the feedback from the underlying Control Plane.

Centralised Facilitator/Orchestrator versus Fully Distributed Service Orchestration: The next option is whether service orchestration is to be performed by a central, possibly third-party facilitator, who is trusted by all the 5GEx Providers and is responsible for meeting the supply of services by the 5GEx Providers with the demand of Customers. The alternative would be to rely on possibly cascading bilateral communication among the 5GEx Providers so that the desired service is negotiated and built in a fully distributed fashion.

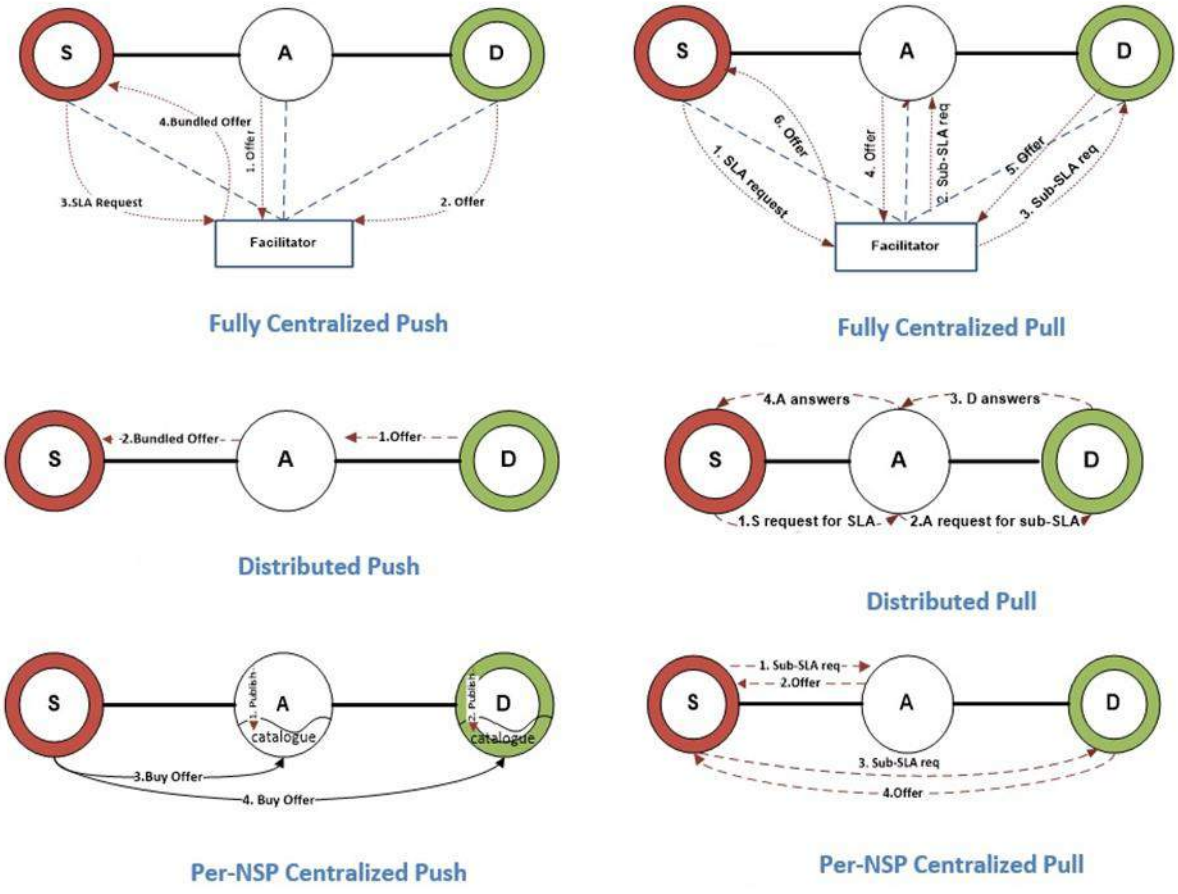


Figure 3-4: 5GEx coordination models

Fully Centralised versus Per-NSP Centralised: A centralised Facilitator/Orchestrator entity may not be appealing to all 5GEx Providers, since especially bigger Providers may be unwilling to hand off service orchestration of their customers to a third party entity. Though smaller Providers may be better off with such a solution, larger NSPs may choose to roll out their own Orchestrator and keep service composition and thus customer ownership as a key asset of their business. They might team up with other 5GEx Providers with whom they maintain business relationships to join their service orchestrator solution, in a similar fashion that alliances among airline carriers are formed around the biggest airlines. Finally, a fully centralised solution may face scalability limitations and constraints, especially as the number of 5GEx Providers and service requests/offers increases.

The differences between the models in the way that a service is composed alter the entities that are responsible for the SLA commitment. In the Fully Centralised models the Facilitator is the only responsible of the end-to-end SLA commitment as the contract is established between it and the buyer. In case of problem, the Facilitator may interrogate each NSP that is involved in the contract to determine the faulty network. In Distributed models the first contract is established between the buyer and the seller. Thus the latter has the responsibility of the end-to-end SLA commitment. Since each NSP in the chain subcontracts his neighbour in

order to form buyer-seller pairs until the destination is reached, the seller NSPs is always responsible. In Per-NSP Centralised models the primary provider which is a buyer in relation to its subordinate providers is responsible for the contracts it establishes with each of these other NSPs. The end-to-end SLA commitment is guaranteed only by the primary NSP as all the subsequent NSPs are not aware of the specific customer usage of their respective offers in the service composition. In case of failure the primary NSP is responsible to determine the faulty provider.

In the models we assumed that the "baseline publishing" phase has been concluded already. In this phase the SLA capabilities or event offers (cf. Push model) and/or Network Capabilities (respectively for the push and the pull model) are published as an initial stage. In fact this step has not been determined yet for each model.

There are four different options for the publishing phase:

1. Publish only to direct neighbours. This scenario protects confidentiality, since it does not allow a global vision of what SLA offers or Network Capabilities. Due to its nature, this scenario is only pertinent in the distributed push and pull approaches. To overcome this possible limitation, NSP relations without direct connections could be set up.
2. Publish only to the Facilitator. This is only available in the Fully Centralised scenarios.
3. Publish to all NSPs. In this case, the architecture must support a flooding mechanism that can overcome non-cooperative NSPs.
4. Publish to a subset of NSPs governed by policy rules. This is more general than the options above and might need complicated mechanisms from a technical point of view.

So far we have presented the coordination models for connectivity services. These models can be extended for compute and storage services as well, or bundles of them, for 5GEx customers that are members or external to the 5GEx community, as depicted in the figure below for the Distributed Pull model.

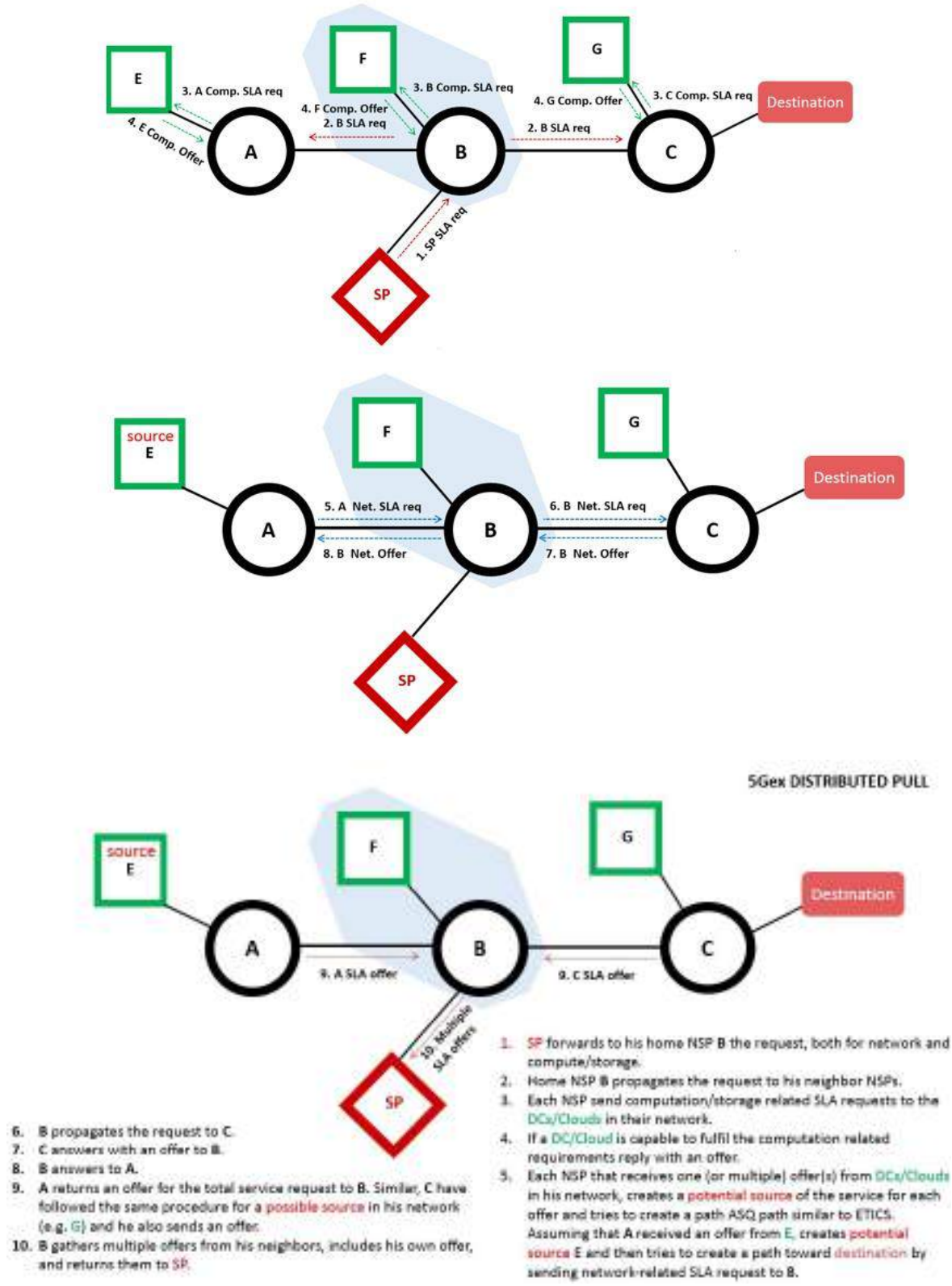


Figure 3-5: 5GEx distributed pull

4 Use cases and Requirements

4.1 Use cases

4.1.1 Introduction

This subsection introduces the main use cases of interest for 5GEx. It also describes a methodology to perform a grouping of use cases to use case categories ("families") that can be used as starting point for analysis in the 5GEx project, both in terms of WP2 architecture insights and WP4 demonstration. The use case family specification aims to cover the three "use case categories" described in the 5GEx Description of Action (DoA), and depicted below, to ensure a comprehensive approach while limiting the complexity of addressing so many specific use cases at this stage, which is not beneficial for advancing the architecture work.

An additional benefit of the use case family specification is that they allow their agile enrichment with potentially new use cases that are becoming more interesting and trending in the industry, so as to ensure that the 5GEx architecture is capable of meeting the needs of new services.

The 8 use cases identified in the Description of Action were grouped to 3 phases: Connectivity, NaaS and MdIaaS. The differences among the use cases of the first two categories are typically small in terms of functional and non-functional requirements, elementary functions and data models/interfaces to be supported by the 5GEx architecture. 5GEx focuses on multi-operator infrastructure services on top of heterogeneous technical and administrative domains, thus the technology-specifics of the underlying infrastructure have incremental impact on the architecture requirements and functional blocks, which are rather generic. Therefore, rather than addressing in detail the specifics of the underlying technology over a large number of use cases, it is more cost-efficient to focus on the wider use case families to progress the architecture work and use the specific use case instances as verification, refinement and demonstration feedback loop for the 5GEx architecture.

This way, the specification of fewer use case families can help the progress on the architecture specification, while also meeting the project's contractual obligation to support the Description of Action use cases.

Phases	*Id*	*Use Case*	*Short Description*
Connectivity	UC-1	Network creation across multiple optical domains	Network operators have deployed optical domains with multiple vendors that cannot be interconnected because of the particularities of each implementation. Therefore each optical domain becomes an isolated island in terms of provisioning.
	UC-2	Multi-technology Connectivity Service Provisioning	In this use case an abstract, packet oriented connectivity service is provided, such as a L3 or L2 VPN, across multiple domains including ones with legacy, distributed control (such as IP/MPLS) and one with SDN control. The use case also covers recovery from a failure.
	UC-3	Packet services Multi-domain	The "packet based" services imply the exchange on the control plane of "routing information" between domains. There are at least two alternative solutions: (1) a client-server relationship following a hierarchy; (2) A peer relationship, where the controllers interchange the routing information.
Network as a Service (NaaS)	UC-4	Multi-domain mobile backhauling	Mobile operators can rent backhauling capacity from a wholesale provider. The incremental step respect to current deployments is the ability of dynamically controlling the leased capacity by the contracting operator. By that means, the contracting operator can achieve a total control of the infrastructure, either own or rented, for seamless provisioning and operation.
	UC-5	Multi-domain network sharing	Operators can agree on mutual sharing of access and transport infrastructure capacity owned in separate regions, as a way of reducing network deployment costs. Under this assumption for any of the above mentioned regions, each operator performs homogeneous control through owned and non-owned capacity, ensuring recovery and protection in case of network failures.
	UC-6	Network slicing	In this scenario, in one or more network domains the physical infrastructure is sliced into logical virtual partitions allowing a homogeneous control independently of the ownership of the underlying network.
Network + Storage + Compute as a Service (MdIaaS)	UC-7	Deployment Content Delivery service across several domains	Video and, in general, multimedia content is one of the drivers of current capacity consumption growth in operational networks. The use case refers to the orchestration of the live deployment of CDN caches on different network infrastructure according to the perceived real demands.
	UC-8	Multi-operator IaaS	In this use case the end user can request an IaaS service from its cloud service provider. The requested service is a mix of VMs (and associated) storage and connectivity between them using connectivity resources from different network providers.

According to the progress of the project, new specific use cases will be taken into consideration for assessment and refinement of the architectural definitions. The classification around 3 families also allows aligning the software releases that WP3 is performing through the project lifetime, as well as the different experiment waves that WP4 will perform. This set of use case families, besides technical merit, should also be useful from a *business perspective* in the 5G ecosystem, to ensure that

there is actual market demand for and impact of the 5GEx infrastructure services and use cases in the 5G services ecosystem.

5GEx is the focal point for providing *multi-operator infrastructure services*, hence is focused on the *wholesale market* among infrastructure and service providers. In order for these infrastructure services to be meaningful, it is important to relate them to the end-user 5G services (henceforth interchangeably referred to as *product-oriented use cases or "verticals"*) of the end consumers (the *retail market*). This is a key factor that has been highlighted by SDOs and fora such as NGMN and industry white papers (cf. Figure 4-1).

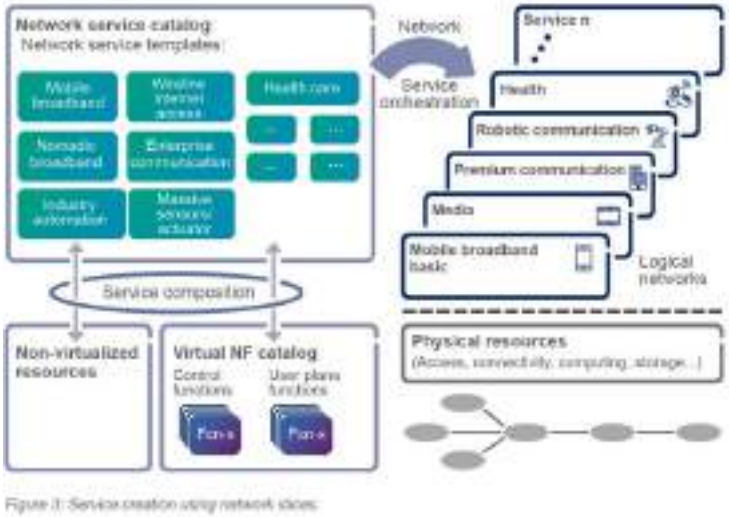


Figure 4-1: The correlation of wholesale infrastructure services and retail verticals. Source: Ericsson whitepaper "5G Systems"

4.1.2 The grouping procedure for the definition of the use case families

The *first step* towards specifying the preliminary set of use case families for progressing the project advances is a wide categorisation of product-oriented use cases that could be supported by a limited set of infrastructure services. Rather than start from scratch, we opt to use the NGMN use case classification to 8 families, since: a) NGMN has wide industry participation, also in line with the 5GEx consortium synthesis, b) the use case grouping is based on requirements that the network (including the access) should meet in order to jointly support each set of verticals, c) the product-oriented use cases selected are considered important from an industry point of view, d) the NGMN grouping was also performed in order to promote the 5G services requirements and architecture work by NGMN.

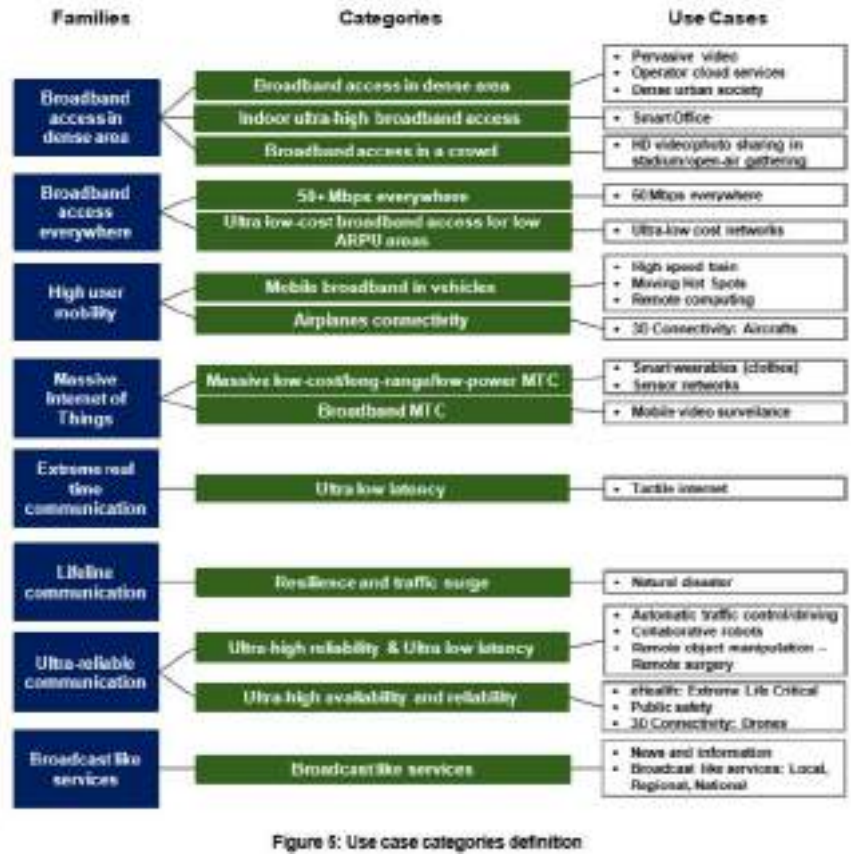


Figure 4-2: NGMN use case categories

The *second step* is to further reduce the categories, depicted as Figure 4-2. Hence, we group categories that support similar product-oriented use cases/services, are closely related in terms of requirements and mostly differ in terms of user equipment and mobility/speed patterns, which do not fundamentally affect 5GEx. Therefore, we group families 1-3 and 8 to Family 1, families 5-7 to Family 2, and family number 4 to Family 3, as depicted in Figure 4-3.

The *third step* is to specify the families of wholesale infrastructure services, based on this categorisation. This is performed in the next subsections.

4.1.3 5GEx Use Case Summary

Based on the methodology described in section 4 and the Description of Action use case categorisation presented in subsection 7.1, 5GEx envisions a preliminary set of use case families, covering multiple 5G infrastructure services, use cases and verticals. In this subsection, we provide a brief use case summary and discuss the value creation aspects of the use cases.

Figure 4-3: The wide categorisation of use case families motivating 5GEx use case families

In particular, Connectivity is a use case family of wholesale connectivity services, including both Core and VACS services (cf. Section 6) over multiple domains, capable of supporting next-generation connectivity verticals of Group 1, such as VPNs and broadcast services. It also maps to the use case Phase 1 of the Description of Action.

Virtual Network Function as a Service (VNFaaS) is an evolution of the Description of Action Phase 2 (NaaS) and partly Phase 3, with advanced management and elasticity capabilities and VNFs for broadband and infotainment verticals of Group 1 and 3. The consumer has access to the VNFs to support verticals such as (virtual) CDN for content delivery of cacheable or streaming content.

Slice as a Service is the widest use case family, building on top of the Connectivity and VNFaaS use case families with the additional requirement and complexity that the customer has full access to the virtual resource, and can support additionally the more demanding verticals of Group 2. It maps to the use case Phase 3 of the Description of Action. This is the use case family that allows the support of XaaS (Anything as a Service) and constitutes one of the core value propositions of the 5GEx architecture and project.

Thus, the resulting use case families are as follows:

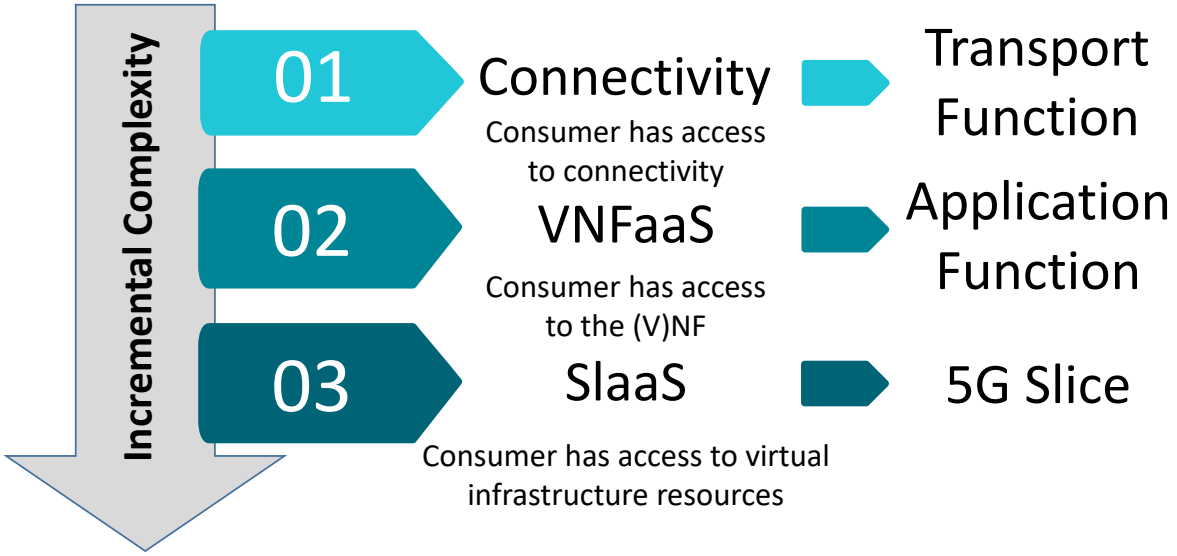


Figure 4-4: The 5GEx use case families

A more detailed overview of the use cases is provided in the next subsection. We now briefly comment on the positioning of the use case families and their value proposition in the 5GEx ecosystem and layered service provisioning model. The 5GEx hierarchy of resources and services is depicted as Figure 4-5: Lower-level resources are the low-margin commodity building blocks of 5GEx, input to virtualisation. Virtual resources and NFs are composed into slices under the Network Function Virtualisation Infrastructure as a Service (NFVIaaS) paradigm. Slices are traded (via interface 2) and used to build infrastructure services, by means of the concept of Slice-as-a-Service (SlaaS) which is internal to 5GEx and visible only to 5GEx Providers (see Section 6 for details on the 5GEx Actor-role model and definitions). Finally, infrastructure services enable custom wholesale services, including VACS and customer specific VNFs, which are also made available for the 5G Enterprise customers. It is envisioned that the most frequently demanded and popular infrastructure services, such as those contained in the use case shortlist of this section, can be offered by means of service catalogues, as also shown in Figure 4-1. Therefore, the 5GEx use cases by-design consider the needs of 5G customer-facing services and their requirements.

There is a clear analogy with the cloud ecosystem and business models in terms of layered service provisioning and value proposition. The 5GEx layers are similar to the layers of cloud resources and services ranging, e.g., from the low-layer Amazon's S3 and EC2 to the AWS CloudFront high-level streaming service (and similar). Similarly, 5GEx lower-level resources are the *low-margin commodity building blocks* of low value that through the added value of the 5GEx Multi-domain orchestration and management functions are used to support differentiated higher-level wholesale infrastructure services for serving the 5G verticals, targeting specific markets and offering complete and customizable enterprise customer solutions. The higher the placement of a 5GEx service on the

layer of the pyramid is, the higher the technical complexity, as well as the customer value and monetisation potential for that service are.

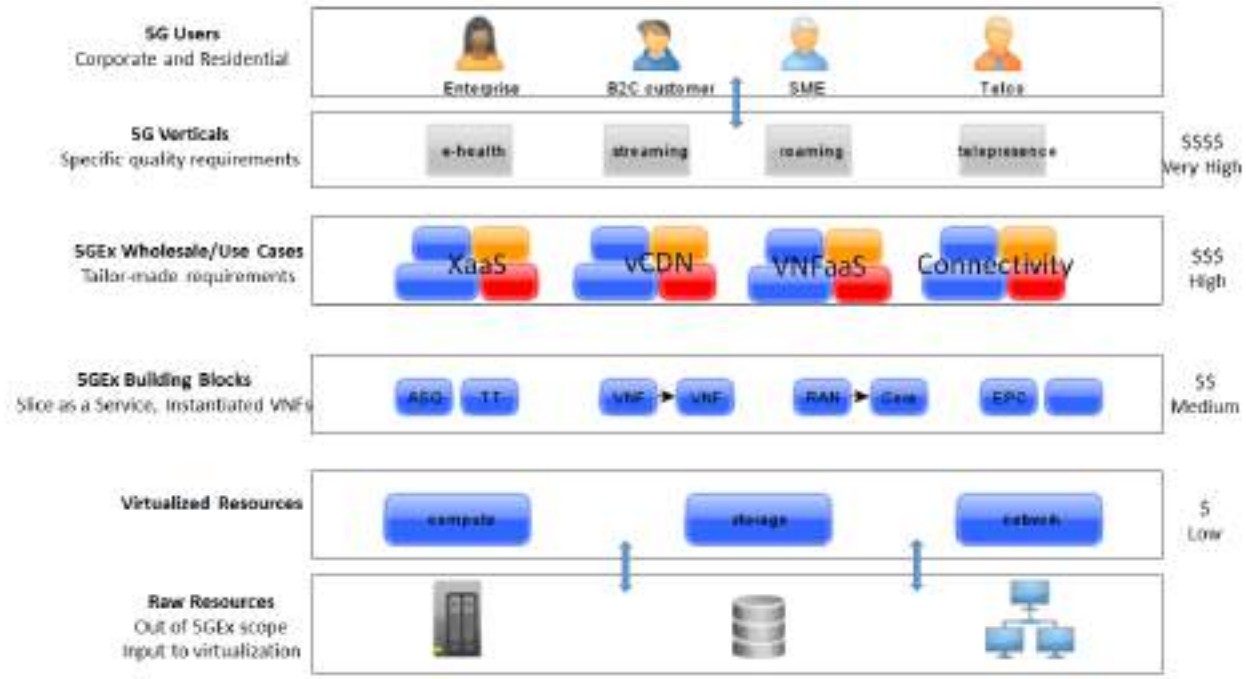


Figure 4-5: The 5GEx service and value creation layers: from commodity resources to high-margin tailored services

Finally, we comment on the relation of the use case families to the 5GEx experiments and also provide some new use cases that are relevant and interesting for the project below.

Families	*Id*	*Use Case*	*Short Description*
Connectivity	UC-1	Network creation across multiple optical domains	Network operators have deployed optical domains with multiple vendors that cannot be interconnected because of the particularities of each implementation. Therefore, each optical domain becomes an isolated island in terms of provisioning.
	UC-2	Multi-technology Connectivity Service Provisioning	Provisioning of an abstract, packet oriented connectivity service, such as a L3 or L2 VPN, across multiple domains including ones with legacy, distributed control (such as IP/MPLS) and one with SDN control. The use case also covers recovery from a failure.
	UC-3	Packet services	The "packet based" services imply the exchange on the control plane of "routing information" between domains. There are at least two alternative solutions: (1) a client-server relationship following a hierarchy; (2) A peer relationship, where the controllers interchange the routing information.
VNF as a Service (VNFaaS)	UC-4	Mobile backhauling	Mobile operators can rent backhauling capacity from a wholesale provider. The incremental step respect to current deployments is the ability of dynamically controlling the leased capacity by the contracting operator. By that means, the contracting operator can

			achieve a total control of the infrastructure, either own or rented, for seamless provisioning and operation.
	UC-5	Network sharing	Operators can agree on mutual sharing of access and transport infrastructure capacity owned in separate regions, as a way of reducing network deployment costs. Under this assumption for any of the above mentioned regions, each operator performs homogeneous control through owned and non-owned capacity, ensuring recovery and protection in case of network failures.
	UC-6	Network slicing	One or more network domains the physical infrastructure are sliced into logical virtual partitions allowing an homogeneous control independently of the ownership of the underlying network.
	UC-7	Deployment Content Delivery service (vCDN)	Video and, in general, multimedia content is one of the drivers of current capacity consumption growth in operational networks. The use case refers to the orchestration of the live deployment of CDN virtual caches on different network infrastructure according to the perceived real demands.
Slice as a Service (SlaaS)	UC-8	IaaS	In this use case, the end user can request an IaaS service from its cloud service provider. The requested service is a mix of VMs (and associated) storage and connectivity between them using connectivity resources from different network providers.
	UC-9	GILAN / Roaming	Network slicing plus VNF placement (controlled by the remote operator) on another operator showing the local break out case.
	UC-10	My Cloud Anywhere	Dynamic cloud/VNF deployment/migration following the user location.

4.1.4 Use Cases Description

A brief description of the 5GEx use cases is included next. The interactions per use case are indicative; multiple coordination models are possible, thus differentiating the entities, nature and sequence of interactions.

4.1.4.1 Connectivity

Description: Connectivity is a family of wholesale connectivity services, and in particular managed assured quality inter-working services between multiple autonomous systems. Connectivity includes both Core and VACS services:

A) *Core Services* of Assured Quality paths among the 5GEx NSPs that transport traffic aggregates, thus there is no per-flow control or management functionality. In general, these ASQ paths may be point-to-point or point-to-region, with point being either a Point of Interconnect or a Point of Enterprise Interconnect. These ASQ connectivity service create

an ASQ backbone where Assured Quality services can be exchanged among the 5GEx NSPs. For instance, a point-to-point connection interconnecting two different ASes (or Datacenter islands) and crossing multiple intermediate NSPs, and providing specific bandwidth, delay, jitter, loss, availability guarantees is an example of such a service.

B) *Value Added Connectivity Services (VACS),* which are the customer-facing connectivity services of assured or improved (relative performance objectives) network performance where the end user and QoS must be taken care of, e.g., to support the broadcast of a Live Event from a studio to multiple end points across the network, serving a large number of end users.

Mapping: This 5GEx use case maps to the "Connectivity" group of use cases described in subsection 4.1.1. Adding advanced features such as UC-5 "Multi-domain network sharing" or elastic reconfiguration of the connectivity path resources allow this wholesale service to fall into the Network as a Service (NaaS) category as well.

Interactions: The following stakeholders are involved in an example of this use case, with the major interactions being:

1. The 5GEx Customer, e.g., a Video Delivery Service Provider, needs to interconnect its datacenters from country A served by ISP1 to location B served by ISP2 and location C served by ISP3. To this end, it submits a service request (plus Service Level Specification, SLS) for an assured connectivity service to ISP1 and in particular to ISP1 orchestrator (Interface 1).
2. ISP1 can deliver what the customer asks for (checks via Interface 3) in his own region and then contacts its business partner ISP3 (Inter-Operator Orchestration API of Interface 2), to deliver the rest of the service.
3. ISP3 checks that is capable to meet the SLA in its own network and reaches out to ISP2 with whom it is interconnected to provide the rest of the service.
4. ISP2 accepts and provides the SLA to ISP3.
5. ISP3 bundles this SLA into its response to ISP1, providing an SLA for the assured quality connectivity service.
6. ISP1 created an integrated SLA for the entire service, which corresponds to the SLS of the 5GEx Customer.

4.1.4.2 VNFaaS: the vCDN example

Description: The Content Delivery Network as a service, similar to what is also offered in the market now by platforms such as OnApp, but with advanced management capabilities and VNFs, also offering added value services such as dynamic reconfiguration. In the NFV context vCDN allows to deploy caches as VNFs (vCaches) instead of hardware appliances.

It is expected that providing vCDNaaS gives more flexibility and acceleration versus a traditional CDN based on hardware content servers. By means vCDNaaS it will be possible to easy re-scale the virtual caches that are part of the vCDN service across different domains. Therefore, the orchestration of the live deployment of virtual CDN caches on different network infrastructure according to the perceived real demands is envisioned.

Additional details about the vCDN use case can be found in Annex D and E.

Mapping: This use case maps to the "VNFaaS" category in particular UC-7 "Deployment Content Delivery service across several domains". Among other network appliances that can be virtualised by means of NFV orchestration to be offered as VNFaaS, such as e.g., firewalls, proxys, traffic classifiers, etc., vCDN represents a special suitable case that can benefit of its deployment in a multidomain environment in order to improve QoE by replicating the content in that domain that maybe closer to the end user.

Interactions: Sample interactions are indicated below for the on-demand composition of the vCDN service:

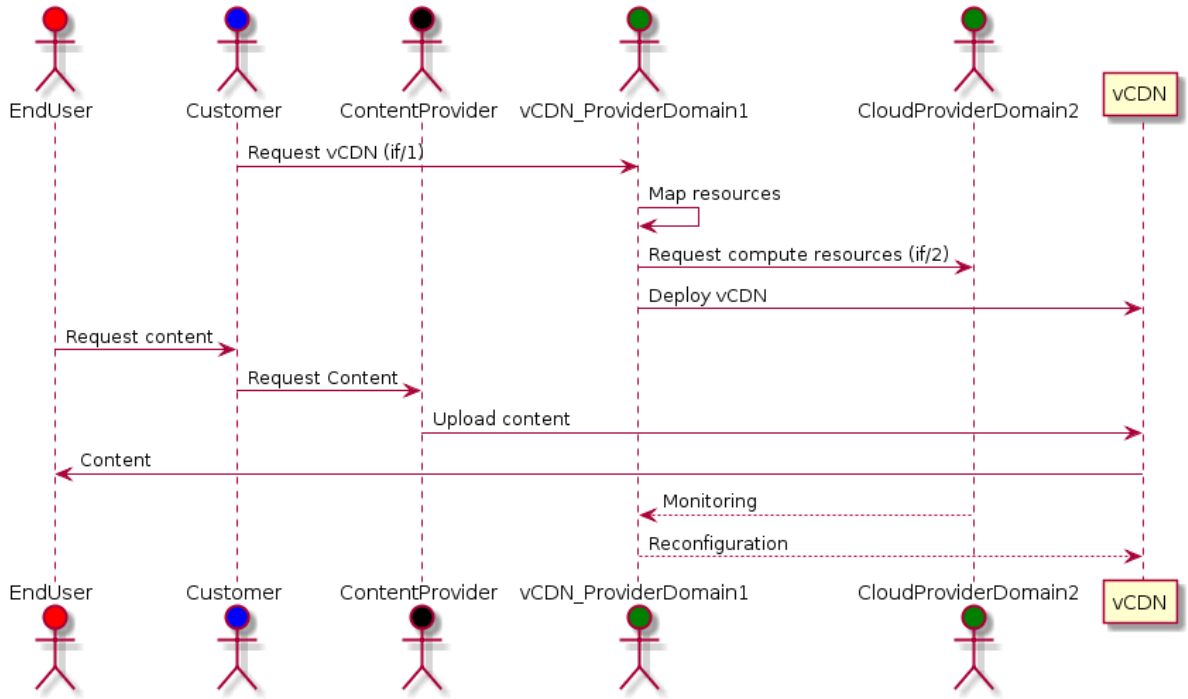


Figure 4-6: The vCDN use case interactions of the main stakeholders for on-demand bi-lateral service composition

4.1.4.3 SlaaS: the XaaS example

Description: Anything as a Service (XaaS) is the wholesale infrastructure service, which in its most generic form combines network, storage and compute resources from multiple 5GEx Providers. We refer to it as Slice as a Service (SlaaS) when those resources are traded in the form of a resource slice. To depict the potential of XaaS, a use case variant could

focus on advanced VACS, performance-critical networking with stringent QoS, reliability and potentially cloud/compute requirements, suitable for the e-health, telemedicine, and life-line support verticals. In the remainder of this subsection we will identify a type of Use Case involving the instantiation of services requested by Customers to be deployed on a set of computational, storage and network resources.

For a given provider (e.g., Provider A), the process of building up a service involving other external (foreign) Service Providers should consists of two different steps. In the first step, Provider A starts creating a global "picture" of what services other providers are able to offer, evaluating also the commercial/economical aspects. As soon as this first step is carried out, each time a service request is received by Provider A, the second step will consist in evaluating the current snapshot of the Service Providers belonging to the federation "picture" in terms of resource availability, offered QoS and granted SLA.

In the XaaS UCs context, a particular example/scenario that may be considered is depicted in Figure 4-7, and refers to the particular case of a Service Provider (A), which relies on its internal resources to provide services to its customers, that is overwhelmed by a temporary load peak due to unexpected high customers' demands. Is such a situation, as the Service provider may lack of internal resources to satisfy the instantiation of the requested services, it may need to borrow additional resources from other external Service Providers (B and C) to satisfy its customers' requests and ensuring the stipulated SLAs are still met. This will result in the reservation/allocation of computational (and/or storage) resources on different domains and will also require setting up connectivity between the entities that build up the E2E services requested by the customers. In Figure 4-7, a customer requests to SP A the instantiation of a service S1 which is then mapped on two different sets of resources (each one identified by a red rectangular shape): S1(A) belonging to SP A (including both computational and virtual network resources from an internal OpenStack domain) and S1(B) belonging to SP B (including both computational and storage resources from an internal CloudStack domain).

In the same XaaS context, a slightly different may depict the situation where another Service Provider may receive along with a service instantiation request some additional particular constraints/rules, requiring for a service to be deployed on resources located in different geographical areas (even outside of the administrative domain boundaries of the Service Provider itself). This can be requested for instance to cope with services instantiations in proximity to end-users and dense geographical distribution to reduce latency, improve QoS and achieving better mobility support (i.e., Mobile Edge Computing).

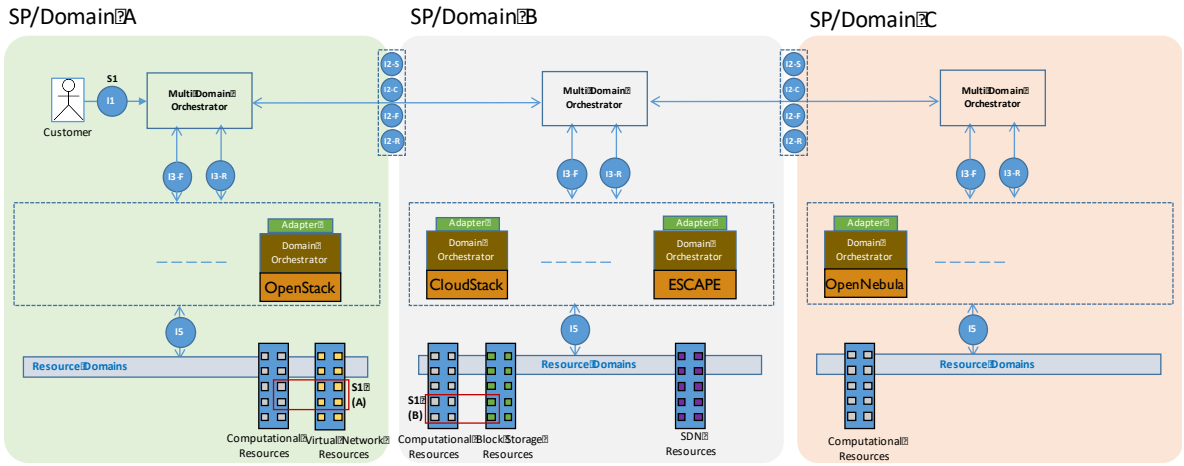


Figure 4-7: Example of XaaS involving three different SP in three different Administrative Domains

Starting from the above examples of SlaaS, we could try to generalise what the role of 5GEx will be as enabler for their implementation. 5GEx should be able to create, manage and orchestrate IaaS instances potentially spanning across different administrative domains. Furthermore, as for each administrative domain different technological domains may take part to the instantiation of the resource infrastructure where the services will be deployed, 5GEx should also be able to deal both with different IT (Cloud) Domain Orchestrators to allow the dynamic reservation/creation of computational resources and different Network Domain Orchestrators needed to properly set up the whole inter-domain communication layer. Finally, from a customer perspective all the services should be deployed and accessed transparently, regardless of the particular domains where resources have been allocated.

The demonstrable product-oriented use case could be eHealth in order to depict the reliable and critical aspects of the SlaaS service.

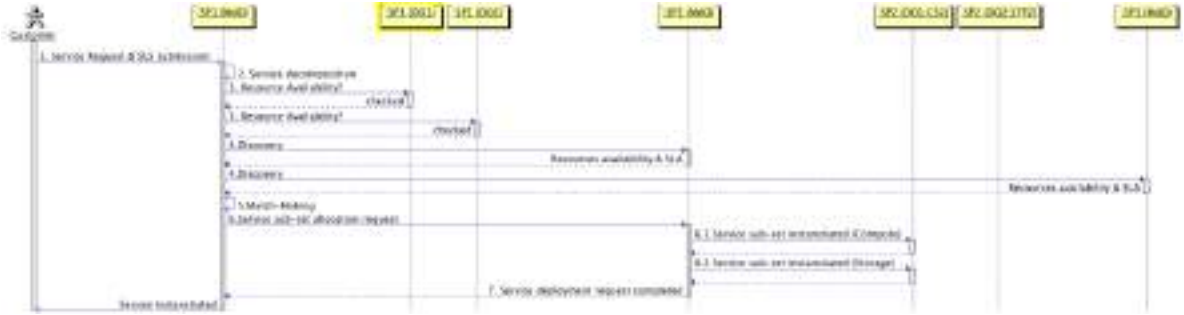


Figure 4-8: XaaS actors interaction

Interactions: The 5GEx Customer, for instance an eHealth Service Provider, needs to provide eHealth services over a region and also uses IoT data (e.g., sensor data on temperature, humidity, pollution) to predict on the fly the risk for certain groups of patients. This particular scenario might be considered in the context pointed out above where, in a Federation of different Service Providers, one (or more) will be responsible for managing a *Mobile Edge Domain* located in proximity to

the geographical location(s) where data will be gathered from. The following steps refer to Figure 4-8.

1. The 5GEx Customer submits a service request (plus Service Level Specification, SLS) for an assured connectivity service to SP1 and in particular to SP1 orchestrator (Interface 1). The service specification might include for instance: a) assured quality connectivity for point to regions services in order to reach a set of customers; b) caches and VNFs to manage the patients' data locally; c) cloud/fog computational resources to predict risks for patient groups, potential times for emergency transfers based on traffic patterns etc. As consequence of point c), may be required the live deployment of caches and pools of interconnected VMs to allow the execution of computational distributed algorithms based for instance on the Map-Reduce programming model.
   The SLS may specify requirement on the tolerable delay while data in transmitted and computational tasks are carried out, as well as minimum granted resource availability.
   The service specification can also include details on the dynamic scale of both the computational infrastructure (i.e., the VMs) and the reconfiguration of the network connection on different network infrastructures (elasticity rules) to be applied on the service when SLS breaches occur. These tasks intend to provide elasticity and flexibility to the service instances and may be carried out also as reaction to perceived real demands (e.g., provisioning of ultra-reliable fast connection to remotely monitor a group of patients; extension of the needed computational power by increasing the number of nodes composing a virtual Cluster of IT resources) based on current resource status and utilisation described by real-time monitoring data (collected by custom probes deployed along with the service instance).
2. In order to actually deploy the service, the MdO in SP1 performs its decomposition into a set of elementary sub-services. Each of these sub-services should then be mapped on a list of needed resources (that may potentially belong to different technological domains).
3. SP1, in first instance checks whether or not it can deliver the service the customer asked for in his own region (through Interface 3) and then possibly starts a discovery process to find what external Service Providers (in the Federation) may be contacted to complete the requested service deployment.
4. If a discovery process is needed, once it is completed, SP1 will have a clear global view of the service capabilities offered by the other Service Providers belonging to the Federation and, after a matchmaking process, will be able to pick up the one(s) which are able to offer the requested service while also satisfying the SLS

initially specified by the Customer for that service (which includes both expected KQIs and non-functional requirements).

5. SLS submitted by the customer for the service, should be also decomposed into a list of SLA requirements expected for each involved technological domain. The above list will be matched against the SLA values offered by the Service Providers identified during the discovery process to pick up the most suitable ones. Also non-functional requirements associated to the service request (such as offered levels of security, availability and reliability and satisfaction of the rules of compliance) should be checked against what each Service Provider is able to offer.
6. At the end of the match-making process (5.), SP1 will contact the most suitable business partner (e.g., SP2 in this example) through the Inter-Operator Orchestration API of Interface 2 to deliver the rest of the service, relying on Cloud Service Provider CS2 (6.1) and Storage as a Service Infrastructure Provider STP2 (6.2) located within the same administrative domain of SP2. In this particular example we assume that a subset of the IT and storage resources required to deploy the service can be instantiated within the administrative boundaries of SP1 but, due to the requirements specified by the customer regarding the minimisation of latency while collecting the IoT data, a part of the IT infrastructure will have to be instantiated in a different external region.
7. Finally, SP2 relying on its internal Domains Cloud Service Providers CS2 and Storage as a Service Infrastructure Provider STP2 deliver the missing sub-set of the service that was requested within a Resource Slice that will be used by Service Provider 1 in addition to the Resource Slice already available locally (created in step 3.). Eventually, those external resources lying in the "external" resource slice will be logically "linked" to the set of resources already allocated by SP1 within its own premises. The external Service Provider will also specify information on how the Slice can potentially be either stretched or shrunk to deliver on demand a set of additional resources on the fly if/when needed to deal with emergency scenarios. This information has to match the service specification details on the dynamic scale of the resource infrastructure (elasticity rules), and was considered during the match-making process discussed at points 4 And 5.

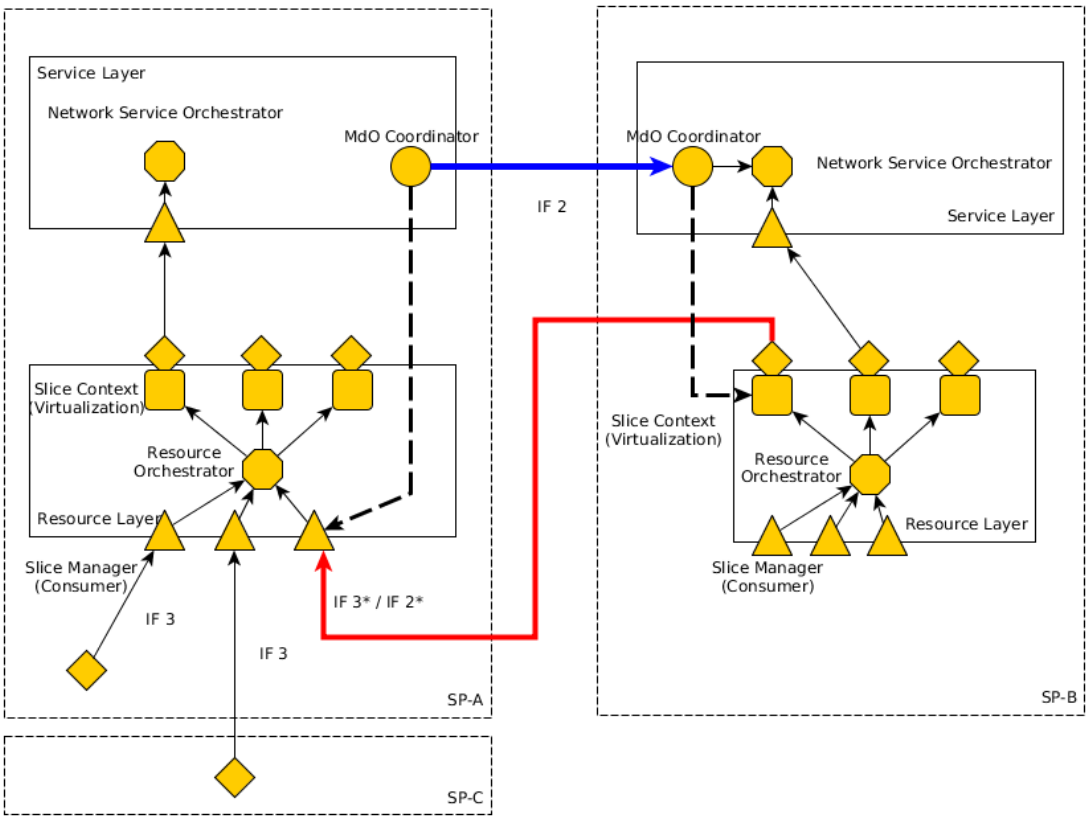


Figure 4-9: Slice trading and management to compose the SlaaS service

SlaaS is composed from lower lever services and resources of multiple Providers. These resources can be purchased in a cascading way in order to meet the initial SLS requirements by means of trading among the MdO Coordinators of the 5GEx Providers who own suitable resources, as depicted in Figure 4-9(hierarchical trading would be also feasible e.g., in environments where the customer entry point provider does not own resources). After the purchase is completed, the leased resources can be controlled via Interface 3 and they become part of the resource pool of the 5GEx Provider, to be used in a slice tailored to serve the customer request.

More details about this use case and how it will be implemented can be found in D3.1 [69].

4.1.5 The role of use cases binding 5GEx WP interactions

This section has provided a shortlist for defining (an indicative set of) 5GEx use cases. These wholesale infrastructure use cases suffice to support a wide range of verticals with actual market value thus maximising the market coverage, potential revenue and impact of the 5GEx project. Moreover, they can be used as drivers for interface, information and coordination model specification, further enhancing the 5GEx architecture and interfaces specification, as also depicted below.

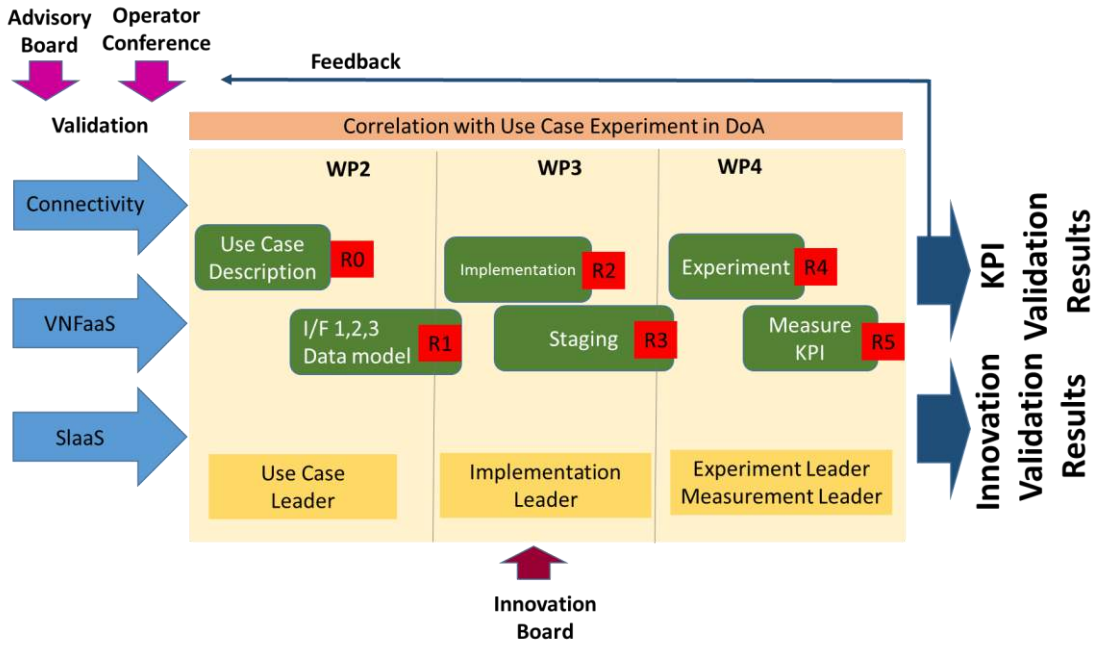


Figure 4-10: Role of use cases binding 5GEx WPs interactions

In particular, the use cases defined initially in WP2 contain a brief use case description, included in this document. A dedicated group of WP2 members led by the respective Use Case Leader produce the respective Wholesale Service Definition (Reference Point R0), i.e., the Service Catalogue entries for the respective use case, and a detailed description of the use case along with the respective Information Model for Interfaces 1, 2 and 3 (R1). These outputs are then handed to WP3, where under each use case Implementation Leader the use case is implemented by means of software (R2) that is subsequently deployed in the staging environment (R3). This drop allows the respective WP4 group, led by the Experiment and Measurement Leader, to experiment (R4) and measure Key Performance Indicators of the use case (R5). The Innovation Board overviews the entire process assessing the respective innovation results and performs the KPI validation, providing feedback to the Advisory Board and the Operator Conference as an external validation and feedback loop.

4.2 Requirements

This section reports on the different requirements identified by the project [12]. We classify them according to three different families: *i)* business related, *ii)* 5G related, *iii)* the ones originally included in the DoA, and *iv)* the ones coming from the use cases.

An analysis of these requirements against the 5GEx architecture will be performed and reported in D2.2, as part of the revision of the architecture design.

4.2.1 Business requirements

The business requirements reported below, incorporate and address the business aspects of the use cases that have been specified by the 5GEx consortium and are described in Section 4. These high-level requirements reflect the desired properties and functionalities that must/should be supported by the 5GEx architecture so as to materialise its objectives and goals. Consequently, the high-level requirements will be afterwards translated and mapped to technical, low-level requirements to be fulfilled and met by an appropriate architecture design.

BUS-01	The 5GEx Framework shall support different 5GEx external customers, either providers or enterprise customers.
BUS-02	The 5GEx Framework shall allow multiple infrastructure, network, storage, cloud and application service providers to interact / interwork with each other, also at run-time.
BUS-03	The 5GEx Framework shall support interoperability of legacy and modern network, storage and cloud infrastructure.
BUS-04	The 5GEx management functionality shall be able to unify the management of network resources, cloud resources and VNFs over multi technological and administration domain in a uniform standard way.
BUS-05	The 5GEx Framework should facilitate collaboration among independent or federated 5GEx providers and customers.
BUS-06	The 5GEx Framework shall expose appropriate interfaces to external customers to allow them to communicate with and buy services from providers, to providers to communicate and interwork with each other, and to the lower layer comprising slices for its manipulation.

[12] We follow the IETF terminology when listing the requirements, meaning that the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [70], though we use lowercase.

BUS-07	The 5GEx multi-domain orchestrator must be able to perform translation and mapping of the 5GEx customer service request received via a dedicated interface (interface 1) to 5GEx resources and slices.
BUS-08	The 5GEx multi-domain orchestrators shall be able to interoperate by exchanging information over a dedicated interface (interface 2) via a standard API.
BUS-09	The 5GEx slice client shall purchase slices from the 5GEx slice provider and be able to manage them similarly to own resources over a standard dedicated interface (interface 3).
BUS-10	The 5GEx orchestration, control and management functionality must adhere to industry multi-tenancy requirements and standards (including isolation, scalability, elasticity, security).
BUS-11	The 5GEx Framework shall allow the 5GEx Provider to expose appropriate interfaces to 5GEx customers and other 5GEx providers to negotiate and monitor SLAs.
BUS-12	The 5GEx Framework shall support advanced monitoring of resources and activities with appropriate granularity to perform SLA monitoring and assurance.
BUS-13	The 5GEx Framework shall support SLA nesting and stitching for infrastructure aggregates.
BUS-14	The 5GEx Framework shall respect the policies of independent and federated 5GEx providers.
BUS-15	The 5GEx Framework shall be open and extensible so as to support any interconnection model and charging scheme, existing or emerging, applicable to the 5GEx customers.
BUS-16	The 5GEx Framework shall support open coordination models for multi-domain multi-service technology-agnostic and vendor-agnostic service orchestration.
BUS-17	The 5GEx Framework shall support many coordination models among the 5GEx community members, including push and pull models, bilateral cascading (peering model), hierarchical relationship, and models based on multi-domain topology view.
BUS-18	The 5GEx Framework shall be capable of supporting value/revenue sharing models applicable among 5GEx participants.
BUS-19	The 5GEx Framework shall expose interfaces that will allow exchange of information, negotiation and trade among multiple providers.

BUS-20	The 5GEx Framework shall enforce a minimum set of information elements (according to the specific collaboration and service model agreed during establishment of business relationship) that must be provided for the resources traded in 5GEx.
BUS-21	5GEx Framework should be designed to take into account that multiple 5GEx Solution instances can materialised and deployed, which can be designed according to appropriate standard APIs for their business relationship specific interoperability.
BUS-22	In order to facilitate the automated provision of enterprise customer services, any 5GEx solution must provide enterprise customers with service catalogue information about available service offers and capabilities. In particular, the MdO shall provide the customers with a catalogue containing the list of available services (e.g., IaaS, VNFs, connectivity).
BUS-23	Service catalogue entries may contain a service manifest and a price tag.
BUS-24	In order to facilitate the automated provision of enterprise customer services, any 5GEx solution must provide enterprise customers with the means to submit detailed requests including information regarding the placement of resources, the location of service points, QoS, charging options. In particular, the MdO shall provide the customer with the ability of requesting a service from the catalogue along with the expected SLS describing the whole service performance expectation.
BUS-25	Any 5GEx solution must assure that the enterprise customer has a single management interface allowing the concatenation, partitioning and management of all purchased resources and services via slicing.
BUS-26	Any 5GEx solution may provide towards the enterprise customer the ability to interrogate the QoS feasible for the service elements and end-points.
BUS-27	Any 5GEx solution must provide towards the enterprise customer the ability to monitor the QoS attained for the service elements and end-points.
BUS-28	5GEx solution may include a portal to interface with the enterprise customer.
BUS-29	Any 5GEx solution must provide a mechanism to perform end-user related service accounting and charging on service end points.
BUS-30	Service catalogue entries and satisfied service requests should result in an SLA for the respective service.

BUS-31	Any 5GEx solution should provide a mechanism for reward/penalty of the involved providers in service provisioning in case of SLA conformance/failure.
BUS-32	The SLA must contain a parameter describing the service Time To Live (TTL).
BUS-33	Offers and requests for 5GEx resources and services must describe (explicitly, by including a parameter, or implicitly, until explicit termination) the service maximum duration.
BUS-34	The 5GEx advertising policies for service offers and requests must support private, i.e., towards specific receiver(s), and public dissemination.
BUS-35	The service request, offer and SLA must contain (implicit or explicit) the price for the service or an indicative price range from which the exact price will be decided at run-time.
BUS-36	The 5GEx management system should provide a mechanism to set-up, re-size and terminate services, according to their Time To Live.
BUS-37	The Multi-domain Orchestrator should be able to accept customers' SLSs specification including both functional and non-functional requirements expected for a service.
BUS-38	The Multi-domain Orchestrator shall be able to derive from: a) the service description, b) the SLSs description and c) elasticity rules a set of performance parameters to be satisfied during the service execution. This set of parameters should be decomposed for each technological domain involved in the service instantiation to identify KPIs to be monitored (through the instantiation of probes) during the service execution lifecycle.
BUS-39	The Multi-domain Orchestrator shall allow the customer to specify a set of policies associated to the service to describe "elasticity rules" to be enforced when the service requires re-deployment/re-configuration.

4.2.2 5G Requirements

The following functional requirements have been identified in the context of wider 5G context:

5G-01 (5GEx Multi-domain Coordination)	5G Multi-domain Orchestration should coordinate the infrastructure components with the view of protecting it from instabilities and side effects due to the presence of many service components running in parallel. It ensures the proper triggering sequence of components and their stable operation. It defines conditions and constraints under which services will

	be activated, taking into account operator service and network operation requirements.
5G-02 (5GEx Multi-domain Information handling)	5G Multi-domain Orchestration should enable information collection, aggregation, storage, registry, distribution and use across multiple domains for all service components and infrastructure functions. The importance of the use of uniform information system cannot be overstated as the risk of semantic mismatch is exacerbated if different functions have incompatible information models or systems. This allows purpose-specific APIs to be produced, while enforcing common semantics for the resources of concern.
5G-03 (5GEx End-to-end Slice Orchestration)	5GEx End-to-end Slice Orchestration should enable e2e slice life cycle management, including: *(i)* Concatenation of slices in each segment of the infrastructure (access networks, core network, edge network, edge/central cloud, software network) and vertical slicing of the data pane + control plane + management plane + service plane). *(ii)* Slice elasticity, placement of VMs in slices. It takes over the control of all the virtualised network functions and network programmability functions assigned to the slice, and (re-) configure them as appropriate to provide the end-to-end service. *(iii)* Slice aggregation by collecting virtual network functions connected by links to create an end-to-end networked system. Slices are composed of multiple virtual resources which are isolated from other slices. *(iv)* Slicing isolation by allowing logically isolated network partitions with a slice being considered as a unit of programmable resources such as network, computation and storage. *(v)* Slice extension - Considering the wide variety of application domains to be supported by 5G network, it is necessary to extend the concept of slicing targeted by the current SDN/NFV technologies.
5G-04 (5GEx Recursiveness)	E2E Slicing, virtualisation and orchestration should be recursive and involve more than simply subdividing, aggregating or combining resources. A multi-domain orchestrator sees a set of resources for its exclusive use in satisfying the service request. Recursively within each subordinate/sub domain, the local orchestrator likewise sees and coordinates resources for its own use.
5G-05 (5GEx Multi-tenancy)	5G Multi-domain Orchestration should enable tenants (hard isolation) and some other can be shared (soft isolation) via both shared and/or dedicated service and/or application components (service/network functions)". Multitenancy domain refers to set

	of physical and /or virtual resources in which a single instance of a software runs on a server and serves multiple tenants. A tenant is each of a group of users sharing a common access with specific privileges to a software instance. A service or an application may be designed to provide every tenant a dedicated share of the instance including its data, configuration, user management, tenant individual functionality and non-functional properties.
5G-06 (5GEx Multi-domain Orchestration Primitives)	5G Multi-domain Orchestration framework should enable a number of primitives (for use cases other than connectivity) including: *(i)* VNF Placement: The programmability framework shall allow the customer to deploy VNFs at arbitrary points into the network and set where the components/ gateways will be placed on the network. *(ii)* Service chaining: the programmability framework shall allow the customer to interconnect VNFs in an arbitrary graph, with traffic (re-)classifications. *(iii)* Multiplicity: Orchestrator should be able to orchestrate multiple VNF execution environments located in arbitrary places in the operator's domains.
5G-07 (5GEx Multi-domain Federation)	5GEx Multi-domain framework should enable multiple federation models enabling providers/operators to collaborate and share their resources to create a larger virtual pool of resources at multiple locations. Different types of federation models can be used and implemented for the physical and /or virtual infrastructures (e.g., on-demand network elasticity, network brokering, combination, composition, aggregation) with different level of resource coupling and interoperation among the network and cloud resources, from loosely coupled, typically involving different administrative and legal domains, to tightly coupled federation, usually spanning multiple networks/datacenters within an organisation.

4.2.3 DoA Requirements

The following functional and non-functional requirements were identified in the DoA:

DoA-01 (5GEx Multi-domain management functionality)	The 5GEx Framework should include a multi-domain management and operation system that includes realisation of Multi-domain Infrastructure as a Service enabling: (i) Autonomic management functions (monitoring, configuration, performance, optimisation, security) of the peer-to-peer operators environments, where only certain elements within each domain can interact with each other as directed by the agreements between operators; and (ii) Interworking with the

	multi-domain orchestrator and with the controllers, which are providing actual operational regulator mechanisms on the undelaying connectivity, computing and storage resources.
DoA-02 (5GEx non-functional characteristics)	The 5GEx Framework should include: *(i)* Reliability: it describes the degree to which a system must work. Specifications for reliability typically refer to stability, availability, accuracy, and maximum acceptable bugs. It includes stability as it refers to the ability of a system to handle growing amounts of work or usage in a graceful manner and its ability to be enlarged to accommodate that growth and Availability as it describes the ease with which a system performing certain functions or features can be adopted and used. *(ii)* Performance: it describes the degree of performances of the system (according to certain predefined metrics, e.g., convergence time). It is including recovery and security - it refers to the ability to prevent and/or forbid access to a system by unauthorised parties. *(iii)* Resilience: it refers to the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation. *(iv)* Extensibility to new functions and services: it refers to the ability to extend a system and the level of e ort and complexity required to realise an extension. Extensions can be through the addition of new functionality, new characteristics or through modification of existing functionality/characteristics, while minimizing impact to existing system functions. *(v)* Inter-operability: it refers to the ability of diverse (sub)systems to work together (interoperate). Operability refers to the ability to keep a system in a safe and reliable functioning condition, according to predefined operational requirements. *(vi)* Scalability: it refers to the ability of a system to handle growing amounts of work or usage in a graceful manner and its ability to be enlarged to accommodate that growth. *(vii)* Security: i.e., a trusted and secure end-to-end architecture by re-using as much as possible existing security mechanisms.
DoA-03 (5GEx Multi-domain orchestrator)	The 5GEx Framework should include plug-ins extensions enabling: *(i)* Governance, operational control and inter-working with the single administration multi-domain orchestrators. *(ii)* Mapping of service requirements and global SLA manifest into local single domain service and network functions

	components with local manifests. *(iii)* The deployment, execution and autonomic management (configuration, performance, optimisation, security) of the group of service and network functions components while enforcing the global manifest. *(iv)* Achieve a 90-minute service setup, activation and management in a multi-domain environment compared to the 90-day needed today.
DoA-04 (5GEx Multi-domain Inter-working Interfaces)	The 5GEx Framework should include interfaces enabling: *(i)* Establish tenancy agreements. *(ii)* Exchange information regarding the utilisation of service resources. *(iii)* Control over service resources. *(iv)* Maintain SLAs over service resources.

4.2.4 5GEx Use Case Requirements

Next we include a list of additional functional requirements derived per use case family. These are important to understand the specific needs coming from the use cases families.

4.2.4.1 Connectivity

CON-01	The Multi-Domain Orchestrator of a SP should be in place to receive the service request of the Customer, including the SLS specification, and respond, accept or reject it, within bounded time.
CON-02	The 5GEx connectivity services may be complemented with a set of management and monitoring tools (e.g. connectivity quality ping/traceroute) so as to estimate or overview the quality of a 5GEx connectivity service.

4.2.4.2 VNFaaS (e.g., vCDN)

VNFaaS-01	The Multi-Domain Orchestrator of an SP shall be able to map a service deployment on resources coming from its internal domains and simultaneously define the necessary resources to be asked from "foreign" domains.
VNFaaS-02	The Multi-Domain Orchestrator of an SP shall be able to integrate/instantiate new VNFs (e.g., vCaches for vCDN) so as to meet demand.
VNFaaS-03	The Multi-Domain Orchestrator of an SP shall be able to steer traffic to, from and between VNFs instantiated by himself.

VNFaaS-04	The Multi-Domain Orchestrator of an SP shall support scaling up/down of resources allocated to a VNF on request.
VNFaaS-05	The Multi-Domain Orchestrator of an SP shall be able to perform configuration actions on physical and virtual elements composing a service instance instantiated by himself, regardless the location of the elements.

4.2.4.3 SlaaS

SlaaS-01	The Multi-Domain Orchestrator of an SP shall be able to decompose the slice request and to map the requested slice on own resources and simultaneously define the necessary slice from "foreign" domains to be requested for honouring the customer request.
SlaaS-02	The Multi-Domain Orchestrator of an SP shall expose to another SP a service catalogue comprising the list of available slice resources, i.e., topology of compute, storage and network resources with their capabilities, where capabilities include supported VNFs, costs, etc.
SlaaS-03	The Multi-Domain Orchestrator of an SP shall support scaling up/down of slices according to customer requests.
SlaaS-04	The Multi-Domain Orchestrator of an SP shall be able to isolate the usage of resources from different slices.
SlaaS-05	The Multi-Domain Orchestrator of an SP shall be able to perform configuration actions on physical and virtual elements composing a slice.

4.2.4.4 Common requirements

Some of the requirements coming from the use cases are common for more than one family. To avoid repetitions, we list them below in a separate table.

5GEx-01	The Multi-Domain Orchestrator shall maintain a list of technological domains that are available within its premises. The list should be dynamically updated to reflect potential modification in respect to the available technological domains.
5GEx-02	The Multi-Domain Orchestrator shall have an overview of the overall resource availability in each technological domain within its administrative boundaries.
5GEx-03	The Multi-Domain Orchestrator should be able to identify what technological domains have to be considered to address a service instantiation request.

5GEx-04	The Multi-Domain Orchestrator should be able to instantiate probes within each element composing a service instance in order to monitor the service status. The probes should be dependent on the particular service element and the technological domain it is related to.
5GEx-05	The Multi-Domain Orchestrator shall be able to re-deploy/re-configure/scale a service using resources slices within its boundaries, according to the monitoring information and the policies.
5GEx-06	The Multi-Domain Orchestrator shall be able to map a service deployment either on resources coming from its internal domains or asking for resources to "foreign" domain.
5GEx-07	The Multi-Domain Orchestrator should be able to discover other Service Providers outside of its Administrative Boundaries which are able to provide services compliant with the ones it already offers to its customers.
5GEx-08	The Multi-Domain Orchestrator should be able to perform a match-making to identify what are the external Service Provider that best matches the set of requirements of a given service request.
5GEx-09	The Multi-Domain Orchestrator shall be able to collect monitoring data from probes within element composing a service instance located outside of its administrative boundaries.

5 Pricing

This section is a high-level overview (a detailed specification for implementation is to be provided in D2.3, due by M28) of pricing schemes for 5GEx resources and services in lieu of the use case families specified in Section 4.

5.1 Connectivity

Sending Party Network Pays (SPNP), shown below was introduced in the ETICS project: two networks exchange assured quality traffic over Assured Service Quality paths (ASQs) according to agreed SLAs. That is, when Network A (buyer) sends ASQ traffic to Network B (provider) Network A pays Network B for transporting the IP packets according to the SLA (A-to-B) to destination end-points of an agreed destination region (set of IP prefixes) R-x. For traffic in the opposite direction, the roles of A and B will change, as well as destination region R-y. Under SPNP, the charges for the traffic in the two directions are in principle separate issues.

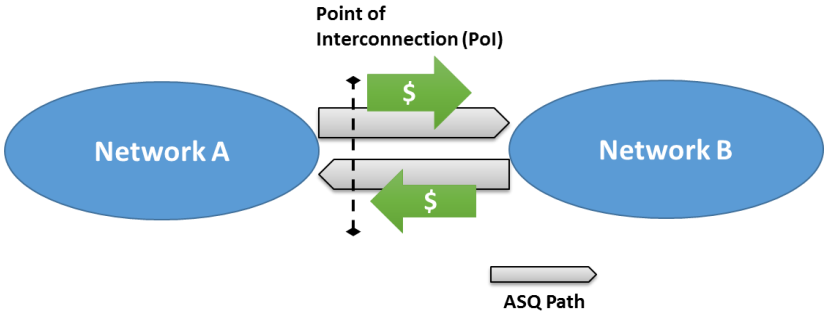


Figure 5-1: The Sending Party Network Pays principle

SPNP provides appropriate incentives to the provider NSP to deliver the traffic according to the agreed SLA; it also empowers the sender to indicate which IP-packets shall be sent with the given quality. SPNP is a wholesale ASQ traffic exchange approach that is intentionally kept simple and low-cost [55]. SPNP applies between NSPs; NSP offerings to the Application Service Provider is a different issue, depending on the service type and should not be confused with the end-customer application service.

The original SPNP principle left unexplored the specific pricing schemes to apply it in practice. We foresee for 5GEx the following two schemes:

(1) SPNP charging based on the nominal capacity requested *C*, regardless of its actual usage. This is a payment rule used in various exchange peering and its major pro is simplicity. The unit price of the capacity *p* is expected to be region-dependent and also

reflecting the quality assurance requested. Thus *total charge* = *p* * *C* for a given availability and QoS.

(2) SPNP charging based on 95th percentile charging *perc* given the incentive properties of 95th percentile rule for traffic shaping of peaks and thus enhanced multiplexing potential of the network. Thus *total charge* = *p* * *perc* for a given availability and QoS. Traffic must be sampled e.g., per 5-min intervals to compute the 95th percentile which is lower than the nominal capacity. 95th percentile is the industry de-facto transit pricing and provides incentives for efficient network usage.

On top of the SPNP wholesale layer, additional charging layers and business models can be supported, including scenarios where even the "initiating end-customer" can pay for traffic in both directions if needed. In this case, the initiating party customer is paying his NSP, and this NSP must then pay the remote NSP for the traffic in the opposite direction, thus supporting multiple end-to-end money flows. The Initiating Party Network Pays (IPNP) operates on top of the wholesale (transit/SPNP) layer for a subset of the wholesale traffic, thus metering and clearing is needed for the interconnected NSPs.

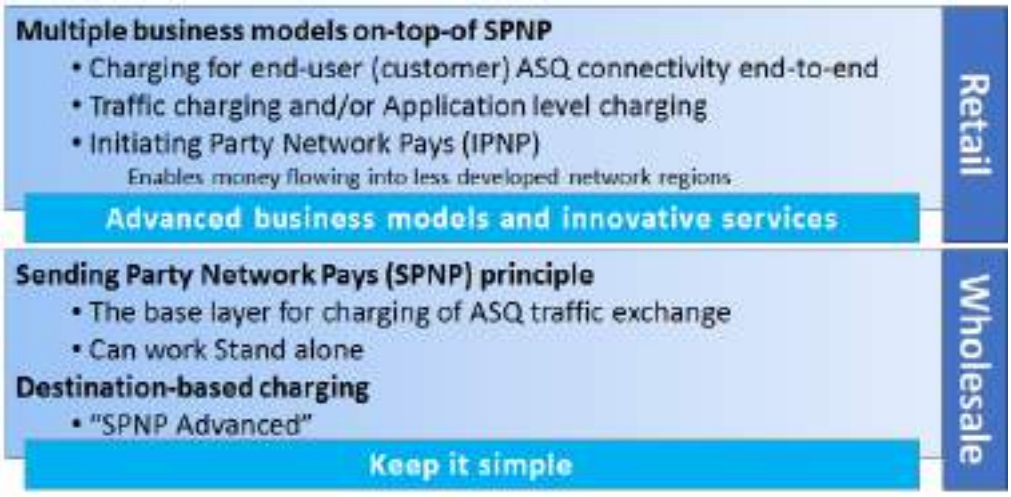


Figure 5-2: Wholesale and retail pricing for CORE and VACS connectivity services

Note that this modular vertical layering is expected to coexist in the 5GEx multi-operator setting, motivating pricing schemes that are simple enough to operate in a standalone fashion and also combined for the composite multi-operator services demanded, i.e., also horizontally across operators. Thus, e.g., a VNF forwarding graph translated to multiple links, VMs, connectivity services and VNFs will result in a total charge that will be the sum of the individual service elements composing the service. Each service element (VNF, connectivity service) will be priced according to the schemes specified in this section. Note that this is similar to e.g., a CDN service where the total CDN service charge is the total charge of the transit charge for the connectivity and the cloud charge for the compute and storage portion of the service.

Regarding connectivity, we propose that the Core Connectivity services are always priced according to SPNP and the two aforementioned charging schemes; a discussion on the motivation behind SPNP and its advantages can be found in [55][56]. This will enable the provision of proper incentives for creating a backbone of assured quality connectivity services, which is crucial for 5G services. Therefore, in terms of 5GEx connectivity service catalogue entries, both ASQ PoI-2-Region and ASQ PoI-2-PoI (including its variants PoI-2-PoDI, PoI-2-PoEI) services should be charged with one of the two aforementioned SPNP charging schemes. This is also applicable to the ASQ Traffic Adjacency service (that is offering ASQ traffic termination service by an ASQ tunnel to the remote PoI). Regarding ASQ peering (among NSPs or NSP and multiple CSPs similar to the "donut peering" model), SPNP can also apply here for the pricing of each traffic direction: clearing will allow to automatically resolve connectivity disputes (e.g., de-peering) due to traffic asymmetry since the built-in metering and pricing of the SPNP mechanisms can ensure that each party is compensated according to the effort it exercises and to the traffic it carries.

Regarding Multidomain VPN and additional VACS services, the IPNP becomes relevant so that for instance in a VPN or a two-way streaming/teleconference service there can be one party paying for the entire service. This means that the IPNP layer will be utilised to pay for the service and also compensate for the underlying ASQ wholesale SPNP charge (or even the transit charge when crossing non-5GEx compatible domains where ASQ wholesale services are not available). We anticipate the VACS services to be mainly instantiated on top of the backbone wholesale (long-lived) ASQ services, thus comprising an additional service/pricing layer. At the application layer there may be additional charging schemes, e.g., session-based or monthly subscription for a video streaming service, which are out of the 5GEx scope.

Concluding, our pricing framework and proposals are in line with both research and industry best practices and follow the layered pricing approach, as also defined in [57] and illustrated in Figure 5-3 and Figure 5-4. Figure 5-3 depicts the different granularities of traffic managed, with the interconnection traffic aggregates carrying multiple sub-aggregates and flows in an opaque way, while Figure 5-4 depicts how pricing operates on each of the layers and the respective pricing operations and requirements for metering and clearing.

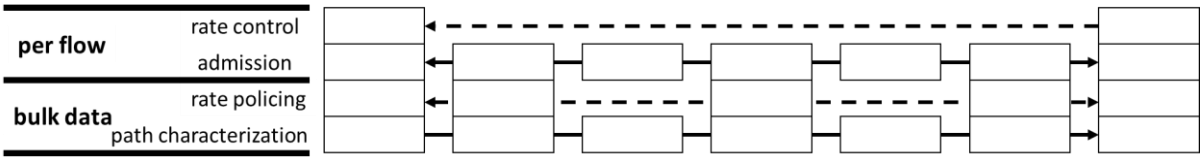


Figure 5-3: QoS control and pricing layers [57]

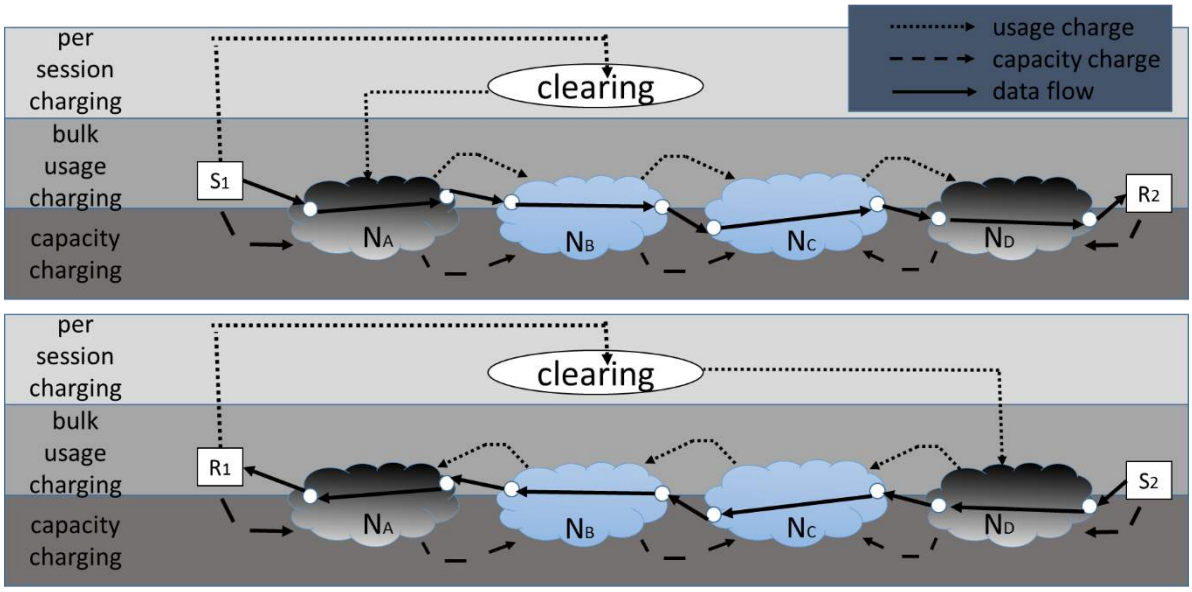


Figure 5-4: Examples of clearing function for duplex flows with a SPNP model [57]

The proposed pricing schemes are relevant for multiple Core and VACS services which may be differentiated in terms of (sets of) quality parameters such as *Bandwidth*, *Delay*, *Time duration*, *Jitter*, *Loss*, and *Availability*. Especially for Core connectivity services *Availability* is considered to be extremely important in order to be able to offer Core connectivity services that are robust, fault-tolerant and carry sensitive traffic such as signalling. Different values of the *Availability* parameter are expected to correspond to different unary prices *p* for the aforementioned pricing schemes.

5.2 VNFaaS

Pricing VNFaaS can be seen as a special case of Software as a Service (SaaS). SaaS pricing is known to be extremely rich and complex, including multiple dimensions such as versioning, packaging, regional pricing, customer/market segmentation, loyalty and volume discounts, payment and usage type adjustments, promotions, upgrades fees, channel discounts [58]. It is important for 5GEx to be able to come up with simple yet efficient pricing schemes for VNFaaS that could allow the inclusion of the aforementioned pricing aspects by means of VNF configuration and pricing model parameters setting [59], [60]. To this end, also inspired by the pricing models used for popular software services ranging from desktop applications to elementary cloud functions such as AWS Lambdas [61], we propose the following pricing schemes for VNFaaS:

(1) **Pay per time duration per VNF instance:** This is the simplest scheme where the customer is granted access to executing a single service instance (or up to a fixed number of instances) *n* for a pre-

specified amount of time *t* for a price *p*. Thus, *total charge = p * n * t*, where *p* is independent of the actual usage. The major advantage of this scheme is its simplicity, lack of monitoring and the fact that customer's charge is pre-specified. The major disadvantage is that it does not provide any incentive for reducing the actual usage and the fact that the pre-specified usage limits (in terms of instances or time limit) may not serve all customers' needs. E.g., if the seller prescribes that there is a price *p0* for executing a single instance and a price *p1* for 10 instances for a period of 1 month, this scheme may not be convenient for users needing 5 instances for a week.

(2) **Pay per request and execution time duration:** This is the scheme used for AWS Lambdas [61]. The charge of the VNFaaS instance is computed as the sum of the *Request charge* defined as the total number of function requests *r* times the unary price *p_req* (*Request charge = r * p_req*) plus the *Compute charge* specified as the VNF execution time *t* times the respective unit price *p_run (Compute charge = t * p_run)*. Therefore, *Total charge = Compute charge + Request charge*.

The unary prices of the *Compute charge* and *Request charge* may differ for different utilisation limits with a different unary price *price(v)*, i.e., price(v) is actually a piece-wise constant function, which may also depend on the network location of the VNF instance. Thus, for actual utilisation *v*, the resulting price is p(v) = price(v) * v, with *price(v)* having a set of discrete values for different utilisation ranges. The dependence of price(v) on utilisation limits provides different incentives and allows the service seller to perform market segmentation so as to increase the attained revenue.

These both pricing schemes are compatible with the Pay-as-You-Go model proposed in T-NOVA project (NFaaS over Virtualised Infrastructures) where different billing options were explored for VNFaaS model, including licensing and subscription. These 2 were showed as not profitable nor fair for this case, concluding the Pay-as-You-Go (PAYG) as the most suitable one for the VNFaaS business case [66].

In a multidomain environment as the one that 5GEx proposes it will be interesting to explore the applicability of sharing revenue models among the different providers in the chain that will be part of the VNFaaS provisioning. Intermediate providers may receive a concrete percentage of the total revenue that the main provider billed to the customer.

The storage and connectivity charges that may be entailed are in principle a separate issue and are computed as specified in the other parts of this section.

5.3 Slice as a Service - Additional considerations

The multi-domain service setup in 5GEx, especially for non-commodity connectivity resources and services, entails a significant amount of signalling, orchestration and business coordination processes and can potentially involve the reservation of a significant amount of resources. It is thus advised that for the pricing of connectivity services and slices when usage-based pricing schemes are applied, they are combined with an initial service set up cost *Psetup*, which depends on to the amount of resources and performance features requested. Especially for slices, for both simplicity and scalability reasons we propose that the price to be paid by the customer is the set-up cost *Psetup* of the slice and the respective charge for the resources and services instantiated, as defined in the previous parts of this document. The set-up cost *Psetup* can depend on the slice parameters reflecting how demanding the service request is in terms of orchestration and set up overheads.

In general there can be push (pre-computed) service composition, pull (on-demand) service composition or even marketplaces for service trading (e.g., similar to T-NOVA or Amazon spot markets). *This means that the price schemes should be able to work both in an independent and combined fashion under all these models.* Therefore, modularity and layering of the pricing schemes is needed for a generic and functional pricing framework. This is also depicted below

Figure 5-5: Pull (left) and push (right) data objects exchange

Price dynamicity is an additional important factor to be considered at later versions of the 5GEx prototype. In principle, there are several ways to deal with dynamicity: Either create pricing schemes and market mechanisms where prices are set dynamically according to multiple factors (e.g., utilisation) or create markets that can generate the values of the parameters of the pricing schemes presented in this section. An example of the latter is a spot market where a market price for a certain resource or service is generated given the intersection point of demand and supply; this is the approach used in Amazon, electricity grids, etc. These issues are not addressed in this section as they are considered to

be out of scope for the first 5GEx prototype and are to be investigated within the project at a later stage. Elasticity, scaling up/down the service are additional factors that may create uncertainty regarding the resulting total charge. Also note that the price may not appear as a price tag; its bounds may be provided and the exact value can be computed on demand based on the underlying infrastructure scarcity, utilisation and conditions in general.

5.4 Resources

Pricing of storage and compute resources is expected to be according to the current market status quo where a predefined ontology of virtual compute and storage nodes of standard types are offered for a price for a given amount of time. It is also possible to have spot markets a la Amazon for the on-demand opportunistic leasing of resources. The fixed price approach can be an initial step for resource pricing in 5GEx, while the spot market approach is to be investigated further later, in a way customised to the scope of 5GEx. Regarding the former, a piece-wise constant pricing scheme is typically followed: There are multiple utilisation limits with a different unary price, which may also depend on the physical location of the resources. Different prices for the same resource in different regions reflects the different costs of ensuring the availability of the respective resources over different regions, e.g., due to the different network and cloud infrastructure availability.

For instance, for Amazon S3, the following price structure is used for the region US East [62] (there is a similar table with different prices offered if the selected area is for instance EU - Frankfurt):

Table 2. Amazon S3 price, region US East

Standard Storage	Standard - Infrequent Access Storage	Glacier Storage	
First 1 TB / month	$0.0300 per GB	$0.0125 per GB	$0.007 per GB
Next 49 TB / month	$0.0295 per GB	$0.0125 per GB	$0.007 per GB
Next 450 TB / month	$0.0290 per GB	$0.0125 per GB	$0.007 per GB
Next 500 TB / month	$0.0285 per GB	$0.0125 per GB	$0.007 per GB
Next 4000 TB / month	$0.0280 per GB	$0.0125 per GB	$0.007 per GB
Over 5000 TB / month	$0.0275 per GB	$0.0125 per GB	$0.007 per GB

6 SWOT Analysis

This is a first round of SWOT analysis applied to the three types of 5GEx solutions envisioned (see Section 3.3). Note however that the SWOT methodology and template used are generic and will be used in the future to assess more aspects of the 5G ecosystem and 5GEx.

6.1 SWOT Template

The template proposed for the 5GEx SWOT analysis is as shown in Table 3 below.

Table 3. SWOT analysis template

Strengths	**Weaknesses**
High-quality low-cost automation	Low-quality automation, high cost to support it
Higher prob. of service request orchestration	Lower prob. of service request orchestration
High confidentiality assurance and trustiness	Low confidentiality and no trust assurance
Facilitates bootstrapping-reaching critical mass	No bootstrapping, low adoption
Collaboration stability	Opportunistic/uncertain collaboration
Fair competition and trading	Uneven market power and/or discrimination
Compatibility with existing business processes	Lack of compatibility to standard business
Powerful strategy	No clear strategic direction
Strong revenue flows	Unclear revenue streams
Strong brand name/standard	No brand name/standard
Innovation hub	Unsustainable innovation
Price and service stability	Price wars/service unavailability/fluctuations
Low CAPEX/OPEX for service deployment and orchestration	High CAPEX/OPEX for service deployment and orchestration
Opportunities	**Threats**
Serving additional customer groups	Competitors attracting more customers
Attracting InfSPs/verticals	InfSPs/verticals prefer alternatives (or locked in)
High end user acceptance	Low end user acceptance
Expanding to new geographic areas	Slowing market growth
Expanding product offerings	Opposing regulations (national/EU wide)
Vertical integration	No vertical integration sustainable
Opportunity to exploit new technologies, architectures	Technology/architecture lock-in, limited ability to change
Synergies with 5G research and industry solutions	Opposing 5G research and industry solutions
High Standardisation Impact (SDOs and de-facto industry)	Low Standardisation Impact

In this template, we classify a set of qualitative criteria as Strengths, Weaknesses, Opportunities and Threats for 5GEx. These criteria appear as pairs (e.g. "High-quality low-cost automation" versus "Low-quality automation and high cost to support it") so that each criterion may be valid only as a strength or weakness, or only as a threat or opportunity. This approach can provide qualitative insight without being too restrictive.

The evaluation of each 5GEx solution variant can be performed by checking the fitness of each (paired) criterion under the specific 5GEx solution envisioned (Case A, B and C). If a certain criterion is not directly applicable for a certain solution then both the values are omitted from the respective table, or equivalently the "Neutral" option is selected.

A justification of the selection is provided as structured text under the respective table for each of the 5GEx solutions. Note also that these 5GEx solutions (A, B or C) complement each other and are all considered feasible, although with (somewhat) different strengths and weaknesses. The market will decide which approach is more appropriate under the given condition and business relationship.

6.2 SWOT Analysis for 5GEx Solution "Direct Peering" (Case A)

We apply the template for the "direct peering" at an already established local or remote IXP or IPX exchange point, but evolved towards compatibility with the 5GEx Framework, thereby operating as a 5GX.

Table 4. SWOT analysis for "Direct Peering"

Strengths	**Weaknesses**
High-quality low-cost automation High confidentiality assurance and trustiness Facilitates bootstrapping-reaching critical mass Compatibility with existing business processes Powerful strategy Strong revenue flows Low CAPEX/OPEX for service deployment and orchestration	Lower prob. of service request orchestration Opportunistic/uncertain collaboration Uneven market power and/or discrimination No brand name/standard Unsustainable innovation Price wars/service unavailability/fluctuations
Opportunities	**Threats**
Attracting InfSPs/verticals High end user acceptance Expanding to new geographic areas Expanding product offerings	Competitors attracting more customers No vertical integration sustainable Low Standardisation Impact

6.2.1 Template Justification

High-quality low-cost automation: Efficient automation with marginal cost by integrating 5GEx with the existing business process is feasible. All the other 5GEx solutions include more roles and additional coordination in order to operate compared with the direct bilateral peering approach.

Lower Pr of service request orchestration: Due to the peering-like way of establishing business relationships supporting the 5GEx service models and business processes, no actor and no orchestrator will be able to obtain a full view of the infrastructure resources and services available to be used for meeting service requests. This lack of global information is expected to result in lower probability of service orchestration and request fulfillment.

High confidentiality assurance and trustiness: Since this model leverages on top of existing business relationships forged by trust and due to the fact that no "global" publishing or information dissemination is carried out, this solution results in high confidentiality assurance and trustiness.

Facilitates bootstrapping-reaching critical mass: Due to the minimal requirements, roles and functionality needed – compared to all the other possible 5GEx solutions – this is an ideal solution for bootstrapping. Also experimenting with bilateral peering-like relationships can be a convincing way to attract attention on the new 5GEx product offerings relying on existing customer base and trust relationships.

Opportunistic/uncertain collaboration: Collaboration relies on existing relationships thus making it hard for new entrants to forge such relationships or compete against established stakeholders. Also larger stakeholders (e.g. large Network Service Providers of significant footprint, customer base and market power) can use this power to deny collaboration with smaller stakeholders so as to control the market (in a way similar to denying traditional IP interconnection even in cases where this is theoretically mutually beneficial). Therefore, though this solution is ideal for bootstrapping, it can be seen as a first and intermediate step of the roadmap to support 5GEx solutions in the market for maximizing social welfare. Hence, such deployments may be sustainable and very profitable for high-power large-size stakeholders even in the long run, while smaller players have limited chances to compete; they can also structure their business to be complementary to the large players, rendering likely for the market to reach inefficient oligopoly equilibria.

Uneven market power and/or discrimination: The use and abuse of market power (in a similar way to traditional interconnection as explained above) results in re-enforcing and not mitigating the probability of uneven market power and/or discrimination, assuming no regulatory intervention or industry self-regulation.

Compatibility with existing business processes: This form of solution is continuation of the existing model, thus fully compatible.

Powerful strategy: Stakeholders can use their existing business strategies to extend them to 5G(Ex) services and orchestration, thus there is no strategic uncertainty induced.

Strong revenue flows: Enhancement of existing revenue streams with new ones from 5GEx services.

No brand name/standard: Due to the fully distributed nature of this solution, it is expected to result in multiple variants of 5GEx solution as time and technology evolves, rendering the establishment of a common 5GEx brand name/standard in the long run less likely.

Unsustainable innovation: Bilateral relationships are most likely to result in the long run in customised tailor-made solutions and due to the limited view of the market limit potential for innovation as opposed to 5GEx solutions aggregating the market view of multiple stakeholders.

Price wars/service unavailability/fluctuations: Due to the lack of market-wide view and the bilateral competing nature of contracts, it is

expected that cut-throat competition and price niche wars are likely, as also observed in all agent-based economies with automation.

Low CAPEX/OPEX for service deployment and orchestration: Incremental technology deployment and minimalistic changes to business processes combined with no need to support for new roles results in limited incremental costs. Orchestration CAPEX may be significant for stakeholders for which service orchestration is not part of their core business.

Attracting InfSPs/verticals: The low overhead and high trust result in high probability of attracting InfSPs/verticals willing to try the 5GEx solution. Incremental overhead to offer infrastructure and attract more revenue exploiting existing business relationships. No drastic changes in customer and infrastructure ownership, thus likely to gain acceptance in the market.

High end user acceptance: Additional services are offered to the end users without any modification on business relationships and processes or formation of large coalitions that could be intimidating for end users, especially with respect to pricing and quality of service aspects

Expanding to new geographic areas: Feasible due to the establishment of new peering-like relationships to build incrementally on top of existing ones with trusted business partners.

Expanding product offerings: Immediate available upon integrating the 5GEx technology using existing and new interconnections with business partners.

No vertical integration sustainable: Vertical integration less likely to happen due to higher friction and less coordination of this solution.

Low Standardisation Impact: Due to the fully distributed nature of this solution, it is expected to result in lower standardisation impact due to market fragmentation among competing similar solutions that serve some fraction of the market stakeholders' needs better than others.

6.3 SWOT Analysis for 5GEx Solution "Exchange Point" (Case B)

We apply the template for the case where the instance of 5GX infrastructure is operated by a standalone entity called 5GX Provider (5GXP); 5GXP is somewhat similar to the AMS-IX example in Section 3.

Table 5. SWOT analysis for "Exchange Point"

Strengths	**Weaknesses**
High-quality low-cost automation Higher prob. of service request orchestration High confidentiality assurance and trustiness Facilitates bootstrapping-reaching critical mass Collaboration stability Fair competition and trading Compatibility with existing business processes Powerful strategy Strong brand name/standard Innovation hub Price and service stability	Unclear revenue streams High CAPEX/OPEX for service deployment and orchestration
Opportunities	**Threats**
Attracting InfSPs/verticals High end user acceptance Expanding product offerings Vertical integration Opportunity to exploit new technologies, architectures Synergies with 5G research and industry solutions	Competitors attracting more customers Slowing market growth

6.3.1 Template Justification

High-quality low-cost automation: Efficient automation with marginal cost by integrating 5GEx with the existing business process in a common and shared environment like the Exchange Point. Some overhead can be expected because of the mediation of the entity operating the Exchange Point (infrastructure devoted to data plane interconnection, control plane participating from the orchestration process between providers).

Higher Pr of service request orchestration: High potential environment for establishing business relationships among multiple parties present in this common point, as neutral platform for business. Failed attempts of orchestration between parties can result in new relationships being established between two parties not previously under any agreement, now being facilitated by the presence in the Exchange Point.

High confidentiality assurance and trustiness: Common and shared environment with applicable rules known and accepted by all the parties present. Existence of mechanisms to prevent incidents.

Facilitates bootstrapping-reaching critical mass: Neutral environments, with concentration of actors, facilitate the bootstrapping of the business relationship between parties, creating a virtuous cycle of growth due to the increasing number of participants, a fact that attracts more parties to the environment.

Collaboration stability: The membership to this kind of environments is conceived from the beginning as a long-term participation, providing the necessary stability to consolidate business.

Fair competition and trading: The neutral nature of these environments facilitates equal opportunities to all the participants in the Exchange. The rules that govern the Exchange, similar to all participants, also guarantee fair competition, with all the parties having equal capabilities for accessing the services offered by the entity running the Exchange.

Compatibility with existing business processes: This form of solution is continuation of the existing model for these environments, thus fully compatible.

Powerful strategy: Participation of the Exchange facilitates access to multiple customers, behaving as a meet-me point for enabling new business opportunities.

Unclear revenue streams: Risk of commoditisation since multiple competitors can be present as well, then lowering margins despite having the opportunity of accessing a larger number of potential customers.

Strong brand name/standard: The idea of Exchange as neutral environment attracting high number of stakeholders, with a clear and identifiable offer of services and capabilities can provide a clear recognition in the market. Some marketing re-branding, as it could be a "5GEx-enabled" label, can help to create a strong name in the market.

Innovation hub: Two factors, like the presence of multiple parties, and the need for differentiation among Exchanges, can drive the innovation in this space. The first mentioned factor impacting the innovation for final services, while the second focusing on the innovation developed by the entity running the Exchange in order to be better positioned in this foreseen market.

Price and service stability: Because of the potential commoditisation motivated by the presence of multiple (competing) actors in these environments, a stable pricing scheme can be expected, due basically to competition and the easiness of trading with alternative parties.

High CAPEX/OPEX for service deployment and orchestration: the usage of the facilities provided by the entities running these Exchanges

will motivate a higher CAPEX and OPEX with regards the option of the direct peering. Such higher costs should not be prohibitive for making the parties incentivised to participle in the Exchange. Most probably, as it happens today, providers could decide to migrate the services from the Exchange to a direct peering agreement once such relationship is more cost-efficient out of the Exchange, but yet staying in the Exchange for some other relationships with other parties.

Competitors attracting more customers: A higher number of competitors will be faced in these environments which lowers any entry barrier.

Attracting InfSPs/verticals: The Exchanges can represent an attractor point for infrastructure service providers as a way of offering their resources to a wider market, especially considering the potentially larger number of verticals that could make use of these environments looking for cost-efficient resource offerings (i.e., resource slices). The high presence of potential customers in these neutral environments attracts different stakeholders looking for more alternatives in the provider space with simple mechanisms for trading, negotiating, and interconnecting.

High end user acceptance: This kind of environments have high acceptance currently with the existing limited interconnection services. It can be expected a similar acceptance level for future services.

Slowing market growth: The commoditisation effect can prevent particular (i.e., per provider) fast market growth, even if the global market growth increases faster than outside the Exchange. Furthermore, the locality of these Exchanges can reduce the market opportunities to the geographical region where the Exchange could be located.

Expanding product offerings: Because multiple parties participate in the Exchange, innovations and new product offerings will be rapidly adopted by other participants in order not to lose any competitive advantage.

Vertical integration: Vertical integration is feasible due to the expected presence of Verticals in Exchanges to access resources and services from providers in a cost efficient manner.

Opportunity to exploit new technologies, architectures: Once again, the presence of multiple parties motivates that innovations and new product offerings is rapidly adopted by other participants in order to not lose any competitive advantage.

Synergies with 5G research and industry solutions: The Exchange will facilitate the rapid trading of slices over multiple alternative providers. At the same time, it brings the meeting point for Verticals to trade such kind of capabilities in a cost-efficient manner.

High Standardisation Impact (SDOs and de-facto industry): The fact of congregating a huge number of participants makes the procedures, technologies and solutions more easily adopted, and then generalised.

Customers and providers will become used to such procedures, technologies and solutions, demanding them in other similar environments (in order to reduce unnecessary customisation per Exchange).

6.4 SWOT Analysis for 5GEx Solution "Distributed Multi-Party Collaboration" (Case C)

We apply the template for the case where the 5GEx Framework can be realised via distributed multi-party collaboration, where the operators implement the exchange functionality in a distributed manner inside their own infrastructure. That is, we consider here the case where the NSP[13] owning for instance a central office datacenter (CODC) or even an edge datacenter, i.e. we consider here a combined Network and Infrastructure SP (NISP), allows another NSP (the remote NSP) or OSP to be present based on virtualised technologies and on-demand ASQ connectivity into the CODC. Furthermore, this case allows the remote NSP to trade wholesale 5GEx services not only with this NISP but also with OSPs (OSP present at or via the CODC) of different verticals or other enterprises that buy 5G services enabled by such 5GEx multi-domain services. This case considers also 5GEx distributed capabilities that enables and support abstractions and service parameters that reaches across multiple such CODC virtualised remote private meeting locations.

[13] We use the notion of NSP, although the notion Telco can also be used, as the provider here may offer services that goes beyond pure NSP services.

Table 6. SWOT analysis for "Distributed Multi-Party Collaboration"

Strengths	**Weaknesses**
High-quality low-cost automation Facilitates bootstrapping-reaching critical mass Powerful strategy Strong revenue flows Innovation hub Price and service stability Low CAPEX/OPEX for service deployment and orchestration	Lack of compatibility to standard business
Opportunities	**Threats**
Serving additional customer groups Attracting InfSPs/verticals High end user acceptance Expanding to new geographic areas Expanding product offerings Opportunity to exploit new technologies, architectures Synergies with 5G research and industry solutions High Standardisation Impact (SDOs and de-facto industry)	No vertical integration sustainable

6.4.1 Template Justification

High-quality low-cost automation: Efficient automation with marginal cost by integrating 5GEx with the existing business process is feasible. Automation and efficiency gains can be achieved by this 5GEx approach where more direct multi-party inter-operation with verticals can be achieved also due to aggregation and economies of scale.

Higher / Lower Pr of service request orchestration: (Neutral) The focus of the business relationships for this case is more on multi-party integration with verticals. It is difficult to predict how this will impact current peering business, but the efficiency of service orchestration for such services is expected to be good.

High/Low confidentiality assurance and trustiness: (Neutral) The focus of the business relationships for this case is more on multi-party integration with verticals. This represents a new area and way of doing multi-party business. It is difficult at the current state to predict how this will impact confidentiality assurance and trustiness.

Facilitates bootstrapping-reaching critical mass: Due to the moderate complexity of requirements, roles and functionality needed this solution case is considered as feasible from a bootstrapping point of view.

Collaboration stability vs. Opportunistic/uncertain collaboration: New collaboration can be built on existing relationships while still allowing new entrants to build similar relationships or compete against established stakeholders. This way of using 5GEx can facilitate the smaller actors as well.

Fair competition and trading vs. Uneven market power and/or discrimination: On one hand the use and abuse of market power (in a similar way to traditional interconnection as explained above) results in re-enforcing and not mitigating the probability of uneven market power and/or discrimination, assuming no regulatory intervention or industry self-regulation. On the other hand the new opportunities enabled by this approach may result in a richer and more diverse set of players with a better incentive balance and in an ecosystem where value creation from local presence is more important.

Lack of compatibility to standard business: This form of solution represents new ways of doing business and will at least initially, require new innovation for the business processes as well.

Powerful strategy: Stakeholders must renew their existing business strategies to extend them to these new 5G(Ex) services and orchestration opportunities.

Strong revenue flows: Enhancement of existing revenue streams with new ones from 5GEx services.

Strong vs. No brand name/standard: Due to the fully distributed nature of this solution, it is expected to result in multiple variants of 5GEx solution as time and technology evolves, rendering the establishment of a common 5GEx brand name/standard in the long run less likely or neutral. However this will depend on potential new business community collaboration initiatives.

Innovation hub: Bilateral relationships for business opportunities in central office or even edge Telco cloud datacenters are most likely to result in the long run in a mix of customised tailor-made solutions on one hand and highly standardised solutions on the other hand. Potential partial lack of openness to the market may limit scale of innovation in some areas as opposed to 5GEx solutions aggregating the market view of multiple stakeholders.

Price and service stability: Due to a more localised or regional oriented market and value creation a potential lack of market-wide view may not cause negative effects as see in the bilateral peering competing nature of contracts.

Low CAPEX/OPEX for service deployment and orchestration: NFV and SDN technology development will improve the operational efficiency over time and the 5GEx solutions will be further developed to take full advantage of these. Orchestration CAPEX/OPEX may be significant for

stakeholders for which service orchestration as a starting point is not part of their core business.

Serving additional customer groups: Case C in particular address directly the opportunities with more direct business interaction with verticals, which both directly and indirectly can attract new customer groups. However, letting remote NSP into more direct interaction with local players may be seen as a threat of competitors attracting more customers.

Attracting InfSPs/verticals: Incremental overhead to offer new advanced 5G infrastructure services and attract more revenue exploiting both existing and new business relationships. Some changes in customer and infrastructure ownership may result, thus some uncertainty on wholesale market acceptance. The low overhead and high trust result in high probability of attracting InfSPs/verticals willing to try the 5GEx solution.

High end user acceptance: Additional and even new 5G based services are facilitated and offered in perhaps even more efficient ways to the end users of various vertical. However, this approach will need new business relationships and processes, but can be done without the formation of large coalitions that could be intimidating for end users.

Expanding to new geographic areas: Feasible due to the establishment of new peering-like relationships.

Expanding product offerings: Immediately available upon integrating the 5GEx technology using existing and new interconnections with business partners.

Vertical integration: Vertical integration less likely to happen due to higher friction and less coordination of this solution.

Opportunity to exploit new technologies, architectures: Case C in particular addresses directly the opportunities coming from 5G access and edge technology innovations and how 5GEx can help facilitate business development and multi-actor innovation. Technologies such as Central Office Re-architected as a Datacenter [14] (CORD), currently under development and supported by large NSPs and OSPs, and Mobile Edge Computing[15] (MEC) may be nicely integrated with Case C.

Synergies with 5G research and industry solutions: In line with the above in particular for case C there is a more direct line from 5G access and edge technology research and development.

High Standardisation Impact (SDOs and de-facto industry): There is a need for standardisation to lower uncertainty and improve efficiency in such a new area of innovation, so the drive toward and impacts on

[14] http://opencord.org/
[15] http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing

standardisation will be high. On the other hand there will also be a drive towards customised and tailor-made solutions to differentiate from competitors, which might diverge from standards.

6.5 Conclusions

Having applied the template for all three 5GEx solutions, we now summarise our findings using a more condensed template. In particular, when filling in this condensed template with "scores" for each of the cases A, B or C below we put for instance an A in the left cell if the factor to the left is strong, in the second left cell if the factor to the left is considered as not so strong, the middle cell if the factors to the left and right are considered as balanced or neutral for the considered case, to the very right cell if the factor to the right is considered as strong, and to the second to the right cell if the factor to the right is considered not so strong.

Table 7. SWOT analysis conclusions

Strengths		**Neutral**	**Weaknesses**	
High-quality low-cost automation				Low-quality automation, high cost to support it
A, B, C				
Higher Pr of service request orchestration				Lower Pr of service request orchestration
		B, C	A	
High confidentiality assurance and trustiness				Low confidentiality and no trust assurance
A		B, C		
Facilitates bootstrapping-reaching critical mass				No bootstrapping, low adoption
A, B	C			
Collaboration stability				Opportunistic/uncertain collaboration
	B	C	A	
Fair competition and trading				Uneven market power and/or discrimination
B		C		A
Compatibility with existing business processes				Lack of compatibility to standard business
A, B			C	
Powerful strategy				No clear strategic direction
A, B	C			
Strong revenue flows				Unclear revenue streams
A	C		B	
Strong brand name/standard				No brand name/standard
B		C		A
Innovation hub				Unsustainable innovation
B, C			A	
Price and service stability				Price wars/service unavailability/fluctuations
B	C			A
Low CAPEX/OPEX for service deployment and orchestration				High CAPEX/OPEX for service deployment and orchestration
A, C			B	

Opportunities		Neutral	Threats	
Serving additional customer groups			Competitors attracting more customers	
	C	A	B	
Attracting InfSPs			InfSPs prefer alternatives (or locked in)	
A, B	C			
Attracting Verticals			Verticals prefer alternatives (or locked in)	
B, C		A		
High end user acceptance			Low end user acceptance	
A, B, C				
Expanding to new geographic areas			Slowing market growth	
C	A		B	
Expanding product offerings			Opposing regulations (national/EU wide)	
A, B, C				
Vertical integration			No vertical integration sustainable	
	B			A, C
Opportunity to exploit new technologies, architectures			Technology/architecture lock-in, limited ability to change	
B, C		A		
Synergies with 5G research and industry solutions			Opposing 5G research and industry solutions	
B, C		A		
High Standardisation Impact (SDOs and de-facto industry)			Low Standardisation Impact	
B, C			A	

As a next step for further work we will consider adding a likelihood or uncertainty indication. For instance for Case A, we could put A-L for what is believed to be a likely outcome and A-U where the outcome is more uncertain. Hence, for the time being we have filled in the SWOT table without such likelihood / uncertainty indication but this is to be revisited in future deliverables.

7 5GEx Overall Architecture

7.1 5GEx Architecture Design Methodology

Due to the innovation character of the 5GEx project, the objective is to define an architecture not only based on the requirements to support the use cases relevant for 5GEx, but also built upon existing solutions in the state of art. These approaches come from different on-going research initiatives, projects and open source initiatives in the multi-domain exchange environment and software network architectures.

In order to address this challenge, 5GEx follows an architecture definition process based on combining, on the one hand, a top-down approach starting from the analysis of 5GEx use cases (Section 4.1) and their requirements (Section 4.2) and, on the other hand, a bottom-up approach based on an exhaustive analysis and identification of existing suitable software components (Section 2.10). As final step, the outcomes of both approaches are mapped to the 5GEx baseline architecture defined in the Description of Action (DoA), and included in Section 7.2 for reference.

These two different approaches have taken place in parallel, and, putting in common results by means of continuous feedback between them, they led to perform the gap analysis and eventually define the architecture that 5GEx aims to implement (see Figure 7-1).

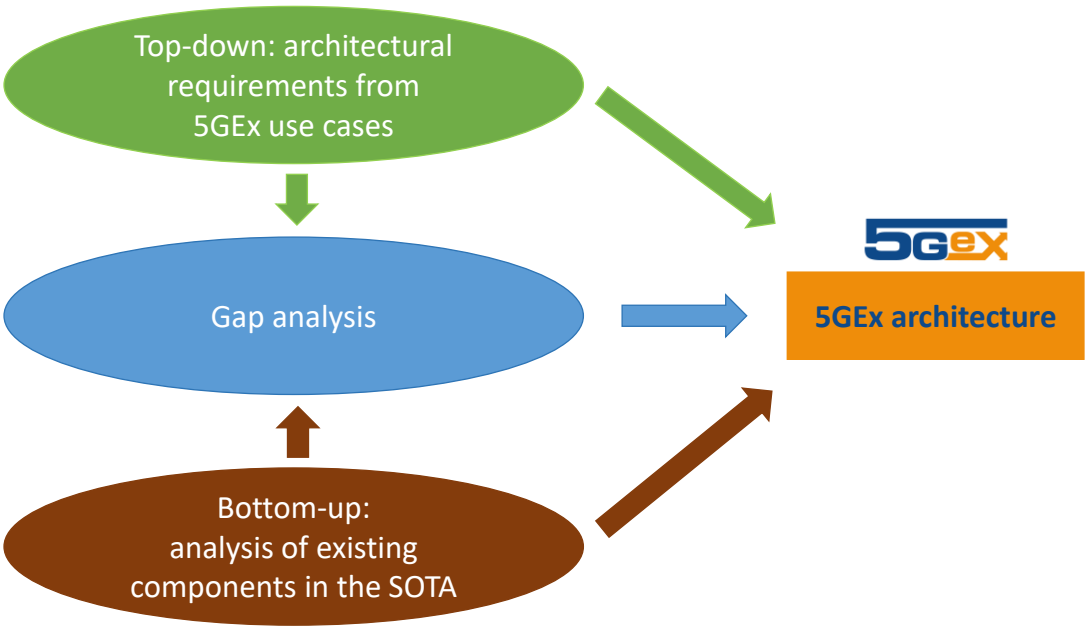


Figure 7-1: 5GEx architecture definition methodology

This architecture definition methodology has been used at the beginning of the project and has led to the results that we later report in this

document. The initial architecture-definition exercises, top-down and bottom-up, are included at the end of this document (Annex C.1 and C.2).

7.2 5GEx reference framework

The 5GEx reference framework for organising the components and interworking interfaces involved in multi-domain orchestration is shown in Figure 7-2. At the bottom there are Resource Domains, exposing a resource abstraction to the domain orchestrators. In the middle, Domain Orchestrators perform Resource Orchestration and/or Service Orchestration exploiting the abstractions exposed by Resource Domains.

A Multi-provider Multi-domain Orchestrator (MdO) coordinates resource and/or service orchestration at multi-domain level, where multi-domain may refer to multi-technology (orchestrating resources and/or services using multiple Domain Orchestrators) or multi-operator (orchestrating resources and/or services using Domain Orchestrators belonging to multiple administrative domains). The MdO interacts with Domain Orchestrators via I3 interface APIs to orchestrate resources and services within the same administrative domains. The MdO interacts with other MdOs via I2 interface APIs (business-to-business, B2B) to request and orchestrate resources and services across administrative domains. Finally, the MdO exposes on interface I1 service specification APIs (Business-to-Customer, B2C) that allow business customers to specify their requirements for a service.

The framework also considers third party MdO service providers, which does not own resource domains but operate a multi-domain orchestrator level to trade resources and services from other providers (the ones actually owning such resources).

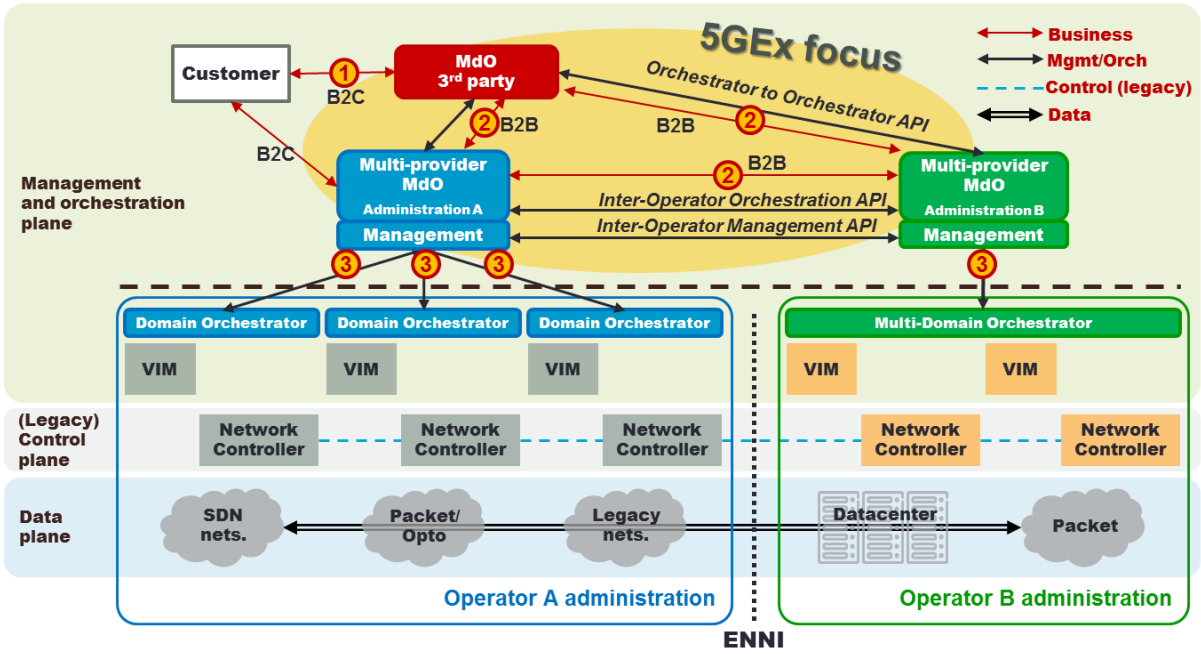


Figure 7-2: 5GEx reference architectural framework

This approach allows for a clear separation between the multi-domain elements and the local elements, while still ensuring the flexibility to handle both multi-technology and keeping local infrastructure details confidential. The multi-domain orchestrator is in charge of abstracting the underlying infrastructure before it announces what utility and functions the operator is capable of to its neighbouring operators. Using such an inter-working architecture for multi-domain orchestration will make possible use-cases that are nowadays hard to tackle due to the interactions of multiple heterogeneous actors and technologies.

7.3 Key features and architectural principles of 5GEx

To address the project objectives, an integration framework (the 5GEx baseline model was shown in Figure 7-2) is required which can accommodate software-defined specifications of networks and of computational and storage resources, as well as all of the modules and components which provide the facilities and functions for the multi-domain operations and business interactions. The main ideas and assumptions of the 5GEx model are based (A) Multi-operator wholesale relationships, (B) Multi-vendor inter-operability and within that, the possibility for Multi-technology, and (C) Physical Resources.

Regarding (A) we expect that a Customer will specify the ”Service” they require via an electronic Service Manifest document to a provider. This provider will be the origin provider for that customer. This requires the origin provider to provide a Business-to-Business (B2B) or Business-to-Consumer (B2C) facility to the Customer. In order to deliver the ”Service” the origin provider may be able to fulfil all the requirements himself, however for fully cross-domain service deployments he will need to engage with third parties to procure network resources, or compute resources, or other third party capability, in order to fulfil the full Customer request (see Section 3.6). From a business / economics viewpoint, the origin provider will become a buyer of wholesale goods from a third party, who is in a fulfiller role. There will be a sub-contract relationship whereby the fulfiller can deliver the wholesale goods to the buyer. Due to the nature of the possible services that may be requested, the origin provider can initiate these buyer/fulfiller requests to many other third parties in order to construct the elements needed for a full service deployment. As any provider can interact with customers, the model can be recursive (i.e., cascading building upon existing trust and business relationships) and stakeholders can have both roles depending on the nature of the request.

Regarding (B) we consider a model based on orchestrators and controllers. Each orchestrator will be deployed to manage different kinds of technology domains (core networks, datacenters, etc) and will interact with a set of controllers that directly interact with the devices themselves. The controllers accept high-level commands from the orchestrators and each contains different device drivers depending on the technology of the

underlying resources, and in this way 5GEx can address multi-technologies.

Physical resources (C) that are allocated to the customers can include the full set of network resource options whether Access networks, e.g., LTE (wireless), DSL (wireline), IP/MPLS, optical/GMPLS, OpenFlow based Software Defined Networks or other network technologies, as well as the full set of compute options including virtual machines, storage, bare-metal hosts, or applications. From the perspective of 5GEx these resources are considered to be a black box with a wrapper which will enable the device driver to configure and maintain the resources.

In order to overcome the traditional separation of network resources from compute and storage resources, 5GEx will be (i) fully software driven, (ii) allow the combination of networks and compute / storage within a service, (iii) define economic enabler components in the architecture and standard interfaces and SLAs that enable the automated trading and orchestration of networks and compute / storage in a service that comprises also an attractive market product.

Within a single domain, the modules and components will have specific well-defined functionality, interacting with the other modules and components using task specific APIs. For the inter-domain activity, there will be a set of these components that support various negotiation, trading and control operations between administrations. The inter-domain activities can be viewed with respect to two major configurations. The first is the operator to operator viewpoint, where the inter-domain activities are between entirely separate administrative domains that are operated by separate organisations, where only certain elements within each domain can interact with each other. The second is the in-operator viewpoint, where the inter-domain activities are within a single operator, and each of the domains may be a partition of or a logical domain within the organisational resources.

7.4 High-level description of 5GEx main architectural entities

In this section we extend the ETSI MANO NFV management and orchestration framework to implement Network Service and resource orchestration across multiple administrative domains, which may belong to different infrastructure operators or service providers, hereby referred as “providers”. For multi provider Network Service orchestration, a multi domain orchestrator (MdO) offers Network Services by exposing an OSS/BSS – NFVO interface to other multi domain orchestrators belonging to other providers. For multi provider resource orchestration, a multi domain orchestrator presents a VIM-like view and exposes an extended NFVO – VIM interface to other multi domain orchestrators.

Figure 7-3 shows the different functional blocks responsible for service orchestration (SO) and resource orchestration (RO) as defined by ETSI

OSM. Resource orchestration is provided by the NFV Management and Orchestration, together with Network Service orchestration. On the other hand, service orchestration, which among others is responsible for configuring parameters within VNFs e.g., via element managers, is implemented by an OSS/BSS system.

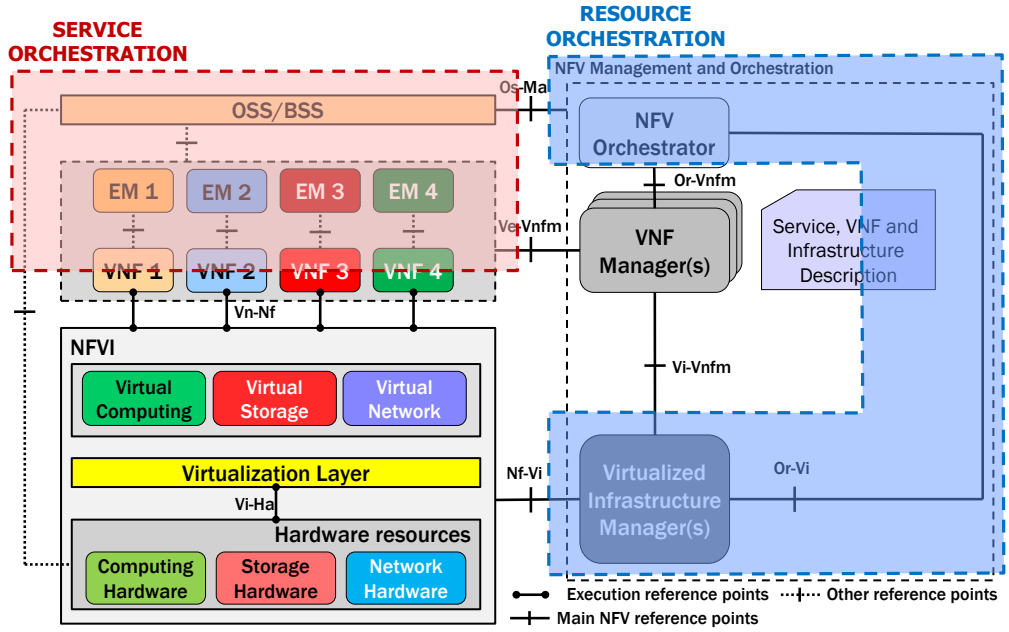


Figure 7-3: Service and resource orchestration

The functional blocks of the multi domain orchestrator are shown in Figure 7-4 and enumerated in Table 8.

As illustrated by Figure 7-4, the (left) MdO consumes interfaces, such as I2-S or I2-RC, to other MdO-s. In addition, the right MdOs may also consume the same interfaces offered by the left MdO (symmetric interfaces, consumer – provider role is situational), but for this case the corresponding arrows are not depicted for simplicity.

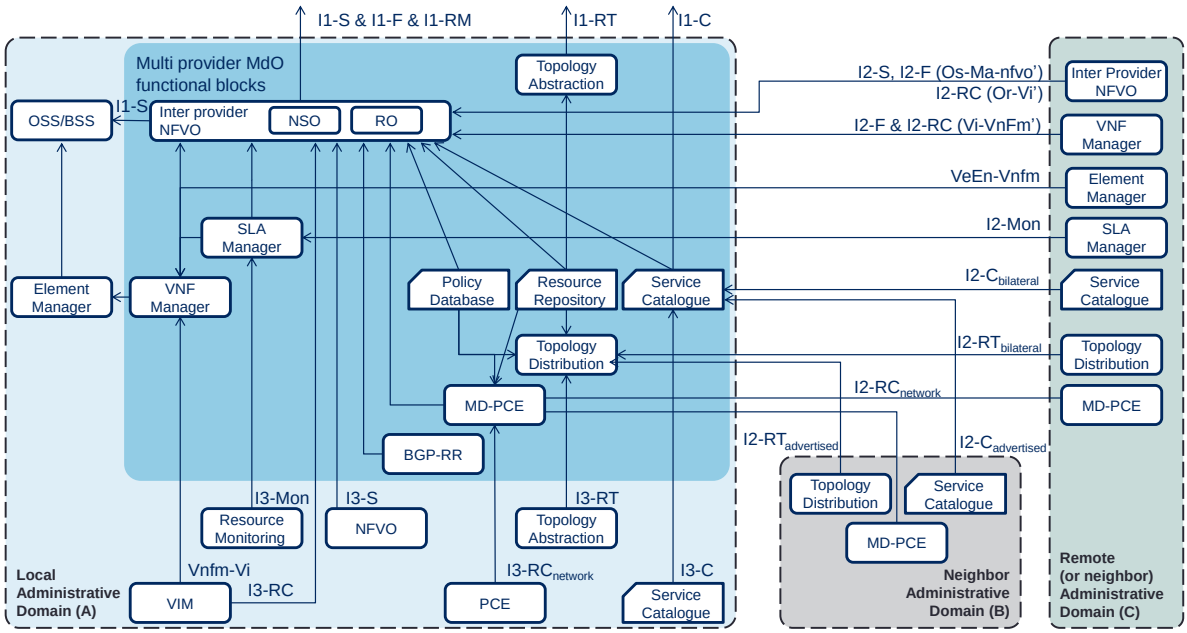


Figure 7-4: Functional model of multi domain orchestration

The notations of I2-S/C/R and I3-S/C/R are used as defined in Annex C.2. Resource orchestration related interfaces are broken up to I2-RC, I2-RT, I2-RMon to reflect resource control, resource topology and resource monitoring respectively. Furthermore, this notation is generalised and also used for interface I3 and I1.

Table 8. Summary of main 5GEx functional blocks

Functional block	Main Functionality/purpose
OSS/BSS	Include collection of systems/applications that a service provider uses to operate its business.
Element Manager	Responsible for the FCAPS (Fault, Configuration, Accounting, Performance and Security management) of VNF.
VIM	Controls the assignment of resources from NFVI to support services.
VNF Manager	Manages VNFs (lifecycle, FCAPS of VNFs, VNF scaling).
NFVO	Provides Resource Orchestration and Network Service Orchestration.
Inter-Provider NFVO	NFVO implements multi-provider service decomposition.
Topology Abstraction	Performs topology abstraction elaborating the information stored in the Resource and Topology Repository.
Topology Distribution	Exchanges topology information with its peer MdOs, to be included in the Resource Topology Repository.
SLA Manager	Responsible for reporting on the performance of its own partial service graph.
Policy Database	Database containing policy information.
Resource Repository	Keeps an abstracted view of the resources at the disposal of each one of the domains reachable by the MdO.
Resource Monitoring	Dynamically instantiates monitoring probes on the resources of each technological domain involved in the implementation of a given service instance.
Service Catalogue	Exposes available services to customers and to other MdO service operators.
PCE	Path Computation Element as defined by IETF.
MD-PCE	In charge of making the necessary path computations and setting up the connection between domains.
BGP-RR	BGP Route Reflector.

The Inter-Provider NFVO implements service decomposition by mapping Network Service components on its current resource view. The resource view consists of the Inter-Provider topology, potentially augmented with detailed provider internal topologies and resource locations and capabilities. At first, the Inter-Provider NFVO selects providers that may need to be involved in delivering the Network Service. This decision is policy based considering the Inter-Provider topology and service catalogues advertised by other service providers on interface I2-$RT_{advertise}$ (resource topology) and I2-$C_{advertise}$ (service catalogues). If needed, the multi provider NFVO may collect further details on charging, offered capabilities, Network Services, resources and topology from selected providers and may establish / update bilateral (or direct) business relationship to some of them as decided / necessary, as proposed in Annex C.1.3. Then, the Network Service components are mapped on the inter-provider, or optionally on more detailed topology, based on the information collected bilaterally from involved providers. Then, the multi provider NFVO sends the Network Service/resource requests to other providers using the I2-S/I2-RC interfaces.

The multi provider NFVO also implements policy enforcement points on behalf of its administrative domain to profile incoming requests received from other providers. Policy enforcement is needed to allow authorised providers to implement resource orchestration (I2-RC) and/or lifecycle management (I2-F) in their own domain. Administrative domain wide policy enforcement is needed to enforce aggregate resource limits.

To assist the multi provider NFVO in service decomposition, there is a need to distribute topology and resource information in two ways:

1. Providers advertise basic Inter-Provider topology and optionally also their service catalogue information to all or to a predefined group of providers. This is done via the I2-$RT_{advertised}$ and I2-$C_{advertise}$ interface.
2. Providers exchange information on a bilateral basis in a consumer provider relation. This is done via the I2-$RT_{bilateral}$ interface.

Providers advertise their basic Inter-Provider topologies to support an initial mapping of the multi provider NFVO orchestration process. Optionally, depending on provider policies, the advertisements may also comprise of more detailed provider internal topology, IT resource capability and location (i.e., compute capacity attached to virtual nodes), as well as access information of the originator provider's orchestration interfaces. Such advertisements may get propagated hop-by-hop, e.g., by BGP-LS, in which case the propagation is subject to the policies of all intermediate providers.

In addition, providers establish bilateral communication between potentially remote, i.e., non-directly connected, Inter-Provider orchestrators in a customer – provider relationship. This is needed to avoid 3rd party involvement in relaying bilateral business information.

Furthermore, this also improves scalability by limiting the scope of detailed information distribution to specific providers. Such bilateral communication is supported for all Inter-Provider interfaces.

Figure 7-5 illustrates the high level signalling chart between multi provider orchestrators. The flow chart refers to the scenario where two tenants request services from administrative domain C (in Figure 7-5), which requires Network Services and/or resources from administrative domain A and B to provide the services to tenant 1 and 2. The signalling consists of three phases:

1. The advertisement phase implements the basic Inter-Provider topology distribution.
2. The bilateral phase consists of the establishment of a business relationship and bilateral information sharing.
3. The orchestration phase involves initiating Network Service or resource requests.

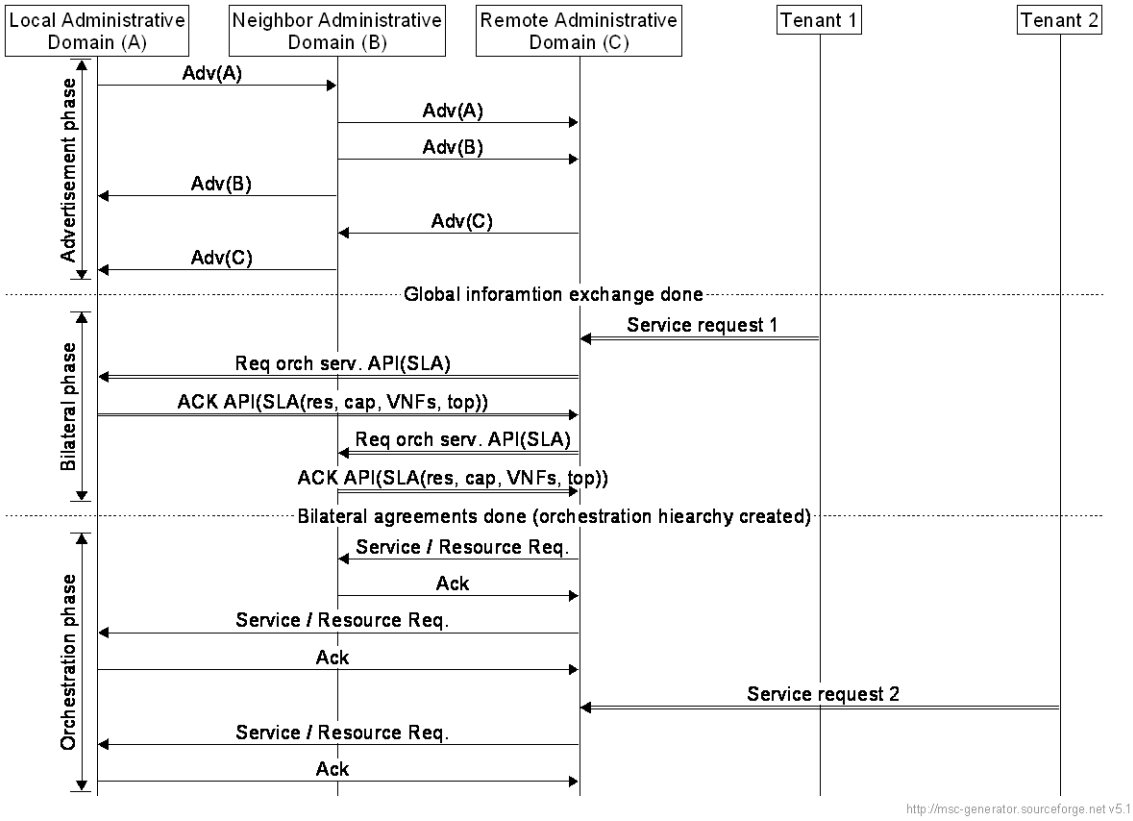


Figure 7-5: High level orchestration flow chart

As part of the service decomposition, the multi provider NFVO must be able to initiate potentially traffic engineered multi-provider connectivity. To be able to manage connectivity constraints, the multi provider NFVO interworks with a potentially external PCE, which has the visibility of Inter-Provider topology. For example, the PCE may be a consumer of the topology information gathered to support the multi provider orchestration.

Typically, the connectivity data plane is configured by a control plane protocol, such as MP-BGP or PCEP. In this case, the multi provider NFVO programs the control plane to implement resource orchestration, e.g., for allocating and distributing labels on ENNI links. To achieve this, the multi provider NFVO may use the PCEP protocol to ask an active stateful PCE to set up connectivity. Intermediate providers should verify that an incoming connectivity request is coming from an authorised partner via orchestration states/policies. Such an orchestration state may a priori exist (see Figure 7-6) or it may need to be established by the Inter-Provider NFVO (see Figure 7-7). Section 8.1 contains further details on operation and terminology for TE connectivity setup. Note that Figure 7-6 and Figure 7-7 refer to multi provider connectivity setup only and do not cover aspects of NFV provisioning.

Alternatively, the Inter-Provider NFVO may configure directly the connectivity data plane along the principles of ONF SDN for OpenFlow controlled administrative domains. In this case coordination for ENNI data plane resource orchestration must be implemented by the Inter-Provider NFVO.

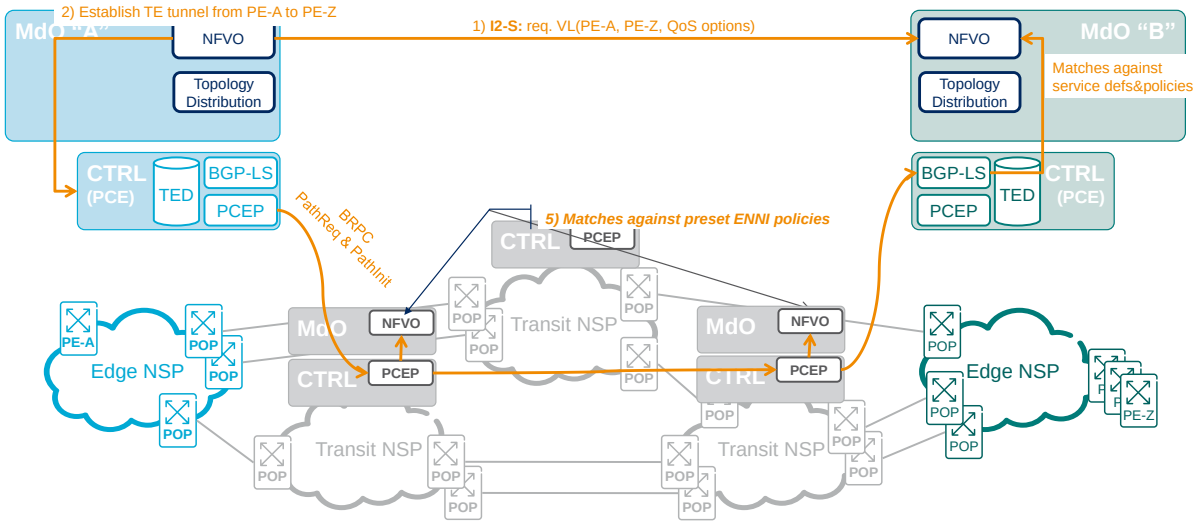


Figure 7-6: Aggregated (e.g., per ENNI) policies exist a priori in MdO-s

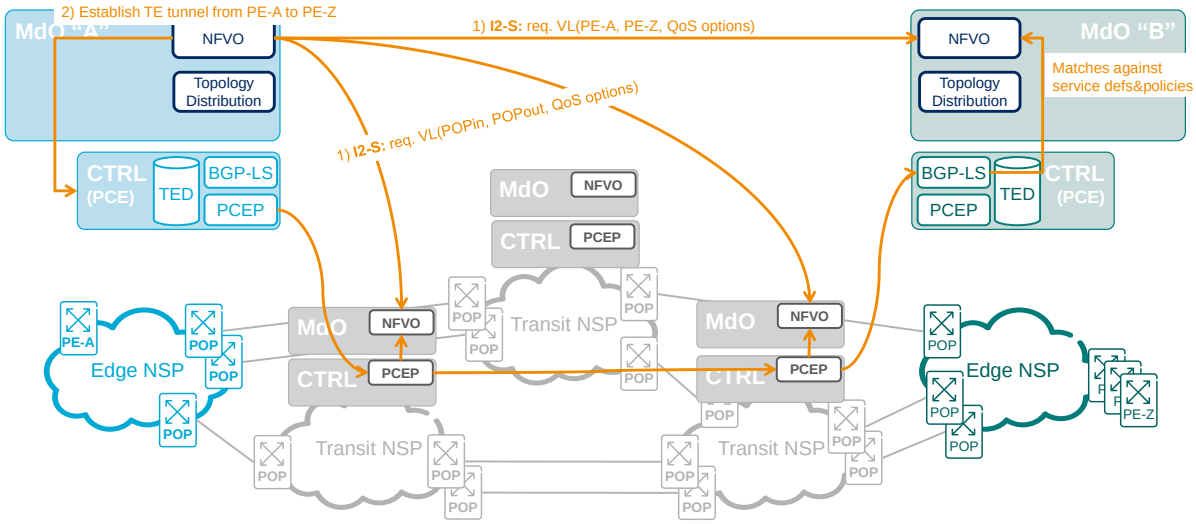


Figure 7-7: Per Network Service policies set up during orchestration

The service catalogue contains information on the Network Services and VNFs provided by various other domains. Furthermore, due to potentially different charging and/or different implementation templates and/or different flavours, the same VNF may be included multiple times as per flavour at virtual host at virtual provider. Scalability of the service catalogue and methods that allow querying remote domains for service capabilities and attributes on demand may be required.

Functionality of SLA management is defined as collecting and aggregating quality measurement reports from probes provided by the (virtual) infrastructure or initiated by the Inter-Provider NFVO as part of the service setup. Depending on the already deployed provider internal management and orchestration structure, measurement results may already represent aggregated views. In a multi provider setup, parts of the SLA management are delegated to the remote domain as the Inter-Provider NFVO defines requirements with the Network Service/resource request. In addition, the SLA manager correlates faults (alarms) and performance degradation events and may report SLA violations to remote multi provider orchestrators or directly to customers if it was requested as part of the service request.

The southbound interfaces of the multi provider orchestrator shown in Figure 7-4 illustrate the interfaces to be provided by underlying domains to support multi provider orchestration. The functional blocks cover interfaces for two provider internal orchestration scenarios:

1. Flat orchestration, when the multi provider NFVO is deployed directly over domain internal VIMs.
2. Layered orchestration, when the multi provider NFVO (functionality) is deployed over one or more existing (administrative domain internal) NFVOs.

8 Deployment Scenarios for Connectivity

This section describes how to apply the functional architecture blocks to set up example services across multiple administrative domains in specific network scenarios. The purpose is to verify the applicability of the functional architecture in the deployment scenarios and identify improvement areas.

Three deployment scenarios are considered from connectivity setup point of view, which complements the VNFaaS and SlaaS scenarios of D3.1:

1. Traffic Engineering (TE) connectivity setup.
2. Setup of a pair of VMs interconnected by an inter AS L3 VPN.
3. Value added connectivity service setup.

The TE connectivity setup section below explains how to set up TE tunnels. The VPN section focuses on how to set up inter AS VPNs and by default it uses best effort paths, optionally VPNs may use TE paths. Finally, the Value Added Connectivity Service (ASQ) section describes how IP traffic may be mapped to Assured Service Quality paths between an application provider and a selected region. An ASQ path is an abstracted QoS path that does not have to be implemented by a TE tunnel. . An ASQ path is realised through the establishment of Core ASQ Interconnection services and Enterprise ASQ Interconnection services. (See Section 3.2 for more information. The detailed specification of ASQ Interconnection services is for further study.)

The deployment scenarios consist of a network scenario with example data and control planes to support proof points that relevant aspects are covered with the functional blocks and the aspects are assigned to a given functional block.

Throughout the subsections below, illustrations of ETSI Network Service Descriptors are used to request Network Services from other administrative domains. The syntax used in the NS illustrations serves as an example syntax and there is no intention to rule out other candidate syntax.

8.1 Traffic engineered connectivity

The proposed solution has been considered for the setup of core connectivity with specific QoS requirement. With the term "core connectivity" we refer to the infrastructure between DCs of different providers. The target is to create TE tunnels between the gateways of DCs, with specific QoS also spanning across multiple providers, which can be used for the Network Service orchestration by the Inter-Provider NFVO. More specifically the interaction between different MDOs is

considered, focusing on the exchange of topology information and control plane interaction across multiple administrative domains.

According to the MdO architecture proposed in Section 7.4 the main functional blocks involved in this operation are: the Topology Distribution and the MD-PCE.

In Figure 8-1, the reference scenario to discuss the TE connectivity is presented. Three administrative domains are considered, where a local WAN domain for each administrative domain is managed by a Wide-are Infrastructure Manager (WIM – as a special type of VIM). The reference WAN data-plane is an MPLS network. The administrative domains A and C also include one IT domain, managed by a VIM. Only DCs and related gateways are shown in the reference scenario, just to highlight the main data-plane components involved in the process. The reference DCs data-plane considered in this discussion consists on an IP fabric. The WIM includes a topology abstraction module, to maintain an abstracted view of the local domain, and a LocalPCE to perform path computation on the physical topology. The WIM is in charge of sending the abstracted topology of the local domain to its MdO, in order to maintain an updated view of the available resources. The VIM sends to the MdO information about the status of the DC.

On top of the WIM and VIM the MdO is in charge of orchestrating the inter-provider interaction with other administrative domains. Only the functional blocks involved in the TE connectivity process are depicted here for sake of simplicity. In particular, the *Resource Repository* is a DB where the abstracted views of the domains are stored. It includes both the view of local domain (received from the WIM) and the abstracted topologies of other administrative domains. The exchange of topology information across the MdOs of different administrative domains is managed by the *Topology Distribution* functional block. The *MD-PCE* is the functional block in charge of computing multi-provider paths according to the information stored in the Resource Repository. Then it provides the resulting core connectivity tunnel to the *Inter-Provider NFVO* to perform the network service orchestration.

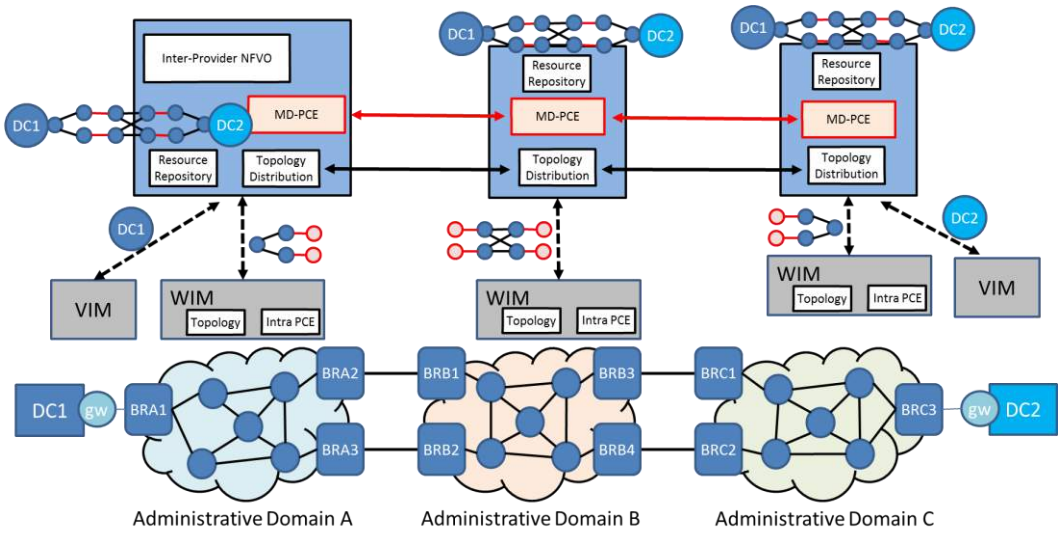


Figure 8-1: Reference scenario with three administrative domains

8.1.1 Topology exchange

As briefly described, the Topology Distribution functional block is in charge of managing the exchange of topology information. In particular, considering the "local" exchange of information, it receives the abstracted topology from the local domains (in Figure 8-1 just a WAN and one IT domain each is considered for administrative domains A and C) and store it in the Resource Repository. The local topologies coming from local domains are then aggregated, to have an overall abstracted topology related to all local domains. The Topology Distribution module is in charge of the management of inter-provider topology information exchange. According to the policy agreed with other providers, a specific session is established to import/export topology information. In fact, the local abstracted view is exported to peer providers, while the abstracted view of the others is received. All these information are stored in the Resource Repository, to be used for further path computation processes. The transit providers, administrative domain B in the reference scenario, are in charge of distributing also the topology information of other providers that do not have a direct peering session. In particular, considering Figure 8-1, the Topology Distribution module of administrative domain A has a peering session with Topology Distribution module of administrative domain B. Within this exchange, it exports local abstracted topology containing abstracted intra-domain links (in blue) and inter-domain links (in red) to administrative domain B, while it receives the abstracted topologies of administrative domain B and administrative domain C. The same happens on the communication between the Topology Distribution module of administrative domain B and the Topology Distribution module of administrative domain C. At the end of the process resource repositories of all the administrative domains contain the same information, so that all the providers are able to perform multi-provider path computations.

The abstraction strategy to be considered for the representation of topologies is a key factor. In fact, the selection of the abstraction model impacts both the time required for the exchange of the information and the time for the computation of the abstraction. On the other hand, providing more details of the abstracted topology improves the path computation process. Two possible abstraction strategies were discussed in the project: the star and the full-mesh. Considering the features of the two solutions, the star abstraction model is more scalable since it includes few links, while it adds more computational complexity with respect to the full-mesh. This is mainly due to the processing required to abstract the full network topology.

8.1.2 MD-PCEs interaction

To setup a TE connectivity between the gateways of two DCs across multiple-providers the PCE has been considered as candidate. In particular, the MD-PCE module is exploited to activate the control-plane interaction between MdOs. Moreover, acting as Parent PCEs, the MD-PCE communicates with the LocalPCE at WIM level, which acts as child PCE, to take care of the deployment of TE tunnels in the local domain.

So far, two possible solutions have been considered: a distributed Backward Recursive Path Computation procedure (BRPC) and a centralised Hierarchical Path Computation Element solution (H-PCE).

To explain the differences of the two solutions, a multi-provider network with administrative domains A and D that are the end-points of the TE tunnel (represented with a green bold line) has been considered, while administrative domains B, C and E are marked as transit providers (see Figure 8-2 and Figure 8-4 With black arrows the sessions for the topology distribution are represented, while red arrows highlight the interaction between the MD-PCE of different providers. The AS path computation (the list of providers to be traversed) is always performed at the source administrative domain (e.g., administrative domain A) according to the information present in the Resource Repository. In both the presented examples the AS path, matching the constraints of the request, is A-B-E-D.

8.1.2.1 BRPC procedure

Figure 8-2 shows the example interactions between the MdO modules involved. Keeping in consideration the red arrows and starting from the administrative domain A (source administrative domain), the interaction follows the computed AS path. In fact, the MD-PCE of each administrative domain requests the path computation to the MD-PCE of the next administrative domain in the AS path, so that at the end of the backward interaction the overall path is computed. More specifically, the path computation within each local domain is performed by the LocalPCE within the WIM. Each MD-PCE interacts with other MD-PCE in the BRPC fashion,

while it is acting as Parent PCE respect its LocalPCE, which is acting as Child PCE.

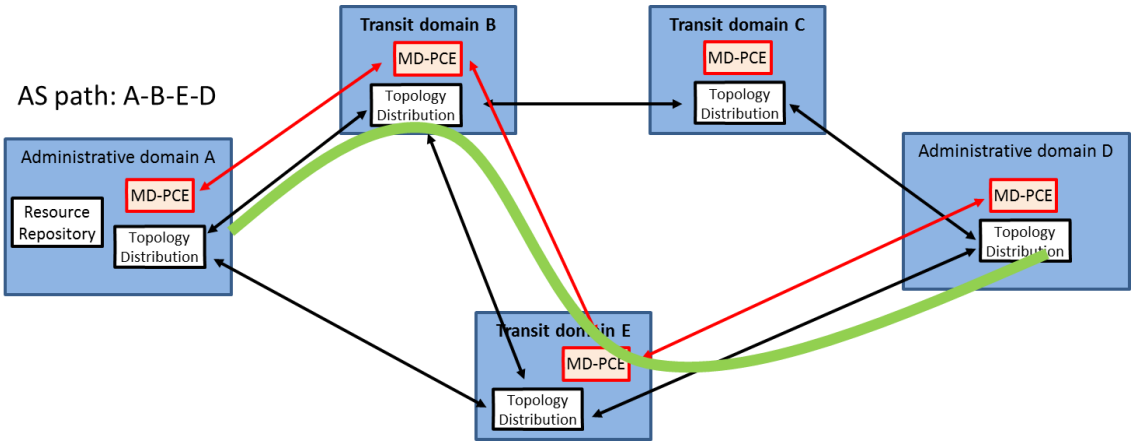


Figure 8-2: Distributed BRPC solution

The details of the message exchange are shown in Figure 8-3, considering three administrative domains involved in the e2e connectivity setup.

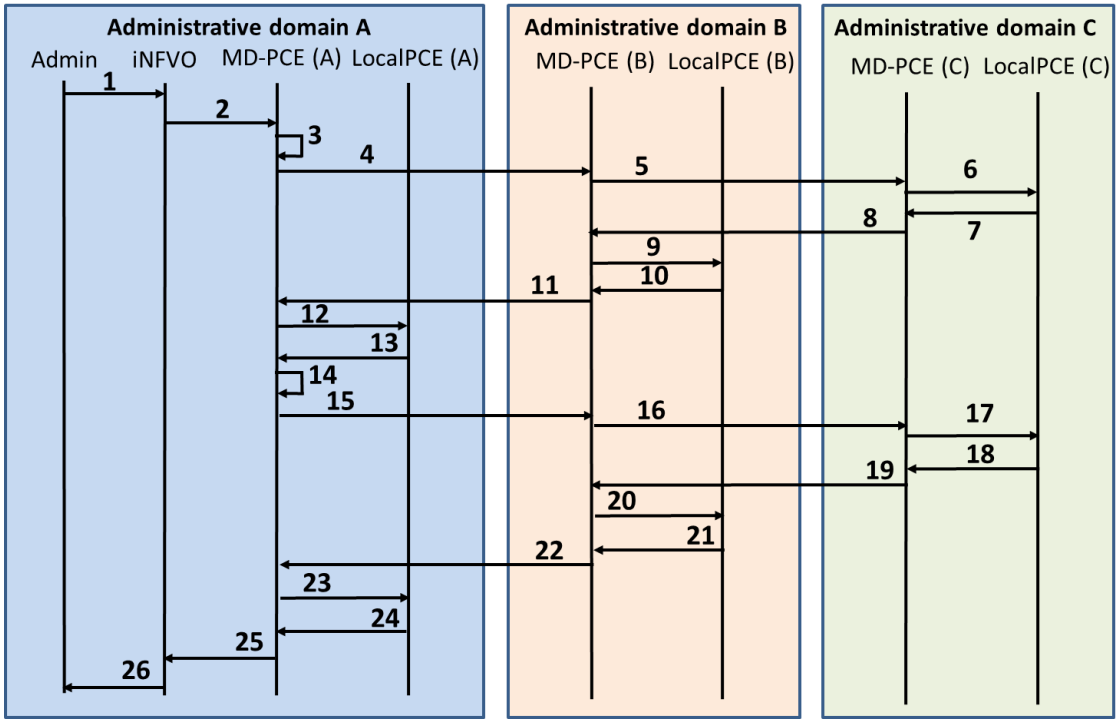


Figure 8-3: Message exchange in BRPC

The first 14 steps are needed to perform the path computation, while the rest of the messages are exchanged for the deployment of the end-to-end multi-provider path.

Labels need to be exchanged between providers to setup the tunnelling on the inter-provider links. At the end of the procedure the e2e TE connectivity is achieved.

8.1.2.2 Hierarchical (H-PCE) procedure

Figure 8-4 shows the example interactions between the MdO modules involved. In particular, it refers to the centralised solution where the MD-PCE of the source administrative domain (e.g., A) is in charge of interacting with the MD-PCEs of the other administrative domains involved in the TE connectivity setup. The MD-PCE module within the MdO can assume two different roles. In case of source administrative domain, after receiving the path request directly from the NFVO, the MD-PCE acts as Parent PCE and sends a PCRequest and/or PCInitiate messages to other MD-PCEs. Considering the case of an administrative domain involved in the deployment of the connectivity that is not the source, the MD-PCE works as child PCE and receives the path request from the MD-PCE of the source administrative domain.

Moreover, within each administrative domain, a further communication is required, involving the MD-PCE of the MdO and the LocalPCE of the WIM. Also in this case, the H-PCE solution is adopted, since the MD-PCE acts as ParentPCE and the LocalPCE acts as ChildPCE.

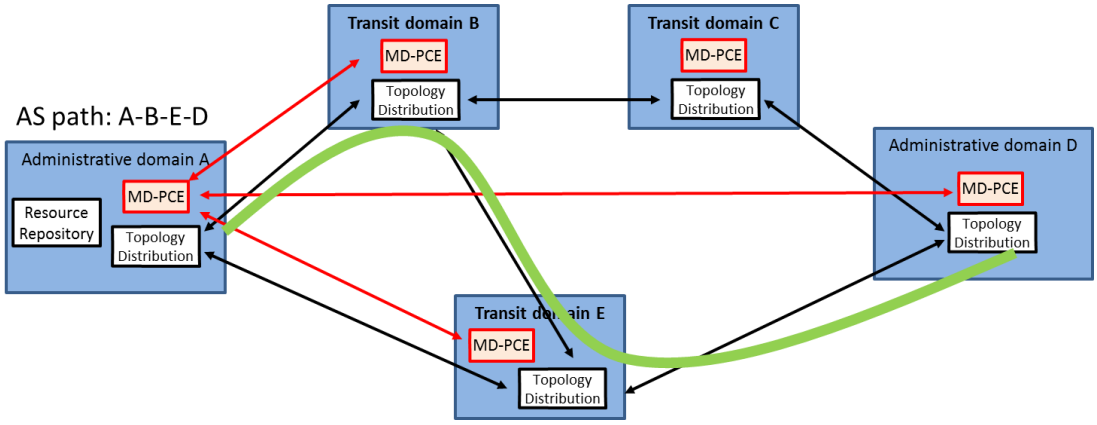


Figure 8-4: Centralised H-PCE solution

The details of the message exchange are shown in Figure 8-5. In particular, the active PCE capability has been considered for the initialisation of the TE connectivity.

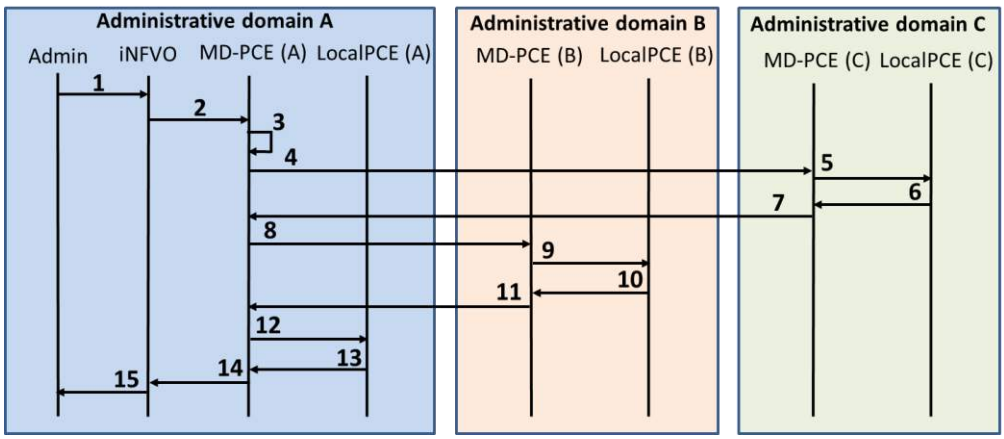


Figure 8-5: Message exchange in H-PCE

As discussed, the MD-PCE of administrative domain A manages the interaction with other MD-PCE. The way to compute the inter-provider labels can be managed in a centralised way (i.e., is MD-PCE of source administrative domain that selects and communicates to all the other MD-PCEs the labels to be used) or it can be advertised by the different MD-PCE of the involved administrative domains. In the considered example, the latter option has been considered.

8.1.2.3 General comments

The two procedures follow different interaction schemes, achieving the same result.

Considering that the administrative domains (i.e., providers) can use different solutions, in the context of the 5GEx project, both described procedures (i.e., BRPC and H-PCE) are viable solutions and 5GEx should allow using either of those.

Comparing Figure 7-4 and Figure 8-4 the different interactions between MdOs can be analysed. In the case of BRPC, each MdO interacts only with neighbours, without requiring addition connections. This feature is very important, since it simplifies the interaction at MdO level. The BRPC path selection presents good flexibility, since it leverages in the single administrative domain path computation. In fact, at each administrative domain the MD-PCE is invoked as "entry point" for submitting the requests, then the path computation is left to the Local PCE. In case of failure or unavailability of an abstracted link, the path computation scheme automatically adapts the topology change, without requiring further steps. Moreover, the complexity for computing the end-to-end multi-domain path is high. In fact, at each step the administrative domain are exchanging a tree information, in order to keep in consideration more paths. Analysing the diagram related to the message exchange, shown in Figure 8-3, the BRPC procedure requires 26 messages to setup the end-to-end path across three administrative domains. Moreover, the path selection is totally distributed, so that the source administrative domain selects only the AS path to be followed. Then, the selection of the edge nodes, internal links and inter-provider links is performed at within each administrative domain.

Conversely, in the H-PCE scheme, the MD-PCE of source administrative domain, acting as Parent PCE, interacts with the MD-PCEs of all the other administrative domains involved in the TE connectivity setup, which work as child PCEs. In this way, the scheme requires that all the providers have an established PCE session. This requirement is very critical and adds complexity in the communication at MdO level, since the possibility to have a PCE session is not always allowed. For this perspective, the BRPC procedure seems to be a better choice, because it is possible to follow the peering "topology" between different providers, according to the agreements across providers. However, in H-PCE the path selection is performed in a centralised way, according to the information of the

abstracted topology. In fact, the source administrative domain, other than computing the AS path, is in charge also to compute the "e2e abstracted path". Then, the deployment of the computed path is left to the different administrative domain. Basing the selection on the centralised computation provides less flexibility on the path selection. On the other hand, the complexity for the path computation is lower than the complexity in BRPC. Keeping in consideration the diagram of Figure 8-5, the H-PCE solution requires 15 messages to perform the deployment of an end-to-end multi-provider path with three administrative domains.

Output to the Inter-provider NFVO

The result of the computed TE connectivity tunnel is then sent to the Inter-Provider NFVO, which can exploit this information to perform the orchestration of Network Service requests.

Figure 8-6 shows the above reference scenario enhanced by three gateway-to-gateway TE connectivity (i.e., TE tunnels) between the two DCs. More specifically, three tunnels are shown, with different parameters: the red tunnel presents a guaranteed bandwidth of 10Gbps, the yellow tunnel has a guaranteed latency of 20ms, while the green tunnel is a Best Effort (BE) tunnel, with no guaranteed QoS.

Besides the abstracted topology view retrieved through Topology distribution module, the NFVO keeps also track of TE core connectivity. In fact, also the view, which consists of two DCs (DC1 and DC2) interconnected by three logical links (red, yellow and green links) in the top part of the picture in administrative domain A is maintained at NFVO. Receiving a new Network Service requests, the Inter-Provider NFVO will perform the service orchestration, according to the QoS parameters in the request, by using the TE connectivity available. If no specific requirement on the connectivity request the BE tunnel can be used. While, if no paths match the request requirement (no TE tunnels yet established fit the requested QoS), a new TE connectivity tunnel can be established, if enough physical resources are available.

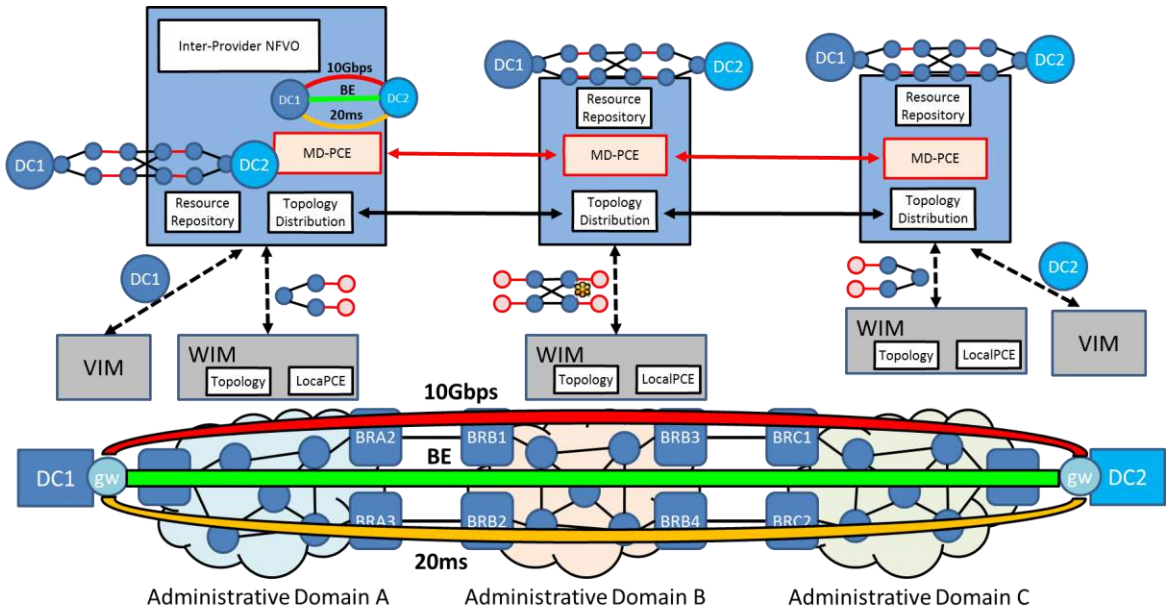


Figure 8-6: TE connectivity view in the reference scenario

8.2 [Section removed from the public version]

[This section will be made available publicly later.]

8.3 Value added connectivity services

8.3.1 Introduction to Value Added Connectivity Services

Value Added Connectivity Services offer controlled QoS between selected pairs of public IP addresses and are provided to fix or mobile subscribers. In this section, we consider two implementation approaches to value added connectivity services. The first approach is based on the loose model, where the global routing table is used for forwarding. This option assigns selected IP packets to better than best effort queues and still uses best effort Internet paths. The second approach is based on the hard model which builds VACS service specific routing tables, as service specific VRFs, and maps IP traffic to Assured Service Quality paths. Both approaches overlay wholesale Value Added Connectivity Service (VACS) on top of an Assured Service Quality (ASQ) Service (see Section 8.3.1). We consider an ASQ region whereby autonomous system owner have made a range of bi-lateral contracts and implement the ASQ and VACS service in that region.

8.3.2 VACS based on better than best effort slices

We describe next a model for value added connectionless QoS based on existing BGP forwarding plane. We consider two service types of complementary wholesale services:

- ASQ Service: Assured Quality Interconnection Services.
- VACS: Value Added Connectivity Services.

These complementary services are similar in structure but are implemented at different parts of the value chain. The ASQ service assumes ownership of an autonomous system data plane infrastructure and is generally invoked on interface 2 of the 5GEx Exchange. The VACS service generally assumes no ownership of data plane infrastructure and rely on an underlying ASQ service.

Firstly, we describe initial business conditions and VACS and ASQ wholesale products the establishment of the ASQ region. Then we describe the product sold in the supply chain. Next we give an example of the data plane. Sequence charts are shown and there is a walkthrough of the process.

8.3.2.1 Business relationships Initial conditions

The initial conditions for the business relationships are that parties who intend to join the ASQ region already have an interconnection relationship where BGP is already used. The ASQ relationship can be built on top of the existing commercial arrangements. Exact charging functions are out of scope of this work. But some indication is that charging for the ASQ would be some premium (e.g.) over best effort. It could be implemented on a 95% basis as is often used in interconnection charging. Charging could also be implemented on a flow basis (e.g., by volume or duration) and would be initiated once the service is invoked for usage.

We note that the functionality of initiating business contracts have not been addressed so far. This and the associated parameters are exchanged are for further study. It is also a question whether or not it is the NFVO and/or the OSS/BSS system that should host that functionality.

8.3.2.2 Establishment of ASQ Region

Figure 8-7 shows the internet as a 'global slice' of best effort forwarding giving global reach. In practice this is constructed, among the larger operators, as a traffic engineered mesh built with MPLS-TE/RSVP and similar techniques. Diffserv EF and AF is usually implemented within an autonomous system and supported by MPLS EXP –QoS bits in the MPLS header - and offered to enterprise market. But today there is no interconnection of the Diffserv topology slice of EF regions. See Figure 8-7.

Figure 8-7: Global Slice with pre-existing Local AS slices of expedited forwarding

In this use case we connect these pre-existing Diffserv slices on a bilateral basis. See Figure 8-8. In order to connect these slices we need to make a contract and publish interconnection points.

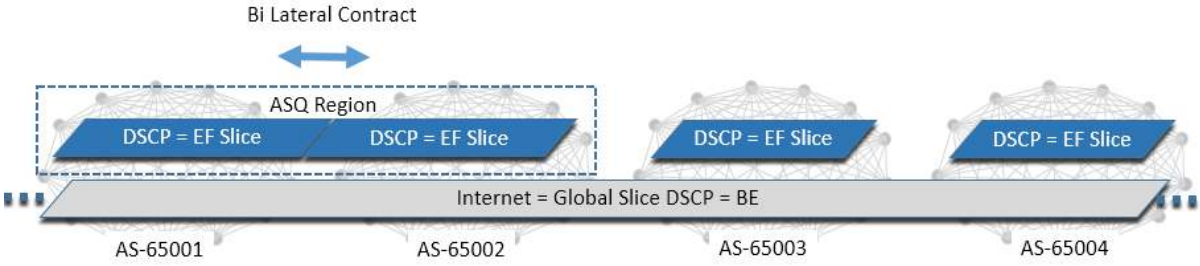


Figure 8-8: Bilateral interconnection of EF slices

The suggested bi-lateral contract terms are:

- Agree to carry EF traffic between two end points in the autonomous system. End points exist in the autonomous system as hosts or gateways to another region.
- No bleaching of EF traffic - EF bit remains intact.
- Agree to dimension X% of resources for EF traffic. X% is an internal policy decision related to dimensions of capacity dimensioned for EF in the ASQ region. The quantum of X is then sliced based on capacity requests. If no capacity is available then a blocking signal is sent to the requesting party. The quantum of traffic is the capacity available for subsequent slicing into virtual path slices with a sustainable or minimum guaranteed bit rate.
- Agree to accept bandwidth reservation for quantum of traffic.
- Quantum of traffic = minimum guaranteed bitrate.
- Agree to bound EF domain for ASQ traffic to the MdO CAC model (or overprovision EF domain). Implementing CAC is part of the per flow model.
- Use of Global Routing Table – GRT.
- 95% percentile agreement.
- ASQ Services can be configured in the services library with a flexible range of bit rate to vary traffic (See Figure 8-14).
- Explicate policing of EF traffic on ingress to AS.

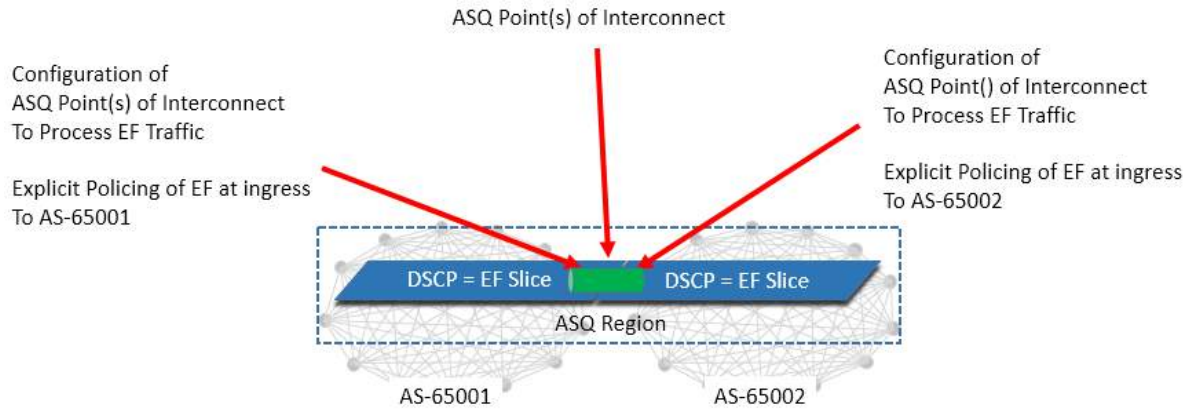


Figure 8-9: Configuration of Point of Interconnect

Figure 8-9 shows the configuration of the point of interconnect which must be enabled to handle EF traffic with explicit policing on the ingress of each AS.

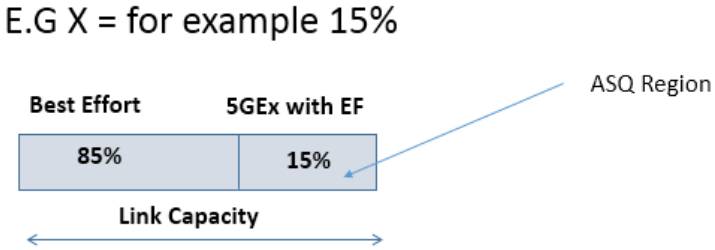


Figure 8-10: Quantum of capacity allocated to EF in the ASQ region

Figure 8-10 shows that a certain quantum of capacity of allocated to the ASQ region. Perhaps 15% initially but this could be expanded depending on capacity demand.

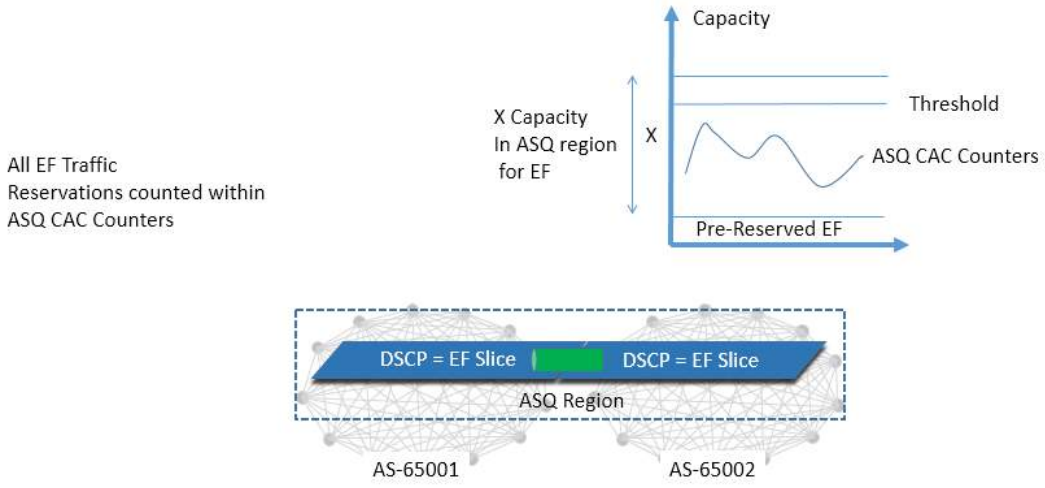


Figure 8-11: Capacity Reservation Counters for the CAC

Figure 8-11 shows the reservation counters for the ASQ region. All EF traffic requests in the ASQ region must be represented in these counters. Existing EF background traffic (e.g., for voice) must be bounded as part of the pre-reserved value. The counters count EF requests in the ASQ region

up to the limit X. If the requested capacity reaches the threshold, then this is an advisory to deploy more capacity or to repurpose BE capacity as EF capacity. If the capacity counter reaches the limit of X, then a blocking signal must be given at the MDO.

We define an ASQ region as a minimum of two Autonomous Systems where there is a bi-lateral contract (on terms similar to above) between each interconnecting Autonomous System and where there is an end to end prioritisation of Diffserv Expedited forwarding traffic.

8.3.2.3 Supply chain for VACS and ASQ Services

Figure 8-12 shows the supply chain. There are three stakeholders supplying the end user. The 5G-WAN provider is selling the ASQ service (Assured Service Quality Interconnection) at wholesale level to the DC provider. The DC provider is selling the VACS (value added connectivity service) to the applications provider. The Appco is selling a value added service retail service to the end user.

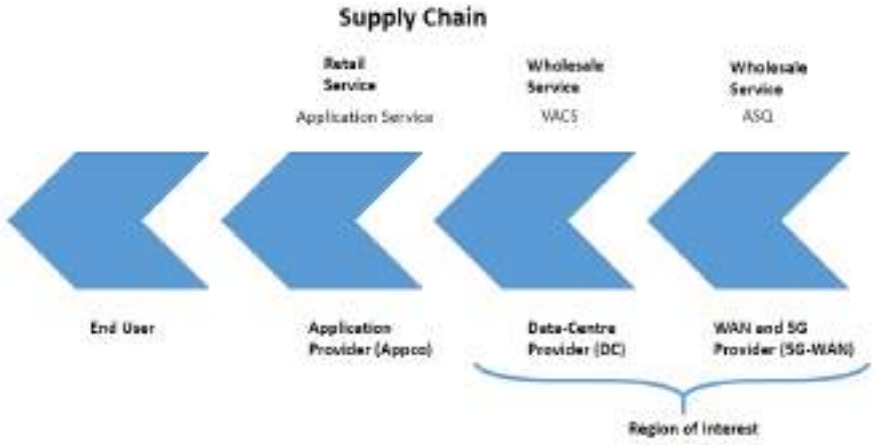


Figure 8-12: Supply Chain

Service Category	ASQ Wholesale Service	VACS Wholesale Service
Reachability	Between any two AS in the ASQ region	
Invocation Rights	Can be invoked by any member of the ASQ region or wholesale customer of any ASQ member	Can be invoked by any member of the ASQ region
Service Description	Multi AS, expedited forwarding service with sustainable bit rate guarantee.	
Traffic Class	DiffServ EF	
Direction	Uni Directional	
SLA	Bandwidth – as specified in service definition Loss not specified Delay not specified (expected same as bees effort)	
Charing Model	Sender pays. (e.g., 30% premium over best effort)	
Service Library	ASQ-1 (1mbps sustainable bit rate) ASQ-10 (10mbps sustainable bit rate) ASQ-50 (50mbps sustainable bit rate)	

	Etc	
End Points	Origin End Point: • any IP host • or gateway to a region. Destination End point: • any IP or host • or gateway to a region	Origin End Point: • any IP host Destination End point: • any IP host • any 4G/5G radio bearer
Relevant 5G interface	Interface 1	Interface 2

Figure 8-13: ASQ and VACS services in detail

8.3.2.4 Example of the data plane and control plane

The data plane consists of the classical Layer 3 controlled by BGP and the Global Internet Routing table in an IP wide area wireline configuration with Layer 3 and EPC providing access to the customer. Figure 8-14 shows the associated topology. The control plane consists of BGP plus the 5G exchange.

Note that the Point of DC Interconnect, (i.e., PoDI) is the ingress edge switch located in the data centre.

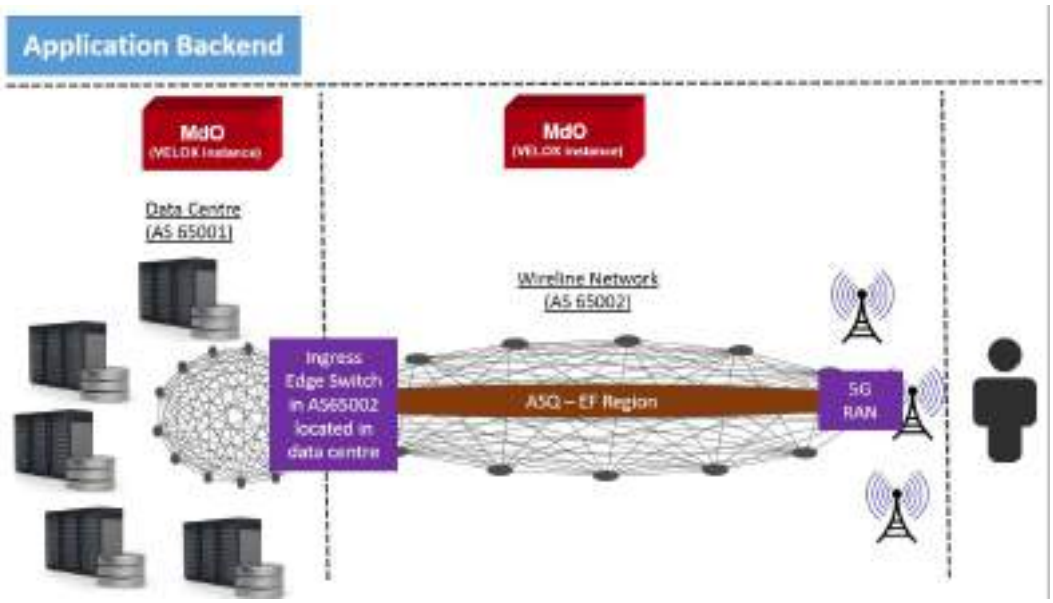


Figure 8-14: Topology

8.3.2.5 Sequence Charts

Figure 8-15 show the sequence associated with establishing the bilateral contract for the ASQ. The owner of ASN65001 proposes a contract with ASN65002.

Figure 8-16 shows the contracting and publishing of the ASQ and VACS contracts. By publishing we mean that the provider exposes and sends to a counterparty the services in the catalogue which are available. Once a framework contract exists for these services then the counterparty may select them and subsequently invoke them for usage. By select we mean

that the counterparty incorporates the published data into their software backend.

Figure 8-17 shows the invocation sequence.

Note: In the sequence charts a solid line means an initiating/requesting action and a dotted line means a returning action.

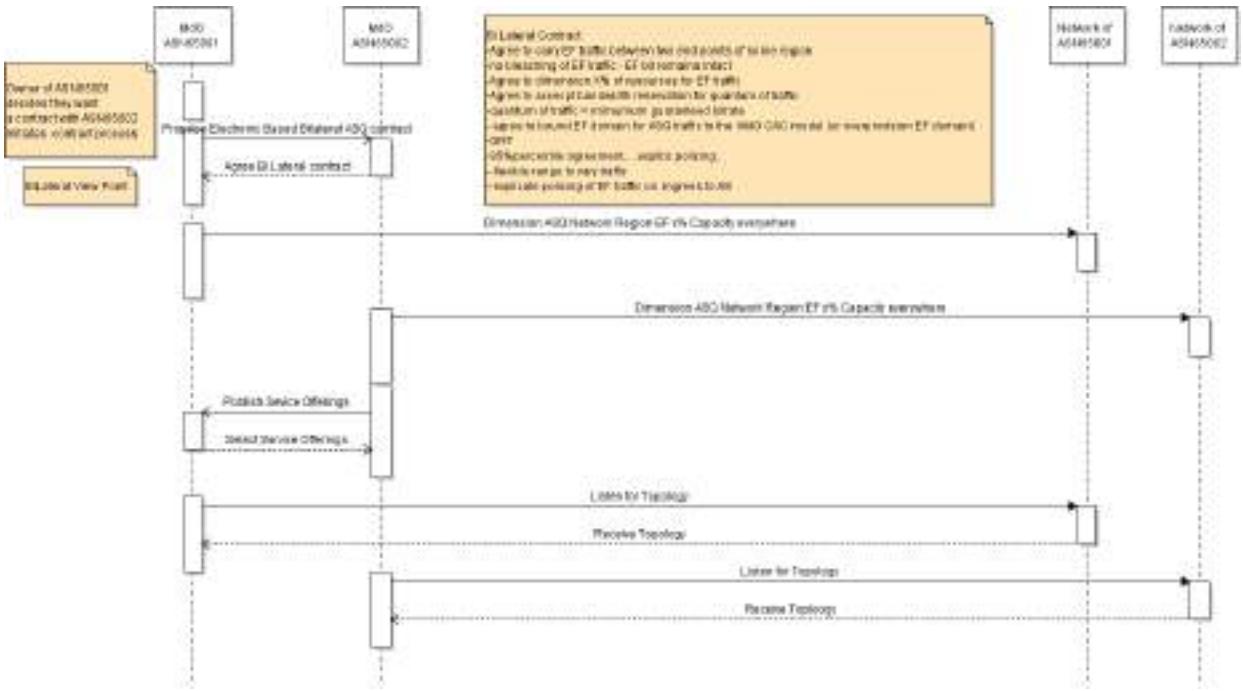


Figure 8-15: Sequence Associated with Bilateral Contract

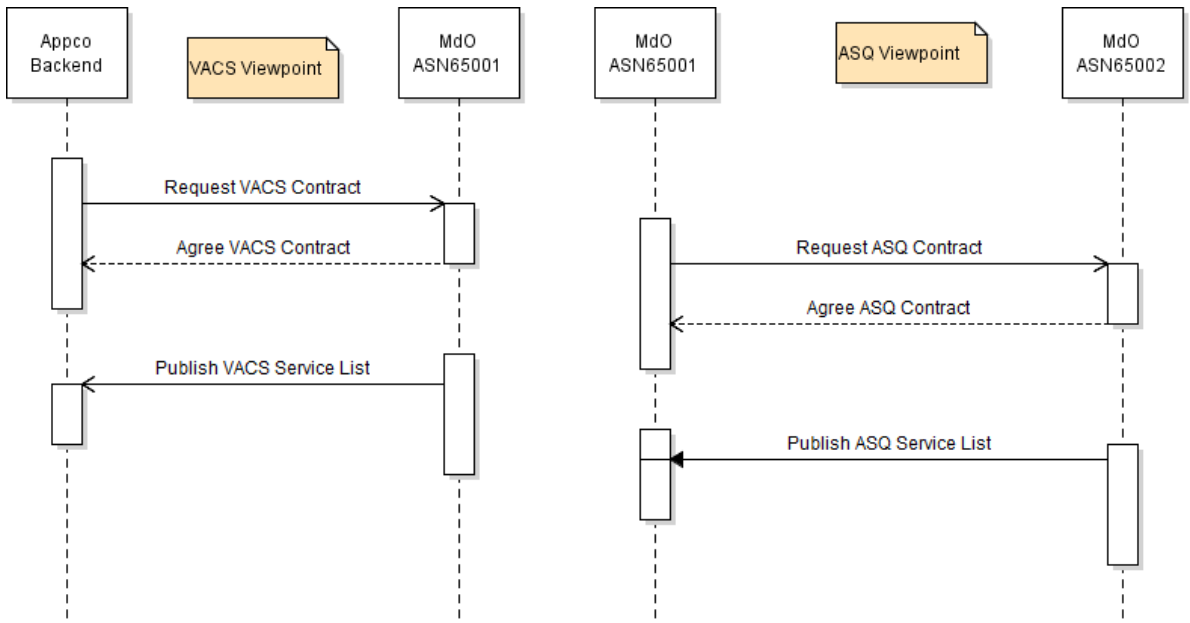


Figure 8-16: Contracting and Publishing

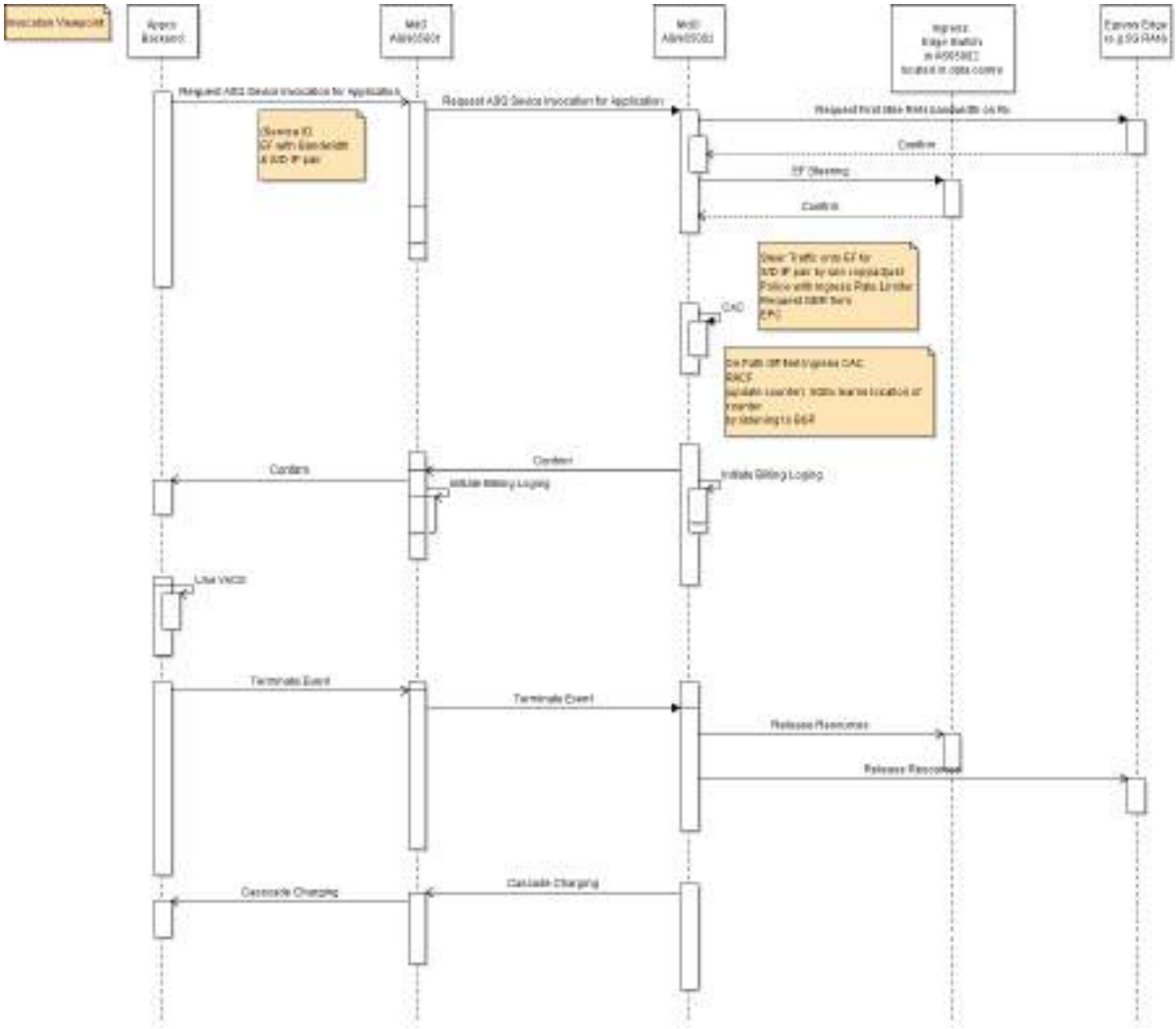


Figure 8-17: Invocation

8.3.2.6 Invocation Walkthrough

The table below summarised the steps and these are described in further detail below. Our intention is to build QoS path along the same forwarding path (so as to use the global routing table of the internet). To do this we invoke the VACs at interface 1 of the MDO and invoke the ASQ at interface 2 of the MDO. The result is the red line as a virtual path slice in parallel to the best effort forwarding (in green) are as shown in Figure 8-18.

Step 1	Simple ASA Bilateral put in Place	VACS	ASQ
Step 2	Publish Defined Service -VACS at interface 1 and ASQ at interface 2 Select and Contract for Service This is from the 5G-WAN to the DC and also from the DC to the Appco. Publishing is necessary so that the customer knows what services are on offer. Contracting is necessary in order that the	Yes	Yes

	customer will pay for consumed services. This is relevant for both relationships (i) Appco to DC and (ii) 5G-WAN to DC		
Step 3	Acquire Topology It is necessary to acquire the topology so that the CAC function can be implanted along the path.	No	Yes
Step 4	Invocation We invoke the service by providing the Service ID and colour (EF) with Bandwidth & S/D IP pair. Request GBR from EPC Egress Resource - request if User on 5G RAN (or other Resource constrained access network)	Yes	Yes
Step 5	Steering Traffic steering is where we steer the traffic from a BE queue into an EF queue. To reduce OPEX and processing overhead and IT complexity we are not steering by path or network element we use the existing global routing table.	No	Yes
Step 6	Connection Admission control – Resource Admission control Function We implement the CAC using the CAC counters described in Figure 8-11. Note these CAC functions are not implemented in the data plane, but are implemented off net above the control plane. The quality path is now available as is shown in Figure 8-18.	No	Yes
Step 7	Cascade Charging Cascade charging can occur from (1) 5G-WAN Charges DC and (2) DC Charges Appco. Both charges are contractually separated. The two levels of charging have some nice properties on how they complement each other.	Yes	Yes

Table 9 Table of steps related to 5GEx architecture

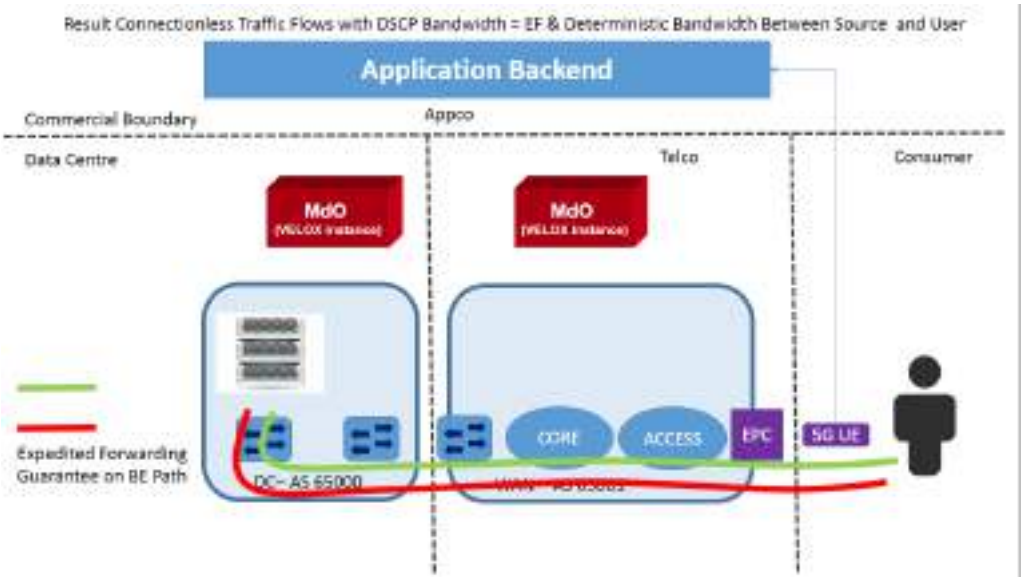


Figure 8-18: Integrated VACS and ASQ

8.3.3 VACS sessions steered over ASQ paths

This section illustrates how the MdO functional architecture is used to set up a Value Added Connectivity Service (VACS) API that allows steering Value Added Connectivity Service sessions over Assured Quality Service Paths between a Data Centre and one or more (residential) regions. The VACS API and the ASQ paths represent two different service types:

1. ASQ paths are provided by WAN operators (or NSPs) to e.g., DC operators. The setup of an ASQ path is initiated by the DC operator.
2. VACS API is provided by a DC operator to an Application provider. In this example, the VACS API setup is initiated by an Application provider between its application and a (set of) given region(s).

An example data and control plane implementation of an ASQ path and the VACS sessions are shown in Figure 8-19.

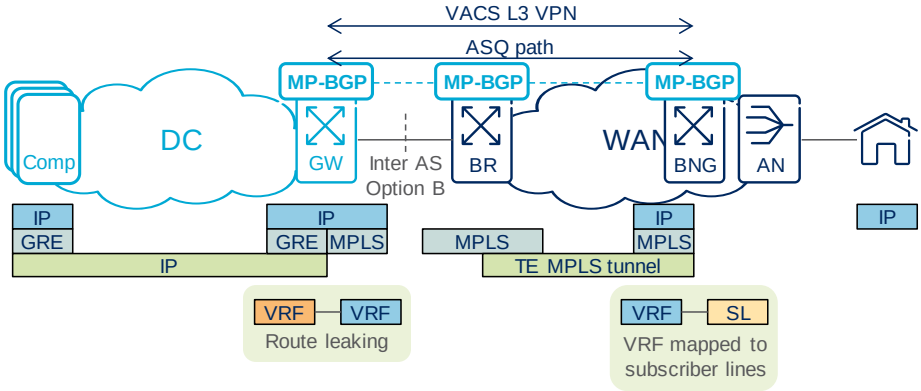


Figure 8-19: Example data and control plane of VACS sessions steered over ASQ paths

The ASQ path is set up between the DC Gateway and a WAN network internal Service Edge node, which in the example is a BNG. The ASQ path is implemented by two stitched path segments: the ENNI link and the WAN network internal (MPLS) TE tunnel. The stitching is implemented in the Border Router (BR) node by MPLS label switching on the VPN label of an IP/MPLS L3 VPN. Label switching on the VPN label is configured by MP-BGP as standard L3 VPN Inter AS Option B. VPN label switching hides the IP reachability details of the WAN end of the ASQ path, i.e., all data and control plane connections between the DC and the WAN go via the BR(s).

Steering of VACS sessions are implemented in the two end nodes of the ASQ path: in the DC-GW and in the BNG. In the upstream direction, the BNG maps subscribers with VACS sessions to the VACS VRF that routes IP traffic to the appropriate ASQ path or to the Internet. In the downstream direction, the DC GW leaks required destination IP addresses to the Application providers' VPNs (VRFs) and routes them via the VACS L3 VPN.

MP-BGP is needed to distribute route reachability within the VACS L3 VPN. For upstream direction, the DC-GW needs to advertise MPLS VPN labels for public IP address ranges of the Application providers. For the downstream direction, the BNG needs to advertise the IP address ranges of subscriber lines involved in a VACS session.

An ASQ path is initiated by the OSS/BSS system of the DC operator in the format of a Network Service provided by the DC NFVO, as illustrated by Figure 8-20. The NS consists of two parts: 1) the ASQ path request with QoS attributes and 2) the steering functionality requested on the ASQ path termination points, represented by NF_1 and NF_2. The DC NFVO decomposes the Network Service to a DC internal Network Service and a Network Service requested from the WAN network. In order to do so, the DC NFVO reads the WAN Service Catalogue to see inter AS options supported and the data plane steering functions available. The DC NFVO also check AS PATH from BGP-RR to ensure loop operation and asks MD-PCE to estimate WAN part of QoS. Then, the DC NFVO selects the handoff point(s) to the WAN and the L3 VPN inter AS option. The handoff point(s) are given as reference points on the inter AS topology and inter AS option functionality is requested e.g., in the form of a NF_3. If the NS setup returns successfully, the DC OSS/BSS may initiate on-boarding a VACS API service for the specific ASQ path into its Service Catalogue.

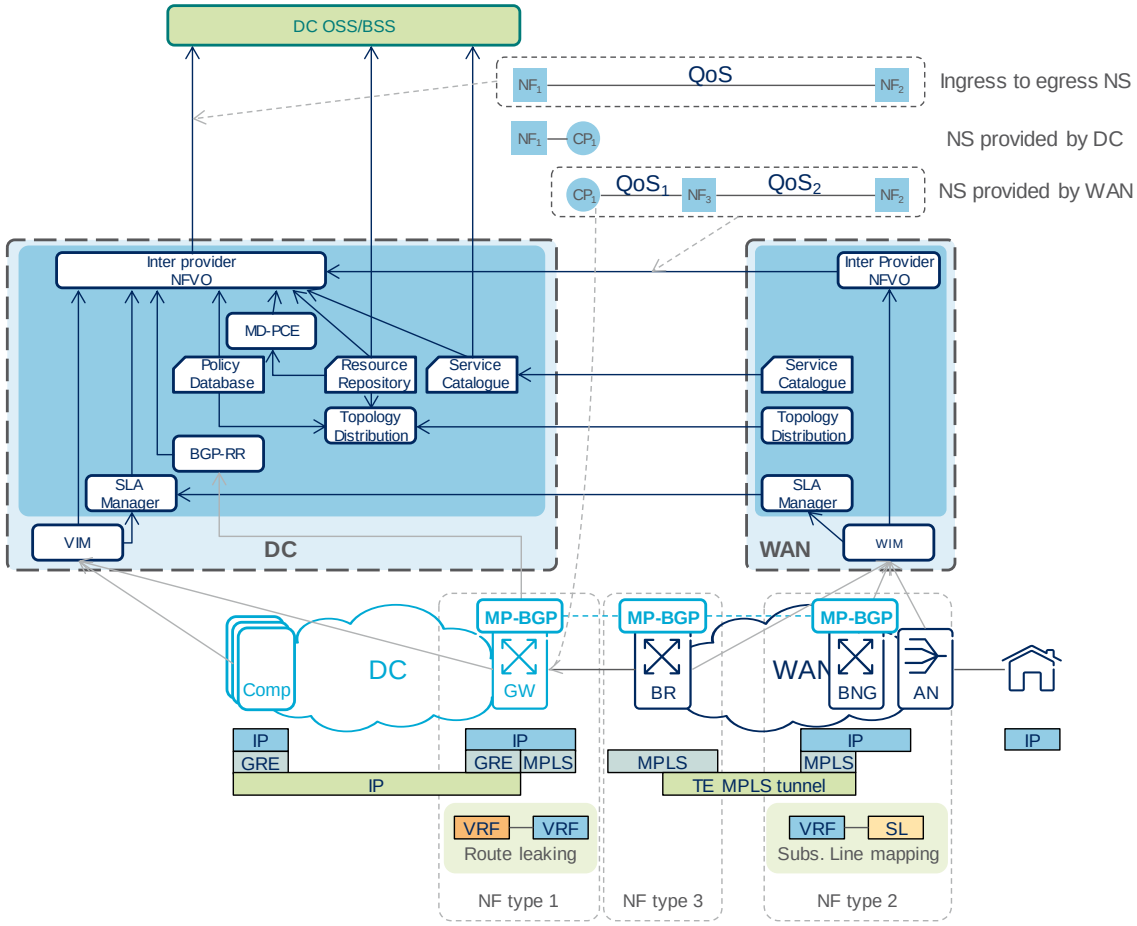


Figure 8-20: Deployment scenario and example NSDs for ASQ path setup

The VACS API allows an application provider to request a given QoS between its application and one or more regions. The VACS API supports specifying the targeted regions, e.g., as a set of public IP address prefixes, and a reference to an existing ASQ path or a target QoS.

There are two implementation options to provide a VACS API to an application provider:

1. VACS API may be provided by an NFV that is provisioned as part of VACS Network Service (See Figure 8-21).
2. VACS API may be provided by the DC NFVO as part of the Network Service's VNF-FG (See Figure 8-22).

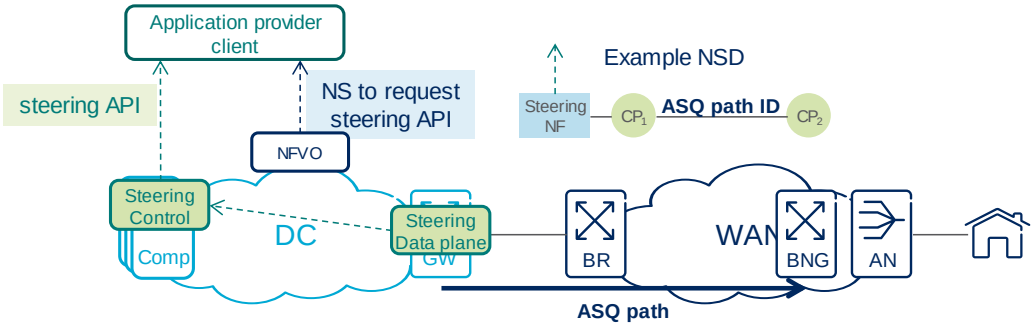


Figure 8-21: VACS API NSD to request (downstream direction) steering API implemented in a VNF

In the VACS API implementation in Figure 8-22, the DC NFVO provides a Network Service that consists of a steering control network function and a reference to an ASQ path. By invoking the Network Service, a new steering service specific API is opened to the application provider. The new API may be accessed via a public IP address or it may be accessed by a VPN if VPN access is requested as part of the Network Service. The steering control network function provided by the DC operator allows the DC operator to oversee the control given to the application provider.

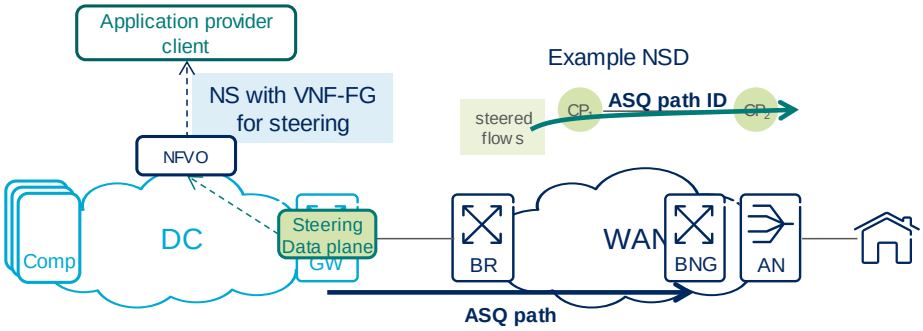


Figure 8-22: VACS API NSD with VNF-FG that implements (downstream direction) steering API

In the VACS API implementation in Figure 8-23, the DC NFVO allows the application provider to request steering of IP addresses by using the VNF-FG part of the Network Service. In this case, it is the role of the NFVO to ask the VIM/WIM to configure the steering data plane accordingly.

The pros and cons of the above options are left for further study. In addition, the following list summarises the currently known aspects:

- VNF based implementation may be scaled up/down and in/out on-demand.
- VNF based implementation allows separating resources used for particular a VNFs and MdO.
- VNF based implementation allows introducing new, non-ETSI compliant functionality, e.g., CAC.
- Integrated approach may suit network providers without an NFVI capable infrastructure.

Figure 8-23 shows the deployment scenario for VACS sessions steered over ASQ paths including both VACS API implementation options. Note that the same two options exist also for the VACS API provided by the WAN network to the DC. The NSD is created by using the same principles as show above, i.e., the NSD contains a reference to an ASQ path and either it requests a steering VNF or the VNF-FG of the NSD communicates steering requests.

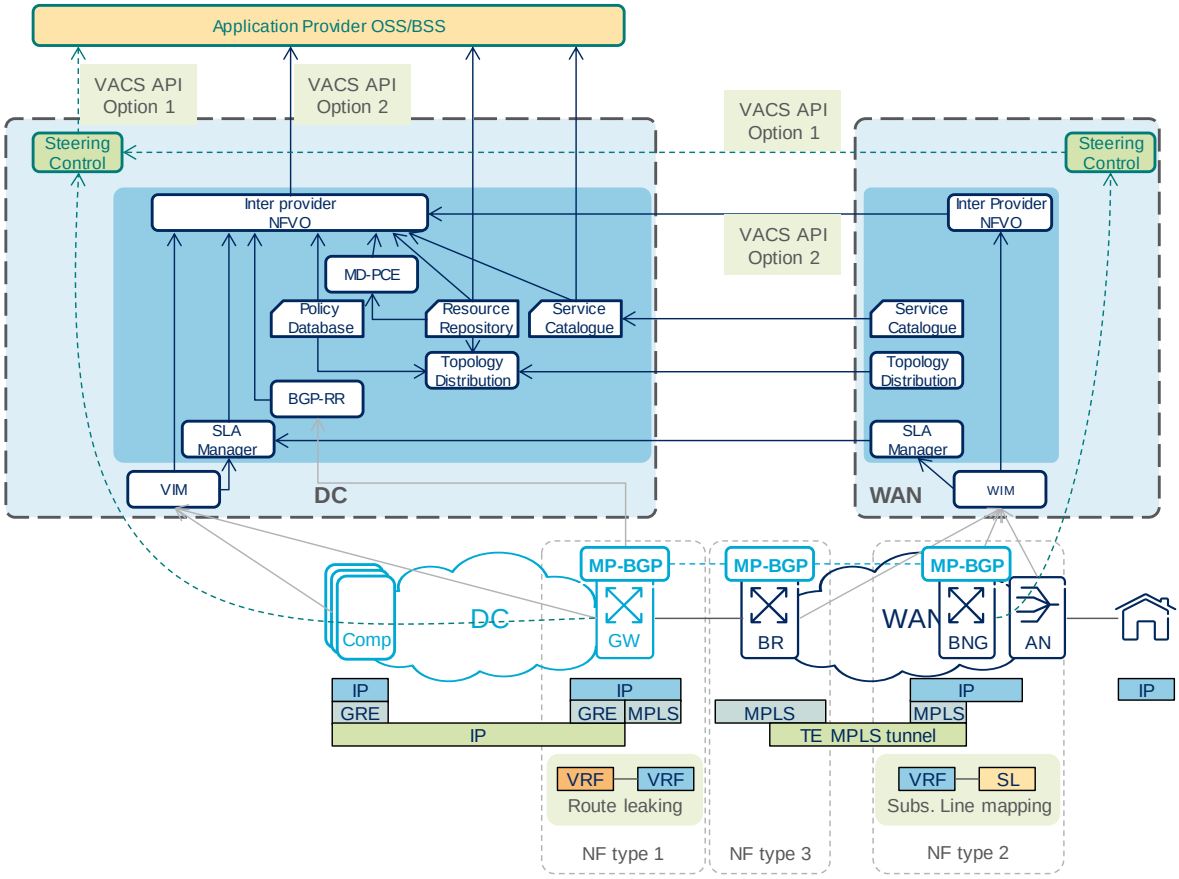


Figure 8-23: VACS API implementation options in the deployment scenario

A similar structure is followed also for VMs, DB instances and cloud resources [63], [64], [65].

9 Business Cases and Business Modelling

9.1 Introduction

5GEx is intrinsically a multi-provider environment where goods are offered and traded between the distinct stakeholders on benefit of the final customers making use of the exchange.

This section provides an overview of initial business cases of interest for 5GEx and its stakeholders, and for 5G in general. The presentation of the business cases is complemented with overviewing the related business model aspects for completeness reasons, providing insight to value proposition, value network and financial configuration aspects. The methodology used for this relies on having a business case and business modelling template, which is used in order to have a structured presentation of the respective issues across the different business cases. This template used, presented in Section 9.2, has been adapted with small customisations and simplifications from other projects where it has been successfully applied, such as ETICS [3] (with a similar multi-provider problem space), where it was originally introduced, and SmartenIT.

The business cases selected for the presentation in this section are of high market value and attract the interest of both 5GEx partners and 5G stakeholders in general. In order to keep the length of the presentation tractable, only a subset of business cases are presented in this deliverable, covering all the use case families of the project. The shortlist of business cases presented have been motivated by the partners' interests and analysis, as well as the ecosystem overview activity carried out in the project. Moreover, it is consistent with the findings of the 5GEx research and market analysis, as well as with the 5G PPP whitepapers[16] targeting verticals.

In particular, for the Connectivity use case family, we present the SD-WAN business case in subsection 9.3.1. This is a connectivity value proposition suitable for 5G that can be seen both as a potential 5GEx proposition and as a competing product. Note that the business case selection of this section builds *incrementally* on top of the previous sections, avoiding the repetition of material that has already been presented earlier. This is why business cases related to the Connectivity use case family do not contain those elaborated in Section 7 of this deliverable. Instead, we present a broader ecosystem business case that is also of interest to 5GEx, so as to also depict the generality of our

[16] https://5g-ppp.eu/white-papers/

business modelling approach and its fitness to accommodate both internal to the project and external ecosystem business cases.

The Virtual Network Function as a Service (VNFaaS) use case family is covered by the "Multi-operator IPTV services in 5G networks" business case, presented in subsection 9.3.2, which encompasses features of the project's vCDN use case (UC-7) and is associated with the Media and Entertainment vertical sector identified by 5G PPP [71]. Additionally, we also present the "VNFaaS as managed service" in subsection 9.3.6.

The Slice as a Service (SlaaS) use case family is also covered in this Section with a representative business case, namely Gi-LAN/Roaming, presented in subsection 9.3.3. This is the most demanding use case family and the business case selected is a use case of the project (UC-9) that has a clear value proposition of high market value. Since this is the most challenging and innovative use case family, we also provide two additional business cases that complement each other: the more generic "Mobile Edge Computing through SlaaS" targeting the wholesale providers' market and the "Smart Car – Balancing Robot" depicting a concrete business case of SlaaS for the Factories of the Future [72], and the Automotive Vertical [73] sectors.

Furthermore, we apply the business model template to the "5GEx Business to Interface model and a medical video application example service" business case, which is used to describe a 5GEx model and value proposition and how this could be exploited in the e-Health vertical sector [74], which is also of high importance to 5G PPP. This is also an additional proof of how generic the business model template used is and how convenient it is to describe business cases that are either ecosystem offerings competing to 5GEx, internal to 5GEx like this one, across the various use case families and targeting different vertical sectors.

Finally, the Conclusions part of this Section depicts the dependencies of the business cases presented and provides insight to further work regarding the business cases presentation and analysis.

9.2 Template

We present below a business modelling (BM) framework, as a suggested methodology, for specifying the appropriate values for the key business model parameters so as to provide insight to the way business is conducted.

Table 10. Template for business modelling

Model parameters	Value
Value proposition	
Product/Service Delivered	Basic product or service provided and delivered from one stakeholder to another in the 5G Exchange.
Target Customer	Basic customers of the basic product or service described above.
Customer Value	The conceived value derived by the customers with regard to the service or product delivered.
Resources and Competencies	The set of resources and competencies of all stakeholders involved in the provisioning and delivery of the product or service, so as to deliver it to its customers.
Value Network	
Vertical Integration	Considering infrastructure layer lies as the bottom, while service layer as the top, inter-layer integrated activity by stakeholders providing and delivering the product or service.
Customer Ownership and Relationship	Provider/operator-to-customer relationship as direct or indirect (intermediated), depending on the existence of other stakeholders as intermediaries.
Interconnection Modality-Business Agreements	Inter-connection and inter-operation agreements in place, mainly among stakeholders with similar roles. E.g., in case of NSP interconnection, transit or peering agreement.
Service Delivery Model	Inter-operation agreements in place, mainly among stakeholder performing different roles. E.g., in case of content delivery, client-server model, P2P model, CDN model.
Financial Configuration	
Revenue model, revenue sharing & money flows	Model describing the revenue and money flows among involved stakeholder in the product or service delivery and also customers.
Cost Model	Charging models applicable among stakeholders providing/delivering the product or service, as well as towards the customer.

9.3 Business cases overview and modeling

9.3.1 SD-WAN

The BM is here applied to a connectivity product that seems relevant and potentially competing to the 5GEx portfolio.

Table 11. SD-WAN business model

Value proposition	
Product/Service Delivered	Talari Networks' Software-defined WAN (SD-WAN) http://www.talari.com/solutions/sd-wan/
Target Customer	Enterprises with extended geographical footprint interested in inter-connecting remote branch offices and sites with guaranteed network services.
Customer Value	Prioritisation of critical applications; best quality path; high uptime; adaptation to bandwidth demand and actual network conditions.
Resources and Competencies	Built as an overlay solution employing both physical and virtual appliances that perform network controlling and WAN bandwidth aggregation on top of existing MPLS, Internet WAN, LTE or satellite links offered by NSPs.
Value Network	
Vertical Integration	No vertical integration is identified. Talari SD-WAN is built as an overlay solution on top of existing, NSP-provided MPLS, Internet WAN, LTE or satellite links.
Customer Ownership and Relationship	End-user, namely the Enterprise Customer, interacts with Talari Aware, a centralised management software that allows configuration, monitoring, analysing a Talari SD-WAN.
Interconnection Modality-Business Agreements	End-user, namely the Enterprise Customer, has contracts with NSP(s) providing him the MPLS, Internet WAN, LTE or satellite links. Moreover, he also has a contract with Talari Networks that provides, installs, deploys and maintains the physical and virtual equipment that supports the SD-WAN solution.
Content-Data Delivery Model	Not applicable.
Financial Configuration	
Revenue model, revenue sharing &	End-user compensates NSP(s) for MPLS, Internet WAN, LTE or satellite links by traditional charging schemes.

money flows	Moreover, end-user compensates Talari Networks for physical and virtual appliances, and management software. 
Cost Model	NSP(s) links: Traditional charging scheme employed by NSP to charge for MPLS, xDSL, cable or Metro Ethernet. Talari Networks' physical & virtual appliances and Talari Aware, Talari Networks' central management tool: Customers are free to choose either a CAPEX-centric traditional perpetual license or subscription model that enables them to implement an OPEX-based SD-WAN acquisition model that distributes costs over time. In specifically, a bundled rate includes product, maintenance and support, flexible billing and a pay-as-you-grow approach that allows customers to add products to their subscription at any time.

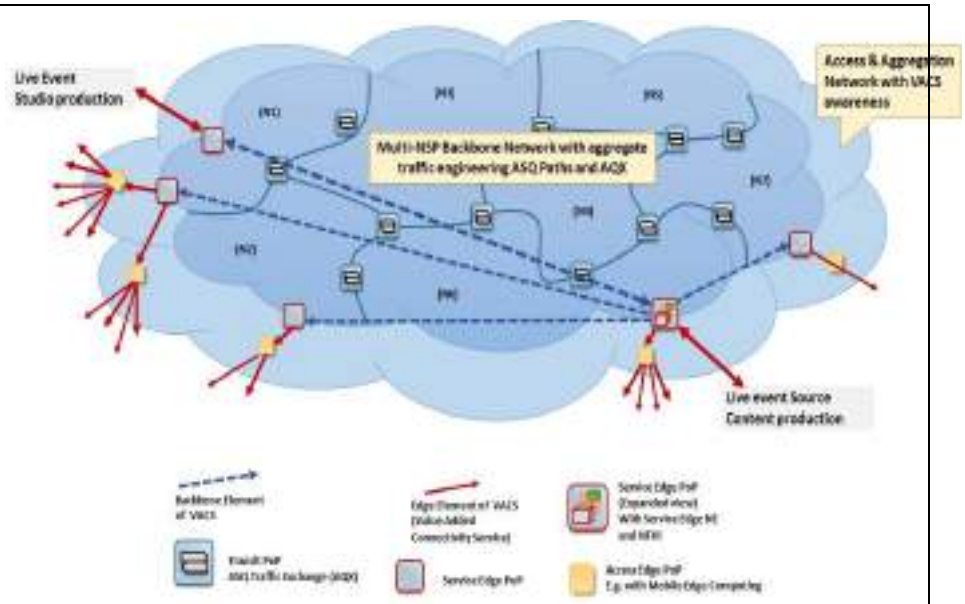
9.3.2 Multi-operator IPTV services in 5G networks

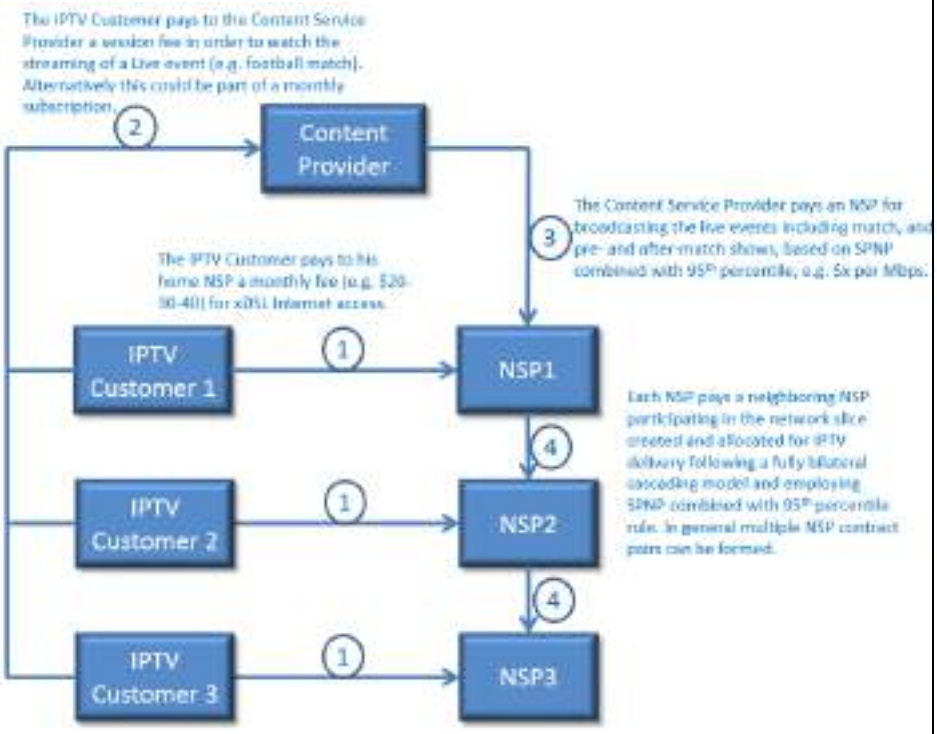
In this section, we apply the BM framework to analyse the multi-operator IPTV services in 5G networks case, as introduced in [75].

Table 12. Multi-operator IPTV business model

Value proposition	
Product/Service Delivered	The service is multi-operator IPTV services, including the broadcast of live events, over 5G networks. For instance, consider the following example scenario: the Norwegian football team plays against Hungary in Budapest. In addition to the Norwegian broadcaster (NRK) there are several national, regional and local media teams that would like to produce live event content following up on pre-match, during the match and after the match happenings, advanced real-time statistics and interviews suitable to local interests. In such a scenario, the content an actual user sees could be the result of distributed content production (on-site video feed and commentary, NRK studio and local studios). Adding to this, some Norwegian viewers/subscribers will be in the area of the live-event (possibly using a roaming mobile broadband connection), some in different regions of Norway,

	and some all over Europe (e.g., in the coast of Spain), necessitating a truly multi-operator effort for service delivery.
Target Customer	The multi-operator IPTV service targets the retail market but requires multi-operator coordination in the wholesale market so that it can be materialised. Regarding the retail market, it addresses mainly residential end-users and SMEs, as well as larger enterprises in fewer cases, interested in entertainment services stand-alone or bundled with other networking services, e.g. broadband Internet access.
Customer Value	High-end/premium quality content, possibly real-time, delivered with adequate/high/guaranteed video quality and networking performance in specific time.
Resources and Competencies	The IPTV service is delivered by means of service-aware slices exploiting SDN/NFV principles over computing facilities across operator's networks. Using virtualisation, programmability, and slicing capabilities, there becomes possible to deploy delivery nodes across visited networks for facilitating the local delivery of content. Such video delivery nodes can come in the form of VNFs instantiated on top of computing elements (commonly x86 servers constituted in the form of Network Function Virtualisation Infrastructure Points of Presence or NFVI-PoPs) with a virtualisation layer (hypervisors, software containers) executing the delivery function as by the traditional specialised equipment. The Content Service Provider communicates its needs to the NSP from where the service is purchased. The NSP focuses on slice management and slice scaling up/down (acquiring resources and/or VNFs) from adjacent NSP(s).
Value Network	
Vertical Integration	Lower-level resources are the low-margin commodity building blocks of differentiated higher-level services. Virtual resources and NFs are composed into slices under the Network Function Virtualisation Infrastructure as a Service (NFVIaaS) paradigm; slices make up infrastructure services, by the concept of Slice-as-a-Service (SlaaS); finally, infrastructure services enable VNFs for the support of IPTV. Multi-operator IPTV services by definition imply that full vertical integration is not feasible; however it is possible that the roles of transit and (a portion of) edge NSP is played out by the same actor; also some NSPs may offer vCache functionality as a bundled product.

Customer Ownership and Relationship	 Each IPTV customer interacts directly with the Content Service Provider portal for the service. Depending on the customer's location, an edge NSP who is member of the multi-operator consortium is supporting the connection of the end user to the multi-operator IPTV service, as part of a multi-operator slice purchased and managed by the Content Service Provider. In any case, the IPTV customer interacts solely with the Content Service Provider, while the NSPs involved in the IPTV service delivery are indifferent to him.
Interconnection Modality-Business Agreements	Multi-operator IPTV service allows and supports a variety of specific inter-connection deployments and coordination models prescribed by 5GEx, including: i) "direct peering" among NSPs at an already established local or remote IXP, ii) distributed multi-party collaboration, where the operators host the exchange mechanism in a distributed manner inside their own infrastructure, and iii) a dedicated Exchange Point Provider as a standalone entity, offering exchange point services.
Content-Data Delivery Model	At least one NSP in the multi-operator consortium needs to establish an agreement with a Content Service Provider, while also the case of multiple NSPs establishing agreements for content with different Content Service Providers and effusing the content into a multi-operator pool of content. Each IPTV customer is considered to have a contract directly with the NSP offering him main access to the multi-operator IPTV service, e.g. fixed broadband service, and a contract directly with the Content Service Provider that feeds the content that the customer is interested in.

Financial Configuration	
Revenue model, revenue sharing & money flows	Pricing and charging schemes are control mechanisms that operate on the two main layers, namely wholesale and retail. The IPTV session would be initiated by a customer having a certain willingness to pay. A clearing function would then receive the payment by the 5G IPTV session initiator and re-apportion the associated revenues to the involved NSPs for the quality provided. The way revenue is apportioned and used to finance underlying network infrastructure services is crucial for monetizing the required Assured Service Quality infrastructure needed for 5G IPTV and similar services. In particular, we foresee the application of SPNP model, based on which the IPTV customer as Session Initiating Party is paying his NSP, and this NSP must then pay the next NSP in a fully bilateral cascading model for the traffic in the opposite direction, thus supporting multiple end-to-end money flows as depicted in the figure below.  Further details on the pricing schemes per layer are detailed in Section 5.
Cost Model	Subscription-based and on-demand charging for content (pre-match, match, interviews, happenings, commenting) are the two prominent charging models envisioned. The service can be charged as it grows in terms of users and geographical areas served. The cost of the needed infrastructure, network, storage, compute and VNF grows along with the session-based subscriptions to the (live) video

	sessions and thus the incurred costs can be recovered from the retail market, thus financing the wholesale 5G(Ex) infrastructure deployment, usage and lifecycle management.

9.3.3 GiLAN/Roaming

Through this section we detail the BM of the instantiation of mobile operator GiLAN capabilities remotely on a different administrative domain.

Table 13. GiLAN business model

Value proposition	
Product/Service Delivered	Roaming extension of GiLAN capabilities (e.g., PGW) by a mobile operator for supporting own customers in roaming in a foreign country.
Target Customer	MNO interested to offer infrastructure and services to their customers using the network infrastructure of another operator
Customer Value	Roaming alliance between operators Local breakout of mobile data traffic reduces transport costs within the IPX Latency can be reduced to improve application performance for CDN and other applications
Resources and Competencies	Resources will be used from 3 parties: the visited network, the home network and any required intermediate provider (of connectivity, content, etc) participant in the 5G exchange point. The following resources will be used: network resources, compute resources, and EPC as a network function (or collection of functions). Additional recources could complement the service (vCDN, vDPI, firewalls, etc) The process as such needs a pre-established roaming agreement between the parties.
Value Network	
Vertical Integration	Two basic resources are needed: compute services (CPUs and memory) and network services (bandwidth and routes). In addition a complex resource, the EPC, is needed. This will use an existing EPC service and subscribe higher-level services. As a second step, slices are needed, which use the resources of the respective services

	The trigger is a certain number of roaming customers present in the guest network. This number will be determined by a monitoring function inside the network.
Customer Ownership and Relationship	The end user interacts with the *home network operator* (MNO 1) based on the customer contract between the customer and the home network operator. The MNO 1 interacts with the visited network operator (MNO 2) who offers the resources inside his network via the use of a third party NSP.
Interconnection Modality-Business Agreements	The contractual relationships are: MNO 1 ↔ end customer (unchanged) MNO 1 ↔ MNO 2 MNO 1 ↔ third party NSP (if continuity of the connectivity between MNO1 and MNO2 is needed)
Service Delivery Model	Roaming agreements need to be in place. Each participating MNO receives a slice in another network and is given full control over the resources limited by the slice only. The configuration of the slice is done by means of a control interface that is returned as a result of slice booking.
Financial Configuration	
Revenue model, revenue sharing & money flows	There are three options: MNO 1 buys all services described above from MNO 2 and MNO n. The second is that there is an alliance between MNOs that mutually grant access to data and network resources to each other. The third option is a third party, commissioned by the MNOs, that acts as an exchange provider.
Cost Model	Various options are possible: - Charging per individual IMSI - Charging per traffic volume (compute and resources) - Charging according to cloud service model

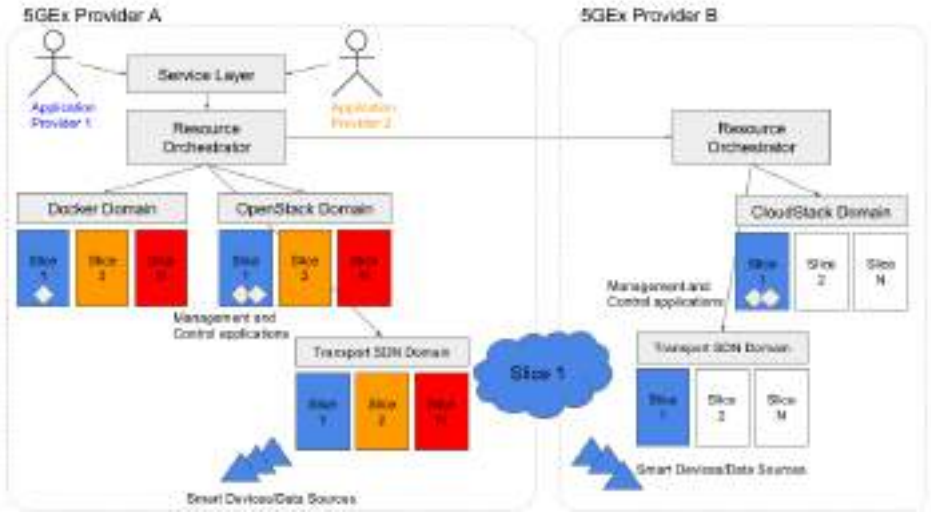
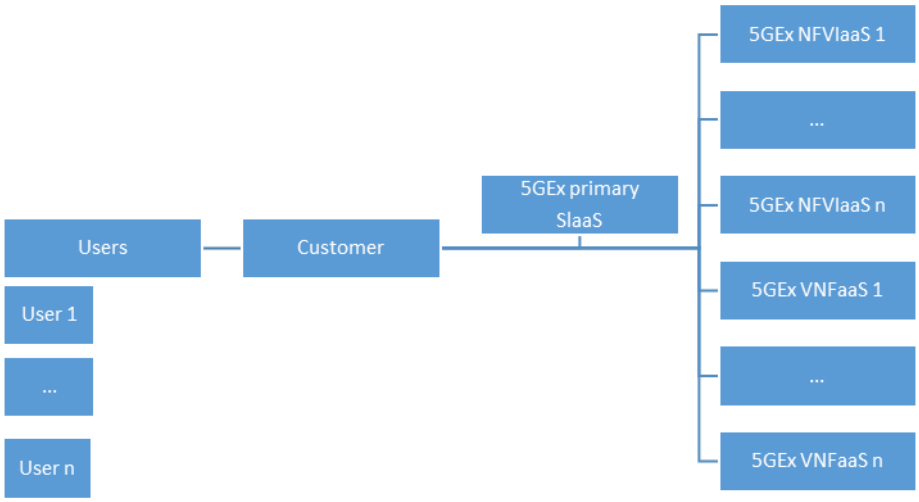
9.3.4 Mobile Edge Computing through SlaaS

This sections elaborates on the BM of the availability of MEC capabilities leveraging on Slice as a Service offering between 5G Exchange stakeholders.

Table 14. MEC through SlaaS business model

Value proposition	
Product/Service Delivered	Mobile Edge Computing through SlaaS Compute capabilities made available close to the end user for different purposes and applications (data intensive applications, low latency services, etc).
Target Customer	Application providers with potentially very high computational resources demands dealing with unforeseen load peaks. Moreover, considered applications come with geographical constraints due to the need of minimizing delay and network traffic while interacting with data sources and/or devices needed to implement the services. This is accomplished by exploiting computational resources that are located at the edge of the network in order to perform data aggregation and filtering and/or enforcing control/management procedures. Resources are requested to the external providers in the form of slices which are transparently including computational, storage and connectivity. Other target customers can be service providers which by some circumstance require resources in a non-permanent way for occasionally serving some areas or events (big sports or gaming events, commercial campaigns, massive software upgrades, seasonal demands, etc).
Customer Value	The customer may be relieved from the burden of owning/maintaining his own resource infrastructure and can cope with the aforementioned users load peaks without performing resources overprovisioning. One-stop shop for buying communication and computation service for time sensitive management purposes, no matter the geographical coverage offered to its respective customers. Lowest delay between cloud control and migrant devices and/or data sources located in various geographical locations according to services requirements; prioritisation of critical operations; best quality path; high uptime; adaptation to bandwidth demand and actual network conditions.
Resources and Competencies	Deployment of application logic and High Performance Computing infrastructures on scalable computation resources built across several slices and the dynamic migration capability thereof. Network overlay creation and dynamic network control over the physical networks of network operators: WAN on top of existing MPLS, wireless last mile over LTE or WiFi offered by NSPs.

Value Network	
Vertical Integration	The proposed services span the whole spectrum of 5GEx services. Lower-level resources are the low-margin commodity building blocks of differentiated higher-level services: the virtualised computation and network resources are provided as Network Function Virtualisation Infrastructure as a Service (NFVIaaS) paradigm; NFVIaaS's from various domains and/or providers are composed into the concept of Slice-as-a-Service (SlaaS); and finally, application composition services delegated to be managed by the 5GEx operator are onboarded into the slice as instances of Virtual Network Function as a Service (VNFaaS).
Customer Ownership and Relationship	The customer (the application provider) interacts with the primary, customer-facing 5GEx provider. The customer submits the application related requirements, which can include both devices to be managed (with their SAPs), data sources and their geographical constraints as well as the resources required to perform computational intense control/management algorithms. The provider, in turn, offers management that allows configuration, monitoring, analytics.
Interconnection Modality-Business Agreements	The customer has only one contract, which is with the primary 5GEx provider. The primary provider has 5GEx contracts with all the providers that offer the lowest cost NFVIaaS and the best delay communication among the control logic and the managed migrant data sources and devices. Also, contracts with VNFaaS providers might be in place.
Service Delivery Model	The Figure below depicts a possible representation of the aforementioned scenario, where two different Application Providers (Application Provider 1 and Application Provider 2) buy the orchestration of their application from the primary 5GEx provider (Provider A) on the left-hand side of the picture. The figure details the acquisition of resources and service deployment related to the Application Provider 1, as they are realised within a Slice as a Service offering (Slice 1, represented in blue). Provider A fulfils the request with the available local resource and buys NFVIaaS from other 5GEx providers (Provider B in the picture) in order to: • Acquire additional *computing resources* to deploy the application logic and • *Network resources* (e.g. transport SDN domain in the Figure) to both interconnect the customer with the management logic as well as the control logic with the roaming smart devices and data sources.

	The orchestrating primary provider migrates the application logic to the closest (i.e., yielding the lowest delay) computation infrastructure while continuously following the movement of the mobile entities and the data sources producing raw data to be processed or filtered according to the control and management algorithms requested by the service execution. 
Financial Configuration	
Revenue model, revenue sharing & money flows	Its users pay to the customer for the application, the customer pays to the primary 5GEx provider for orchestrating the application in a SlaaS, primary 5GEx provider pays to other 5GEx providers for deploying (NFVIaaS) and managing (VNFaaS) components of the service. 
Cost Model	Usage-based: the service can be charged as it grows in terms of users (managed migrant smart devices and data sources) and geographical areas served. The cost of the needed

	infrastructure, network, storage, compute and VNF grows along with the session-based subscriptions and thus the incurred costs can be recovered from the retail market, thus financing the wholesale 5G(Ex) infrastructure deployment, usage and lifecycle management.

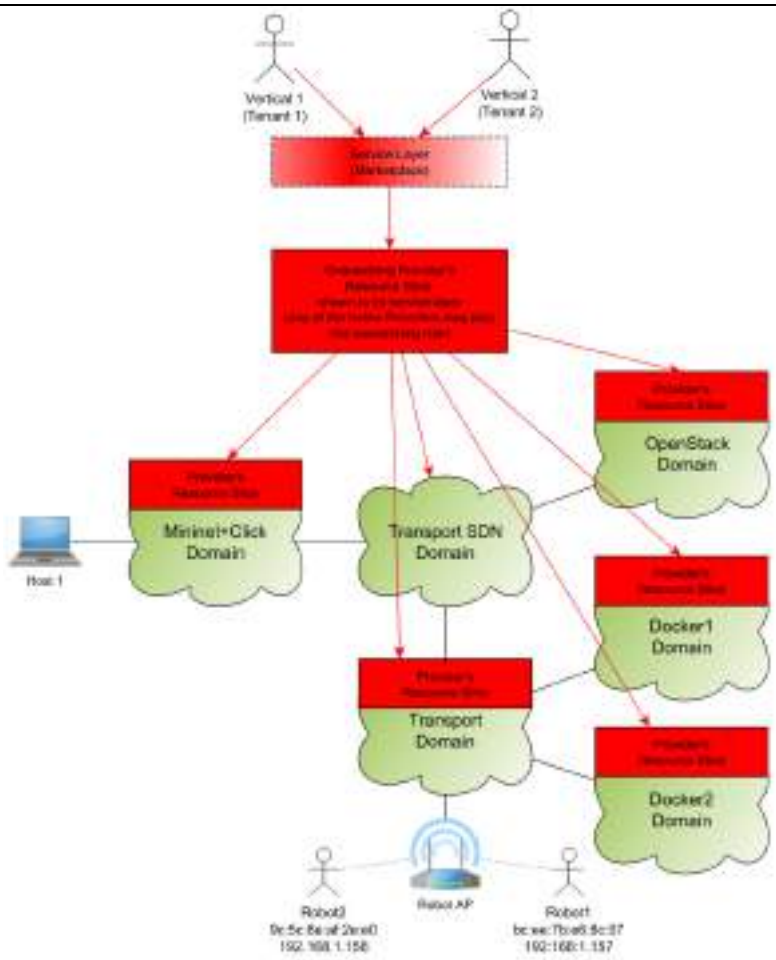
9.3.5 Smart Car – Balancing Robot

This case represents another exemplification of the Slice as a Service use case family. Even with a different technical realisation and purpose, the BM shares commonalties with the previous one for MEC.

Table 15. Smart Car - Balancing Robot business model

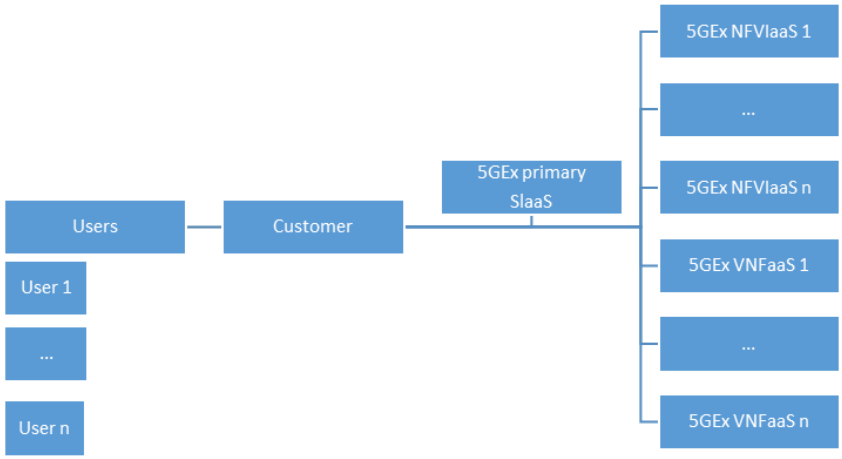
Value proposition	
Product/Service Delivered	Smart Car – Balancing Robot Time sensitive cloud control for migrant smart devices Support for Industry 4.0
Target Customer	Application providers managing and controlling smart mobile devices that roam with an extended geographical footprint and require network services with guaranteed delay.
Customer Value	One-stop shop for buying communication and computation service for the time sensitive management of its device(s), no matter the geographical coverage offered to its respective customers Lowest delay between cloud control and migrant device; prioritisation of critical operations; best quality path; high uptime; adaptation to bandwidth demand and actual network conditions.
Resources and Competencies	Deployment of application logic on computation resources and the dynamic migration capability thereof. Network overlay creation and dynamic network control over the physical networks of network operators: WAN on top of existing MPLS, wireless last mile over LTE or WiFi offered by NSPs.
Value Network	
Vertical Integration	The proposed services span the whole spectrum of 5GEx services. Lower-level resources are the low-margin commodity building blocks of differentiated higher-level services: the virtualised computation and network resources are provided as Network Function Virtualisation Infrastructure as a Service (NFVIaaS) paradigm; NFVIaaS's from various domains and/or providers are composed into the concept of Slice-as-a-Service (SlaaS); and finally,

	application composition services delegated to be managed by the 5GEx operator are onboarded into the slice as instances of Virtual Network Function as a Service (VNFaaS).
Customer Ownership and Relationship	The customer (the application provider) interacts with the primary, customer-facing 5GEx provider. The customer submits the devices to manage (with their SAPs) and the application related requirements, the provider, in turn, offers management that allows configuration, monitoring, analytics.
Interconnection Modality- Business Agreements	The customer has only one contract, that is, with the primary 5GEx provider. The primary provider has 5GEx contracts with all the providers that offer the lowest cost NFVIaaS and the best delay communication among the control logic and the managed migrant smart devices. Also, contracts with VNFaaS providers might be in place.
Service Delivery Model	In the below figure there is a layout of the proof of concept demonstration of the proposed service. Tenants 1 and 2 are application providers that buy the orchestration of their application from the primary 5GEx provider, denoted as Overarching provider. The application is realised within a Slice as a Service offering. The primary provider buys NFVIaaS from other 5GEx providers in order to acquire compute resource to deploy the application logic (e.g. OpenStack domain in the Figure) and network resource (e.g. transport SDN domain in the Figure) to interconnect the customer with the management logic and the control logic with the roaming smart devices. Also, the primary provider buys access from the network provider that has wireless coverage in the region where each device is situated (e.g., transport domain in the Figure). The orchestrating primary provider migrates the application logic to the closest (i.e., yielding the lowest delay) computation infrastructure while continuously following the movement of the devices.



Financial Configuration

Revenue model, revenue sharing & money flows	Its users pay to the customer for the application, the customer pays to the primary 5GEx provider for orchestrating the application in a SlaaS, primary 5GEx provider pays to other 5GEx providers for deploying (NFVIaaS) and managing (VNFaaS) components of the service.



Cost Model	Usage-based: the service can be charged as it grows in terms of users (managed migrant smart devices) and geographical areas served. The cost of the needed infrastructure, network, storage, compute and VNF grows along with the session-based subscriptions and thus the incurred costs can be recovered from the retail market, thus financing the wholesale 5G(Ex) infrastructure deployment, usage and lifecycle management.

9.3.6 VNFaaS as managed service

The following case is of interest for 5GEx when extended a multi-provider environment. It is referred here as one of the first commercial offers in the direction of VNFaaS use case family.

Table 16. VNFaaS as managed service business model

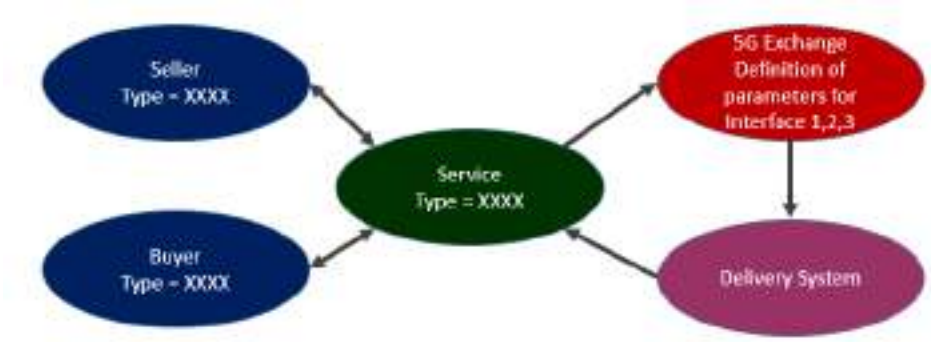
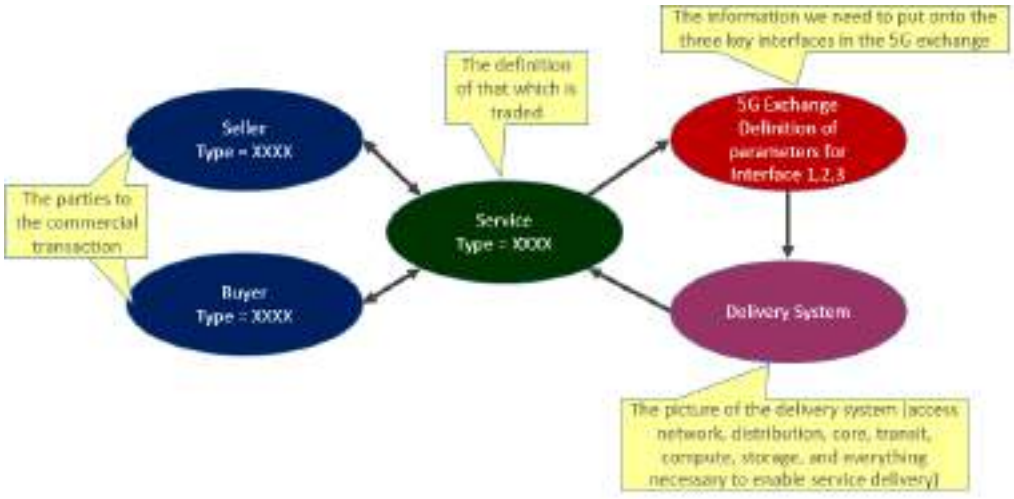
Value proposition	
Product/Service Delivered	**AT&T FlexWare (VNFaaS as managed service)** https://www.business.att.com/enterprise/Family/network-services/virtual-network-functions/#tab1
Target Customer	Enterprises that require from network infrastructure (e.g., DPI, firewall, etc) for running their business.
Customer Value	Usage of the NFV approach to avoid investments on specific appliances and solutions for networking functions.
Resources and Competencies	The customer deploys COTS x86 servers (provided and managed by AT&T). Certified applications (also provided by AT&T from a portal) are installed on top according to the customer's needs. The service is complemented with VPN services if required.
Value Network	
Vertical Integration	The x86 devices are managed in an overlay manner, with applications being provided and deployed by AT&T. The customers services make use of the provided functions as in the case of physical network functions.
Customer Ownership and Relationship	Managed service where the customer deploys AT&T devices and access AT&T portal for deployment of functions or applications. Apart of the deployment on customer premises, it is also possible to consider it in data centers, in network points of presence, including cloud locations, or in a combination of these areas

Interconnection Modality-Business Agreements	AT&T provides x86 devices that are installed in customer premises. AT&T can access and manage those devices, deploying functions as requested by the customers.
Content-Data Delivery Model	The customer access a service portal and request certain functions from a catalog of certified applications.
Financial Configuration	
Revenue model, revenue sharing & money flows	The customer compensates AT&T for: • The AT&T FlexWare x86 devices to be deployed locally at the customer premises • The AT&T FlexWare certified applications deployed on the referred devices • The VPN connectivity if needed • The managed services overarching all the points before
Cost Model	Despite there is no public information, since the FlexWare service is a managed service, it can be deduced that the cost model will be influenced by: • Cost of the devices deployed and managed, including annual support, maintenance and replacement (if needed) • Right of use licenses for the applications being deployed for the customer, including support • Connectivity service, if VPN is needed according to the customer's need.

9.3.7 5GEx Business to Interface model and a medical video application example service

As a complementary approach to the Business Modelling exercise before, in this section we describe a sample reference model for mapping from a generic business use case to data structure on 5G Exchange interfaces I1, I2 and I3. This is later exemplified with an additional business case, a medical video application for eHealth.

Table 17. 5GEx Business to Interface model

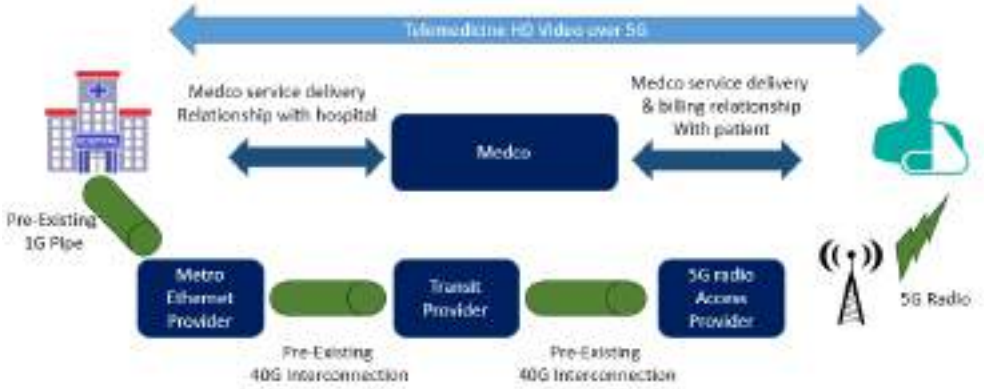
Danube Model	Proposed Danube[17] Model for 5Gex interface & system Definition 
Danube Model Details	The model contains • The parties to the commercial transaction • The definition of that which is traded • The information we need to put onto the three key interfaces in the 5G exchange • The picture of the delivery system (access network, distribution, core, transit, compute, storage, and everything necessary to enable service delivery 
Example	ASQ example with medical video application • ASQ Assured Quality Service (See ETICS) • Medical Application Company (Medco) using Tele-medicine with HD video quality over 5G • Retail service (Medical Telemedicine) out of scope of exchange • Two step wholesale transaction from point of view of 5GEx • MedCo to Transit Provider • TransitProvider to 5GAccessCo

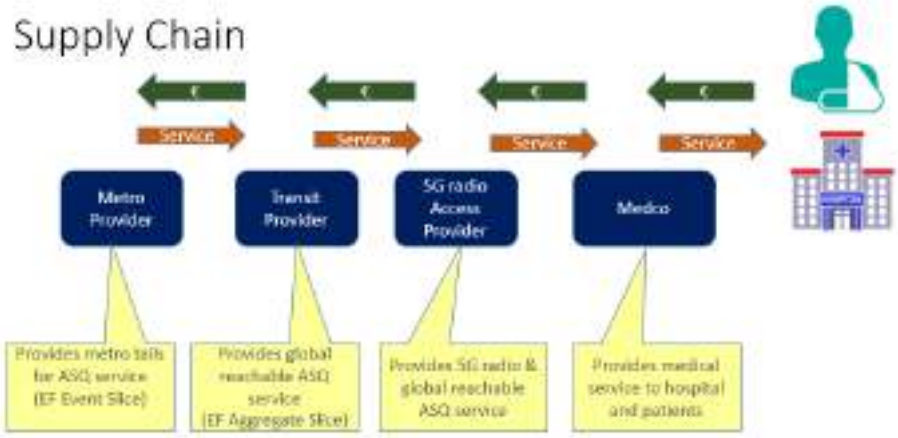
[17] Named in this way in honor to the river beside the 5GEx kickoff meeting

<table>
<tr><td></td><td>


Pre-Conditions assumptions

Hospital has 1G connection of which 33% (peak) is allocated to best effort service
Transit provider has 40G Interconnection to both metro provider and 5G provider of which 25% (peak) is allocated to best effort interconnection.
Telemedicine Application is based on 5Mbps bi-directional video requiring expedited forwarding



</td></tr>
<tr><td>Supply Chain</td><td>


</td></tr>
<tr><td>Analysis</td><td>5GEx Service Relationship:- 5G Telco buys from transit. What goes into interfaces I2 and I3 is for further analysis in the project.</td></tr>
</table>

9.4 Conclusions

While NFV and SDN in general will allow greater flexibility and cost efficiency 5GEx is even more about creating and enabling new value propositions and business cases. The above analysis can be considered as a first iteration of identifying value propositions and business cases that

the 5GEx framework and its solution variants can enable. For each of the covered business cases a business model analysis has been conducted to get insight into the drivers and properties of these business cases. The business model analysis was conducted based on a template that has shown to be very useful in previous European projects.

The business cases cover all layers of resources and services addressed by 5GEx. On one side we recognise the aggregate level connectivity and transport connections and the value added connectivity services and on the other side the NFV infrastructure and datacentre oriented services. From these basic services higher level business cases can be built that are composed using these basic services as resources for higher level services. This is illustrated by Figure 9-1 below.

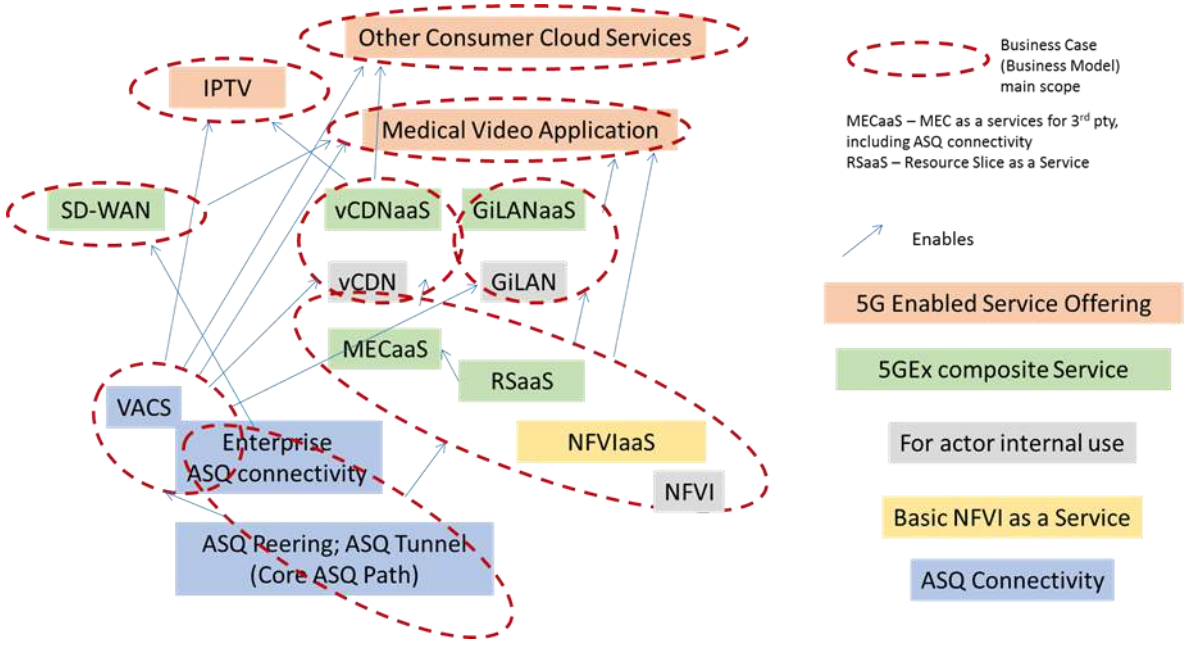


Figure 9-1: Business cases and dependencies

Note that the "Enables" relation may represent different kinds of dependencies, from a strict dependency to optional or more of a support and indirect dependency.

As the 5GEx framework and ways of deploying and using this framework becomes more mature, and experience is gained by the sandbox experiments the business cases and business modelling work can further be extended and detailed. This can for instance be in the area of "Other Consumer Cloud Service" such as the My Cloud Anywhere, and in detailing the vCDN and CDN interconnection business case that for now is addressed in the IPTV case. It will be important to evolve and detail the service model specifications, to better understand the more detailed dependencies and how a service is dependent on other resources and their service counterparts and representations. Moreover, it is important to better understand the multi-actor end-customer dependencies and on-boarding processes, and how alternative end-customer features, charging

principles and money flows impact the capabilities needed and supported by the 5GEx framework.

This work is already of importance and will become even more important as the work matures, in helping network operators and Telcos of different kinds as well as other players in the 5G ecosystem. This work helps to gain insight and knowledge in what it takes to prepare for, to design and build services and offerings to existing and new customers. Still there are bootstrapping challenges and great uncertainties related to technology maturity as well as regulatory issues such as net neutrality. The insights and knowledge provided by 5GEx is important when working with strategy, prioritisation and roadmap topics which as well will be addressed in the further work by 5GEx. Moreover, these topics are important to provide incentives and to help the players to collaborate and coordinate and to support the preparations needed for the anticipated future multi-actor, multi-service offerings. These multi-player coordination issues are seen as one of the greater challenges in evolving and moving the ecosystem forward.

10 Summary and conclusions

This document describes the initial specification of the 5GEx architecture. We have identified first a set of primary requirements mainly considering business aspects together with the set of use cases identified as relevant for the multi-domain 5G environments.

Keeping in mind these key requirements, we have followed an architecture design methodology based on converging two different approaches:

(i) a top-down approach providing a green field architectural vision from the identified requirements,

(ii) *bottom-up approach* based on existing orchestration components that 5GEx can leverage on, adding the missing pieces required by the enablement of multi-domain orchestration.

This initial 5GEx architecture is, on the one hand, capable of meeting the identified multi-domain requirements, and, on the other hand, easy to start prototyping and testing.

The main innovations (findings) reported in this document are:

1) The definition of the main architecture multi-domain building blocks of 5GEx and their interfaces, considering not only the technology gaps but also the business considerations. This architecture vision is based on a **revised vision of the ETSI NFV** ISG framework, which is being **contributed to relevant standards,** namely ETSI and IETF. It is also ancored in the emerging **overall 5G networking architecture** focussing on the Infrastructure Softwarisation, Control and Integrated Management Planes, which is being contributed to **ITU-T IMT 2010** standard group.

2) A novel analysis of **business roles in a multi-domain environment, looking at the 5GEx framework, 5GEx services definition as well as describing possible coordination models that can apply to the 5GEx framework.** A main conclusion is that distributed coordination models scale better and build upon existing business relationships, resulting in lower deployment costs, less trust issues and easier bootstrapping of the 5GEx solution. Centralised coordination on the other hand can increase both the multi-domain service orchestration probability and the overall system efficiency. On-demand service composition can be used to discover the 5G market needs, which is useful in early markets, serving as a feedback loop for the specification of service catalogues that can significantly reduce the amount of on-demand customer requests and promote automated and fast service orchestration and trading.

The extensive analysis of the state of the art we have conducted and reported in this document has allowed us, not only to analyse what are the main open aspects that the architecture design had to focus on, but also to identify how to maximise the impact of 5GEx innovations. We are currently bringing our key innovations to main standardisation bodies, mainly the IETF/IRTF, ITU-T IMT2020 and shortly also the ETSI NFV ISG.

The analysis of the current eco-system and the related business and economics implications, where the 5GEx operators' participation is vital, together with the vision of the SMEs of the project, has been key during the first stage of the architecture definition. Initial pricing considerations has been included in the document, to be extended in the next months of the project.

The initial 5GEx architecture definition, which is one of the main tangible outcomes of WP2 during the first months of the project, has been taken by WP3, which is responsible of further specifying the software architecture and implementing it, and by WP4, which will take the software prototypes delivered by WP3 and experiment with it in the 5GEx sandbox.

Feedback from WP3, WP4 and other external initiatives will be considered in revising and updating the 5GEx architecture framework. The final design will be reported in D2.2. The business and economic related aspects will also be further developed in the next phase of the project, and reported in D2.3.

References

[1] D. King, A. Farrell, A PCE-based Architecture for Application-based Network Operations. IETF draft: https://datatracker.ietf.org/doc/draft-farrkingel-pce-abno-architecture/

[2] ONF, OpenFlow Switch Specification 1.4.0, October 2013: https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf

[3] EU-FP7 ETICS Project Grant aggrement no: FP7-248567 URL: www.ict-etics.eu

[4] VITAL project URL: http://www.ict-vital.eu

[5] BATS project URL: http://www.batsproject.eu

[6] IETF CDNi URL: https://datatracker.ietf.org/wg/cdni/charter

[7] SAIL project, URL: http://www.sail-project.eu/wp-content/uploads/2013/01/SAIL_DA8_Final_Public.pdf

[8] Cisco, "Content Delivery Network (CDN) Federations How SPs Can Win the Battle for Content-Hungry Consumers"

[9] The OnApp Federation URL: onapp.com/federation

[10] Cloud28+ URL: www.cloud28plus.eu

[11] Arjuna Agility whitepaper, "Removing the barriers to business agility" URL: www.arjuna.com/files/RemovingBarriersWhitepaper.pdf

[12] Deutsche Börse Cloud Exchange, URL: https://cloud.exchange/en/

[13] CloudStore, URL: https://www.digitalmarketplace.service.gov.uk/g-cloud

[14] NGMN Alliance, "5G White Paper", March 2015 https://www.ngmn.org/5g-white-paper.html.

[15] Huawei, "5G: A Technology Vision".

[16] Nokia, "Looking Ahead to 5G".

[17] Nokia, "Use Cases and Requirements".

[18] Alcatel-Lucent, "5G is Coming: Are you prepared?".

[19] Samsung, "5G Vision".

[20] Ericsson, "5G Systems: Enabling Industry and Society Transformation".

[21] Ericsson, "Five alive! 5G beyond the hype"

[22] Arpit Gupta, Laurent Vanbever, Muhammad Shahbaz, Sean P.

Donovan, Brandon Schlinker, Nick Feamster, Jennifer Rexford, Scott Shenker, Russ Clark, Ethan Katz-Bassett: SDX: A Software Defined Internet Exchange, SIGCOMM'14, August 17–22, 2014, Chicago, IL, USA

[23] IEEE Std. 1903-2011, "Standard for the Functional Architecture of Next Generation Service Overlay Networks", Oct 2011

[24] Seung-Ik Lee; Shin-Gak Kang, "NGSON: features, state of the art, and realisation," in Communications Magazine, IEEE, vol.50, no.1, pp.54-61, January 2012

[25] Thomas Erl, "Service-Oriented Architecture: Concepts, Technology & Design", Prentice Hall, ISBN 0-13-185858-0.

[26] B. Nunes, M. Mendonca, X. Nguyen, K. Obraczka, T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks", IEEE Communications Surveys & Tutorials, vol. PP, no. 99, pp.1-18, doi: 10.1109/SURV.2014.012214.00180

[27] Network Functions Virtualisation (NFV); Architectural Framework, ETSI GS NFV 002 V1.1.1, October 2013.

[28] Paganelli, F.; Ulema, M.; Martini, B., "Context-aware service composition and delivery in NGSONs over SDN," in Communications Magazine, IEEE, vol.52, no.8, pp.97-105, Aug. 2014

[29] Qiang Duan; Yuhong Yan; Vasilakos, A.V., "A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing," in Network and Service Management, IEEE Transactions on, vol.9, no.4, pp.373-392, December 2012

[30] https://standards.ieee.org/develop/project/1903.1.html

[31] https://standards.ieee.org/develop/project/1903.2.html

[32] https://standards.ieee.org/develop/project/1903.3.html

[33] http://sdn.ieee.org/

[34] http://theinstitute.ieee.org/benefits/standards/working-toward-the-next-generation-of-networks

[35] A. Dhamdhere, C. Dovrolis, "The Internet is Flat: Modeling the Transition from a Transit Hierarchy to a Peering Mesh", Proceedings of ACM CONEXT, 2010.

[36] G. Huston, "Interconnection, Peering and Settlements – part I", The Internet Protocol Journal, Vol. 2, Num. 1, pp. 2-16, March 1999, available at http://www.cisco.com/warp/public/759/ipj_2-1.pdf

[37] G. Huston, "Interconnection, Peering and Settlements – part II", The Internet Protocol Journal, Vol. 2, Num. 2, pp. 2-23, June 1999, available at http://www.cisco.com/warp/public/759/ipj_2-2.pdf

[38] GSM Association IR.34, "Inter-Service Provider IP Backbone Guidelines", version 9.1, May 2013, available at

http://www.gsma.com/newsroom/wp-content/uploads/2013/05/IR.34-v9.1.pdf

[39] Open Networking Foundation, "SDN Architecture – Issue 1" TR-502, June 2014, available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

[40] Open Networking Foundation, "SDN Architecture – Issue 1.1" TR-521, January 2016, available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR-521_SDN_Architecture_issue_1.1.pdf

[41] Luis M. Contreras, Carlos J. Bernardos, Diego López, M. Boucadair, P. Iovanna, "Cooperating Layered Architecture for SDN", draft-irtf-sdnrg-layered-sdn-00, work-in-progress, March 2016.

[42] Metro Ethernet Forum, "Lifecycle Service Orchestration (LSO): Reference Architecture and Framework", MEF-55, March 2016, available at https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_55.pdf

[43] C.J. Bernardos, L.M. Contreras, "Multi-domain Network Virtualization", draft-bernardos-nfvrg-multidomain-00 (work in progress), March 2016.

[44] A. Farrel, J. Drake, N. Bitar, G. Swallow, D. Ceccarelli, X. Zhang, "Problem Statement and Architecture for Information Exchange Between Interconnected Traffic Engineered Networks", draft-ietf-teas-interconnected-te-info-exchange-04, March 2016.

[45] T. Kudoh, G. Roberts, I. Monga, "Network Services Interface: An Interface for Requesting Dynamic Inter-datacenter Networks", in Proceedings of the OFC, 2013.

[46] Open Grid Forum NSI-WG, "Network Services Framework v2.0", available at: https://www.ogf.org/documents/GFD.213.pdf

[47] Open Grid Forum NSI-WG, "Network Service Agent Description", available at: https://www.ogf.org/documents/GFD.220.pdf

[48] Open Grid Forum NSI-WG, "NSI Connection Services v2.0", available at: https://www.ogf.org/documents/GFD.212.pdf

[49] Open Grid Forum NSI-WG, "Network Service Interface Signaling and Path Finding", available at: https://www.ogf.org/documents/GFD.217.pdf

[50] FP7 CityFlow Project. Grant agreement number: 317576, http://www.cityflow.eu/

[51] H2020 Endeavour project. ENDEAVOUR: Towards a flexible software-defined network ecosystem. https://www.h2020-endeavour.eu/

[52] NetWorld2020 Whitepaper on Service Level Awareness:

http://networld2020.eu/sria-and-whitepapers/

[53] ETSI GS NFV-SWA 001: "Virtual Network Functions Architecture", December 2014.

[54] 3GPP TS 23.002, "Network architecture".

[55] Darzanos, G., Dramitinos, M., Lønsethagen, H., Papafili, I. and Stamoulis, G.D.: "Internet and 5G Tussles and How to Mitigate Them by Re-Engineering SPNP", EuCnC 2016.

[56] von Bornstaedt, F., Roettgermann, M., Korthals, I., Johansen, F.T. and Lonsethagen, H.: "The Sending Party Network Pays Principle: A First Step towards End-to-End Quality of Service", ICIN 2011.

[57] Briscoe, B. and Rudkin, S.: "Commercial Models for IP Quality of Service Interconnect". In BTTJ Special Edition on IP Quality of Service, 23(2) (Apr 2005).

[58] PWC, "The future of software pricing excellence: SaaS pricing" https://www.pwc.com/mt/en/publications/assets/pwc-the-future-of-software-pricing-excellence-saas-pricing.pdf

[59] https://apprenda.com/library/software-on-demand/saas-billing-pricing-models/

[60] https://blog.kissmetrics.com/saasy-pricing-strategies/

[61] https://aws.amazon.com/lambda/pricing/

[62] https://aws.amazon.com/s3/pricing/

[63] https://aws.amazon.com/rds/pricing/

[64] https://aws.amazon.com/pricing/services/

[65] http://techcrunch.com/2009/03/12/amazon-web-services-rolls-out-new-pricing-model-for-ec2/

[66] SLA and billing, T-NOVA D6.4, http://www.t-nova.eu/wp-content/uploads/2016/03/TNOVA_D6.4_SLAs_and_billing_v1.0.pdf

[67] 5GPPP 5G Architecture WG - 5G White Paper "Views on 5G Architecture" 1st June 2016, https://5g-ppp.eu/white-papers/

[68] Networks Functions Virtualization (NFV); Management and Orchestration, ETSI GS NFV MAN 001 V1.1.1 (2014-12)

[69] Deliverable 3.1: "Description of protocol and component design", 5GEx, July 2016.

[70] Bradner S.: "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, IETF, March 1997.

[71] 5G-PPP IA, "5G and Media & Entertainment" whitepaper, available at: https://5g-ppp.eu/wp-content/uploads/2016/02/5G-PPP-White-Paper-on-Media-Entertainment-Vertical-Sector.pdf

[72] 5G-PPP IA, "5G and the Factories of the Future" whitepaper,

available at: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Factories-of-the-Future-Vertical-Sector.pdf

[73] 5G-PPP IA, "5G Automotive Vision" whitepaper, available at: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf

[74] 5G-PPP IA, "5G and e-Health" whitepaper, available at: https://5g-ppp.eu/wp-content/uploads/2016/02/5G-PPP-White-Paper-on-eHealth-Vertical-Sector.pdf

[75] G. Biczók, M. Dramitinos, H. Lonsethagen, L. M. Contreras, and G. D. Stamoulis, "Towards Multi-operator IPTV Services Over 5G Networks" in "IPTV Delivery Networks" Book, Editors: Suliman Mohamed Fati, Saiful Azad and Al-Sakib Khan Pathan, Wiley, 2016.

A Key Terms

This document uses the following terms:

5G Network Segments. Radio Networks, Fronthaul & Backhaul Networks, Aggregation and Core Networks, Network Clouds, Mobile Network (i.e., combination of network segments where the last link is wireless - a radio network), Mobile Edge Networks, Service/Software Networks, Software Defined Cloud Networks, Satellite Networks, IoT Networks

Separation of Concerns in Distinct Planes:

Service Plane (SP). It defines and implements the business processes of the services along specific value chains. A service in the 5G context is piece of software that performs one or more functions and provides one or more APIs to applications or other services of the same or different layers to make use of said functions and returns one or more results. Services can be combined with other services, or called in a certain serialised manner, to create a new service. An application in the 5G context is a piece of software that utilises underlying services to perform a function. Application operation can be parameterised, for example, by passing certain arguments at call time, but it is meant to be a standalone piece of software; an App does not offer any interfaces to other applications or services.

Multi-service Management Plane (MSMP). The functions and interfaces in this plane are used to setup and manage groups of network instances and/or nodes. In more details, the setup consists of setting up NFs and interfaces according to the available physical and virtual resources. It also comprises the set of functions associated to the network operations such as fault management, performance management and configuration management. It further includes the lifecycle management of individual network functions and mobile network instances as a whole. In current networks, this is often performed by the Operations Support System (OSS).

Network Management & Operations Plane (M&OP). It is to enable the creation, operation, and control of dedicated management functions operating on top of a 5G e2e infrastructure. The collection of resources responsible for managing the overall operation of individual network devices.

Infrastructure Plane (IP). It is to enable the operations of end-to-end heterogeneous networking and distributed cloud platforms including physical and logical resources and devices.

Control Plane (CP). The collection of functions responsible for controlling one or more network resources. CP instructs network devices, network elements, and network functions with respect to how to process elementary data units (packets, frames, symbols, bits, etc.) of the

user/data/forwarding plane. The control plane interacts primarily with the forwarding plane and, to a lesser extent, with the management plane.

Forwarding Plane (FP). The collection of resources across all network devices responsible for forwarding traffic.

Key Architectural Terms:

Access Network. An access network is the part of a telecommunications network which connects subscribers to their immediate service provider. It is contrasted with the core network which connects local providers to each other. The access network may be further divided between feeder plant or distribution network, and drop plant or edge network.

Administrative domain. It is a collection of systems and networks operated by a single organisation or administrative authority. Infrastructure domain is an administrative domain that provides Virtualised infrastructure resources such as compute, network, and storage or a composition of those resources via a service abstraction to another Administrative Domain, and is responsible for the management and orchestration of those resources.

Core Network. A core network is the central part of a telecommunications network that provides various services to customers who are connected by the access network. One of the exemplary functions is to route telephone calls across the PSTN. Typically, the term refers to the high capacity communication facilities that connect primary nodes. Core/backbone network provides paths for the exchange of information between different sub-networks. For enterprise private networks serving one organisation, the term backbone is more used, while for service providers, the term core network is more used.

Interface. A point of interaction between two entities. When the entities are placed at different locations, the interface is usually implemented through a network protocol. If the entities are collocated in the same physical location, the interface can be implemented using a software application programming interface (API), inter-process communication (IPC), or a network protocol.

Physical Resource - A physical network, compute or storage component available within a system. Resources can be very simple or fine-grained (e.g., a port or a queue) or complex, comprised of multiple resources (e.g., a network device).

Logical resource. An independently manageable partition of a physical resource, which inherits the same characteristics as the physical resource and whose capability is bound to the capability of the physical resource.

Mobile Network. A cellular network or mobile network is a communication network where the last link provides wireless access to the network. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or

base station. This base station provides the cell with the network coverage which can be used for transmission of voice, data and others. In a cellular network, each cell uses a different set of frequencies from neighbouring cells, to avoid interference and provide guaranteed bandwidth within each cell.

Multitenancy domain. It refers to set of physical and/or virtual resources in which a single instance of a software runs on a server and serves multiple tenants. A tenant is part of a group of users who share a common access with specific privileges to the software instance. A service or an application may be designed to provide every tenant a dedicated share of the instance including its data, configuration, user management, tenant individual functionality and non-functional properties.

Network Device. A device that performs one or more network operations related to packet manipulation and forwarding. This reference model makes no distinction whether a network device is physical or virtual. A device can also be considered as a container for resources and can be a resource in itself.

Network virtualisation. A technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collection of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider, appearing as a single resource.

Orchestration. The capability of consistently partition and combine operational coordination actions (i.e., configuration, event notifications, etc) among domains in a network (being then technological, topological, etc) is defined as orchestration of such control domains. Different types of orchestration can be further identified:

> **Service Orchestration.** It is performed by traditional management functions (e.g., EM, OSS, BSS).
>
> **Virtualisation Service Orchestration.** Any service specific configuration within VNFs. **Network Service Orchestration** is also part of this, mainly dealing with IP, Ethernet network or service chaining configurations.
>
> **Virtualisation Resource Orchestration.** Placement and creation of virtual structures (VMs, VRFs), management of global (lower layer) ID space. Its role is to aggregate resources from multiple VIMs.

Programmable networks. This term refers to networks that allow the functionality of some of their network elements to be programmable dynamically. These networks aim to provide easy introduction of new network services by adding dynamic programmability to network devices such as routers, switches, and applications servers. Network Programmability empowers the fast, flexible, and dynamic deployment of new network and management services executed as groups of virtual

machines in the data plane, control plane, management plane and service plane in all segments of the network. Dynamic programming refers to executable code that is injected into the execution environments of network elements in order to create the new functionality at run time. The basic approach is to enable trusted third parties (end users, operators, and service providers) to inject application-specific services (in the form of code instructions) into the network. Applications may utilise this network support in terms of optimised network resources and, as such, they are becoming network aware. As such the behaviour of network resources can be customised and changed through a standardised programming interface for network control, management and servicing functionality.

Resource. A physical or virtual (network, compute, storage) component available within a system. Resources can be very simple or fine-grained (e.g., a port or a queue) or complex, comprised of multiple resources (e.g., a network device).

A **radio access network** (RAN) is part of a mobile telecommunication system (i.e., a Mobile Network as defined above). It implements a radio access technology. Conceptually, it provides a device, such as a mobile phone, a computer, or any remotely controlled machine with connectivity to its core network.

Slices. A slice is grouping of physical or virtual (network, compute, storage) resources which can act as a sub network and/or cloud and it can accommodate service components. For slice creation, management planes create virtual or physical network functions and connects them as appropriate and instantiate all the network functions assigned to the slice. On the other hand, for slice creation, the slice control takes over the control of all the virtualised network functions and network programmability functions assigned to the slice, and (re-)configure them as appropriate to provide the end-to-end service.

Software Network. Software network is an approach to computer networking that allows network administrators to manage network services through abstraction of higher-level functionality. This is done for example by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).

Softwarisation. An approach for designing, implementing, deploying, managing and maintaining network equipment and/or network components and /or network services by software programming, exploiting the natures of software such as flexibility and rapidity all along the lifecycle of network equipment / components / services, for the sake of creating conditions enabling the re-design of network and services architectures, optimizing costs and processes, enabling self-management and bringing added values in network infrastructures.

Virtual resource. An abstraction of physical or logical resource, which may have different characteristics from the physical or logical resource and whose capability may not be bound to the capability of the physical or logical resource.

Virtual Network Function. One or more virtual machines running different software and processes on top of industry-standard high-volume servers, switches and storage, or cloud computing infrastructure, and capable of implementing network functions traditionally implemented via custom hardware appliances and middleboxes (e.g., router, NAT, firewall, load balancer, etc.).

B 5G Network Architecture Context

5GEx project has contributed and acted as an editor of the 5GPPP Overall Architecture [67] which is summarised in this section.

5G networks are conceived as extremely flexible and highly programmable E2E multi-domain connect-and-compute infrastructures that are application- and service-aware, as well as time-, location- and context-aware. They represent:

- an evolution in terms of capacity, performance and spectrum access in radio network segments; and
- an evolution of native flexibility and programmability conversion in all non-radio 5G network segments: Fronthaul and Backhaul Networks, Access Networks, Aggregation Networks, Core Networks, Mobile Edge Networks, Software Networks, Software-Defined Cloud Networks, Satellite Networks and Edge IoT Networks.

5G Architecture enables new business opportunities meeting the requirements of large variety of use cases as well as enables 5G to be future proof by means of *(i)* implementing network slicing in cost efficient way, *(ii)* addressing both end user and operational services, *(iii)* supporting softwarisation natively, *(iv)* integrating communication and computation and *(v)* integrating heterogeneous technologies (including both fixed and wireless technologies).

Based on the abovementioned novel mechanisms, 5G networks are expected to present a number of advantages. One is a high degree of flexibility. They serve highly diverse types of communication – for example, between humans, machines, devices and sensors - with different performance attributes. They also enforce the necessary degree of flexibility, where and when needed, with regard to capability, capacity, security, elasticity and adaptability.

5G networks represent a shift in networking paradigms: a transition from today's "network of entities" to a "network of functions". Indeed, this "network of (virtual) functions", resulting, in some cases, in the decomposition of current monolithic network entities will constitute the unit of networking for next generation systems. These functions should be able to be composed on an "on-demand", "on-the-fly" basis. In fact, a research challenge consists in designing solutions which identify a set of elementary functions or blocks to compose network functions, while today they implemented as monolithic

Further advantages emerge in the areas of management, control of systems and resources. 5G networks enable the uniform management and control operations that are becoming part of the dynamic design of software architectures. They can host service executions in one or more slices.

As such 5G Networking is fostering the followings key separation of concerns:

- Serving at best high diversity types of communications (Human & Machines & Devices & Sensors & Edge Systems) with different performance attributes.
- Separation of concerns between control/management Vs. Softwarisation
- Separation of concerns between logical / physical resources functions (i.e. connectivity, compute and storage resources) and network capabilities
- A shift in networking and a transition form "network of entities", as in current systems, to "network of (virtual) functions / capabilities". As such "network (virtual) functions" are units of networking.
- Network softwarisation is not equated with network slicing. Hosting services executions in one (or more) Slices. Network softwarisation includes functions for programmability of (1) network devices; (2) network (virtual) functions; (3) slices, (4) network services and applications; (5) data plane; (6) control plane; (7) management plane.
- Supporting on demand composition of network functions and network capabilities
- Leveraging natively Network Softwarisation technologies in all network segments and network components.

The proposed 5G framework is aimed at all 5G Network segments: Radio Networks, Fronthaul & Backhaul Networks, Aggregation and Core Networks, Network Clouds, Mobile Network (i.e., a combination of network segments where the last link is wireless - a radio network) and enabling technologies like Mobile Edge Networks, Service/Software Networks, Software-Defined Cloud Networks, Satellite Networks, Edge IoT Networks.

The perspectives of this 5G framework proposal are specified as separate planes. Although separately defined, the planes are not completely independent: key items in each are related to items in the other planes. However, the planes are sufficiently independent to simplify reasoning about the complete system requirements. The interworking between planes is manifested by groups of interfaces (i.e., reference points) that would be used for exchange of information and/or controls between separate (sub)systems sharing boundaries. The projected separation of concerns in distinct planes are: Application and Business Service Plane, Multi-Service Management Plane, Integrated Network Management & Operations Plane, Infrastructure Softwarisation Plane, Control Plane and Forwarding/Data Plane.

The proposed framework for network softwarisation and programmability is presented in Figure A-1, where each plane is exemplified.

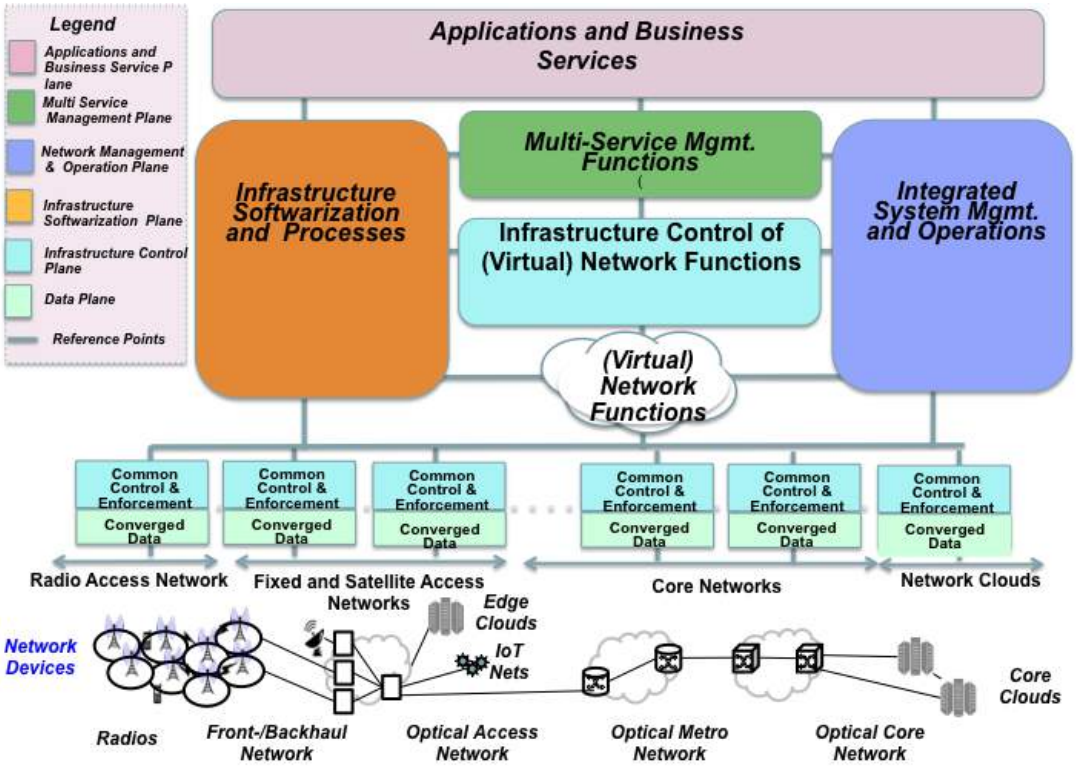


Figure A-1: 5G Overall Network Softwarisation and Programmability Framework

This network softwarisation and programmability framework is based on the following separation in distinct planes:

Infrastructure Softwarisation Plane – Enables the provisioning and operation of software and service networks. It facilitates the operation of end-to-end heterogeneous networking and distributed cloud platforms, including physical and logical resources and devices. It includes software for designing, implementing, deploying, managing and maintaining network equipment, network components and/or network services by programming. The software utilises features such as flexibility and rapidity all along the lifecycle of network equipment/components/services, in order to create conditions that enable the re-design of network and services architectures, optimise costs and processes, allow self-management and bring added value to network infrastructures. It further includes provision of software and service networks, application driven network softwarisation, S/W Programmability of Software Networks, dynamic deployment of new network and management services (i.e., which could be executed in data, control, management, service plane), network capability exposure, E2E slice provisioning and control in software networks. It includes functions for dynamic programmability of (1) network devices; (2) network (virtual) functions; (3) slices, (4) network services and applications; (5) data plane; (6) control plane; (7)

management plane. This planes includes also the artefacts of extensions to the ETSI MANO [68].

Multi-Service Management Plane – The functions and interfaces in this plane are used to set up and manage groups of network instances and/or nodes. More specifically, the setup consists of creating/installing/arranging NFs and interfaces according to the available physical and virtual resources. It also comprises the set of functions associated with the network operations, such as fault management, performance management and configuration management. It further includes Slice –Service Mapper functions, Resources, Domain and Service Orchestration functions, Service Information Management functions and Network Capability Discovery functions. It also includes the lifecycle management of individual network functions and mobile network instances as a whole. In current mobile networks, this role is often performed by the Operations Support System (OSS). The idea is to enable the creation, operation, and control of multiple dedicated communication service networks running on top of a 5G E2E infrastructure.

Integrated Network Management & Operations Plane – Enables the creation, operation, and control of dedicated management functions operating on top of a 5G E2E infrastructure; and the collection of resources required for managing the overall operation of individual network devices. It further includes E2E Network segments management, FCAPS functionality, Monitoring operations, Network Information Management, In-network data and operations processing and Multi domains management operations

Infrastructure Control Plane - The collection of functions responsible for controlling one or more network devices. Control Plane instructs network devices, network elements, and network functions with respect to processing elementary data units (packets, frames, symbols, bits, etc.) of the user/data/forwarding plane. The control of (virtual) network functions include Control of Network Softwarisation functions, Control of Orchestration functions, Control of Mobility control functions, Cloud Control functions, Mobile Edge Computing Control functions and adaptors to different enforcement functions. The control of (virtual) network functions is generally 5G-applicable, and they are separated from the control and enforcements functions which are network segment-specific. The control plane interacts primarily with the forwarding plane and, to a lesser extent, with the management plane.

Forwarding Plane / Data Plane - The collection of resources across all network devices responsible for forwarding traffic.

Application and Business Service Plane – Defines and implements the business processes of the services along specific value chains. A service in the 5G context is a piece of software that performs one or more functions, provides one or more APIs to applications or other services of the same or different planes to make usage of those functions, and

returns one or more results. Services can be combined with other services, or called in a serialised manner to create a new service. An application in the 5G context is a piece of software that utilises the underlying services to perform a function. Application operation can be parameterised, for example, by passing certain arguments at call time, but it is meant to be a standalone piece of software; an App does not offer any interfaces to other applications or services.

C Architecture design input

Two different approaches were followed in order to provide inputs for a common architecture design. A top-down approach (so called Greenfield) where no dependencies were considered at the time of profiling a potential 5GEx architecture; and a bottom-up approach (so called Brownfield) where an analysis of existing components and it suitability to facilitate the intended 5GEx baseline was performed.

This annex presents the outcomes of such analysis that were taken into account for a deep discussion and further progress son the 5GEx architecture presented in the main body of this document.

C.1 Top-down (Greenfield) approach

We next go through the exercise of designing a *greenfield* architecture.

The concept of exchange in the context of 5GEx considers two dimensions: control plane exchange, and data plane exchange.

The data plane refers to the connectivity of resources to compose the desired service end-to-end. The control plane refers to the interaction of the control plane of the providers involved in the service provision.

C.1.1 Resource Connectivity

The traditional concept of exchange implies direct connection between providers, collocated at the exchange. Realistic scenarios for 5GEx have to address multi-hop cases (i.e., administrative domains not directly connected, but reachable through other domains).

C.1.2 Service

End-to-end service relationship will be one-to-one in nature. Even in the cases where multiple parties are involved, one of the parties will be the one in charge of delivering the service to the final customer. Most probably this last party will be the one coordinating the service provision, and then interacting in a one-to-one fashion with the rest of parties affected.

C.1.3 Greenfield approach

The 5G Exchange should contain a plane for negotiating/requesting services and a different plane for setting up connectivity end-to-end, configuring and managing the necessary resources for doing so.

The service request should be mapped to the network capabilities offered in the exchange.

Each domain will have its own orchestrator to setup the proper paths internal to the domain.

For solving the multi-domain approach a novel idea is proposed. A hierarchical orchestrator is assumed to be in place for multi-domain path resolution. This hierarchical orchestrator is the result of associating

control entities (one per each domain/operator in the exchange) working in a peer-to-peer fashion in order to interchange information relative to the capabilities offered by each party in the exchange.

The mentioned peer-to-peer relationship could be realised in the form of service/resource catalogue, pull/push information exposition, effective

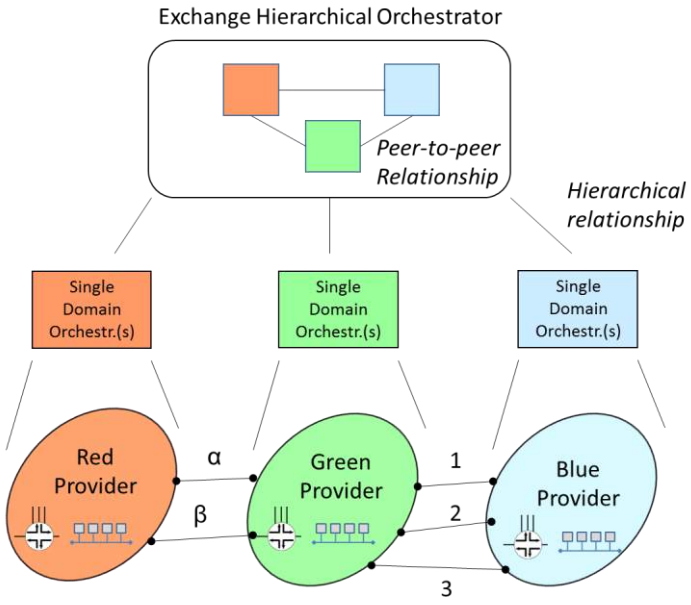


Figure A-2: Architectural approach for connectivity in 5GEx

peer-to-peer info exchange, etc. Figure A-2 illustrates the concept.

Example: Operator B could advertise that it is capable to reach Operator C through link 1 with KPIs *X, Y, Z*; through link 2 with KPIs *U, V, W*; etc. The KPIs to be advertised should be defined. The information exchanged includes networking, compute and storage information.

The associated control entities forming the Exchange Hierarchical Orchestrator (EHO) only advertise interdomain information to the other parties. Intradomain information is not exposed, and it is responsibility of each of the domains to handle this information properly.

This idea can recall the role that peering/transit routers play today since they are the only ones maintaining BGP peering sessions with their correspondents, while the rest of the routers in the internal of the network take information from them (directly or via the route reflectors).

The way of exposing information in the EHO is to be defined. Pub/sub schemes could be in place. Even BGP mechanisms could be leveraged for that (probably complemented or extended to provide richer information).

The domain orchestrator(s) will be in charge of interacting with different underlay controllers. The concept of domain can have multiple considerations:

- Per technology
    - IT / Compute, storage, etc
    - Optics / IP
    - Etc
- Per network segment
    - Core
    - Metro / MBH
    - Etc
- Per (internal) domain
    - Area1
    - Area2
    - etc

The relationship between controllers/orchestrators for the instantiation of the service will be direct. No intermediation is needed, as far as the service controller/orchestrator has a clear idea where the service has to be deployed, according to the customer request.

A service controller/orchestrator will be the entry point for the customer request. The customer could be either internal or external to the operator that receives the initial request.

Three types of recipient for service requests could be expected:

- The service request is sent over the service controller/orchestrator of one operator. In this case, the service controller/orchestrator has to map the service request to its internal capabilities. If the service implies a multi-domain setup, the operator should trigger the multi-domain mechanisms through the interaction with the EHO (how this trigger will be done is under further analysis: from the service controller or from the connectivity controller of the operator being the entry point for the service). Figure A-3 top-left illustrates this case.
- The customer sends a service request to multiple operators. In this case the customer is multi-homed, and it is aware of the distinct capabilities offered by the operators that it is connected to. The initial split of mapping the service per operator is done by the customer itself. For each operator-based request, the procedure should be similar to point 1. Figure A-3 top-right illustrates this case.

- The service request is sent over the exchange. The exchange could offer an entry point for service requests. In this case the service controller/orchestrator at the exchange has to map the service requests to the capabilities offered by the distinct operators being

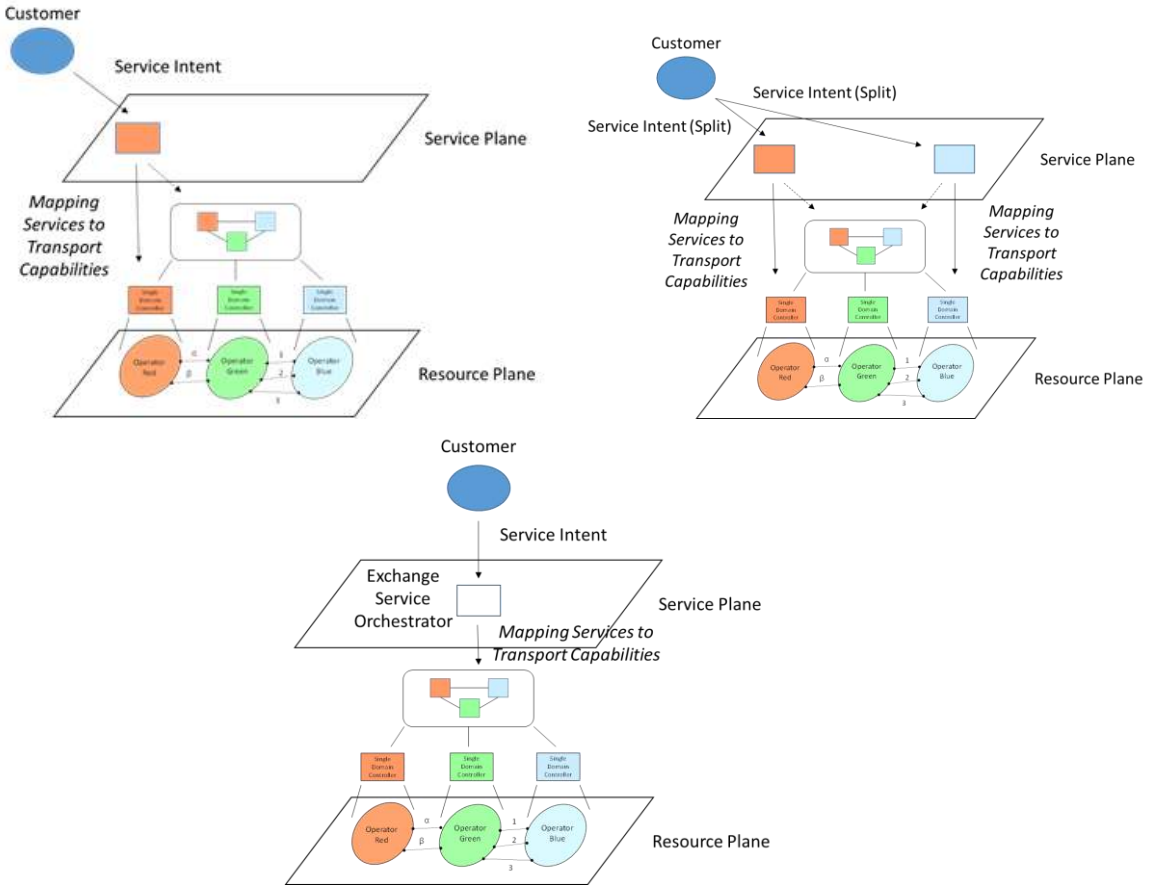


Figure A-3: Types of recipient for service requests

part of the exchange. Figure A-3 bottom illustrates this case.

The 5GEx becomes then a distributed exchange where the interaction is twofold:

- One to one interaction for service composition and delivery.
- Peer-to-peer interaction for resource connectivity setup in multi-hop scenarios (if the domains are one-hop far, also here one-to-one interaction will occur).

The connection among domains will be implemented by some way of tunnelling in order to isolate and separate the traffic. Mechanisms like IPsec, GRE tunnelling or even MPLS can be foreseen for such as connection. To be defined.

Service requests can be expected to be based on intents in order to mask any particularity coming from the underlying transport/connectivity network.

The following figures represent an initial mapping of 5GEx interfaces per case.

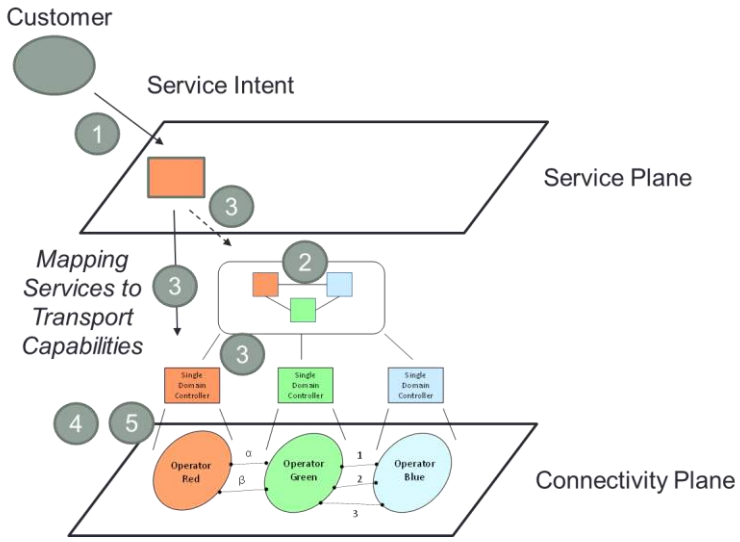


Figure A-4: Service request sent over the service controller/orchestrator of one operator

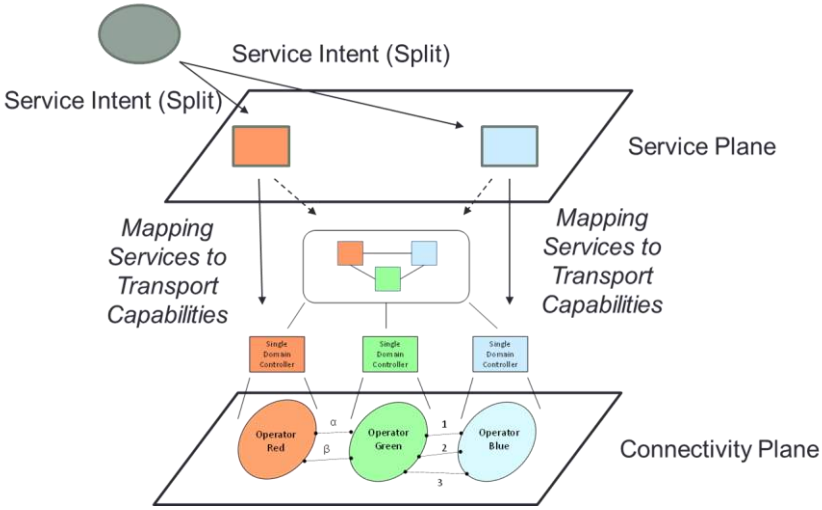


Figure A-5: Service request sent to multiple operators

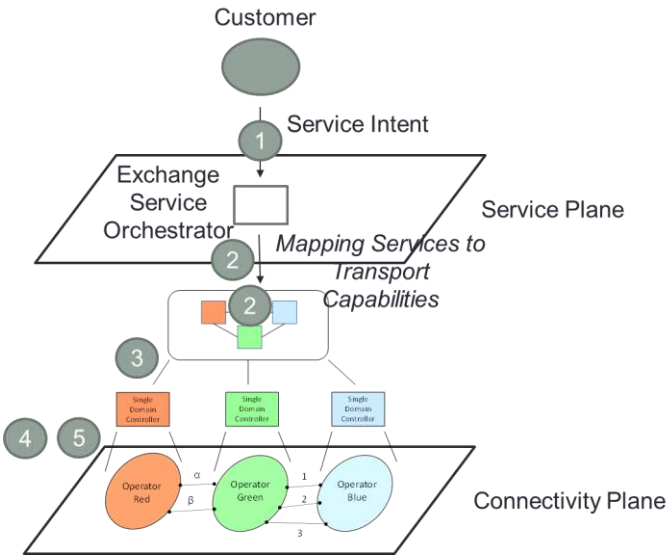


Figure A-6: Service request sent over the exchange

C.2 Bottom-up approach

The analysis of the candidate software components presented in the previous section results in the identification and definition of a set of functional requirements that are expected to be fulfilled by the MdO. Figure A-7 depicts the component-based MdO architecture, including its functional blocks and interfaces to local domain orchestrators and to MdO modules in other administrative domains. MdO modules are grouped in four major functional areas: Exchange of Information and Control (EoIC), Catalogues, Exchange of Functions (EoF), and Exchange of Resources (EoR).

The following sections describe the role of the MdO modules and interfaces per functional area.

C.2.1 Exchange of Information and Control (EoIC)

The EoIC comprises of functional modules that operate buyer-supplier operations at service level, both for customers on interface *I1*, and for MdOs belonging to other administrative domains on interface *I2*. Moreover, the EoIC includes the modules that perform service mapping to topologies of NFs, or service slices, and SLA management.

The Service Request Management module exposes a northbound interface (*I1-S*) through which an MdO customer sends the initial request for services. It handles command and control functions to instantiate service slices. Such functions include requesting the instantiation, configuration and interconnection of NFs, as specified by the service graph created by the Service Mapping module, to other MdO modules in the EoF functional area. It is also responsible for providing SLA templates and SLA management instructions to the SLA Management module in order to assess if the requested service SLA is fulfilled. Finally, it is also

acknowledging the result of the service instantiation request to the MdO customer.

Interface *I2-S* is meant to perform among EoIC belonging to different MdOs (i.e., to other MdO Service Providers) operations similar to those described for *I1-S*. EoIC modules coordinate using interface *I2-S* when the instantiation of the end-to-end service involves multiple administrative domains. Both for *I1-S* and *I2-S* the service management operations imply the establishment of a business contract among the entities: customer to MdO service operator - interface *I1-S* and MdO operator to MdO operator - interface *I2-S*.

With reference to the frameworks presented in Section 2.10.2, EoIC modules can be realised by the components implemented within the T-NOVA project.

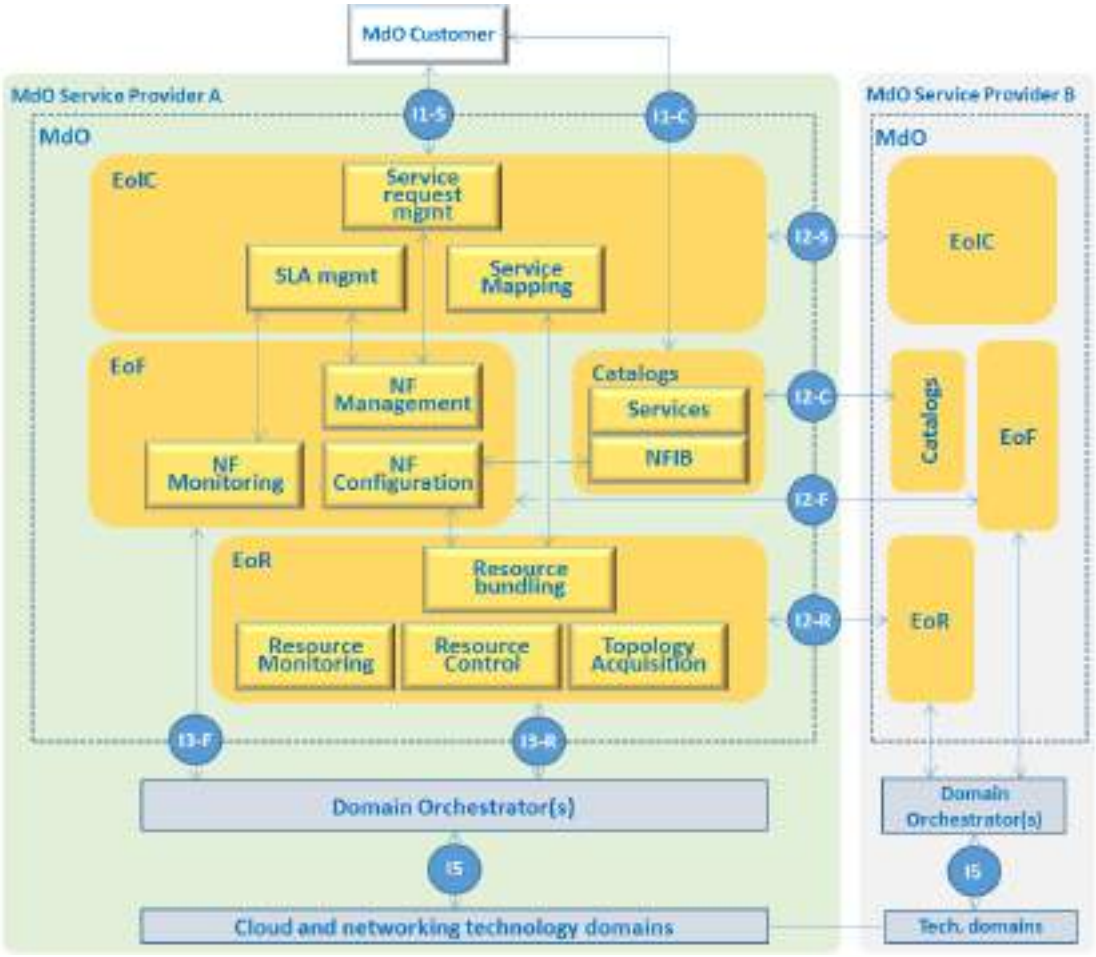


Figure A-7: MdO Architecture Proposal

C.2.2 Catalogues

The modules exposing repositories of available services and available NFs to customers and to MdOs in other administrative domains are part of the Catalogues functional area.

The service catalogue exposes available services to customers on interface *I1-C* and to other MdO service operators on interface *I2-C*.

Services are described by service templates, which include a service graph (SG) of NFs, service SLA options, price information and deployment instructions. NFs could either be a basic service component, as described in the NF Information Base (NFIB), or recursively refer to services in the service catalogue. The pricing information of a service can be described as a function of the requirements on the overall graph (i.e., number and location of the end devices) and the functional and non-functional requirements of its component NFs. Service templates are advertised across MdOs in different administrative domains using interface *I2-C*. For instance, the MdO service provider A in Figure A-7 can request services and/or NFs offered by the MdO service provider B and exposed over interface *I2-C* to provision a certain service to its customers.

NFIB is a repository of NFs, including references to the abstract resources required to implement them, similar to the VNF catalogue in ETSI NFV specification [27], [53]. It contains descriptors for available physical and virtual NFs, e.g., ETSI NFV VNFD and PNFD. Such descriptors specify the interfaces that the NF exposes, dependencies with other NFs, infrastructure resource requirements as a function of NF expected performance (i.e., CPU requirements as a function of the average traffic rate), deployment artefacts, supported lifecycle operations and offered NF SLA options (i.e., reliability SLAs/class).

With reference to Section 2.10.2, the T-NOVA framework implements a service catalogue while Unify provide an NFIB.

C.2.3 Exchange of Functions (EoF)

The EoF functional area includes modules that deals with the instantiation, management, configuration and monitoring of NFs.

The NF Management module performs lifecycle management operations on individual NFs, which are listed in the NFIB, over interfaces *I3-F* and *I2-F*. Performing a lifecycle operation on a given NF may imply reconfigurations of the abstract resources on which it is deployed and/or changes in its operational status (active, inactive, terminated, etc.). Fault management tasks are also handled by this module, such as collecting alarms and notifications from the NF monitoring module. Fault management diagnoses failures in NFs and attempts to repair them. The NF management module provides support for service re-orchestration, performing operations like scaling in/out and migration on individual NFs over interface *I3-F* and interface *I2-F* for NFs deployed by other MdO.

During the service orchestration process, the NFs may be programmed and/or configured according to the given service specification and orchestration decisions. The NF configuration module derives the necessary NF configuration instructions from the service and NFIB and from the orchestration decisions conducted by the service mapping module in the EoIC functional area. Any updates of the specification of the service instance or of its implementation may also trigger the

reconfiguration of several NFs. Service configuration instructions may apply to MdOs in other administrations over interface *I2-F*.

The NFs need to be monitored during their lifecycle to assure that domains controlled by different MdO instances provide enough resources to satisfy the required service specification, e.g., keeping under a given threshold the latency of a virtual path connecting two endpoints in different administrative domains. The SLA requested for a NF, which is agreed between the MdO and its customer throughout the whole service lifecycle, specifies Key Quality Indicators (KQI) values together with a set of expected non-functional requirements, such as resource security, availability, reliability and rules of compliance. The NF Monitoring module gets the monitoring configuration instructions from the NF Management module, implements the required probes at the NF level, collects Key Performance Indicators (KPI) and determines KQIs compliance with the SLA expected by the customer.

Some of EoF modules can be realised by components provided by the ESCAPE orchestrator in the project UNIFY.

C.2.4 Exchange of Resources (EoR)

The EoR modules perform resource orchestration, exposing resource slices to modules in EoIC and EoF. Four modules fall in this functional area, dealing with abstract resources and interfacing with underlying domain orchestrators for their realisation.

The Resource Topology Acquisition module keeps an updated global view of the underlying infrastructure topology exposed by domain orchestrators using interface *I3-R* for its own domain and interface *I2-R* for resources in other administrative domains (collected by the respective EoR modules through the corresponding *I3-R* interface). The topology information provided by the domain orchestrator, or by EoR in other MdOs, is an abstract and limited view of the domain infrastructure resources. For instance, the global view of the infrastructure resources topology gathered by this module may only contain information on aggregates of resources by type, e.g., cloud computing, networking, storage, and geographical location. The topology information is consumed by the service mapping module in EoIC in order to derive a service deployment plan (what are the domain orchestrators chosen to deploy the requested service and what resources are required from them) and accurate pricing information.

The Resource Bundling module aggregates resources belonging to different resource domains, implementing resource slices that may include abstract resources exposed by multiple domain orchestrators, even belonging to other administrative domains. Figure A-8 shows a resource slice that aggregates abstract resources belonging to two different infrastructures belonging to Service Provider A and Service Provider B. Each MdO is in charge of controlling the abstract resources in its own domain, while the Resource Bundling module provides a unified

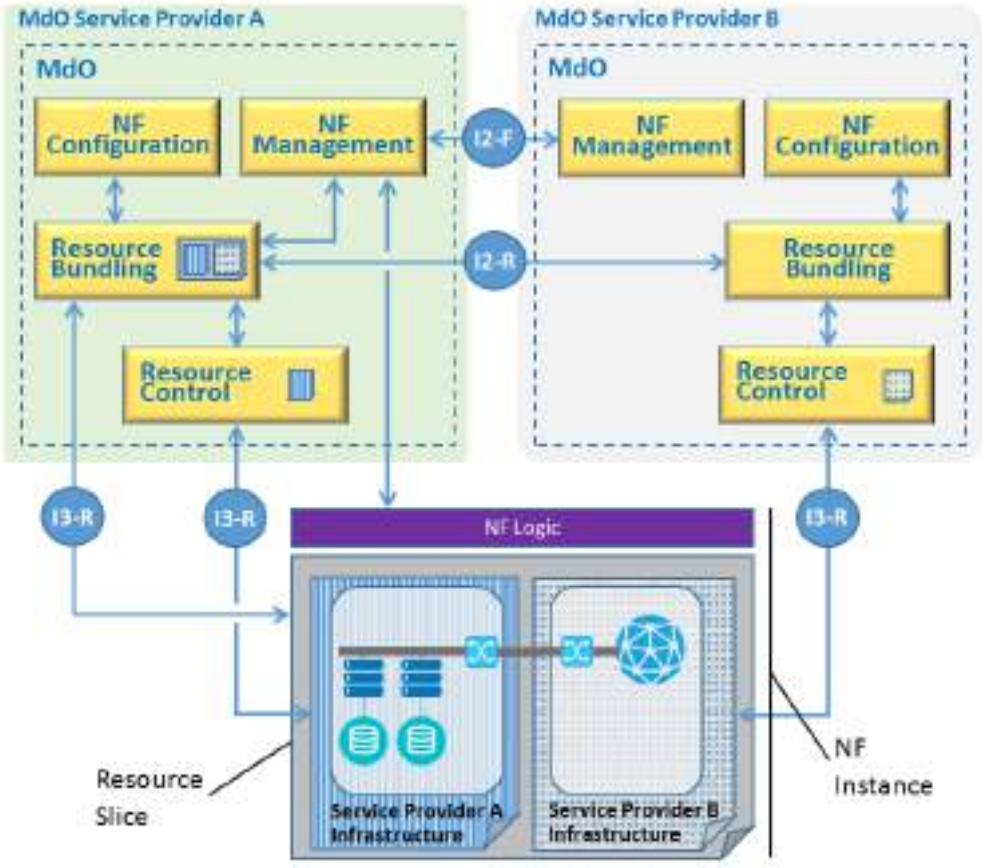


Figure A-8: Resource Bundle across Administrative Domains

view of the aggregate to the upper layers. The Resource Bundling module of Service Provider A coordinates with local (SP A) and remote (SP B) Resource Control modules to execute actions on the resource slice as a single entity, and expose it to EoF modules of Service Provider A.

The Resource Control modules interface with the different underlying domain orchestrators in the same administrative domain to perform resource level control operations as required by NFs, e.g., releasing infrastructure resources during the service shutdown process, scaling up/down computing resources, etc. These control operations are agnostic of the NF logic deployed on the resource slice. For instance, in order to perform a graceful shutdown of a given NF instance, NF management modules send a shutdown signal to the NF logic via its management interface. After the NF logic stops, NF management requests the release of the resource slice to the Resource Bundling module. The first command stops the software implementing the NF, while the second one triggers the termination of underlying virtual infrastructure resources and/or the release of physical resources. The Resource Bundling module requests all the Resource Control modules involved in the resource slice to release their respective resource.

The Resource Monitoring module collects and analyses key parameters required for evaluating the status of the system considering both the

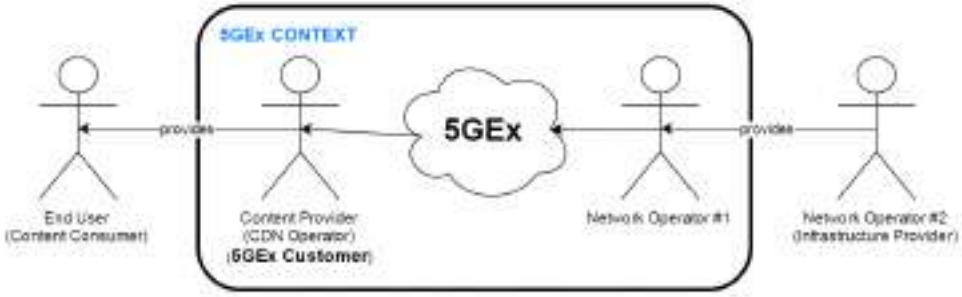
performance and the availability of the resources. By relying on ad-hoc designed tasks, a monitoring function is in charge also to activate and coordinate specific measurement devices ("probes") to retrieve the required information at resource level.

EoR modules can be partly realised by components provided by the ESCAPE orchestrator in the project UNIFY.

D Detailed description of a use case example: vCDN

Business driver	Nowadays, video and, in general, multimedia content is one of drivers of current capacity consumption in operational networks. Content distribution is expected to be the dominant contributor to the data traffic demand. CDNs are being more and more present in everyday life communications, therefore media sector is one the main verticals sector that should benefit from 5G.
Technical rationale	A Content Delivery Network (CDN) is a collection of servers that facilitate distribution of content in a network. Those servers duplicate content from the originating content provider. It allows reducing the distance that content travels, and also reduce the number of hops a data packet must make to deliver content. In this way, the result is less packet loss and optimised bandwidth and performance. The current use case refers to the provision of vCDN this is, vCaches as VNFs on different network infrastructures in a NFV Multidomain framework, instead of hardware content servers.
5GEx relevance /benefits	It is expected that a multi-domain (multi-operator) architecture combined with vCDN allows reducing the distance between network operator and the end-user increasing QoE in terms of reducing delay and packet loss, and optimizing bandwidth and performance, as well as facilitating the reconfiguration of the vCDN service. On the other hand, applying NFV to CDN, versus a traditional CDN, should imply an increase of flexibility thanks to the reconfiguration of the CDN service by means of re-scaling the vCaches instances.
Stakeholders (mapping to roles in the GARM)	The main stakeholders identified for this use case are the following: • End-user. The end-users are the content consumers. They request a multimedia streaming service to the content provider. • Content provider. It uses a vCDN to distribute its content based on end-users requests. • vCDN provider. The vCDN provider provides virtual caches where the content is stored and replicated across network operator's infrastructure. • Network operator 1. The network operator 1 provides network resources and orchestration to deploy the vCDN. This network operator can also be a cloud service provide. • Network operator 2. 5GEx has a multi-domain (multi-

operator) architecture. In case that the network operator 1 is far from the end-user or lacks enough network or infrastructure resources, operator 1 requests outsourcing infrastructure to other network operator as much close to the end-user as possible. This new operator 2 acts as an infrastructure provider.



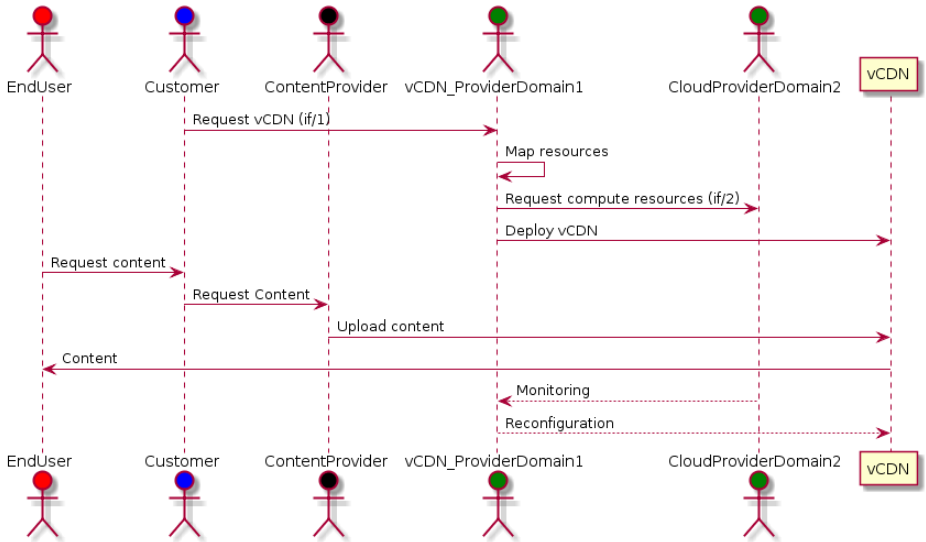
The mapping between the above identified stakeholders and the generic actor role model proposed in 5GEx is collected in the following table:

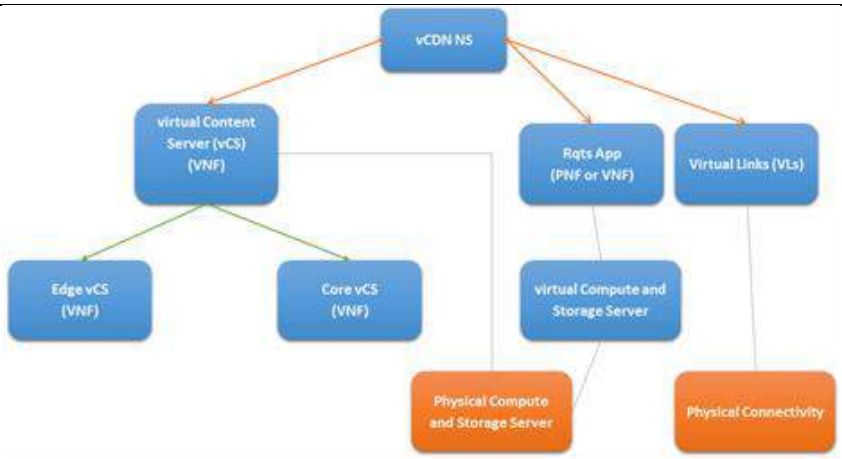
vCDN use case stakeholders	**GARM**
Content consumer	End User
Content Provider	CASP
vCDN Provider (Network Operator #1)	Online SP
Cloud Provider/Infrastructure Provider (Network Operator #2)	Infrastructure SP

Sequence of actions (high-level storyline)

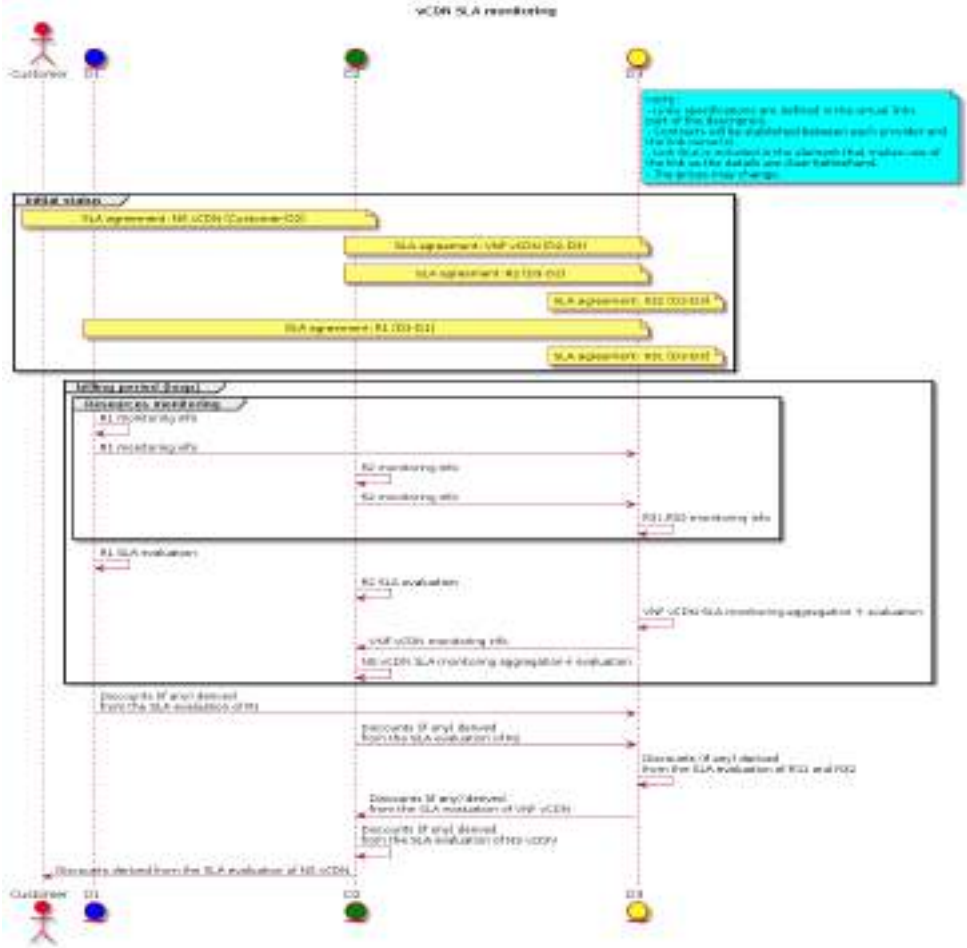
The coordination model chosen for this use case is Distributed/Hierarchical PULL model (see Section 3.6). The sequence of actions is the following:

1. It is assumed that service provider show a service catalogue for the content provider (customer) to ask for a vCDN to be deployed with specific SLA. The content provider certain level of configuration such indicating the vCaches locations in which the content needs to be replicated.
2. Service provider 1 is responsible for vCDN service provision. MdO – NFVO in domain 1 will map how many basic compute and storage nodes are required and instantiates, installs and configures them across

	other domains according to vCS location requirements and resources availability if needed. 3. When an end user content request arrives, the content will be served by the vCS closer to the end user in order to optimise perceived quality by means of reducing latency and packet drops. It could be the case that a content request is coming e.g from an end-user which is further from the operator 1's network than originally dimensioned and operator 1 is not able to achieve the agreed SLA (not enough resources). In that case the service can be reconfigured by the content provider (customer) and further outsourcing infrastructure to other network operator (infrastructure provider) closer to the end-user could be required by service provider 1. This is possible thanks to the virtualisation of the caches that can be easily moved through the NFVI in a multi-domain ecosystem. 4. Monitoring information will be collected continuously by domain 1 to if necessary reconfigure vCDN /reallocating resources to continuously meet the SLAs. 
Service decomposition	The vCDN use case is a particularisation of the VNFaaS use case family in which the Network Service is compose by several VNFs which are vCaches as well as a request management application that can be virtualised or not. This is depicted in the following figure:

<table>
<tr><td></td><td> 

Notes:
- Orange arrows denote aggregation.
- Green arrows denote inheritance.
- The various vCS are connected via VLs by means of a VNFFG which is not shown in this figure.</td></tr>
<tr><td><u>Interfaces requirements</u></td><td>The information identified to be exchange through the interfaces in the 5GEx architecture is the following:
• (If/1) B2C.
• (down) Catalogue request by the customer (content provider).
• (Up) Catalogue retrieve by the customer.
• (down) Service (vCDN) instantiation request + service configuration - > location of VNFs.
• (down) service (vCDN) reconfiguration.
• (up/down) Management/reconfiguration + Service URLs.
• (if/2) B2B
• Catalogue synchronisation for e2e service descriptions (I2-C)
• SLAs negotiation (I2-C).
• vCDN VNFs instantiation order + management (I2-F).
• vCS + Req. provisioning and deployment (I2-R).
• Inter-VNF communication (I2-R).
• Monitoring info + SLA evaluation results (I2-RMon).
• Monitoring info + SLA evaluation results (I2-FMon).
• (if/3)
• (down)Resource allocation order: VNF.
• (down) Provisioning and deployment (I3-R).
• (up) Monitoring collection.</td></tr>
</table>

SLA negotiation	The following diagram explains the SLA negotiation process among the several providers involved in the chain for this use case: 

Service description	The main pieces of information for the description of the service in the current use case are listed below, (separately in those two: the ones to be accessed by the customer, and those that should be used by the system to deploy/orchestrate the service):
	- Customer facing Service catalog items
	  - Values for KPIs (delay, loss) – SLA.
	  - Number of vCS (VNFFG).
	  - Level of flexibility – countries/regions coverage.
	  - Available locations.
	  - Management capabilities.
	  - Storage capacity.
	  - Pricing.
	- Service deployment template information NSD
	  - Values for KPIs.
	  - Virtual Links.
	  - Monitoring parameters.
	  - Reference to the VNFDs (for each vCS and reqs app)

	- For each VNFD
	  - KPIs – expected performance.
	  - Deployment flavours.
	  - Virtual resource requirements: %CPU, RAM, storage.

Evaluation (KPIs)	Virtual Service Deployment - Validate the VNFs chain in order to ensure the proper deployment of the service requested by the customer. - Measure the deployment time. CDN - Average delivery time (server response time): how fast the vCDN (most important component are the vCaches) will be delivering the files to your end users. - Throughput: rate of successful message delivery. - Bandwidth. Multidomain specific KPIs: - Verify the real acceleration of the content delivery due to using vCDN and several domains/operators. - Measure how long the operator takes to have another operator's network in order to deploy its content. - Measure how long it takes for the content provider to get vCaches where deploying its content. Dynamic vCDN Service Optimisation. vCaches could be artificially loaded with high volume of requests in order to: - Validate the response by re-scaling the vCache instance and/or reconfiguring the entire vCDN service. - Measure service reconfiguration time. - Measure service downtime during the reconfiguration. - Verify the gain in resource efficiency due to the dynamic adaptation.

E Reference message sequence charts of an example use case: vCDN

The message sequence chart in Figure A-10 represents the interactions among the 5GEx main architectural funtional blocks and actors in an example in which a vCDN service is deployed across 3 different domains in the way it is ilustrated in the following figure:

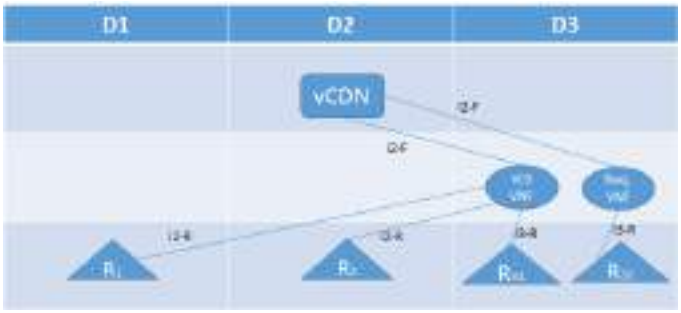


Figure A-9: Example of vCDN service deployed across 3 domains

- Provider in D2 offers a vCDN Network Service in its catalogue, whose VNFForwarding Graph (VNFFG) is composed by 4 VNFs: 3 vContent Servers (vCaches) and 1 Requests Management VNF).
- These VNFs are offered in the VNF catalogue of provider in domain 3. Each VNF is described including the resource requirements (VDUs) in which they should be deployed to operate at optimum performance.
- When the customer (content provider) purchases the vCDN service to provider in D2 he should be able to indicate (by means of service configuration process) up to certain level where he would like each VNF to be deployed: for each VNF, a list of possible locations (fulfilling the VDU requirements of each component) with different prices and SLA should be shown.
- One of the vCS could be deployed in a third domain (D1), so provider in domain 3 will ask for infrastructure resources to provider in domain 1. In the same way, other vCS could be deployed in D2. The third vCS could be deployed in D3 by means of I3-R.
- Req. VNF is deployed in D3.

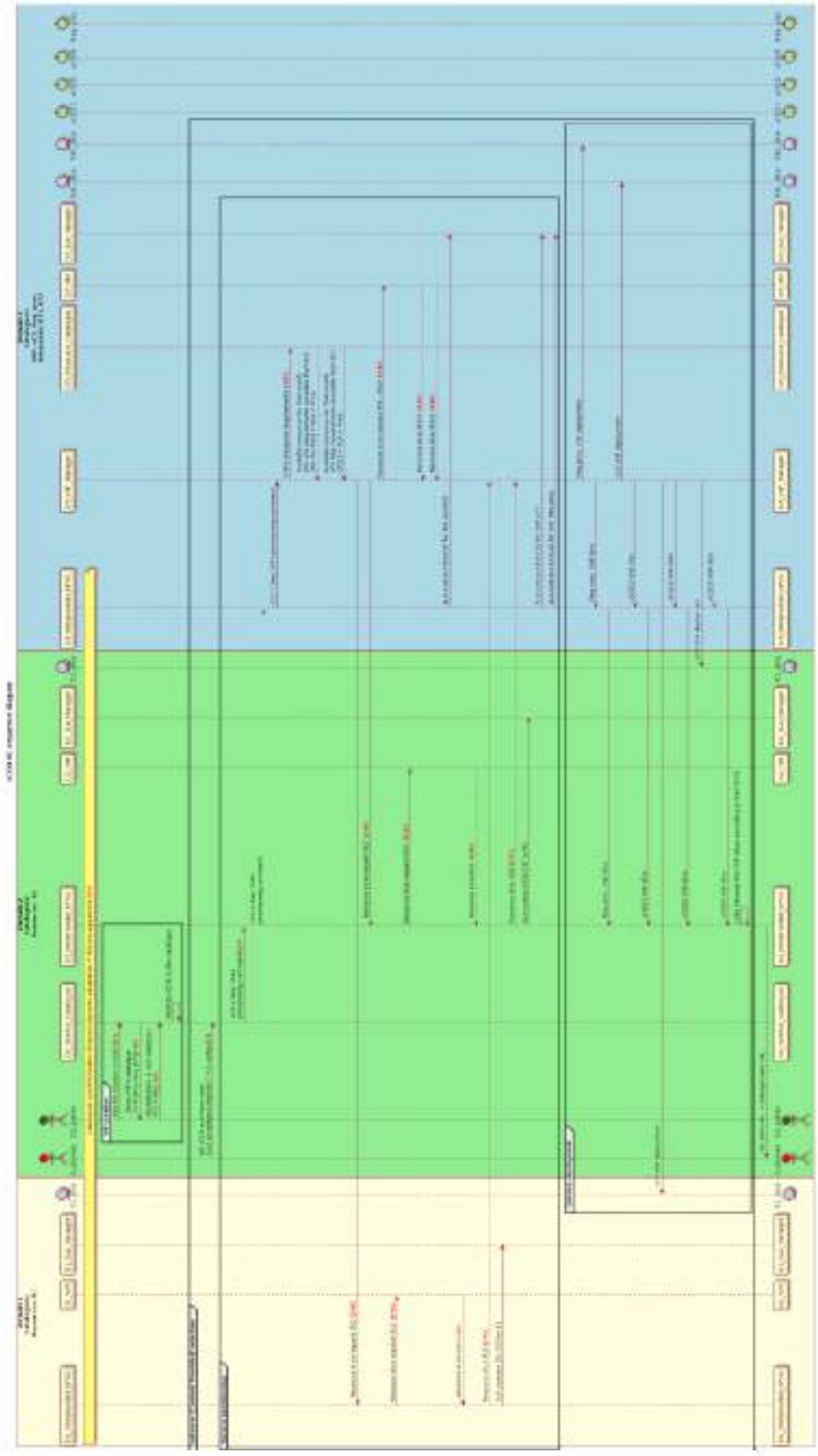


Figure A-10: Example vCDN sequence chart

F 5GEx Service Types and Information Services

The following is an overview and a listing of the services according to the service catalogue categories of Section 3.2. The listings of this Appendix reflect work in progress and are to be revised, elaborated and specified in detail in Deliverable D2.2.

A. Core ASQ connectivity infrastructure services (NSP-to-NSP, Interface 2)

1. Core ASQ Path Interconnection Services
    a. Single-NSP ASQ peering service (aka. PoI-to-Region service, region confined within the neighbour NSP, the NSP having the provider role)
    b. Multi-NSP ASQ peering service (aka. PoI-to-Region service)
    c. Core ASQ tunnel service
2. Core Enterprise ASQ Path Interconnection Services (includes support for VPN services)
    a. Enterprise ASQ tunnel service (consider both Enterprise and Datacenter)
    b. VPN related services
    c. PoI-2-Region service, specific to an upstream enterprise
3. VACS API Management Service
    a. Consumer VACS API Management Service
        i. One end-point is a consumer end-user end-point
        ii. Two end-points are consumer end-user end-points
        iii. Three or more end-points are consumer end-user end-points
    b. Enterprise VACS API Management Service
        i. Two end-points are enterprise end-points
        ii. Three or more end-points are enterprise end-points
    c. Machine Type VACS API Management Service

B. Core ASQ path information services (NSP-to-NSP, Interface 2)

1. Core ASQ path PoP-2-PoP capabilities information service (directory service)

C. Enterprise ASQ connectivity infrastructure services (NSP-to-Enterprise, Interface 1)

1. Enterprise ASQ Interconnection services, includes VPN services
    a. Enterprise ASQ Path Interconnection
        i. Point of Enterprise Interconnect to Region
        ii. Enterprise ASQ tunnel
    b. Enterprise VACS API Management Service ASQ connectivity between two Enterprise sites, on-top-of the Enterprise ASQ Interconnection services
2. Consumer VACS API Management Service (NSP-2-OSP)

D. Value Added Connectivity Session (VACS) services

1. VACS invocation and handling (NSP-2-NSP, **Interface 2**)
    a. For invocation and handling of Consumer VACS service
    b. For invocation and handling of Enterprise VACS service
2. VACS invocation and handling (NSP-2-OSP, **Interface 1**)
    a. For invocation and handling of Consumer VACS service
3. VACS invocation and handling (NSP-2-Enterprise, **Interface 1**)
    a. For invocation and handling of Enterprise VACS service

E. ASQ connectivity Supporting Information services

1. "ASQ connectivity Ping"
2. "ASQ connectivity (Media) TraceRoute"

F. Telco Cloud Infrastructure services

1. NFV IaaS (Resource Slice as a Service - RSaaS)
    a. Single Datacentre location
    b. Multi-Datacentre locations
    c. Bundled with ASQ connectivity

G. Virtual Network Function services

2. VNFaaS (Network Service Slice as a Service – NSaaS)
    a. Single Datacentre location
    b. Multi-Datacentre locations
    c. Bundled with ASQ connectivity