Afolabi, I., Ksentini, A., Bagaa, M., Taleb, T., Corici, M. et Nakao, A. (2017). Towards 5G network slicing over multiple-domains. IEICE Transactions on Communications (Vol. E100B, p. 1992-2006).
doi: 10.1587/transcom.2016NNI0002. © 2017 The Institute of Electronics, Information and Communication Engineers

INVITED PAPER *Special Section on Network Virtualization, Network Softwarization, and Fusion Platform of Computing and Networking*

Towards 5G Network Slicing over Multiple-Domains

Ibrahim AFOLABI[†a)], **Adlen KSENTINI**[††b)], **Miloud BAGAA**[†c)], **Tarik TALEB**[†,†††d)], **Marius CORICI**[††††e)], ***Nonmembers***, ***and*** **Akihiro NAKAO**[†††††f)], ***Senior Member***

SUMMARY One of the key objectives of 5G is to evolve the current mobile network architecture from "one-fit-all" design model to a more customized and dynamically scaling one that enables the deployment of parallel systems, tailored to the service requirements on top of a shared infrastructure. Indeed, the envisioned 5G services may require different needs in terms of capacity, latency, bandwidth, reliability and security, which cannot be efficiently sustained by the same network infrastructure. Coming to address these customization challenges, network softwarization expressed through Software Defined Networking (SDN) programmable network infrastructures, Network Function Virtualization (NFV) running network functions as software and cloud computing flexibility paradigms, is seen as a possible panacea to addressing the variations in the network requirements posed by the 5G use cases. This will enable network flexibility and programmability, allow the creation and lifecycle management of virtual network slices tailored to the needs of 5G verticals expressed in the form of Mobile Virtual Network Operators (MVNOs) for automotive, eHealth, massive IoT, massive multimedia broadband. In this vein, this paper introduces a potential 5G architecture that enables the orchestration, instantiation and management of end-to-end network slices over multiple administrative and technological domains. The architecture is described from both the management and the service perspective, underlining the common functionality as well as how the response to the diversified service requirements can be achieved through proper software network components development.

key words: *softwarization, NFV, SDN, cloud computing, orchestration, multi-domain*

1. Introduction

5G systems are expected to build a mobile network architecture that supports not only classic mobile broadband applications but also specific vertical industry services, such as those of automotive systems, e-health, public safety, and smart grid which previously were supported through private dedicated networks. Vertical services require different and incompatible performance parameter levels, which are difficult to achieve using the same physical infrastructure. For instance, automotive systems require high reliability added to low latency access to remote servers, public safety services need ultra-reliable and highly available system, while enhanced broadband access services require high bandwidth covering a dense area and massive IoT requires the cost efficient connection of a huge number of devices. Consequently, the envisioned 5G systems would need to re-architect the current uniform mobile architecture to allow multiple, logical, self-contained networks on a common physical infrastructure platform enabling a flexible stakeholder ecosystem that allows technical and business innovation integrating network and cloud resources into a programmable, software-oriented network environment.

Meanwhile, 5G systems should support a flexible and on-demand provisioning of network resources, network functions and applications, using a virtual resources layer spanning on top of physical resources of multiple domains. This will enable value added creation for vertical segments that would receive a wide area network support while being cost effective through the transition from dedicated networks to common cloud resources that can be used in an isolated, disjunctive or shared manner allowing customizable network operation. Finally, 5G is anticipated to shift the conventional networking paradigm away from the 4G mobile broadband ideal, wherein a single architecture fits all services, towards sliced network instances using as much as possible the same software components, however tailored to address particular service needs, maintaining in this way a truly differentiated service provisioning.

In this context, network softwerization, based on Software Defined Networking (SDN) and Network Function Virtualization (NFV), represents the enabling way towards 5G; allowing the creation of virtual network flavours customized towards the service requirements. In this light, an efficient integration of SDN and NFV within cloud computing ensures multiple advantages in terms of network configuration, flexibility, scalability, and elasticity, which are highly needed to build the dedicated slices concept next to the usage of the same physical resources for the multiple dedicated networks. Generally speaking, a mobile network slice is composed of a number of Virtual Network Functions (VNF) chained together and connected to at least one Radio Access Technology (RAT) to deliver a complete mobile network functionality, customized to suit the particular requirements of a

Manuscript received April 10, 2017.
Manuscript publicized May 16, 2017.

[†]The authors are with the Communications and Networking Department, Aalto University, Finland.
[††]The author is with the Communication Systems, EURECOM, Sophia-Antipolis, France.
[†††]The author is with Sejong University, Seoul, South Korea.
[††††]The author is with the Fraunhofer FOKUS Institute, Fraunhofer, Germany.
[†††††]The author is with The University of Tokyo, Tokyo, 113-0033 Japan.
a) E-mail: ibrahim.afolabi@aalto.fi
b) E-mail: adlen.ksentini@eurecom.fr
c) E-mail: miloud.bagaa@aalto.fi
d) E-mail: talebtarik@ieee.org
e) E-mail: marius-iulian.corici@fokus.fraunhofer.de
f) E-mail: nakao@nakao-lab.org
DOI: 10.1587/transcom.2016NNI0002

Copyright © 2017 The Institute of Electronics, Information and Communication Engineers

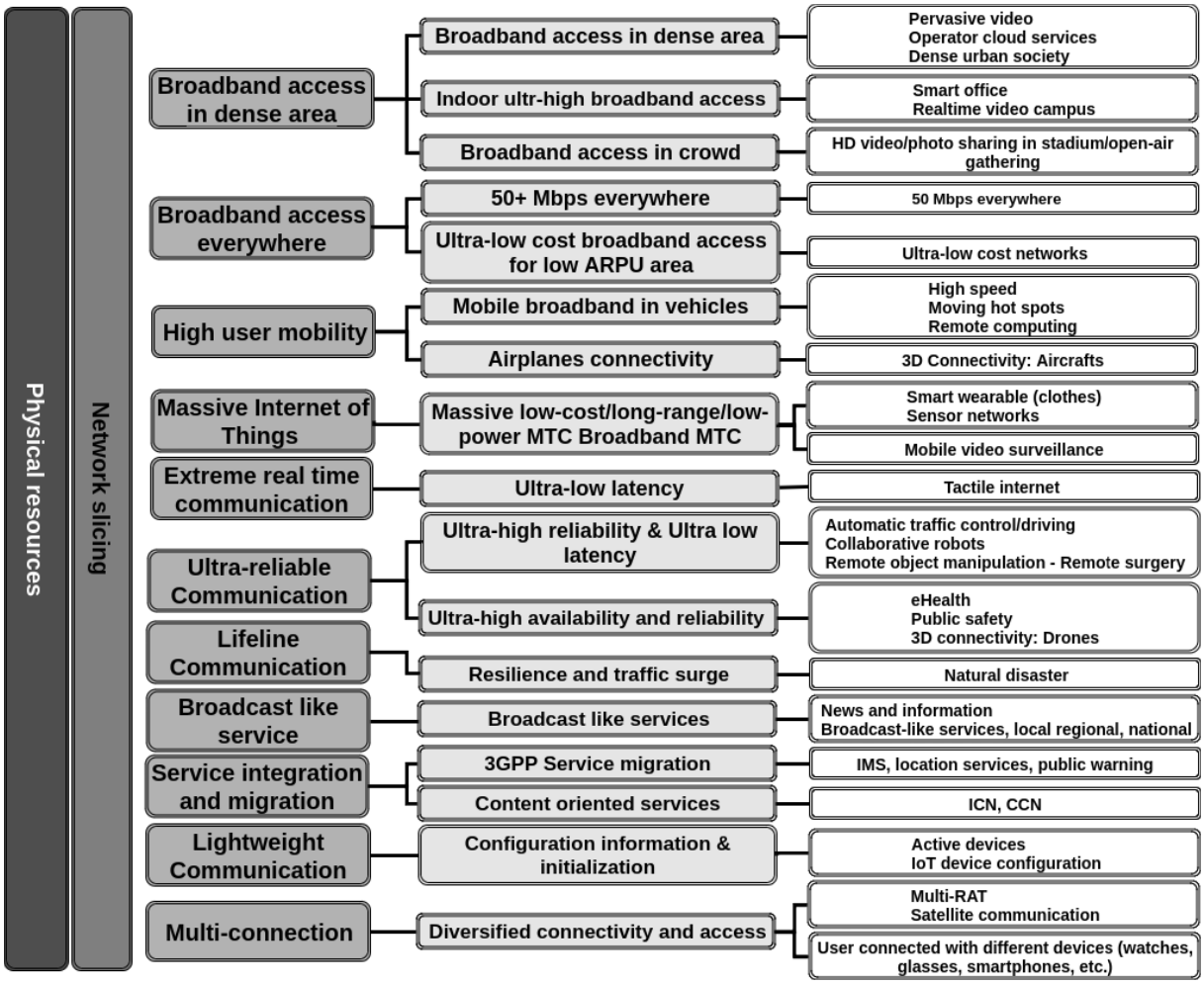


Fig. 1 Use-cases family and category per 3GPP and NGMN [4].

service. The VNFs cover both the Control plane and User plane functions of the Core Network components (e.g. Mobility Management, Authentication, Forwarding, etc.) and the Radio Access Network (RAN) (e.g. Optimal splitting, PDCP-C, PDCP-U, etc.) and may include application specific enablers. Moreover, the VNFs may also include authorized legal Deep Packet Inspection (DPI), Firewall and caching functions and storage resources as well as application specific enablers up to even applications.

The concept of Network Slicing is not new, and found its foundation in the Infrastructure as a Service (IaaS) cloud computing model and overlay networks. In the IaaS model, the aim behind network slicing is to share a computing, networking and storage infrastructure between different tenants, in order to build a self-contained virtual network infrastructure with a required level of isolation. A Network slice is composed of different virtual machines (VMs) connected together on a Virtual network enabled by using Virtual LAN (VLAN) technology in a system setup where the VMs are in the same Data Center (DC); or VLAN and tunneling protocol, like Generic Routing Encapsulation (GRE) and VxLAN (x: extended) in a system setup where the VMs are hosted on different DCs.

The network slices may sometimes require conflicting performance requirements. For example, a slice may require low latency, high bandwidth and high mobility, but would not care about reliability, such as slices for enhanced Mobile Broadband services (eMBB). Another slice may require low latency, high reliability and high traffic density but would not care about the bandwidth such are for Critical Communications (CriC) or others may require efficient communication and high traffic density but would neither care about reliability nor bandwidth such as the massive IoT [3]. These slice flavours may have to be deployed across a multi-domain environment consisting of a mixture of dedicated and shared slices, for this reason, advanced orchestration mechanisms should be explored to enable an elastic allocation of resources in an efficient manner over multiple domains.

In this paper, we present the vision of the 5G!Pagoda project for enabling network slicing for 5G systems. The proposed 5G!Pagoda architecture takes the concept of mobile networking a major leap forward, whereby slices of virtual mobile networks are created on-demand and customized according to the changing needs of mobile services, using

physical resources across multiple domains. Our proposed 5G!Pagoda architecture leverages the ETSI NFV architecture to cover the orchestration of physical resources across multiple domains.

The remaining of this paper is organized as follows. Section 2 presents the concept of network slicing and representative architecture enabling network slicing. Section 3 dissects the network slice requirements as seen by the 5G!Pagoda project. Section 4 details the 5G!Pagoda network architecture featuring network slicing over multiple domains followed by conclusions and next steps in Sect. 5.

2. Background on Network Slicing

2.1 Network Slicing Concept

In addition to cloud computing, the concept of slice in networking was also used in the overlay network research efforts, such as PlanetLab [1], where a network slice has been defined as an isolated set of network resources such as bandwidth, computational functions, storage capacity allocated for a group of users that "program" network functions and services over their overlay network overlaid across "the planet". The concept follows the Slice Federation Architecture [22] used in the large scale GENI federation between the US research institutions. Since then, various network virtualization testbed efforts such as PlanetLab EU, PlanetLab JP, VNode, FLARE [2], Fed4Fire, have inherited the concept of slices as a basis of the infrastructures, as a set of programmable resources to create new network services and protocols. Network slicing in 5G shares some concepts with the cloud computing and overlay network, but it requires more management and orchestration procedures as well as adaptation to the mobile network characteristics, such as mobility, wireless changing resources, fronthaul capacity e.t.c.

Network slicing in 5G has risen from the need to leverage the current 4G LTE architecture shown in Fig. 2, in order to accommodate vertical industries (e.g. automotive systems, smart grid, and public safety) and IoT-based services. These services have been described in the form of use-cases by the 3GPP [3], [4]. Figure 1 summarizes the 5G system use-cases defined by 3GPP and NGMN. The 5G system use-cases are grouped into families, and each family includes one or more categories. Network slicing is involved in all the use-cases, as it is indispensable to enable all these use-cases concurrently over the shared physical infrastructure. Aiming at grouping the 5G use-cases in services, the METIS-II

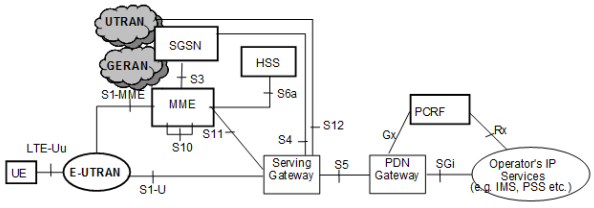


Fig. 2 Legacy 4G architecture [10].

project[5] classifies the most representative 5G system use-cases according to their constraints. It shall be noted that the way of grouping 5G system use-cases has been later adopted by the 5GPPP document [6] on 5G system. METIS-II assumes that most representative 5G services may be classified in one of the following categories:

- Extreme or Enhanced Mobile Broadband (eMBB) type, which requires both high data rates and low latency in some areas, and reliable broadband access over large areas. For example, dense urban areas require high bandwidth as users may upload HD video to their preferred social network application and also low latency because they may use Virtual Reality (VR), remote video presence and Augmented Reality (AR) streaming.
- Massive Machine Type Communication (mMTC) type, which needs efficient and reliable wireless connectivity for massive deployment of sometimes resource constraint devices. An example of this type of service is the deployment of a large number of sensors and actuators (over a million devices per square kilometers) to monitor or control a given area.
- Ultra-reliable and low-latency communications (uRLLC) or ultra-reliable MTC, which covers all services requiring ultra-low latency connections. Notable examples include industrial control systems, real time control of vehicle and traffic, and public safety scenarios.

It is worth noting that other SDO bodies, like 5GMF, has also defined 5G use-cases. In [7], 13 usage scenarios have been studied and expected to be realized in 5G mobile networks. They have been categorized into four facets; 1) Entertainment, 2) Transportation, 3) Industries/Verticals, and 4) Emergency and disaster relief ultimately giving a connected device perspective which spans across the three previous use cases combining multiple applications and services from each into a comprehensive service offering.

2.2 Existing Network Slicing Architectures

Obviously, the current "one-fits-all" network architecture is not efficient to support the different needs of 5G services, in terms of latency, bandwidth and reliability, especially because the different service classes are expanding on the direction of one specific requirement (more capacity, more devices connected and low latency) in the detriment of the others. Enabling network slicing in mobile networks, and building network slices tailored to each service, represent one of the solutions towards supporting 5G services. In this context, several 5G initiatives from industry and academia alike have been proposing a new mobile network architecture, featuring network slicing; mainly based on Software Defined Networking (SDN), Network Function Virtualization (NFV) and cloud computing.

In the 5GNorma project [8] funded by the European Commission, a new programmable and flexible mobile architecture is proposed. The aim is to enable multi-tenancy over a shared physical infrastructure, and hence network

slicing. To this end, the 5GNorma introduces three enabling functional blocks: Software Defined for Mobile networks (SDM)-Orchestrator(O), SDM-Control(C) and SDM-X (Coordinator). SDM-O interfaces the network slice infrastructure to the business domain. The SDM-O handles the slice creation, and translates the slice requirements to network resources in terms of Virtual Network Functions (VNF) and Physical Network Functions (PNF). The SDM-O places and orchestrates the VNFs in the networks, since the SDM-O has a complete view of the network. The resources assigned to a network slice are managed by the SDM-C. The SDM-C builds the forwarding paths used among VNFs and PNFs, while sustaining and managing the constraints and requirements defined by the SDM-O. The SDM-C is also monitoring the slice resources, in case of QoS degradation. The SDM-C is also allowed to request more resources from the SDM-O in a situation where the resources allocated to a slice is not enough to meet its desired level of QoS. While SDM-O is in charge of scaling up and down of the slice specific resources (i.e. compute, storage, transport), the SDN-X is in charge of scaling up and down shared resources among slices (e.g. radio resources).

In [9] 3GPP has provided first analysis of the implications arising from network slicing, without including the RAN. While the RAN remains as a common network segment that includes a new element for slice identification and selection, the Core Network (CN) slicing will be based on the eDECOR [11] model. In the latter the CN instances (slices) are connected to the shared RAN using the classical S1 interfaces. The eNodeB is able to steer the slice traffic to the correct CN instances using the slice ID communicated by the UE during the Radio Resource Control (RRC) procedure. The slice ID could be hard encoded in the UE (i.e. USIM) or encoded through the Public Land Mobile Network (PLMN). In case the devices come without a slice ID, a redirect mechanism was added to the 4G Evolved Packet Core architecture [10] in which a first MME makes the authentication and authorization of the UE and based on the authorization redirects the request to the appropriate MME for further operations.

Therefore, a mobile network slice is basically made up of VNFs of a CN and a RAN connected together to form a fully functioning substrate of a mobile network enabled by the NFV technology. The ETSI NFV architecture has not only introduced a dynamic construct of an NF forwarding graph which aids a flexible NF deployment and dynamic network operation, it has also standardized the concept by defining three major operational domains, namely [23]: (1) VNFs - this operational domain covers the network functions implemented in softwares deployed to run on virtual platforms with an underlying physical infrastructure, (2) NFV Infrastructure - this domain consists of both the physical and virtualized network resources on which the VNFs are running, (3) NFV Management and Orchestration - this operational domain is responsible for the management of all virtualization-specific functions in the NFV architecture, from the life-cycle management of the VNFs to the orchestration and management of the network resources.

Assuming that a network slice is a composition of physical and virtual resources, which might be instantiated over multiple domains, the 5GEx funded EU project [12] has proposed a new architecture extending the concept of ETSI NFV architecture to cover multiple domains. The new architecture is composed of three layers: Resource domain, single domain resource and multi-domain resource. The resource domain represents the lower layer of the architecture. It exposes domain resources to the single domain orchestration layer via specific interfaces. According to 5GEx, a domain may refer to a technological domain or operator domain. The single domain orchestration layer, the middle layer, includes the domain specific orchestrator, which performs resource and service orchestration of a specific domain using the interfaces exposed by the domain resource layer. Domain specific orchestrator are using interfaces to communicate and coordinate. The top layer of the architecture is the multi-domain orchestration, which includes the multi-domain orchestrator. Each multi-domain orchestrator is connected with one or multiple single-domain orchestrator, and managed by the Orchestrator Admin Domain using business-to-business (b2b) interface. Moreover, the multi-domain orchestrator are connected to other multi-domain orchestrators using the same b2b interface. Finally, the Multi-domain orchestrator exposes a customer-to-business (c2b) interface to consumers.

3. 5G!Pagoda Project's Network Slicing Overview

To build an end-to-end network slicing, two significant aspects are required. First, we need to carefully define an end-to-end network slice from UE to cloud data centers using programmable resources per application service. This means that there is a need to enable dynamic creation, modification, maintenance and disposing of network slice(s) to serve user's needs from the radio access to the packet core networks. The slice creation technique has to be meticulously planed and coordinated especially across fixed networks and radio boundaries, i.e. the so called mobile packet core slicing and RAN (Radio Access Network) slicing. Each network slice is made up of a virtualized air-interface, radio access network and mobile packet core network, and transport network combined. Second, in order to support various 5G network applications and service requirements, as well as legacy information networking services, a viable slice architecture should manage and operate a large number of slices in a scalable, dynamic and on-demand, and reliable manner. Such kind of slice instantiation, maintenance and termination capabilities would strongly require the establishment of a highly sophisticated distributed processing scheme and "deeply programmable" E2E networking. In what follows, we describe the network slice requirements as dissected and assimilated in the 5G!Pagoda project.

3.1 Slice Template and Orchestration Overview

As stated earlier, a slice offers a dedicated full network system needed to serve an application, similar to what a current network is offering, replicated and customized as best as possible to satisfy the requirement needs of the connected UEs. For this reason, a slice has to include all the functionalities which are currently available in a physical network e.g. a 4G mobile network. Additionally, as the different slice components are implemented in software on top of common hardware resources, a set of optimizations are considered, especially by adding the flexibility and dynamicity made available by SDN and NFV to the system.

Basically, the underlying high-level functionalities for all the network slices are similar, therefore, the main differences would be in the customization and parametrization of each slice instance to serve a specific application need efficiently. As a result, all the slices can be implemented following our proposed slice template, as illustrated in Fig. 3. On top of a set of common resources, a Data / User Plane is implemented enabling the communication of information between end devices and a network slice, as well as within a network slice. The Data/User Plane is controlled by a separate Control Plane, following the principles of carrier-grade telecom networks enabled through the use of SDN technology whose potential challenges has already been examined and addressed in [20]. Immediately above both the Control and User Plane, there is a Service plane which is established with different application enablers in order to offer the appropriate connectivity service to the specific application(s) using the network slice. Below the End-to-end Applications plane and Next to the Service, Control and Resources planes is the management plane, which controls and manages the appropriate operations of all the other planes and their resources. Considering the latest technological advancements in telecommunication and networking, the control and data/user plane would be implemented following the SDN principles while all the connectivity layers would follow the translation of physical network functions to software modules running on top of a common hardware (generically named softwarization), a principle proposed by ETSI NFV.

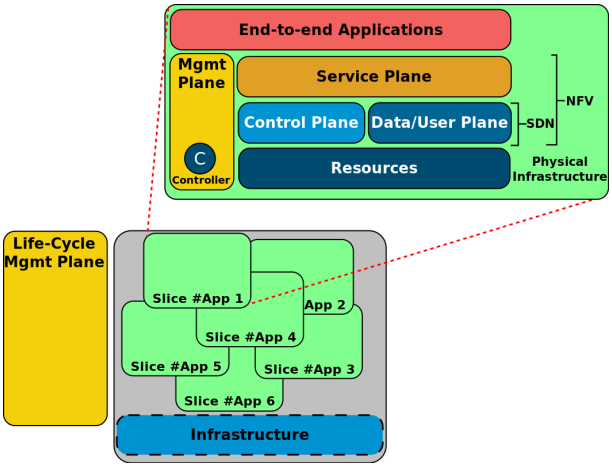


Fig. 3 5G slice template and instantiated slices on top of a common infrastructure.

A network slice is expected to include all the network components such as a RAN, a transport and a core network, application enablers (e.g., video streaming optimizer) and the applications themselves as well as the management for these technology domains which is necessary to provide a specific service to the end customers. However, in order to optimize the network slice functionality, some of the classical network components may be shared using the current network sharing system (without software customization) and not be included in a network slice. For example, the RAN could be shared between multiple slices thereby making a network slice to only include the rest of the components (e.g., core network components and packet data network components–caches, servers, etc.).

Since multiple slices are deployed on top of virtual resources, there is a need to introduce a new capability to operate multiple slices, as a life-cycle orchestration, this functionality is being described in this subsection. As illustrated in Fig. 2, different 5G slices are instantiated and are running in parallel and in isolation on top of the same infrastructure. An infrastructure may be operated and managed by single telecom operator or may consist of multiple sub-infrastructures operated by multiple operators and providers (for instance, telecom operators, MVNOs, cloud providers etc.). This allows the deployment of various types of slices, which are deployed on top of different infrastructural configurations made possible mainly due to the fact that the slices are running on virtualized isolated environment dedicated to serve the need of a particular service.

As the resources are virtualized, the slices can receive dynamic resources during their runtime as well as different resources placement, through this, the infrastructure becomes more flexible and available in a different combination on demand and flavours. Bearing the flexibility and dynamicity of the system in mind, the life-cycle orchestration of network slices is not only able to deploy a network slice according to the specific configuration needs of the slice, but also is able to adapt the network slice to different usage conditions based on the behaviour of the slice users. In addition, the network slice can evolve to accommodate exceptional network situations based on for instance, the available network resources, unexpected fault detection and management, performance optimization and possible network security compromise. All these functionalities have to be covered by a new set of functional elements (especially, to differentiate from the internal management plane operations which are specific and private to each network slice), generally named life-cycle orchestration in this specification.

3.2 Multi-Domain Slicing System

The resources are seen separated per technology domains depending on the technology type (Fig. 4):

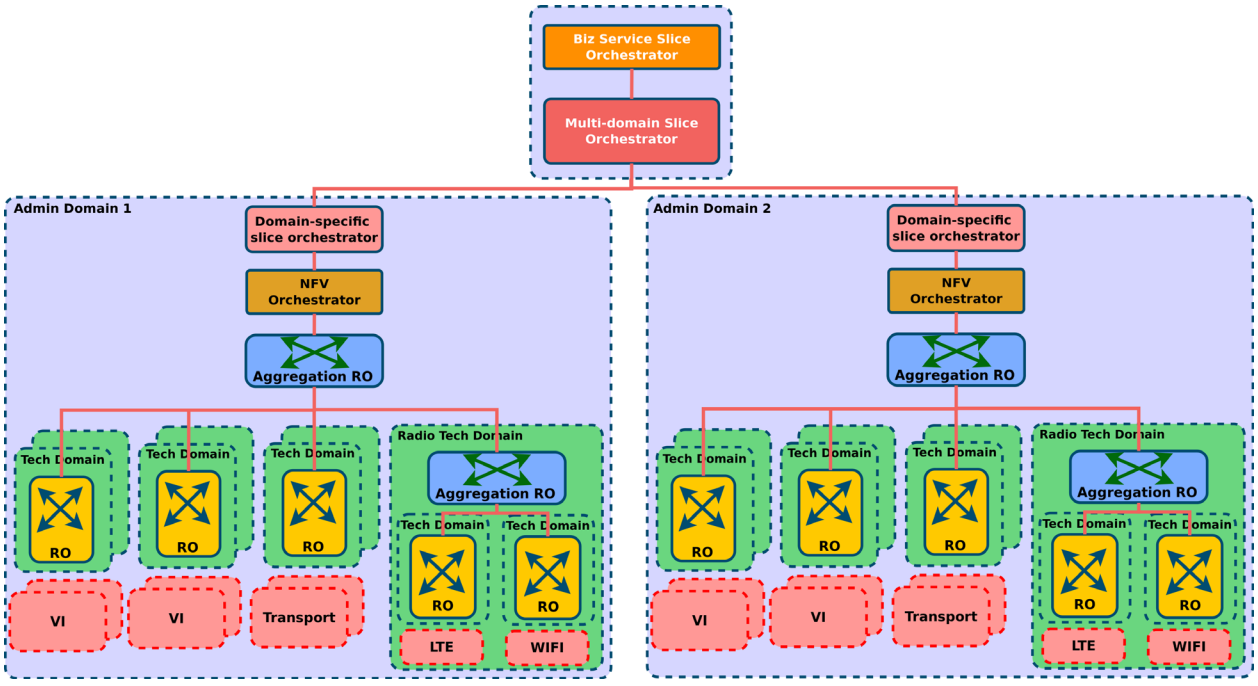


Fig. 4 Recursive resource orchestration.

- Virtualization Infrastructure (VI) is consisting of all the nodes which are offering compute and storage resources as well as the networking to interconnect these resources. Examples of VI include data centres and edge compute units.
- Radio - represents the radio resources in terms of spectrum and allocable spectrum areas and the allocation of the communication channels within the spectrum.
- Transport - consists of the networks which interconnect the VIs and the radio resources within the same or in different administrative domains.

Each of the technology domains has its own Resource Orchestration (RO). We argue this choice by the different structures of the resources, which from the perspective of their respective specifications, should be handled by separate ROs, each specific to a technology domain. It is foreseen that for example, for the transport network, an SDN WAN controller will act as the RO while for a data centre, a typical VI Manager (VIM) (e.g., OpenStack) from the perspective of ETSI Management and Orchestration (MANO) may be used. To be able to use the resources in an appropriate manner across the administrative domain, an administrative domain resource orchestrator (RO), named Aggregation RO is considered on top of the technology specific ROs. The Aggregation RO will aggregate all the resources into the same RO, through this operation, the network resources will become transparent to the domain-specific slice orchestrator. This aggregator RO can be seen as a hierarchical type of resource aggregation, mainly for efficient deployment of the system. For example, in Fig. 4, an Aggregation RO can be considered for the radio technology domain across the different technologies and spectrum used. Please note that the resources of the different administrative domains may be interleaved as in the case where one domain handles the data centers located on the connectivity path while other administrative domains handle the connectivity between the data centers.

Another reason for introducing the additional Aggregation RO is to have an overview of all the resources inside an administrative domain in order to place VNFs and create related NFFG (Network Function Forwarding Graph) across different resources (including multiple data centers, transport, different wireless accesses) efficiently. The underlying reasons for this architecture are manifold. Primarily, with the global view of all the resources inside an administrative domain, the global RO can best place VNFs with optimum usage of the underlying resources according to VNF's requirement. Such requirement could for example be affiliation between NFs and special hardware requirements.

Besides, inside an administrative domain, the environment could be multi-technology as well as multi-vendor, but a network slice orchestration would always follow exactly the same set of procedure. Such recursive orchestration procedure enables clear separation of each domain's responsibilities, facilitates reliability and manages scalability within the administrative domain. It also enables the enforcement of different policies in each domain. The domain specific slice orchestrator is in charge of end-to-end orchestration with the interaction of the global RO. In this case, the domain specific slice orchestrator is similar to NFV Orchestrator (NFVO) defined by ETSI MANO but with additional functions required to interact with the multi-domain slice orchestrator. For example, the northbound APIs for communicating with the multi-domain slice orchestrator. The entity which is handling the end-to-end orchestration has to be able

to collect and transmit the contact points which enable the interconnection with other administrative domains. The information may include IP addresses within the technology domains use in connecting different technologies from different administrative domains, IP addresses used to bound virtual networks from one domain to another, technologies of the virtual networks binding the two domains and VNF level IP addresses. In case the slice network is explicitly distributed across the domains (IP addresses are allocated in the slice based on a common addressing schema which is done through the orchestration as in the case of any PaaS or SaaS and not for IaaS where only resources are allocated and the tenant has to create the network through its own administrative means) the VNF level IP addresses can still be collected and transmitted. To be able to broker and to bind resources within multiple administrative domains, a multi-domain slice orchestrator is introduced into the system. The multi-domain slice orchestrator is communicating with the orchestrator in the administrative domains to be able to stitch a slice across the multiple administrative domains, by using resources allocated in each of them. A business service slice orchestrator is added in the logical multi-domain management to be able to interact with the administrator of the slice in the management of the life-cycle operations as well as to offer the administrative entry points to the software elements from which the slice is composed of.

4. Network Slicing Architecture

To address the above-mentioned requirements in section II, and enable the multi-slice concept, a set of high level architectural reference models are proposed as shown in Figs. 4 and 5. Depending on the perspective towards the system, the orchestration architecture, whereby the specifics of the service deployed in the multi-slice architecture are transparent (i.e., it can work for any type of slice) and the slice architecture, wherein the wholistic functionality within the slice template is detailed towards the appropriate functionalities for each of the features are presented. The two solutions are detailed in the following subsections, including the functional definition of the network elements.

4.1 Slice Architecture

The slice architecture includes all the components that compose the network of virtual network functions within the network slice. The proposed slice architecture is illustrated in Fig. 5 and follows the slice template model described in the previous Sect. 3. From the perspective of the slice administrator, the slice represents a complete virtual network, thus, it is a transpose of the current physical network towards the virtual environment. However, the slice architecture has to account for the underlying differences when compared to a physical infrastructure. Therefore, new functional features are added to them in order to form the basis for new benefits in running fully softwarized networks. This type of network slice architecture will perfectly support the idea propagated by the ANYthing As A Service (ANYaaS) [15] concept whereby a service orchestrator which is capable of delivering services such as dynamic video caching, traffic offloading, light-weight machine type communication EPC on-demand all at the same time is discussed. The slice is running on top of virtual resources (virtual computing, virtual storage, virtual networking and virtual radio) which are acquired on demand through the orchestration architecture. Different from the physical architecture, the resources are varying in time and in place, thus making the slice flexible in terms of capacity and deployment needs. The deployment of a completely virtualized mobile network component (for example, the evolved packet core (EPC) as a service in the cloud has already been evaluated and different deployment options proposed in [18] and a light-weight EPC for MTC in [19]) is no longer new, but developing a high-level template architecture which has all of the VNFs to support any of the slice use-case groups at any particular point in time to enable the deployment of a complete network slice in our opinion is state of the art. For the data/user plane within the slice, a set of components are considered including:

- Data storage and processing components,
- Data plane components related to the connectivity (e.g., Serving Gateway User Plane - SGW-U, Packet Data Network Gateway User Plane - PGW-U),
- Data plane components related to the content routing and storage (e.g., Information-Centric Networking - ICN, Content Delivery Network - CDN), and
- Deep data plane programmed components.

With these, the slice accounts for the possibility to carry out processing of the data directly at the data path, which is mainly possible due to the virtualization of the resources. Moreso, the fact that the slice does not require a separation of the work-flow towards other Apps in the service plane as in the current architecture is an additional benefit. For the control plane within the slice, a set of additional components are considered, providing the connectivity and data control for the specific data plane. It includes functionality for:

- Control of data storage and processing components,
- Control of connectivity related components (HSS, MME, SGW-C, PGW-C),
- Control of forwarding plane (routing and forwarding control), and
- Control of the apps deployed at the data plane level.

In the service plane, a set of Apps (i.e. Application Servers in 3GPP terminology) are deployed enabling the specific service deployment. For managing the slice (this including all the layers of the service), a set of components have to be deployed:

- Slice O&M [13] - the slice operations and management have as main functionality the installation of the specific slice functionality and its maintenance. For the installation related operations, the slice O&M should be able to request on-demand the addition of a new network

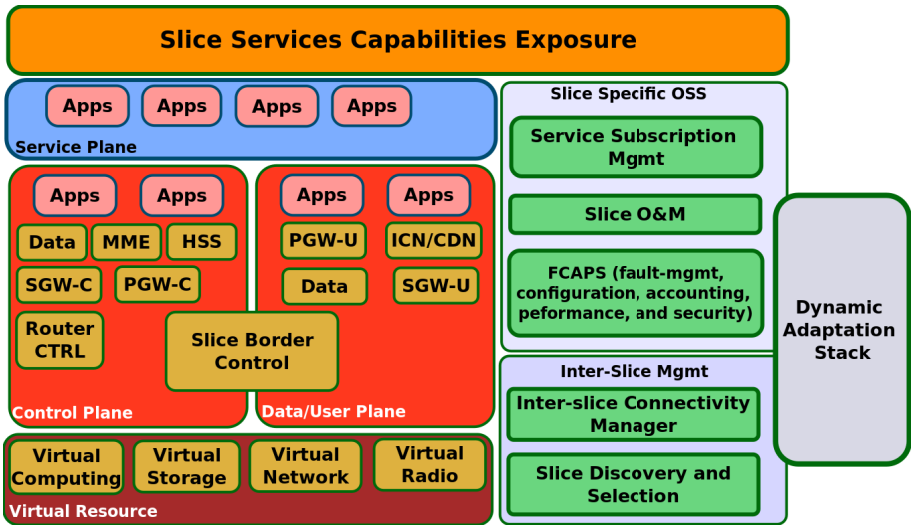


Fig. 5 Slice high-level architecture.

function to a running slice (e.g. the addition of a new firewall) in case it is needed based on the information available in the service catalogue and by addressing a momentary communication need. For the maintenance part, the system has to be able to support continuous integration and replacement of network functions with one that offers better functionality (resulting probably in more complex function descriptors) or an entirely new version. Within the NFV environment, a large part of the O&M can be automated under the supervision of the slice administrator. Additionally, O&M is strictly related to the service, hence, less of the operations are generic. For this reason, the slice O&M cannot be centralized in the MANO stack.

- Slice FCAPS (Fault Management, Configuration, Accounting, Performance and Security)[14]–the FCAPS represents the main management functionality of the system. Based on the monitored information coming from the different components and from the infrastructure, the FCAPS system has to provide the appropriate decisions in order to maintain the slice at the appropriate functioning parameters. It includes the following high level functionalities:
  - Fault management - fault monitoring, correction, detection and mitigation actions including failures at the network function level as well as failures in the functioning of the different components.
  - Configuration - including the specific functioning policies and adapted policies which flexibly change depending on the scaling of the service, beyond the simple configurations provided by the VNF Manager (VNFM)
  - Accounting - gathering usage statistics of the slice
  - Performance - gathering network monitored information, making decisions and enforcing them on the components themselves as well as towards the NFVO in order to be able to maintain the expected service level for the users
  - Security - defining the authentication and the encryption mechanism as well as the access control (firewall) rules for the system and adapting them according to the flexibility of the system as well as changing the network topology in case of threats (e.g. pushing towards sandbox networks users which are perceived as possible threats).
- Subscriber configuration management–one specific type of configuration is related to the subscription profiles. Although it is not foreseen that the subscription profiles will be frequently modified during the runtime of the slice, however, two major operating strategies have to be considered:
  - Completing the database information for authentication, authorization and access control rules (i.e. the subscription profile) for all the users at the deployment of the slice; this highly depends on the number of users projected to connect as well as on a possible previous completed database with such subscription profiles.
  - Adding new subscription profiles during runtime on-demand.

Furthermore, it is expected that the slice will be stitched with other external services or with other slices. For this, a set of inter-slice network functions are considered in order to be able to properly interconnect the network slices. The functionality includes:

- Inter-slice management functionality–enabling the peering between the different slices. The inter-slice management functionality has the following functionalities:
  - Slice discovery and selection–based on the information received from the tenant during the deployment, this functionality enables the discovery

of the peering slices to connect to. Note, this is a service level stitching between running slices, complimentary to the slice deployment on top of multiple domains.
  - Inter-slice connectivity management - provides the peering between the different slices for exchanging information on the contact points of the slices as well as on the protocol stack (including encryption) for the connectivity between the contact points. If any other connectivity related policies have to be exchanged (rate limiting, availability, etc.), they will also be exchanged over this interface.

- Slice Border Control (SBC)–the SBC functions at the control and data plane levels enables the peering of the control and data plane layers between the different slices.
  - SBC-Control - ensures the interconnection at protocol level between the different components within the slices. It may include for Diameter peering a Diameter Router Agent (DRA) and for IMS communication a Session Border Controller, both with the role of peering with the foreign domain, appropriately routing the requests to the other domain, as well as the anonymization of the private slice information and the encryption of the communication.
  - SBC-User - ensures the proper interworking between the data path components in case the communication requires other protocols than IP only. The functionality may include GPRS Tunnelling Protocol (GTP) peering (as in the case of packet core roaming), SFC (Service Function Chaining) peering, multimedia transcoding, and content compression.

Similar to the slice orchestration, there are several functions where a dynamic adaptation may be considered, beyond the current management system. This addresses the following management operations:

- Inter-slice connectivity management policies–can be adapted depending on the momentary network function placement e.g. if functions of two components of the different slices are co-located, it could be better to establish between them a connection compared to components which are located in different data centres.
- FCAPS operations–FCAPS functionality is the main beneficiary of the dynamic adaptation stack which offers a large amount of possible adaptation actions. This would be a comprehensive extension of the current FCAPS functionality deployed for legacy physical system towards complex events processing and towards adaptations which are possible only in the NFV environment. These functionalities could be for instance, actions for re-creating the network on components' failure, configurations depending on the dynamic network as established by the NFVO during the runtime, differentiated accounting systems depending on services, time of day, etc. It could also involve tasks to enhance the performance and security optimizations of the system through adaptation of functions such as deployment of more appropriate VNFs to a momentary situation, reconfiguration of the components depending on a momentary topology of the system for increasing the resilience and the availability, ensuring of the service Key Performance Indicators (KPIs) across deployments on top of heterogeneous infrastructures to the environment.
- Slice O&M–bringing new components into operation in an already running slice including the dynamic deployment of network slices for continuous integration and automation of the maintenance operations. Also the auditing of the components' performance based on the event log and the adaptation of the running policies according to any detected anomalies.

4.2 Orchestration Architecture

The orchestration architecture represents the perspective on the system from the multi-slice system management side. The main functionality is related to the life-cycle management of the slice and less to the slice functionality itself, thus being the same, no matter the deployed slice type and regardless of the domain in which the slice is deployed.
A set of existing functions from the NFV environment as well as from dynamic adaptation stack are included in the system. In the following, they are described together with the other new components introduced into the system, making references towards existing specifications when needed.

4.2.1 NFVI

The Network Function Virtualization Infrastructure (NFVI) as seen from the perspective of the slice management, there are no modifications to the NFVI compared to the existing infrastructure proposed in the high level ETSI NFV architecture. However, a specific implementation of the virtual network is considered covering deep data plane programmability and inter-data centre WANs.

4.2.2 VIM/WIM

The Virtual Infrastructure Manager (VIM) is defined in the ETSI NFV architecture. Additional functionality of the VIM includes the capability to control the user/data plane functionality such as in the form of an SDN controller or an ICN or CDN information and content control in order to be able to provide a separation of the data plane when the data traffic is directly routed through the network (i.e. deep data plane programmability). The Wide Area Network Infrastructure Manager (WIM) has the role to define the virtual networks between different parts of a slice on top of common transport networks (i.e. the inter-data centre environment sharing

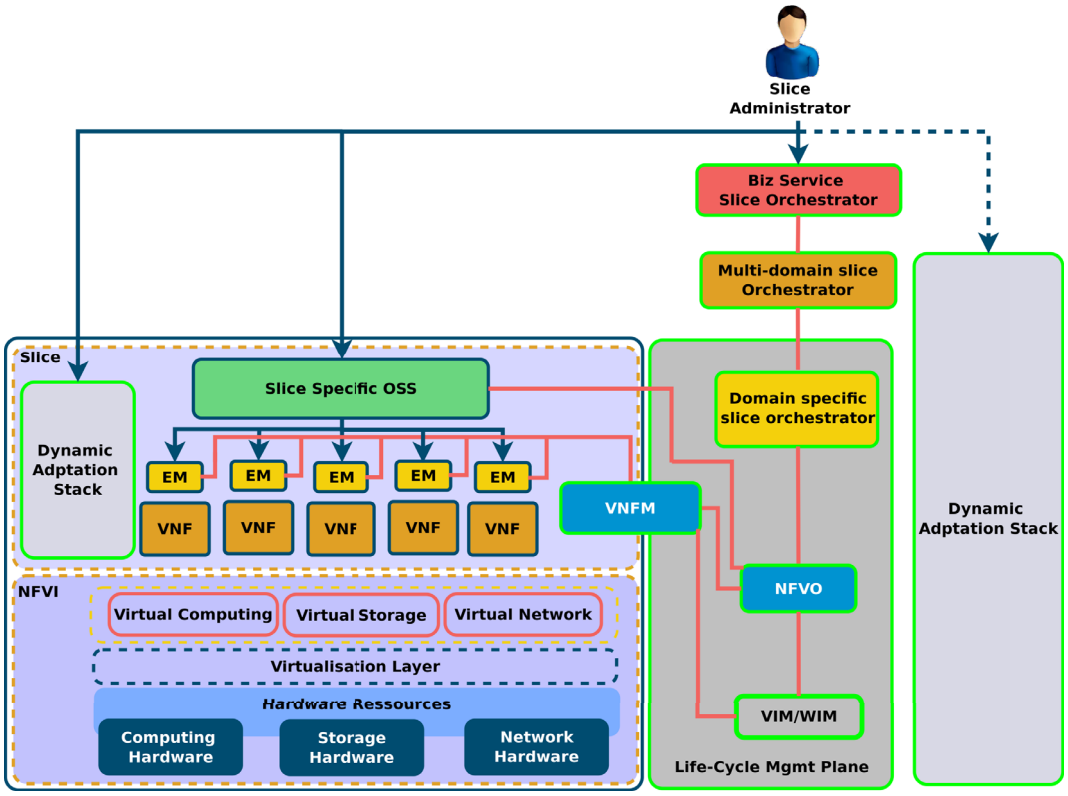


Fig. 6 Orchestration architecture.

rules).

4.2.3 NFVO

The NFVO has the functionality defined by ETSI NFV with its two roles of:

- Resource Orchestrator (RO) enables the brokering of the NFVI resources between the multiple parallel slices. The NFVO represents an aggregation point for the administrative domain for resources management. The NFVO communicates with multiple VIMs and WIMs and is able to allocate the resources appropriately across them.
- Network Service Orchestrator (NSO) provides indications on how the system should scale and where the network functions should be placed following the Network Service Descriptor (NSD) information.
- Additionally, the NSO is extended to support additional commands which may result in the dynamic changing of the NSD information. By this, the active service can be dynamically modified during runtime with additional actions compared to the static NSD based decisions. For example, with this new functionality, new VNFs can be added during runtime to a running system (e.g. a more resilient firewall in case of a network attack).

4.2.4 VNFM

The VNF Manager (VNFM) has the role defined by ETSI MANO specification to:

- Allocate resources to the VNFs appropriately or to delegate this operation to the NFVO,
- To receive events on the completion of the specific operations and information on the dynamic configurations, and
- To configure through the Element Management (EM) the VNFs with the dynamic configurations similar to the operating notion shared in [17]

4.2.5 Domain Specific Slice Orchestration

The domain specific slice orchestrator is able to communicate information on the specific slice split between the different NFVOs with multiple NFVOs located in the same domain. Additionally, the domain specific slice orchestrator receives information on the life-cycle management of part of the slice which is allocated to run on the specific domain from the multi-domain slice orchestrator. Note that this functionality is already offered by the northbound API of the NFVO in the form of the processing of NSDs. It shall be noted that in the envisioned architecture (Figure 6), a domain-specific slice orchestrator and NFVO may be the same entity.

4.2.6 Multi-Domain Slice Orchestration

The multi-domain slice orchestrator has as main role to provide a slice on top of multiple administrative domains. It contains the following functionalities:

- Receive requirements from the business service slice orchestrator on the requirements for the specific slice. The requirements may be received in a static description form such as TOSCA or an NSD file.
- Establish secure connections to the multiple domain specific slice orchestrators
- Acquire, if permissible, knowledge on the available resources in the specific administrative domains in terms of available infrastructure and available services (e.g. stored virtual machine images)
- Negotiate with the domain-specific slice orchestrators the resources and their locations to be allocated for a slice customer
- Make decisions based on the requirements received on the split of the slice functionality across the multiple administrative domains
- Command the installation of the slice over the multiple administrative domains
- When the installation is successful, exchange connectivity parameters between the different domain specific orchestrators to be able to stitch together the slice
- Announce the tenant through the business slice orchestrator on the successful installation of the slice as well as on the connectivity and management points
- Inform the tenant, through the business slice orchestrator and/or the slice-specific OSS, of any SLA breaches or any other types of major failures of the deployed slice

4.2.7 Business Service Slice Orchestration

The business service slice orchestrator has the role of a portal to advertise the possible services, to trigger their deployment and in case of success, to transmit to the slice administrator the specific entry points to the new slice management.

4.2.8 Dynamic Adaptation Stack (for the Life-Cycle Management Plane)

The life-cycle management plane has multiple points in which and through specific policies, the functionality of the system may be adapted. Based on the monitored information from the slice, the NFVI and the life-cycle management components, and the dynamic adaptation stack can provide the following adaptations:

- VIM level - migration of virtual machines, fault management and mitigation at the VM levels, configuration of the infrastructure, infrastructure security protection, authentication and authorization, resources scheduling for performance and resilience for example using such technique proposed in [21];
- WIM level - establishment of new data paths, traffic steering between multiple data paths, QoS classification and differentiation, application differentiation through deep data plane programmability;
- NFVO level - network functions placement in the domain, scaling policies, automatic fault management, resilience and security through application independent mechanisms, modifying the policies in selecting domain specific ROs;
- Domain specific slice orchestrator - modifying policies in selecting NFVOs
- Multi-domain slice orchestrator - modifying the policies in selecting administrative domains, SLA breaching reports;
- Business service slice orchestrator - transmitting to the tenant events in regard to the system on top of which the slice is deployed (i.e. normal behaviour)

4.2.9 Slice Administrator

Using the system, the slice administrator is able to:

- Request a services catalog from the business service slice orchestrator
- Select and configure a slice based on the services provided in the catalog
- Trigger the deployment of the slice according to the configured services
- Administrating the dynamic adaptation stack in both the orchestration and within the slice as much as allowed and possible through policies within the policy engine. Most probably this will be done through pre-defined templates. Administrating the services within the slice through policies within the slice specific OSS as well as through user profiles.

4.3 Dynamic Policy Based Management

One of the major advantages of software slices, deployed on top of common infrastructures, is that the system can be dynamically adapted to new network conditions. This includes the adaptation within the slice (i.e. the slice management which is part of every slice due to the fact that flexible resources can adapt the functionality of the system to the most appropriate conditions). Additionally, it includes the adaptation at the life-cycle management (i.e. the life-cycle management can adapt the resources allocated to the specific slices depending on their momentary needs as well as through brokering the available resources). With a physical system, there was not much liberty in terms of events that could happen and not too many actions possible. In NFV, due to the flexible virtual infrastructure used which can scale on-demand and due to the decoupling from the physical infrastructure, new events may be generated. These events could sometimes be highly complex combining information from different metrics of different components. Also, the software system has

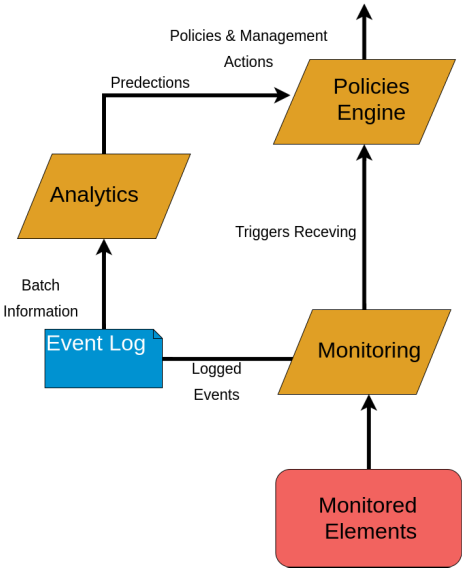


Fig. 7 Dynamic policy based management.

more possibilities into adaptation including scaling opportunities, network function placement and reconfigurations during runtime for the new network conditions. For this reason, the basic event and logging system which accompanies at this moment the network management stack is not sufficient to optimally operate in a software network environment. With this, new dynamic, policy based management stacks are created for different network functions, enabling them to take appropriate decisions on specific events.

As depicted in Fig. 7, the dynamic policy based management stack includes the following classical components, adapted and applied in the new NFV environment:

- Monitored elements - this represents the elements from which the information is gathered, be it part of the service, of the management of the service or as part of the life-cycle management of the service. To reduce the communication needs, the monitored elements may aggregate part of the monitored information.
- Monitoring (server) - the monitoring server receives all the monitored information without any processing or qualification (all information from the monitored elements is uniform). Based on threshold policies, the monitoring server is either logging the events and raising alarms (as in current management systems) or it provides basic events (e.g. CPU over 90% for a component for 3 times in the last 5 minutes) to the analytics and to the management policy engine.
- The Event Log stores information on the outstanding basic events which are logged from the monitoring server. Alternatively, it can be increased by adding more complex events.
- The Analytics component has the role to generate more complex information from the basic events. Depending on the type of analytics, it may provide different granularity level events such as root cause analysis in case of component failure or even subscriber usage pattern information. Regarding the latter, per-subscriber monitoring is technically possible through the processing of information available at the core network (i.e., Home Subscriber System - HSS), however, this operation is highly complex and coping with privacy violation may be a challenge. The complex information is transmitted in the form of policy triggers to the policy engine or in the form of new policies to be added to the system.
- The policy engine is the central decision entity of the dynamic adaptation stack. Based on the received triggers from either an analytics engine or directly from the monitoring, it checks the system conditions and based on this, it generates a set of mitigation actions which may result in the modification of the running system.

Additionally, to this system, an event broker may have to be added to the interconnection between the various analytics engines, the monitoring server and the policy engine. The event broker has the role to properly route the events between the different components.

4.4 Network Slice Orchestration

In this section, we will use the architecture as well as the elements defined in the precedent sections to demonstrate the creation of two types of end-to-end slices, single domain and multi-domain slice.

Figure 8 shows the case of creating a single domain slice via the multi-domain slice orchestrator. This would represent the case, where the BSS-O has no information on whether the resources should be created from one domain or more. After receiving a request from the customer, the BSS-O sends a slice creation request to the multi-domain slice orchestrator. The latter uses its blueprint model to build the slice blueprint, which will be communicated to the domain specific slice orchestrator. It is important to note that the multi-domain orchestrator selects the domain to be used for deploying VNFs using a local logic, which takes into consideration the available resources information communicated by the domain specific orchestrator(s), and other information like the geographical area to cover, etc.

Then, the slice blueprint is created. In some cases, after building the slice blueprint, the multi-domain specific slice orchestrator may update its blueprint model according to the information received from the domain specific slice orchestrator. In this use-case, the multi-domain orchestrator selects only one domain for deploying the VNFs. On receiving the slice blueprint, the Domain specific slice orchestrator adjusts the slice blueprint according to its domain specific model. After that, using the updated slice blueprint, the VNFO follows the same steps, as described in the precedent case, to deploy the VNFs.

Figure 9 displays the creation of a multi-domain slice via the multi-domain slice orchestrator. The main differences with the precedent case are:

- The multi-domain orchestrator selects mulit-domain re-

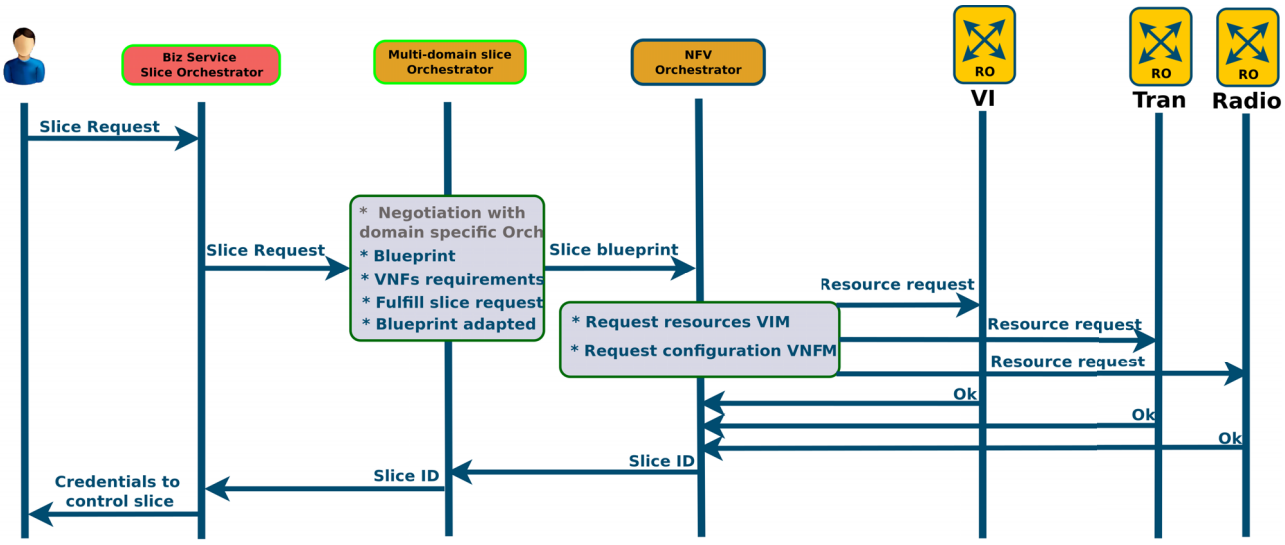


Fig. 8 Single domain slice creation via direct interaction with "multi-domain slice orchestrator".

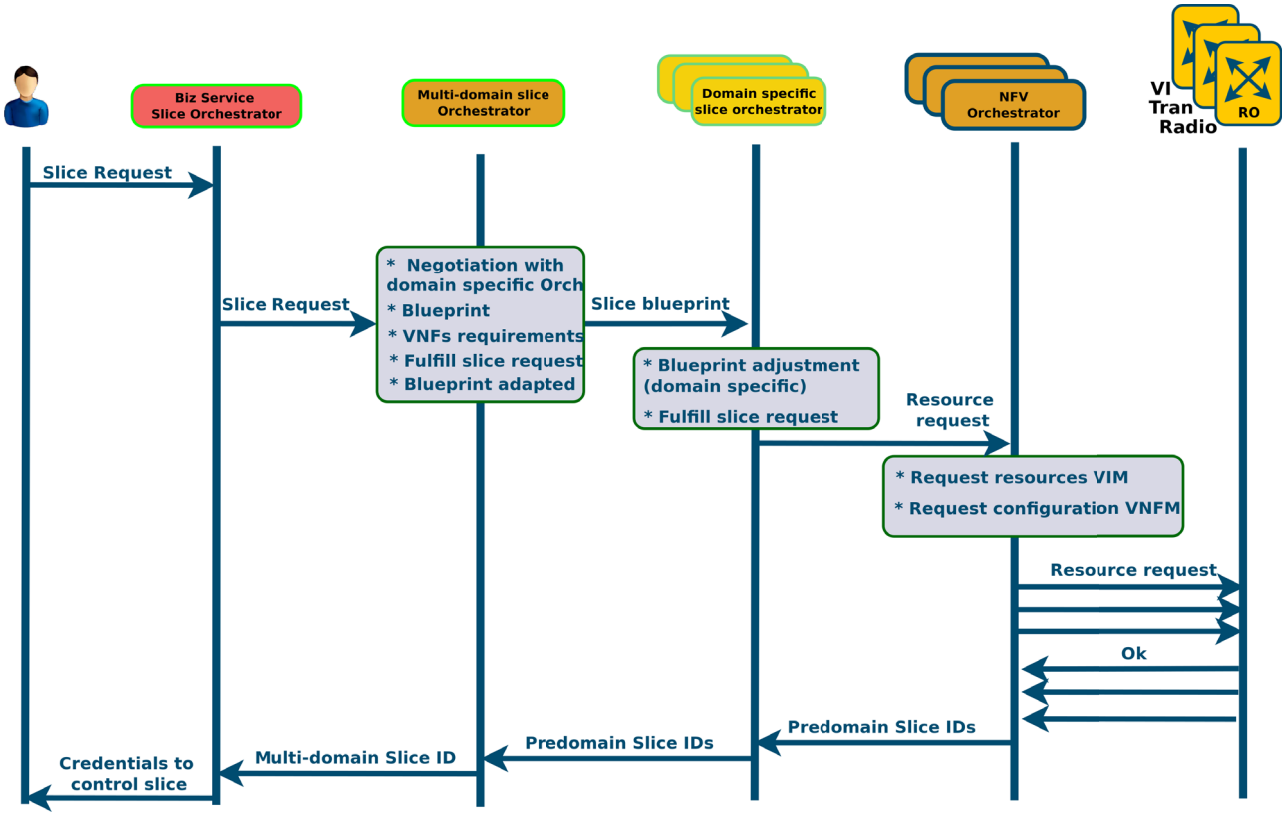


Fig. 9 Multi-domain slice creation via direct interaction with "multi-domain slice orchestrator".

sources to deploy the slice.

- For each domain, a slice blueprint is created. Each one indicates a part of the slice to be deployed. For instance, one domain may deploy only the radio resources, while another domain may instantiate both the virtual infrastructure and the transport network resources. The slice blueprints are sent to each domain specific slice orchestrator in order to be enforced.
- The mutli-domain orchestrator merges the slice IDs, to create a new slide ID along with its credentials, which will be communicated to the customer.

5. Conclusion

In this article, we dissected the challenging requirements envisioned to be addressed by the 5G technology when it is finally ready, based majorly on the 5G white paper and technical reports of SDOs such as NGMN and 3GPP respectively. We studied the diversity and complexity of these technological needs and sought solutions in standardized network softwarization technologies. We realised that any potential framework to address the differentiations in these sometimes conflicting requirements has to be all-encompassing, very comprehensive, flexible, adaptive on-demand and programmable. As a result, we chose the option of network softwarization enabled through SDN and NFV.

Using network softwarization techniques based on major technological enablers such as SDN, NFV and cloud computing, we have been able to design a potential 5G network system and network slice architectures. We developed state of the art network slice life-cycle (from instantiation to termination of network slices to free network resources) management algorithms over a single technology, administrative domain as well as across multiple domains. These architectures are designed to be robust, resilient to NF failures such as the type discussed in and mathematically modeled in [16], reliable and adaptive to changes in users' needs and network behavior on the fly.

We proposed a network slice should be orchestrated in an hierarchical fashion. The cascading orchestration requests and the resulting orchestrated network slice should be composed of orchestrated VI from the core network, virtual RAN and virtual Transport network components. In addition, we proposed and designed a potent standard network slice blueprint composing of seven major components, which are the slice service capabilities exposure (SSCE), slice specific OSS (SSO), dynamic adaptation stack (DAS), service, control, user and virtual resource planes.

Although all of the slices may follow the same template, a careful attention should be paid to the fact that similar components can be instances of the same software functions but with different parametrizations and the different components may also require separate implementations. From the perspective of the architecture here presented, the reconfigurable software components are considered the best alternative for the 5G requirements. Even though it may happen that when further detailing the different components, some functionality may have highly differentiated implementations especially when considering the limit use cases for massive broadband, the huge number of devices connectivity and the low latency high-reliability connectivity.

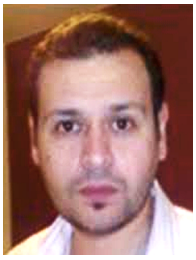
Acknowledgement

This work was partially supported by the European Union's Horizon 2020 research and innovation programme under the 5G!Pagoda project with grant agreement No. 723172.

References

[1] "Planetlab," http://www.planet-lab.org, 2012.
[2] "Flare: Open deeply programmable network node architecture," http://netseminar.stanford.edu/seminars/10_18_12.pdf
[3] "Study on New Services and Markets Technology Enablers," the 3rd partnership project (3GPP), TR 22.891, version 14.2.0, Sept. 2016
[4] "MGMN 5G WHITE PAPER," NGMN Alliance, white paper, https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf, Feb. 2015.
[5] METIS-II Project, https://5g-ppp.eu/metis-ii/
[6] "5G PPP 5G Architecture," the 5G PPP Architecture working Group, white paper, https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-July-2016.pdf
[7] "5G Mobile Communications Systems for 2020 and beyond," the 5th Generation Mobile Communications Promotion Forum (5GMF), white paper, http://5gmf.jp/wp/wp-content/uploads/2016/07/5GMF_WP100_Executive_Summary-E.pdf, July 2016.
[8] B. Sayadi, M. Gramaglia, V. Friderikos, D.V. Hugo, P. Arnold, M.-L. Alberi-Morel, M.A. Puente, V. Sciancalepore, I. Digon, and M.R. Crippa, "SDN for 5G mobile networks: NORMA perspective," Proc. CrownCom 2016, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol.172, pp.741–753, Springer, Cham, 2016.
[9] "Study on architecture for next generation systems," the 3rd partnership project (3GPP), TR 23.799, 14.0.0, 2016-12-16.
[10] "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," the 3rd Generation partnership Project (3GPP), TS 23.401, 14.0.0, 2016-12-16.
[11] "Enhancement of Dedicated Core Networks selection mechanism," 3GPP, TR 23.711, release 14.
[12] R. Guerzoni et al., "Multi-domain orchestration and management of software defined infrastructures: A bottom-up approach," Proc. European Conference on Networks and Communications, Athens, 2016.
[13] IEV operations and maintenance definitions for operations, maintenance support and maintenance, last visited on 29.11.2016, http://www.electropedia.org/
[14] ISO FCAPS standard, last visited on 29.11.2016, http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_19_89(E).zip
[15] T. Taleb, A. Ksentini, and R. Jantti, "Anything as a service for 5G mobile systems," IEEE Netw., vol.30, no.6, pp.84–91, Dec. 2016.
[16] T. Taleb, A. Ksentini, and B. Sericola, "On service resilience in cloud-native 5G mobile systems," IEEE J. Sel. Areas Commun., vol.34, no.3, pp.483–496, March 2016.
[17] F.Z. Yousaf and T. Taleb, "Fine granular resource-aware virtual network function management for 5G carrier cloud," IEEE Netw., vol.30, no.2, pp.110–115, March 2016.
[18] T. Taleb, M. Corici, C. Parada, A. Jamakovic, S. Ruffino, G. Karagiannis, and T. Magedanz, "EASE: EPC as a service to ease mobile core network," IEEE Netw., vol.29, no.2, pp.78–88, March 2015.
[19] T. Taleb, A. Ksentini, and A. Kobbane, "Lightweight mobile core networks for machine type communications," IEEE Access, Vol 2, pp.1128–1137, Oct. 2014.
[20] T. Taleb, "Towards carrier cloud: Potential, challenges, & solutions," IEEE Wireless Commun. Mag., vol.21, no.3, pp.80–91, June 2014.
[21] I. Farris, T. Taleb, A. Iera, and H. Flinck, "Lightweight service replication for ultra-short latency applications in mobile edge networks," Proc. IEEE ICC 2017, Paris, France, May 2017.
[22] GENI: Slice-based Federation Architecture specification, groups.geni.net/geni/raw-attachment/wiki/SliceFedArch/SFA2.0.pdf, last visited on 07.03.2017.
[23] ETSI NFV, Network Functions Virtualisation (NFV); Architectural framework, GS NFV 002, Oct. 2013.

Ibrahim Afolabi obtained his Bachelor's degree from VAMK University of Applied Sciences, Vaasa, Finland, in 2013 and is a graduating Master's student from the School of ElectricalEngineering, Aalto University, Finland. Prior to starting his Master's studies, he workedas an engineer assuming different roles in network administration, embedded systemsprogramming and has experience in web development too. His present research areasinclude Network Slicing, MEC, network softwerization, NFV, SDN, and dynamic network resource allocation.



Adlen Ksentini received the MSc degree in telecommunication and multimedia networking from theUniversity of Versailles, France, and the PhD degree in computer science from the-University of Cergy-Pontoise, France, in 2005, with a dissertation on QoS provisioning inIEEE 802.11-based networks. From 2006 to 2015, he was an associate professor atUniversity of Rennes 1, France, and member of the INRIA Rennes team Dionysos. Recently, he joined the Mobile and Wireless Networking Department at EURECOMInstitute as an associate professor. His interests include future Internet networks, mobile networks, QoS, QoE, performance evaluation, and multimedia transmission.

Miloud Bagaa received his M.E. and Ph.D. degrees from the University of Science and TechnologyHouari Boumediene (USTHB), Algiers, Algeria, in 2005, 2008, and 2014, respectively. From 2009 to 2015, he was a Researcher with the Research Center on Scientific and Technical Information (CERIST), Algiers, where he was a Member of the WirelessSensor Networks Team, DTISI Division. From 2015 to 2016, he was granted a postdoctoral fellowship from the EuropeanResearch Consortium for Informatics and Mathematics, and worked with the NorwegianUniversity of Science and Technology, Trondheim, Norway. Currently, heis Senior Researcher with the Communications and Networking Department, AaltoUniversity, Espoo, Finland. His research interests include wireless sensor network, Internet of Things, 5G wireless communication, security, and networking modeling.

Tarik Taleb received his B.E. degree in information engineering (with distinction), his M.Sc. and Ph.D. degrees in information sciences from GSIS, Tohoku University, Sendai, Japan, in2001, 2003, and 2005, respectively. He is currently a Professor with the School ofElectrical Engineering, Aalto University, Espoo, Finland. He is an IEEE Communications Society (ComSoc) Distinguished Lecturer. He is a Member of the IEEE Communications Society Standardization Program Development Board. In an attempt to bridge the gap between academia and industry, he founded the IEEE-Workshop on Telecommunications Standards: From Research to Standards, a successful event that was recognized with the BestWorkshop Award by the IEEE Communication Society (ComSoC). Based on the successof this workshop, he has also founded and has been the Steering Committee Chair of the IEEE Conference on Standards for Communications and Networking. He is the General Chair of the 2019 edition of the IEEE Wireless Communications and NetworkingConference (WCNC '19) to be held in Marrakech, Morocco. He is /was on the Editorial Board of IEEE Transactions on Wireless Communications, IEEE Wireless Communications Magazine, IEEE Journal on Internet of Things, IEEE Transactions onVehicular Technology, IEEE Communications Surveys & Tutorials, and a number of Wiley Journals.

Marius Corici has been a senior researcher in Fraunhofer FOKUS's Next Generation Network Infrastructures (NGNI) department for 10 years, currently leading the Reliable NetworkInfrastructure team in charge of research and innovation in the areas of 5G, NFV, andSDN, and the development of the correspondent software toolkits: Open5GCore(www.open5Gcore.net) for wireless ecosystem developments, and OpenSDNCore (www.opensdncore.org) for network service enablement based on virtualization technology, sustaining the industry and academia R&D to obtain and to demonstratemeaningful results with high impact toward standardization.

Akihiro Nakao received B.S. (1991) in Physics, M.E. (1994) in Information Engineering from theUniversity of Tokyo. He was at IBM Yamato Laboratory, Tokyo Research Laboratory, andIBM Texas Austin from 1994 till 2005. He received M.S. (2001) and Ph.D. (2005) inComputer Science from Princeton University. He has been teaching as an associate professor (2005.2014) and as a professor (2014. present) in Applied Computer Science, at Inter-faculty Initiative in Information Studies, Graduate School of Interdisciplinary Information Studies, the University of Tokyo.