NESMO: Network Slicing Management and Orchestration Framework

Alisa Devlic, Ali Hamidian, Deng Liang, Mats Eriksson, Antonio Consoli and Jonas Lundstedt
Huawei Technologies, Kista, Sweden
Email: {alisa.devlic, ali.hamidian, deven.dengliang, mats.eriksson1, antonio.consoli, jonas.lundstedt}@huawei.com

***Abstract*—This paper presents a novel network slicing management and orchestration architectural framework. A brief description of business scenarios and potential customers of network slicing is provided, illustrating the need for ordering network services with very different requirements. Based on specific customer goals (of ordering and building an end-to-end network slice instance) and other requirements gathered from industry and standardization associations, a solution is proposed enabling the automation of end-to-end network slice management and orchestration in multiple resource domains. This architecture distinguishes between two main design time and runtime components: Network Slice Design and Multi-Domain Orchestrator, belonging to different competence service areas with different players in these domains, and proposes the required interfaces and data structures between these components.**

I. Introduction

Mobile operators face a tremendous increase of mobile data traffic due to mobile multimedia services and introduction of new market services (also known as verticals), while experiencing a weak revenue growth. The challenge is how to address this traffic increase without new CAPital and OPerational EXpenditures (CAPEX and OPEX, respectively), while supporting in a scalable way the introduction of new services with diverse requirements on mobile network.

Building and operating telecommunication infrastructure presents a significant cost for mobile network operators. It includes the costs of site acquisition and licences, planning, equipment, installation, energy supply, maintenance, and network management. Therefore, sharing the telecommunication infrastructure is an attractive option to mobile operators, enabling cost reduction of the network deployment, cheaper service offerings to customers and faster network roll-outs, while improving the network capacity, coverage, and sharing burden of costly licences and low traffic areas. The operators can invest the capital gained from infrastructure sharing in building better value-added services and gaining competitive advantage on the market.

The idea of sharing the network infrastructure started with passive network sharing, i.e., sharing of site locations and masts (where operators can collocate their sites and even share the antenna frame, but install their own radio equipment) [1]. The passive infrastructure sharing later expanded to active Radio Access Network (RAN) sharing: sharing of access network equipment (i.e., base stations, antennas, and mobile backhaul equipment) and spectrum resource sharing. The dynamic resource sharing also posed new requirements on sharing the core network elements and platforms, such as Mobile Management Entity (MME) [2].

Network sharing can reduce the cost of mobile network infrastructure to some extent. However, the significant part of the operator costs comes from the traditional way of building and operating mobile networks, which is:

- *inflexible* - requires acquisition and operation of specialized network hardware that cannot be redeployed with another functionality
- *static* - cannot dynamically optimize the network for different service requirements, such as high throughput and user mobility or low latency and high bandwidth
- *difficult to adapt* - the platforms lack automatic configuration and customization capabilities, which leads to long deployment times and high operational complexity

These characteristics limit the ability of network service providers to create novel network-based services that can support the diverse requirements of emerging 5G use cases [3]. Operators need to rethink the way how they design, deploy, and upgrade mobile networks in terms of both time and required resources to support the novel mobile applications.

Network slicing is a concept that enables operators to create multiple virtual networks over the same physical infrastructure. Building isolated virtual mobile networks on a shared infrastructure enables allocation of resources and network functions in a dedicated fashion to individual slices that belong to mobile network operators or different types of organizations.

The concept of network slicing for multiple tenants came with Network Functions Virtualization (NFV) [4] and Software-Defined Networking (SDN) [5] mechanisms that have been progressively introduced in 3GPP networks. With implementation of network components as a software running on the virtualized infrastructure, that can be deployed where appropriate in the physical network and provisioned with the required virtual resources on demand, these technologies have the potential of allocating resources *more efficiently* than in traditional network functions based on the custom dedicated hardware.

By virtually partitioning the mobile network components and physical network as well as data center infrastructure resources, different network slices can be created tailored to specific use cases with particular requirements on capacity, latency, security, reliability, user mobility, geographic coverage, etc. Such created network slices contain *only* resources and network functions that are needed to realize the particular use case, thus *reducing the network complexity* and dependencies among network functions and creating an architecture that can *support a wide range of customer' and operator's requirements*.

Building such dedicated and optimized networks on the shared network infrastructure is more *cost efficient*, *speeds up deployment and time to market*, and *enables network customizations* according to special customer requirements, thus *addressing a broader market space*. However, with an increased flexibility comes a risk of higher operational complexity, which is proportional to the number of created customized networks. The key to reducing this risk (and avoiding the CAPEX and OPEX increase) is **automating the network slice design, deployment, and management operations**.

This paper proposes a management system to be used by operators for automating network slice design, deployment, and configuration in multiple infrastructure resource domains that can contain network functions from different vendors. It describes the proposed components, interfaces, and data structures that are needed to meet specific customer requirements, while extending the 3GPP management reference framework with the automated end-to-end network slicing capabilities.

To the best of our knowledge, this is the first paper about **automated end-to-end** network slice design, deployment and configuration in **multiple network infrastructure resource domains** that targets mobile networks. Other proposed network slicing management architectures focus on orchestrating resources in a Network SLice Instance (NSLI) from either a single type of network infrastructure resource domain (e.g., NFV) [6], a single network domain type (e.g., RAN) [7], or using a single type of resource domain manager (e.g., SDN controller) [8].

5G NORMA project proposes a network slicing management architecture that dynamically translates a user service request into a set of network Key Performance Indicators (KPIs) that are used to build a chain of Virtual Network Functions (VNFs) and Physical Network Functions (PNFs) on demand [8], representing a customized NSLI. This management architecture is based on hierarchy of SDN controllers that can virtualize and orchestrate the network, computing and radio resources under their control (i.e., assigned to a network slice or shared among selected NSLIs).

A 5G network slice management architecture applied to cloud RAN slicing is proposed in [7]. Similarly to our proposed architecture, their management system supports design, instantiation, and configuration of NSLIs based on customization of pre-designed network slice templates for specific use cases.

5G SONATA architecture represents a network service programming, orchestration, and management framework that is build on top of the NFV MANO framework, thus focusing on only NFV resources [6].

II. NGMN VISION OF 5G NETWORK SLICING

NGMN defines network slicing as the concept in which a specific service (end-user service or business service) is hosted within or realized by a dedicated network slice containing all physical and virtual resources [9]. Thus, it consists of three layers: service instance layer, NSLI layer, and resource layer, each of which requires management functions.

A service instance layer defines services that need to be supported by network slices. Each service is represented by a service instance that is realized within or by the network slice. Multiple service instances, requiring similar network characteristics, can run on the same NSLI.

A NSLI layer defines network slices that provide the networking and cloud computing support to different types of services, offering specific KPI guarantees. A NSLI, created by an operator, consists of network functions (potentially from different vendors), physical or logical resources to run these network functions, as well as policies and configurations. A NSLI can also consist of one or more sub-network instances containing common network functions and resources, which may be shared by other NSLI(s).

NGMN envisages 5G network architecture to consist of three layers (that can be mapped to the corresponding network slicing layers): *infrastructure resource layer*, *business enablement layer*, and *business application layer* that all interface an *end-to-end management and orchestration* entity (as shown in Figure 1). Each layer exposes functions and capabilities through Application Programming Interface (API) to higher layers and to end-to-end management and orchestration entity. Performance, status monitoring, and configuration capabilities are part of this API.

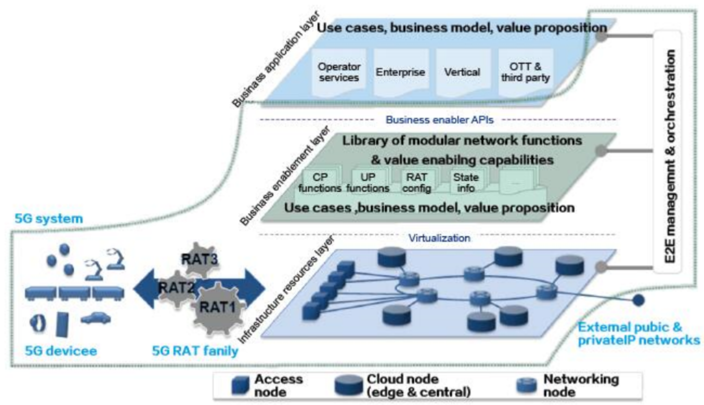

Fig. 1. NGMN 5G network architecture [9]

An *end-to-end management and orchestration* plane spans all three layers and plays a key role: creates and manages 5G network slices. It translates use cases and business scenarios into actual network functions and network slices. Additionally, it defines network slices for different use cases, chains network functions that are relevant for a particular use case, determines the required performance configurations and their location in the network, as well as associates and manages the required infrastructure resources (including scaling of their capacity). An interface to this entity allows building dedicated network slices for an application or mapping an application to the existing network slices.

III. STAKEHOLDERS AND BUSINESS SCENARIOS

Network slicing redefines the business relationships and stakeholder roles in the telecommunication services market. Figure 2 illustrates a new business model, where each stakeholder uses the network services from the stakeholder below to implement their own service, providing it to the stakeholder(s) above in the chain:

- An *Infrastructure Provider (InP)* - owns and operates the physical mobile network & data center infrastructure domains, consisting of raw resources and inter data center connectivity elements. In a mobile network infrastructure domain, the InP implements the passive infrastructure sharing by renting the site locations and radio towers to Mobile Network Operators. In a data center infrastructure domain, the InP provides virtualization layer by logically abstracting the physical infrastructure resources into the virtual computing, storage, and networking resources and installing an operating system on these virtual resources. It can sell these virtual resources to Service Providers.

- A *Mobile Network Operator (MNO)* - owns and operates the mobile network nodes (i.e., PNFs, such as eNodeBs) and links. It implements the active RAN sharing with other MNOs to reduce the infrastructure costs. It also leases virtual resources from the InP, downloads and installs the 3GPP network functions software on these virtual resources, thus instantiating the 3GPP VNFs. It designs, deploys, and configures an end-to-end network according to the customer requirements, using the available PNFs, VNFs, and links. This type of infrastructure partitioning is defined in this paper as *network slicing* and a built end-to-end network as a NSLI. The MNO also provides connectivity services to consumers.
- A *Service Provider (SP)* - provisions and configures communication services for the group of users or individual users on the provided NSLI. If a Service Level Agreement (SLA) is established between the enterprise customer (e.g., government or vertical industries) and a SP, requesting the guaranteed service performance for the enterprise's group of users, the SP also reserves resources (capacity) for this particular service on the NSLI. We refer to this type of slicing as *network service slicing*. A *Mobile Virtual Network Operator (MVNO)* that does not own the mobile network nodes or spectrum can also be seen as a SP, provisioning and configuring access to services to end users on the leased NSLI provided by the MNO.
- *Consumers* - are groups of users belonging to an enterprise customer base or individual end users that request access to connectivity or end user service(s) with service-specific SLA parameters and use the provided services for communication.

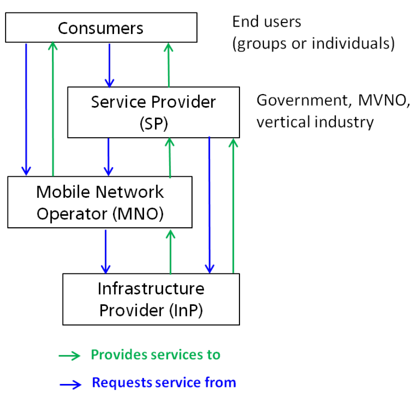

Fig. 2. Business model and stakeholders roles

Customers of telecommunication networks may be very different entities, such as consumers, enterprises, SPs, other M(V)NOs and government agencies. Network slicing attracts traditional and new types of customers in the network services market. Recently, vertical industries (i.e., health, automotive, power transmission, home) and Over-The-Top service providers became interested in the network slicing services, intending to: (1) mobilize and automate their industries and industry processes in order to increase their productivity and (2) deliver services that require high quality, low latency, and other KPIs on demand in highly flexible and programmable manner. Each of these customers can request business services with very different requirements.

Based on specific customer goals, we currently distinguish between two use cases (illustrated in Figure 3):

- **Use case 1: Ordering *service(s)*** - if an enterprise or an end user orders access to specific services with service-specific SLA requirements for a group of users or individual use. Services can range from native telecommunication services (e.g., voice, video, mobile broadband (MBB)) up to more advanced services requiring service composition functionality to solve a complex goal involving multiple systems and devices (e.g., capillary networks or smart grid). The requested services can be provisioned on one or more existing NSLIs, if the running NSLIs can meet these services' requirements.
- **Use case 2: Ordering a complete *network slice*** - if a SP orders an end-to-end NSLI of the specific type[1] with the required characteristics. A NSLI can come with some pre-provisioned telecommunication services (such as voice, MBB, and mobility). Additionally, a customer can add and configure himself additional services for its users (typical examples include analytics, push to talk, etc.).

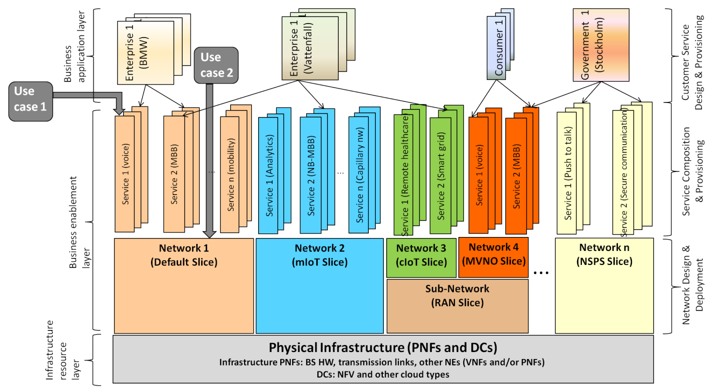

Fig. 3. Business scenarios and use cases for network slicing

The use case 1 refers to provisioning and configuring services to end users on the shared running NSLI and allocating network resources to the particular services, if a specific service performance needs to be guaranteed to the customer. The use case 2 relates to slicing of the shared physical infrastructure and building an end-to-end network for a SP optimized for specific services that can meet the customer requirements.

Table III summarizes differences between two use cases, illustrating a need for separate management frameworks that can design, deploy, and operate slices, hence belonging to two management domains: network slicing and network service slicing.

In this paper we focus on providing the solution for use case 2, which we believe will be the **main use case for network slicing**.

IV. Management Architecture Evolution

A. ETSI NFV MANO Framework

By decoupling software implementations of NFs from the infrastructure they run on, NFV adds new capabilities to the communication network: the *flexibility* of instantiating NFs anywhere in the network or data center and the *elasticity* of allocating

[1]Different types of network slices can be defined, based on the use case they refer to and the required network characteristics. The following slice types have been identified from analyzing 5G use cases [3]: Enhanced Mobile Broadband (eMBB), massive IoT, critical IoT, and National Safety Public Security (NSPS).

additional resources to these NFs when needed. These capabilities require a new set of management and orchestration functions to create the required resources and control the VNFs' lifecycle.

ETSI has introduced an NFV MANO (Management and Orchestration) architecture to realize management of VNF lifecycle and resource allocation. The NFV MANO framework provides management and orchestration of all resources in a data center (compute, storage, networking and virtual machine resources), VNFs, and Network Services (NSs) [4].

NFV MANO consists of three functional blocks:

- **NFV Orchestrator (NFVO)** - onboards new NSs and VNF packages, manages the lifecycle of NSs, and orchestrates the NFV Infrastructure (NFVI) resources across multiple VIMs according to the load and resource requests from VNF and NS instances.
- **VNF Manager (VNFM)** - manages the lifecycle of VNF instances, scales up/down VNF instances, and manages the FCAPS (Fault, Configuration, Accounting, Performance and Security) of VNF instances.
- **Virtualized Infrastructure Manager (VIM)** - controls and manages the NFVI resources.

However, this framework focuses on VNF management and orchestration only, while the future mobile network will contain not only VNFs but also PNFs, thus requiring a unified management across both PNF and NFV resource domains. Additionally, MANO does not specify SDN types of resources in its architecture for interconnection of different domains, rather it assumes that transport infrastructure and services are already established.

3GPP management framework has integrated its management entities with ETSI defined MANO framework in order to enable network management of virtualized networks [10]. The goal was to reuse as much as possible 3GPP management entities when interconnecting with the MANO, while collaboratively managing the VNFs and the VNF's virtual resources from NFVI. However, this integration of 3GPP management of mobile virtualized networks with MANO was focused on management of mobile core networks. Currently, the focus of 3GPP Telecom Management Working Group SA5 is on *end-to-end management* aspects of mobile networks that include the VNFs [11], related to *management and orchestration of network slicing*.

B. Management requirements for network slicing

We gathered and analyzed the requirements for network slicing specified by different industry and standard associations, grouping them into the following categories:

- *Flexibility* - enabling a MNO to dynamically compose and manage network slices, consisting of a set of NFs (e.g., potentially from different vendors, operators or 3rd parties), the resources to run these NFs, policies and configurations. The management system should support end-to-end resource management in network slice.
- *Customization* - enabling a MNO to create, operate, and manage network slices that support a variety of end-user services that require different network characteristics (in terms of mobility, charging, security, policy control, latency, and reliability). The system should efficiently support multiple 3rd parties that have similar network characteristics.
- *Simplification* - simplifying the mobile network logical architecture and reducing complexity of operating mobile network slices. Since the flexibility requirement introduces complexity in design and operation of network slices, the challenge is to find the right balance between complexity and simplification in order to avoid increasing costs.
- *Exposure* - exposing network capabilities through the open APIs to allow 3rd parties to create and manage network slices, within the limits defined by a MNO.
- *Elasticity* - supporting elasticity of a NSLI in terms of capacity, with minimal impact on the services of this slice or other slices.
- *Cloudification* - utilizing cloud computing technologies, such as NFV and SDN, in network slice deployment.
- *Legacy support* - minimizing dependencies between network slicing management solution and Operational Support System/Business Support System (OSS/BSS) in order to support the legacy OSS/BSS systems.
- *Lifecycle management* - implementing network slice lifecycle management and modifications to a network slice with a minimal impact to active subscriber services.
- *Automation* - supporting an automated network slice design and deployment from a business service order.
- *Isolation* - avoiding a fault or high resource usage of a slice to harm the stability or performance of other slices.
- *Multi-domain* - supporting multi-domain architectures.

Figure 4 shows the importance of these requirements according to the analyzed industry and standardization resources [1], [9], [12]–[23]. An interesting observation is that **flexibility** and **customization** are the two most important requirements for management of network slicing. Contrary to what we initially expected, the isolation is not among the most important requirements.

TABLE I
NETWORK SLICING VS. NETWORK SERVICE SLICING

	Network slicing (Use case 2)	**Network service slicing (Use case 1)**
Customer	Service provider	End user(s)
Business service	Optimized network for a service set	Customized service package
Resources to slice	Infrastructure	Network
Management domain	RAN, core, transport (end-to-end)	Network & cloud services (end-to-end)

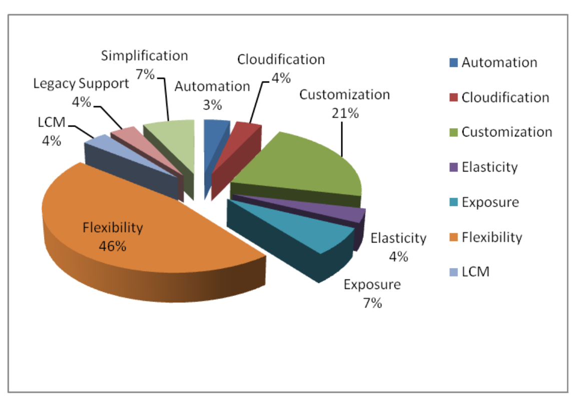

Fig. 4. Network slicing requirements

V. Proposed Extensions of 3GPP Management Framework

The identified network slicing requirements illustrate a need for centralized management and orchestration of various NSLIs. The existing Element Managers (EM), Network Manager (NM), and OSS/BSS do not have this capability.

Figure 5 presents a network slicing management and orchestration architecture, extending the 3GPP management reference framework with the required capabilities:

- *multiple network infrastructure resource domains* that can contain and manage different types of infrastructure resources (not only NFVI)
- the *NEtwork Slice creation and Management tOol (NESMO)*, consisting of the Network Slice Design (*design phase*) and Multi-Domain Orchestrator (*runtime phase*) components that are needed to *design, deploy, configure, and activate a NSLI* in multiple network infrastructure resource domains
- the *interfaces* and *data structures* that are used as inputs into the Network Slice Design and Multi-Domain Orchestrator.

To realize the missing functionalities while ensuring interworking with the legacy operations and management systems, NESMO is logically[2] placed between the 3GPP management entities and the network infrastructure resource domains.

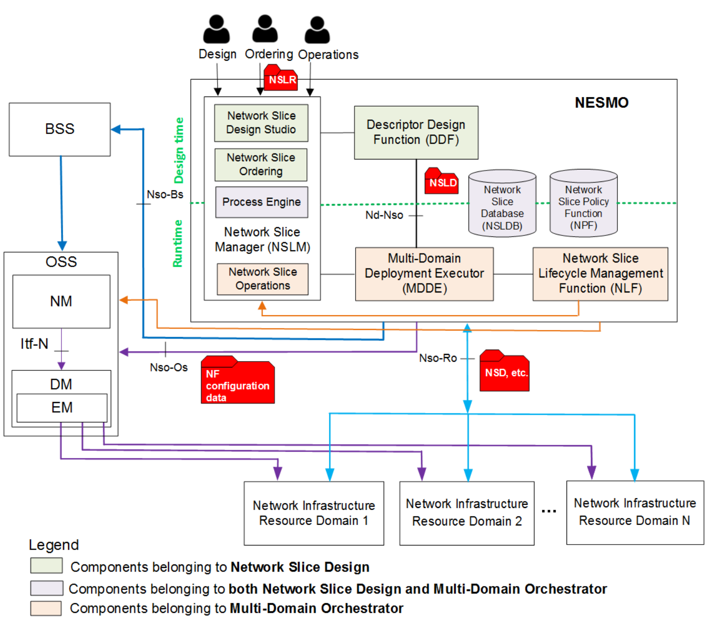

Fig. 5. Network Slice Design and Multi-Domain Orchestration architecture

A. Network infrastructure resource domains

A **network infrastructure resource domain** is defined as a set of **infrastructure resources** (hardware and software components that can be found in a data center or an operator's mobile network) and a **resource manager** that coordinates, allocates and releases these resources on request.

A network infrastructure resource domain can be created for *multiple purposes*, such as:

- to manage resources of the same type
  - **NFV domain** – consisting of NVFI compute, storage, network, virtual machine resources, and VNFs managed by **NFVO** in the MANO framework.
  - **PNF domain** – consisting of Physical Network Resources (e.g., RAN, IPX Transport, or transoceanic cable resources) and the corresponding PNFs (eNodeBs and physical links) orchestrated by **PNF resource manager**. An example of a PNF resource manager is Shared RAN Domain Manager that is responsible for sharing the unallocated radio resources to MVNOs [2] [24].
  - **SDN domain** – consisting of SDN Resources (i.e., SDN-enabled switches) that are managed by **SDN controller** through SDN Northbound Interface (NBI). If SDN-enabled switches are *virtualized*, the SDN controller is managed by *NFVO* in the MANO framework, thus SDN domain is *encapsulated* in the NFV domain.
- to manage resources belonging to different organizational domains within an operator's organization, which can be hierarchically organized
  - In this case each **organizational domain** is mapped to one network infrastructure resource domain
- to manage resources belonging to the same network domain
  - **RAN** – consisting of PNFs, VNFs, and optionally SDN resources
  - **Core network** - consisting of VNFs, PNFs, and optionally SDN resources
  - **Transport network** - consisting of VNFs, PNFs and SDN resources,

  in which each resource type is managed by the corresponding resource manager.

In this paper, we refer to a network infrastructure resource domain as a group of resources of the same type (i.e., NFV, PNF, and SDN domain), each of which can have multiple instances deployed in different network domains that belong to various organizations in a MNO's network (as shown in Figure 6).

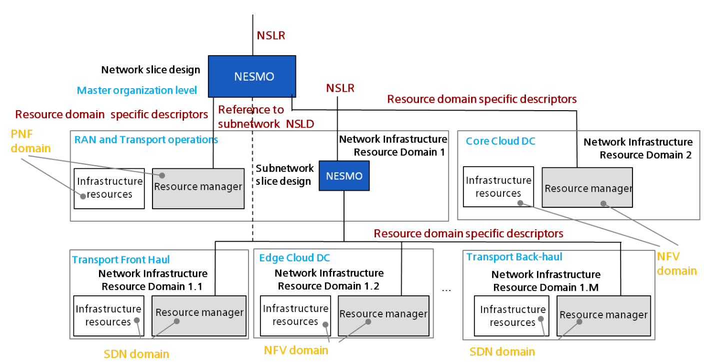

Fig. 6. Illustration of different network infrastructure resource domains

A resource manager uses a set of resource domain descriptors to create and allocate the required resources and services in the respective network infrastructure resource domain. In case of NFV domain, an NFVO uses the following descriptors that have been standardized by ETSI: Network Service Descriptor (NSD), VNF Forwarding Graph Descriptor (VNFFGD), Virtual Link Descriptor (VLD), VNF Descriptor (VNFD) and PNF Descriptor (PNFD) [25]. For other resource domains (such as PNF and

[2] In a real physical implementation, however, NESMO may be integrated with BSS, OSS and/or MANO NFVO.

SDN), the corresponding resource domain descriptors remain to be defined[3].

In case an organizational domain within an operator's network is hierarchically divided into subdomains, a subnetwork slice instance is first designed, deployed, configured and activated using its own NESMO framework that creates a **subnetwork slice descriptor**. A reference to this subnetwork Network Slice Descriptor (NSLD - whose meaning will be later defined in the following section V.C) is used by the Network Slice Design at the master organizational level in end-to-end network slice design, referencing it in an NSLD for the purpose of deployment, configuration, and activation of the NSLI.

B. Interfaces and data structures

The reference points between NESMO and resource managers, BSS, and OSS are named **Nso-Ro**, **Nso-Bs** and **Nso-Os**, respectively. Note that these reference points use existing interfaces if possible. An input data structure to the Network Slice Design is **Network Slice Requirements (NSLR)**.

A MNO uses **NSLR** to order a new NSLI. It contains the information about the customer, the network slice type with the network slice-specific SLA, and the network services that should be provisioned on this NSLI with these services SLAs.

In addition to the reference points that are related to interworking with resource managers and BSS/OSS, there is also a NESMO-internal reference point **Nd-Nso** defined between the Network Slice Design and the Multi-Domain Orchestrator. The information carried over this reference point includes the **Network Slice Descriptor (NSLD)** for a specific NSLI.

An **NSLD** is an output of the Network Slice Design. It contains all information needed to deploy, configure, activate, and operate a NSLI during its life cycle (including the description of network slice capabilities)[4]: workflows, resource domain descriptors, policies, lifecycle management scripts, and NF configuration data.

The southbound reference point **Nso-Ro** carries the resource domain descriptors in the format that is readable by the respective resource managers.

C. NESMO architecture

NESMO consists of four functional blocks:

1) **NSL Manager (NSLM)**
2) **Descriptor Design Function (DDF)**
3) **Multi-Domain Deployment Executor (MDDE)**
4) **NSL Lifecycle Management Function (NLF)**,

that can be mapped to Network Slice Design and/or Multi-Domain Orchestrator (as shown in Figure 5). Additionally, there are two supporting functions: the **Network Slice Policy Function (NPF)** for policies management and the **Network Slice Database (NSLDB)** for storing all information that is created and used by NESMO functional blocks. The NSLDB also acts as inventory of the available network components and infrastructure resource models. This section presents each of the functional blocks.

[3]The definition of these descriptors is out of scope of this paper.

[4]Our definition of NSLD is consistent with the NGMN network slice blueprint definition.

1) NSLM: controls the process of network slice design and deployment. It serves as an entry point into NESMO that can be accessed by a MNO through a portal or by OSS/BSS via a NBI. The NBI offers commands for creating, modifying and deleting a NSLI. The NSLM contains the following parts shown in Figure 5:

- The Network Slice Design & Operations Portal – with the Network Slice Design Studio, Network Slice Ordering and Network Slice Operations components and interfaces
- The Process Engine

The Network Slice Design and Operations Portal: implements support for a MNO when designing a new network slice type, and ordering and building a new NSLI.

The Network Slice Design Studio: provides tools and modelling primitives to a user for correctly defining and on-boarding the information needed to create a new Network Slice Type. Examples of these tools are templates and workflows that guide the user to implement **design algorithms**, **workflows** specifying in which order to execute these algorithms, and other data that is needed to create a NSLI of specific type, referred to as a **network slice type blueprint**. The Network Slice Design Studio also exposes information from the NSLDB that is needed for the network slice type creation, such as available NFs models, infrastructure resources models, and network characteristics. For component- and sub-network level (e.g., VNFs) designers, the portal provides exposure of capabilities and the ability to onboard new component models.

The Network Slice Ordering: provides support to the user when defining NSLR, by offering templates per network slice type containing slice-specific attributes and (range of) values that these attributes can take. It may also support Policies creation.

The Network Slice Operations: provides an escalation point to a MNO during runtime for SLA violations, faults, and other events related to NSLI, enabling the operator to monitor and interact with the NSLI at runtime. A MNO can grant access to this portal to vendors and their partners (e.g., for network capabilities exposure and component model on-boarding) as well as to customers (e.g., for slice ordering and management).

The Process Engine: manages and monitors the state of activities from order, design, and creation to termination of NSLI:

- Order - Upon receiving a new NSLI design order (containing an NSLR), the NSLM forwards this request to DDF.
- Design & Verification - The DDF designs an actual NSLI based on NSLR, creates a customer-specific NSLD, and verifies it in a non-operational environment.
- NSLD onboarding - After successful NSLD design and verification, the NSLM orders a deployment of the NSLI. The DDF on-boards this NSLD to the MDDE.
- Deployment - The MDDE extracts the resource domain descriptors, NF configuration data and workflows from the NSLD. Then, according to the workflow, it sends the resource domain descriptors to the appropriate resource managers to deploy NFs and other resources in the respective resource domains. In parallel with network deployment, the MDDE prepares an OSS to manage a new network, by instantiating necessary managed objects and data structures.
- Configuration - Upon successful deployment, the MDDE notifies the OSS that a new network has been created, forwarding it the NF configuration data. This triggers EM to

configure network components in relevant resource domains, along with performance and fault monitoring and reporting.
- Activation - The MDDE notifies BSS that a new network has been deployed and configured, which forwards the user and service configuration data to OSS to activate the network.
- Operations - After successful deployment, configuration, and activation of NSLI, the NSLM gives the control over NSLI lifecycle to NLF.

2) DDF: designs a NSLI with the support of Network Slice Design Studio tools and algorithms, and using the available network components and infrastructure resource models from a MNO's network. It dynamically converts NSLR into an optimal network design with respect to cost and performance objectives.

A MNO specifies in policies which objectives are more important than others. The DDF extracts this information from policies at runtime and formulates the weighted multi-objective cost function of design algorithms. It also prepares inputs and boundary constraints from the NSLR, available network components (VNFs, PNFs, links) and infrastructure resources.

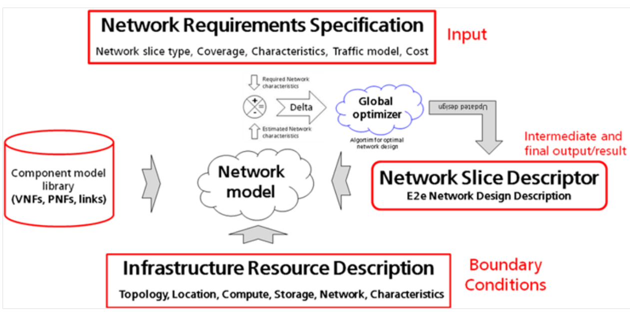

Fig. 7. Automated network slice design

As depicted in Figure 7, an automated network slice design is an iterative process, where design algorithms can be run several times until meeting the intended objectives. In each design attempt there is a possibility of modifying/adjusting its parameters or even some of the objectives. A result of each design attempt is sent back to operator for review. The final result of these algorithms is an optimal end-to-end network slice design that contains: (1) a list of required network functions (VNFs, PNFs) and links to interconnect these NFs, (2) the physical and logical resources that should be part of each NF, (3) instructions about in which resource domain to put each NF, and (4) a set of policies for different purposes.

Based on this network design, the DDF creates the necessary resource domain descriptors and workflows for deploying NFs and links in the respective resource domains, fetches the NF configuration data from the NSLDB, and inserts all this information in a customer-specific NSLD. It verifies and onboards the NSLD.

3) MDDE: The MDDE unpacks the NSLD, using it to deploy, configure and activate NSLI in the appropriate resource domains. It extracts the resource domain descriptors, workflows, and configuration scripts and performs the deployment, configuration and activation activities according to the workflow(s).

At operations time the MDDE gathers the relevant performance, fault, and resource usage data of a NSLI from the corresponding resource managers and EM, forwarding this data to the NLF. Additionally, it collects a list of available infrastructure resources and network components from the resource domains, the information about (organizational) sub-networks, regularly updating this information in the NSLDB.

4) NLF: The NLF receives all the performance, fault, and resource usage events from multiple resource domains and delegates the management responsibility to the relevant management entity. The OSS assigned to a NSLI is responsible for managing the fault and performance events of PNFs, while NFV MANO manages the VNFs fault and performance data. For SLA violations and escalation events related to NSLI there is a Network Slice Operations interface towards a network administrator that can manually resolve an issue. If there is a need to change a VNF placement or reconfigure a NSLI due to the VNF overload, the NLF can send this design modification request to NSLM. The NLF grants additional resources to a slice and orders revoking of resources from the slice (while consulting the slice policy). It also resolves conflicts about resource allocation among NSLIs.

VI. Conclusion

This paper describes a novel network slicing management and orchestration framework that automates network slice design, deployment, configuration, activation, and lifecycle management in multiple network infrastructure resource domains. It extends the 3GPP management reference framework with management of NFs and infrastructure resources in multiple network infrastructure resource domains, the network slice design time and runtime components, and the required interfaces and data structures between these components. Future work includes prototyping and verification of NESMO platform on a selected 5G use case.

References

[1] GSMA, "Understanding 5G: Perspectives on future technological advancements in mobile," White Paper, Dec. 2014.
[2] 3GPP TS 22.852, "Study on Radio Access Network (RAN) sharing enhancements," Release 13, Sep. 2014.
[3] 3GPP TS 22.891, "Feasibility Study on New Services and Markets Technology Enablers," Release 14, Sep. 2016.
[4] ETSI GS NFV 003 V1.2.1, "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV," Dec. 2014.
[5] N. McKeown et al., "Openflow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.
[6] M. Chiosi et al., "SONATA: Service Programming and Orchestration for Virtualized Software Networks," https://arxiv.org/abs/1605.05850, May 2016.
[7] K. Katsalis, N. Nikaein, E. Schiller, R. Favraud, and T. I. Braun, "5G Architectural Design Patterns," in *Proc. of IEEE ICC Workshop on 5G Architectures (5GArch 2016)*, Kuala Lumpur, Malaysia, May 2016, pp. 8–13.
[8] 5G NORMA D3.1, "Functional Network Architecture and Security Requirements," Dec. 2015.
[9] NGMN Alliance, "5G White Paper," Feb. 2015.
[10] 3GPP TR 32.842, "Telecommunication management; Study on network management of Virtualized Networks," Release 13, Dec. 2015.
[11] 3GPP TS 28.500, "Telecommunication management; Management concept, architecture and requirements for mobile networks that include virtualized network functions," Release 14, Sep. 2016.
[12] 3GPP TR 23.799, "Study on Architecture for Next Generation System," Release 14, Nov. 2016.
[13] ONF, "OpenFlow-Enabled Mobile and Wireless Networks," Solution Brief, Sep. 2013.
[14] 5G PPP, "5G Vision," White Paper, Feb. 2015.
[15] IMT-2020(5G) Promotion Group, "5G Vision and Requirements," White Paper, May 2014.
[16] 5G Forum Korea, "5G Vision and Requirements of 5G Forum," Solution Brief, Dec. 2014.
[17] 4G Americas, "5G Technology Evolution Recommendations," White Paper, Oct. 2015.
[18] Qing Wei, DoCoMo Euro-Labs, "An operator's view on 5G network - Towards a flexible network architecture," In Workshop on "5G: Visions, Requirements, Solutions", Dec. 2015.
[19] AT&T, "Domain 2.0 vision," White Paper, Nov. 2013.

[20] Deutsche Telekom, "Network Slicing A Key Concept for 5G," White Paper, Aug. 2015.

[21] China Mobile, "From Industry 4.0 to Internet+," White Paper, May 2015.

[22] Ericsson, "5G Use Cases," White Paper, Jun. 2015.

[23] Nokia, "Programmable 5G Multi-Service Architecture," White Paper, Sep. 2015.

[24] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From Network Sharing to Multi-tenancy: The 5G Network Slice Broker," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 32–39, 2016.

[25] ETSI GS NFV-IFA 014, "Network Functions Virtualisation (NFV); Management and Orchestration; Network Service Templates Specification Disclaimer," Oct. 2016.