Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

L. Geng
L. Wang
China Mobile
S. Kuklinski
Orange
L. Qiang
Huawei Technologies
S. Matsushima
Softbank
A. Galis
University College London
Luis. Contreras
Telefonica

October 30, 2017

Problem Statement of Supervised Heterogeneous Network Slicing
draft-geng-coms-problem-statement-01

Abstract

This document discusses the general requirements and problem statement of supervised heterogeneous network slicing. The purpose of this document is to identify the key network components that are used to create a network slice instance. Base on this information, a general network slice template can be visualized. Furthermore, the requirement of a common information model is identified and corresponding management consideration of heterogeneous network slice instance is also discussed.

Table of Contents

1. Introduction

The concept of network slicing is not new but energized greatly under 5G work in 3GPP. It is expected that further 5G network should be capable of providing dedicated private network for different verticals according to their specific requirements, which are created by diversity of new services such as high definition (HD) video, virtual reality (VR) and V2X applications. Looking at the development of future network, no matter the service is connected via

5G cellular RAN, FTTx optical access network or other dedicated connections, this resource dedication has become a fundamental technology for services requiring extreme quality of user experience. The best effort transport is not good enough as both subscribers and application providers are looking for and willing to pay for certain level of quality dedication. Therefore it is inevitable for service providers (telecommunication infrastructure owners) to rethink the means of management and operation of their networks, which should support end-to-end slicing capabilities.

The requirements from different verticals may be extremely diversified. Typical examples includes high bandwidth, low latency, high level of isolation, specific security and encryption requirements and etc. These requirements may also change dynamically along time since the services of certain industry vertical changes very fast, and sometime spontaneously (i.e. burst bandwidth/latency requirement from on-line shopping provider on certain period). It is expected that the configuration of certain network slice instances are very dynamic in a case-by-case manner. Meanwhile, there are many technology options to fulfil particular requirements depending on considerations on many aspects including cost, TTM and etc. The diversity of both requirements and technology options makes network slices significantly heterogeneous.

In order to provide cost-effective and efficient network slice configuration, service provider needs to understand specifically the components it can make use to create a network slice instance and how these components map with the customer requirements. These components include both network resources and management entities.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.2. Terminology

Network Slicing - A management mechanism that Network Slice Provider can use to allocate dedicated network resources from shared network infrastructures to Network Slice Tenant.

Network Slice - A network slice is a managed group of dedicated network resources to meet certain network functionality and performance characteristics required by the network slice tenant(s). It is re-configurable and is supervised by the network slice provider.

Network Slice Provider - A network slice provider (NSP), typically a telecommunication service provider, is the owner or tenant of the network infrastructures from which network slices can be created. The network slice provider takes the responsibilities of managing, orchestrating and monitoring the corresponding resources to implement a network slice and provide the Network slice tenant certain level of management.

Network Slice Tenant - A network slice tenant (NST) is the user of specific network slice, in which customized services are hosted. Network slice tenants can make requests of the creation of new network slice through NSaaS platform. This request will be delivered to network slice controller for implementation purposes.

2. The Concept of Supervised Heterogeneous Network Slicing

Network slicing is a management mechanism that an NSP can use to allocate dedicated network resources from shared network infrastructures to an NST. This dedication may be performed in various forms on a diversity of resources depending on specific NSP’s network availabilities. Typical examples include physical and logical isolation of network connectivity with certain QoS guarantees, bare metal and virtualized computing resources, dedicated storage and specific pre-define network functions such as NAT server, SDN controller and etc. Other network technologies such as ICN and CDN may also be part of the resource dedication. Network slicing gives the NSP full flexibility to either logically or physically lease a partition of their networks to the NST with required functionalities and performances.

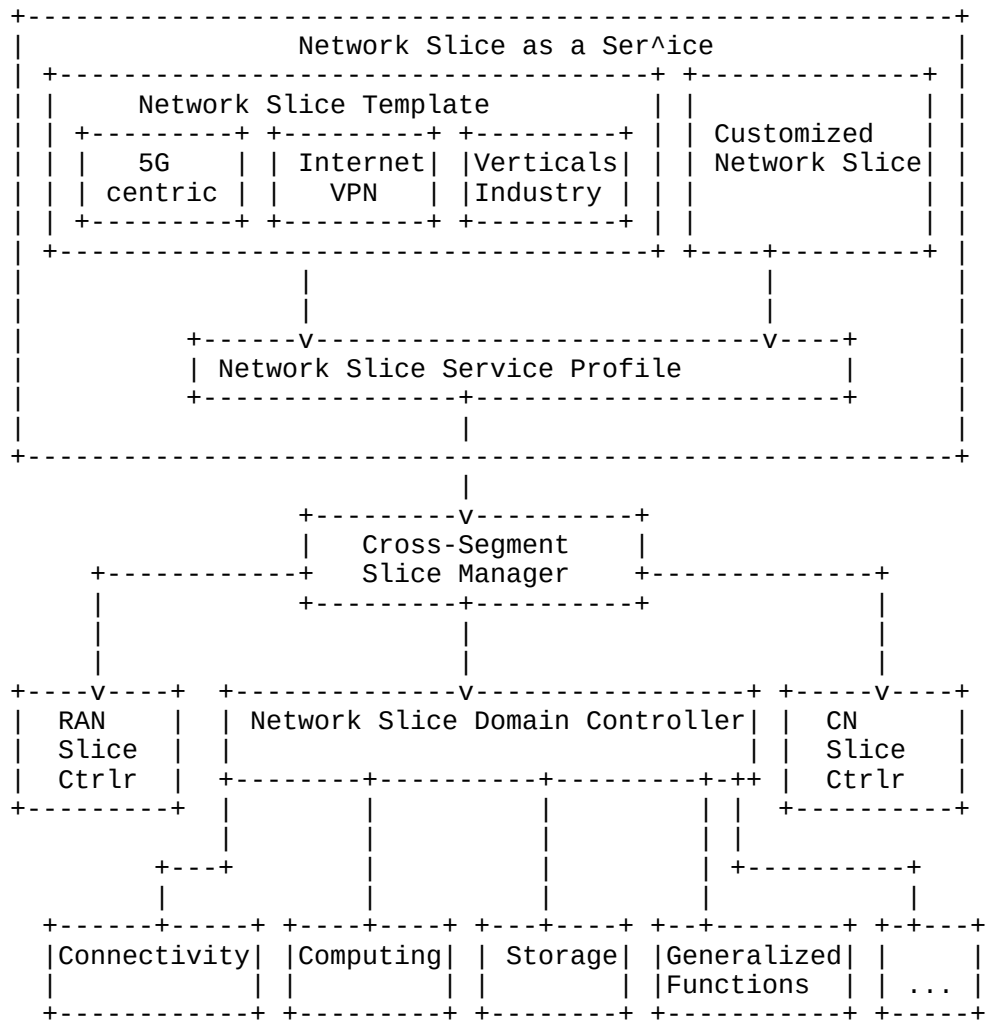

Figure 1: The concept of supervised heterogeneous network slicing

As network slicing is introduced to overall network management, it is anticipated that new business models may be created. With a more flexible, elastic and modularized network, the shared network infrastructures can be sliced and offered as a service to end users and verticals. For instance, a network slice with dedicated network resources with a customized topology can be provided as a service (NSaaS)to the NST.

Figure 1 illustrated the concept of how NSaaS is supervised within a heterogeneous network. In this concept, a network slice can either be implemented according to pre-defined network slice templates or customized requirements. On one hand, network slice template is designed by NSPs for the ease of mapping NST's request to a NSaaS with rather common resources and performance requirements. This includes but not limited to 5G-centric services such as eMBB and URLLC network slices, dedicated internet VPNs for game acceleration and video delivery, specific vertical industrial internet dedications such as smart factory and so on. On the other hand, implementing network slicing using customized approach provides NST with the full flexibility of composing its own network resource pools according to various requirements and constraints respectively. As the NST defines a preferred network slice service either from a pre-defined template or full customization, a network slice service profile is therefore generated.

The network slice service profile is sent to cross-segment slice manager, which coordinate resource from different network segment. The cross-segment network slice manager decomposes the network slice service profile and assigns corresponding segment network slice information to multiple network slice domain controllers. In this illustration, radio access network, transport network and core network are used as common examples of network segments with network slice domain controllers. However, it is worthy of mentioning that backhauling is only one of the use cases of transport segment network slicing.

In the slice controller within a specific network segment, NSaaS information is translated to resource-level description of a network slice for implementation purposes. In particular, it visualizes a network slice with specific resource components that comprise computing, storage, and generalized functions etc. The slice controller also coordinates heterogeneous domain controllers/managers for network slice implementation.

Although a general network slice may consist of resource components from various network segments, the supervised heterogeneous network slicing in this document refers only to IETF segment and sees the managed network slice a stand-alone one within IETF scope. It may be used by the cross-segment network slice manager to create a more comprehensive end-to-end network slice including other network segments that are out of scope of IETF.

2.1. Heterogeneity

Heterogeneity is the nature of network slicing since the requests of NSaaS from the NST are diversified. The slice controller has to supervise heterogeneous resources in various domains in response to NSaaS demands. The different types of resources a network slice controller needs to supervise includes connectivity, storage, computing, generalized functions and others. Furthermore, even for a single type of resources, an NSP may have difference management domains because of either technical or geographical variations. For example, the network slice controller is supposed to have the ability to coordinate multiple typical existing technology domains including optical transport network, IP routing network and layer-2 switched network. It also needs to integrate network domains with different management/control mechanism. For instance, the slice controller is necessary to be compatible with both SDN-enabled ACTN-aware networks and traditional EMS-managed networks. Another case is the management of virtualized resources using VIMs such as Openstack. In order to provide computing/storage resource support for network slicing, these domains are also inevitable required to be coordinated.

No matter it is a green field or brown field implementation, the network resources used to create a network slice are very likely to reside in different heterogeneous management domains. The supervised heterogeneous network slicing provides the capability of coordination and orchestrate the resources from different domains.

2.2. The requirement of general supervision of network slicing

Supervision is required by NSP, making use of OAM tools to maintenance the network slice. The slice controller needs to provide this capability to NSP to supervise the all the network slices that are implemented.

There are varieties of reasons why supervision is crucial in the case the network slicing. First of all, the network slice controller would not be able to deal with the lifecycle management of network slices without supervision abilities. Besides, given the characteristic of heterogeneous environment, the network slice controller must be crystal clear of the underlay resource information that is reported and synchronized by the domain controllers/managers. If this is seen as a network resource capability exposure approach, the network slice controller must supervise this approach to define how this information gathered and used. Furthermore, the network slice controller need to provide slice-level monitoring ability during the complete life circle of a network slice. This is essential for the claim benefits of quality guarantee by the implementation of network slicing. For example, the slice controller

need to supervise and monitor the jitter of a certain link in a network slice with deterministic property requirement by NST. This jitter performance should also be provided to NST for SLA references.

Last but not the least, it is common that some NST would like to participate in the management of its network slice. The slice controller should provide this capability by using the intra-slice management (discussed later in section 5). This management capability exposer must be supervised by NSP to avoid any resource/ performance conflicts with other network slices.

3. Network Resources for Supervised Heterogeneous Network Slice

Fundamentally, network slices are created based on the shared network resources. There are many existing technologies which focus on the management of those network resources. For example, various type of domain SDN controllers supervise the connectivity resources within each technology or geographical domains, and MANO supervises the NFV infrastructures. As previously discussed, network slicing provides a management mechanism for NSP to create network slices from the underlay resources. It oversees all these resources and decides the placement of specific resources according to certain path and topology constraints.

Network slicing does not have any constraints on what type of resources NSPs may or may not use as part of the network slice creation. This is completely subjected to NSP’s policy. However, for the ease of management and operation, it is worthy to have a guideline to at least categorize the common resources that NSP may offer to NST as a network slice service. The section endeavours to provide a prototype catalogue of the resource components for network slice creation. In general, the components that an NSP can use to create a network slice include connectivity, computing, storage and generalized functions. Other wide-scale network functionalities including ICN and CDN are also regarded as customized network resources.

3.1. Connectivity Resources

Connectivity is one of the essential components for a network slice. It can be as simple as a best effort point-to-point VPN or a physical link using a dedicated wavelength. It may also have more complex topology with other specific requirements including bandwidth, latency and etc. The characteristics of the connectivity component may include the following aspects.

- Node - The description of a network node at network slice level abstraction. The abstraction level depends on the provided node

resource information from the south bound interface of the transport network slice controller.

- Link - The description of a network link between two nodes in a network slice.

- Topology - The description of connection topology of a network slice. It should explicitly describe the connectivity relationship between each access point of the network slice. An NSP should be able to understand the overall connectivity requirement of a network slice from this topology information.

- Bandwidth - The description of bandwidth requirements of specific links within a network slice. The requirements includes exactly amounts of assured bandwidth, maximum bandwidth and other bandwidth QoS-specific requirements

- Latency - The description of link latency requirements within a network slice. It should identify the exact amount of latency between a link defined in connection topology.

- Determinism - The description of the determinism of a link latency. This should be defined in addition to the latency, which further specify the jitter of the latency for a given link.

- Isolation level - The description of isolation level of a network slice. A NST may request logical isolation which can be mapped to tunnelling technologies. It may also request explicitly a dedicated lamda or even physical link for specific services.

3.2. Computing Resources

If an NST would like to host virtualized functions in a network slice, it may be interested in asking for specific computing resource including both bare metal servers and virtual machines. The computing resource can be specified considering the following characteristics.

- CPU resources - The CPU specification including CPU model, frequency, quantity of physical/virtual CPU and etc.

- RAM resources - The RAM size associated with the requested computing resources in a network slice.

- Virtual resources - The pre-defined virtual resources including both virtual machines and containers associated with a specific network slice.

- Other - This may include GPU requirements and other specific computing resources

3.3. Storage Resources

It is necessary for NSP to provide storage components in a network slice since NSTs may want to host contents on dedicated resources. Meanwhile, NSP may also prefer to use dedicated storage for specific service policies, authentication information and other management profiles.

- General storage - The description of storage resource in a network slice. This may include the location, type, size and usage of the storage resource. The general storage requirements may closely related to the connectivity topology as well.

- CDN service - If an NSP can provide a turn-key CDN solution for the NST. It can also include CDN service within a network slice.

3.4. Generalized Function Blocks

Many dedicated network functions, either physical or virtual, may requested by a NST. Typical example include common network functions as DHCP server, DNS, NAT, Firewall, SDN controller. Application-level functions may also exist in a network slice, such as session management, mobility management and etc. NSP should be able to provide such generalized function blocks according to NST’s request.

- Physical network function blocks- The description of dedicated physical network functions. Physical network functions are network equipments with dedicated software and hardware, which are strictly coupled for the purpose of a providing specific network function.

- Virtual network function blocks- The description of virtualized network functions. VNFs are software entities which are normally hosted within pre-allocated virtual machines (or containers). The virtual resources which are required by the VNF should be also specified in terms of computing resources as described previously.

3.5. Other Resources

A category of customized resources is reserved for network slicing since NSPs may have unique capabilities that may be used as part of the network slicing to provide even greater innovative functionality. Resources such as ICN-aware subnet, CDN network and etc. are some t potential attributes in this category.

4. The Requirement of Common Operation and Management for Supervised Heterogeneous Network Slice

Network slice can only be created with resource components that are available in its network. It is expected that different NSPs have various constraints and policies. The abstraction of resources is gathered from the network configuration models whose attributes are maintained by heterogeneous domain controllers/managers. Based on this information, a full set of resource capabilities is established. In order to provide network-slice-level OAM, it is extremely important for the heterogeneous transport network slice controller to visualize a network slice in terms of systematic association of these individual resources. This visualization model describes the network slice at a resource granularity and abstraction level that are provided by the underlay heterogeneous domain controllers and managers. It is a technology-unspecific model since how each partition of a network slice should map to specific resource capability is implementation-specific.

In addition, the heterogeneous transport network slice controller receives service delivery model from the cross-segment network slice manager with high level network slice requirements described in the network slice service profile. The service delivery model includes network slice service description in business view point. Before it can be mapped to resources capabilities, it has to be translated to a network-slice level abstraction in network resource view point, with the compatible granularity the is exposed from the underlay resource capabilities.

A common information model is required for the operation and management in the heterogeneous network slice controller to provide the above abilities. It acts as an intermediate guideline model, which provides comprehensive technology-unspecific description of a network slice. This model does not specify the allocation of certain partition of network slice to underlay technology domain or the mapping of certain protocol to network slice performance requirements. However, it is the fundamental model that specifies each node, link, function blocks and corresponding performance requirements in an established network slice.

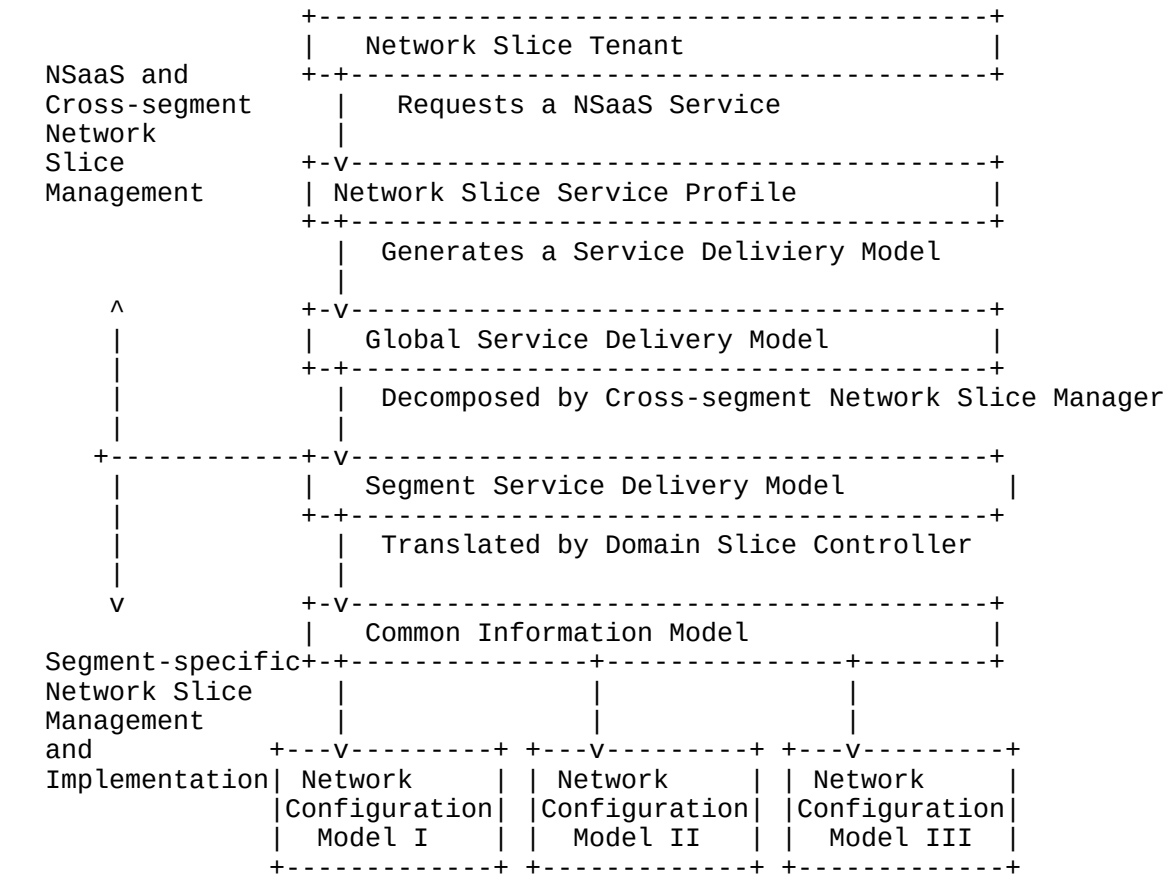

Figure 2: Common Information Model in Network Slicing

Figure 2 demonstrates the relationship between different models in the scope of supervised heterogeneous network slicing management. A service profile is created upon the request from a NST for a network slice service. This service profile is sent to cross-segment slice manager by global service delivery model. The global service delivery model is further decomposed to various segment service delivery model. In IETF's concern, the transport segment service delivery model is the starting point for a network-slice-aware service implementation.

Within the transport domain, the service delivery model is translated into a common information model, which strictly aligns with the underlay resource constraints. A common information model is created

for each network slice, and it comprehensively visualizes all the components topologies within the slice and corresponding functionality and performance parameters

In order to coordinate different technology domains to create the corresponding network slice, the common information model is mapped to network configuration models for different domains respectively.

The common operation and management is essential for network slicing since a network slice consist of resource components typically from diversity of management domains. There is yet a network-slice-aware approach that is able to orchestrate and coordinate these domains. The common operation and management of network slicing is designed for this purpose. At the same time, there are other requirements in terms of heterogeneous network slice management, which are enabled by this approach:

- common resource negotiation and abstraction
- exchanging information between multiple management domains
- operations and monitoring across multiple management domains
- network-slice operational control (i.e. life-cycle management) and management capability exposure to NST

4.1. Problem Scope

The common information model acts as the key element in common operation and management of network slicing. Foresee derivative including network slice monitoring, life cycle management, network slice interconnect, fault detection and protection mechanisms are also interesting and inevitable matters that supervised heterogeneous network slicing need to investigate.

More work is also needed to define a north interface for the slice controller, we can envision how the slice controller could interface with existing systems (e.g. using the NFV-MANO architecture as a guide), and by extension delimit the scope of the slice controller function.

In one scenario, the slice controller can interface with a virtual infrastructure manager (VIM), such as OpenStack. The slice controller can in this case be considered as a lower layer component of the VIM, or as a network management component controlled by the VIM. In another scenario, the slice controller can implement a VIM, and present an interface to an orchestrator.

5. Management of Heterogeneous Network Slice

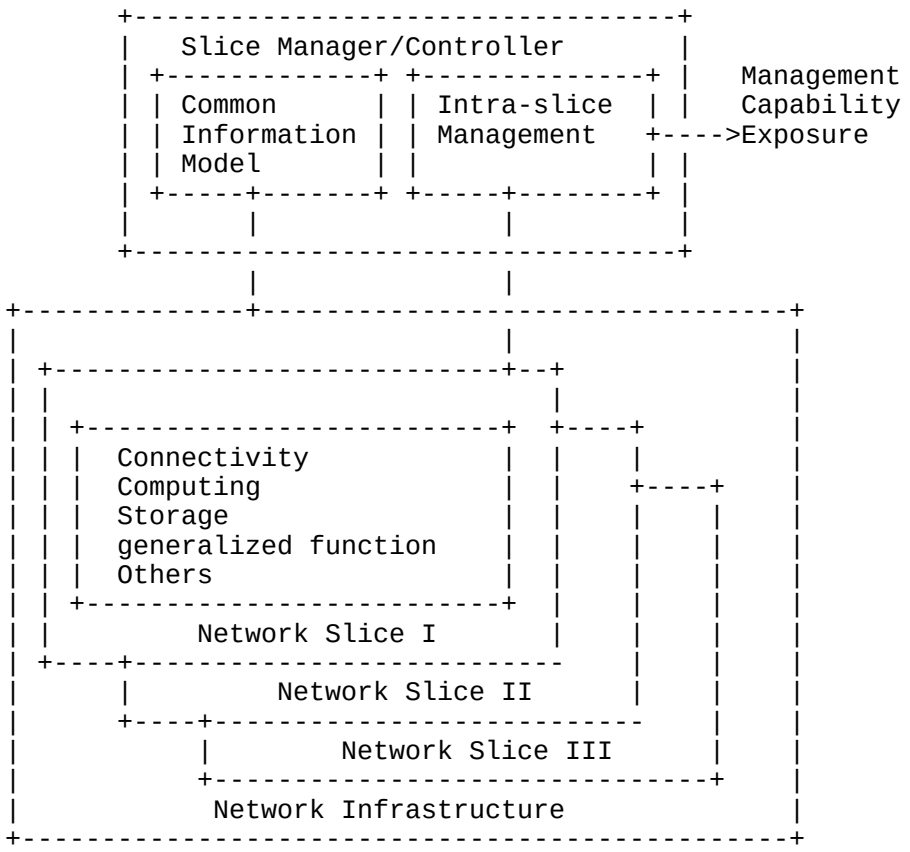

Figure 3: Common Information Model in Network Slicing

Given that common information models are set up for various network slice. The network-slice-level management is carried out by the slice controller accordingly. Meanwhile, an intra-network-slice controller is need for each network slice. The controller oversees the OAM of a single network slice and report to the heterogeneous transport network slice controller. As per agreement between NST and NSP, certain capabilities of intra-slice management may be exposed to NST. NST are authorized to use these capabilities to maintain its network slice in a view of dedicated networks and resources. The network slice-level information must not be exposed, which means the NST should not know he existence of any other network slices through intra-slice manager. The exposed controller capability should be supervised by the NSP, so that the network slice will not violate network slice-level policies.

6. IANA Considerations

This document makes no request of IANA.

7. Security Considerations

Each layer of the system has its own security requirements.

8. Acknowledgements

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

Authors' Addresses

Liang Geng
China Mobile
Beijing
China

Email: gengliang@chinamobile.com

Lei Wang
China Mobile
Beijing
China

Email: wangleiyjy@chinamobile.com

Slawomir Kuklinski
Orange

Email: slawomir.kuklinski@orange.com

Li Qiang
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095

Email: qiangli3@huawei.com

Satoru Matsushima
Softbank

Email: satoru.matsushima@g.softbank.co.jp

Alex Galis
University College London

Email: a.galis@ucl.ac.uk

Luis Miguel Contreras Murillo
Telefonica

Email: luismiguel.contrerasmurillo@telefonica.com