Problem Statement of Supervised Heterogeneous Network Slicing
draft-geng-coms-problem-statement-00

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. Based 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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 29, 2018.
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 Slice Instance - A network slice instance (NSI) is a managed group of subsets of network resources, network functions and network management entities, forming a complete instantiated logical/physical network to meet certain network characteristics required by the network slice tenant(s). A network slice instance may also be shared across multiple services provided by the network slice tenant. It is re-configurable and is managed by network slice provider.

Network Slice Provider - A network slicing provider (NSP), typically a telecommunication service provider, is the owner or tenant of the network infrastructures from which network slices are created. The network slicing provider takes the responsibilities of managing and
orchestrating corresponding resource and management components that the network slicing consists of.

Network Slice End-point - A network slice end-point (NSE) is a network-slice-aware terminal, typically subscribed to the service which is hosted in a network slice instance. A network slice end-point may be capable of subscribing to multiple services hosted independently in different network slice instance simultaneously.

Network Slice Tenant - A network slice tenant (NST) is the user of specific NSIs, in which specific services are hosted and can be provided to NSEs. Network slice tenants can make requests of the creation of new network slice instances. Certain level of management capability should be exposed to network slice tenant from network slice service provider by pre-allocated outsource management entities.

End-to-end Network Slice - A cross-domain network slice which may consist of access network (fixed or cellular), transport network, (mobile) core network and etc. End-to-end network slice can be customized according to the requirements of network slice tenants.

Network Function (NF) - A processing function in a network. It includes but is not limited to network nodes functionality, e.g. session management, mobility management, switching, routing functions, which has defined functional behaviour and interfaces. Network functions can be implemented as a network node on a dedicated hardware or as a virtualized software functions. Data, Control, Management, Orchestration planes functions are Network Functions.

Virtual Network Function (VNF) - A network function whose functional software is decoupled from hardware. One or more virtual machines running different software and processes on top of industry-standard high-volume servers, switches and storage, or cloud computing infrastructure, and capable of implementing network functions traditionally implemented via custom hardware appliances and middle-boxes (e.g. router, NAT, firewall, load balancer, etc.)

2. The components for a network slice instance

Fundamentally, NSIs are created based on the shared network infrastructures. One can not create or define an NSI with components that are not available in the shared infrastructure. Hence, it is extremely important, both for NST and NSP, to understand a clear scope of the usable components for NSI construction. An NSP can therefore refer to this general scope to decide how each component can be orchestrated and provided as a packaged network slice service to NSTs. Based on this information, NSP can also further outline and
figure out the what capability each component can offer and how they meet NST’s demands. Overall, it is not possible to map the offered capability of a network slice instance with the specific demands from an NST if an NSP is not clear on what components and corresponding characteristics can be provided.

Network slice instance consists of dedicated network resources which are orchestrated using all the available components offered by a NSP network. In general, the components that an NSP can use to create an NSI include connectivity, computing, storage, and management entity.

2.1. Connectivity of network slice instance

Connectivity is one of the essential components for an NSI. It can be as simple as a best effort point-to-point VPN or a dedicated complex topology with other specific requirements including bandwidth, latency and etc. The characteristics of the connectivity component should include the following aspects.

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

- **Bandwidth** - The description of bandwidth requirements of specific links within an NSI. The requirements includes exactly amounts of assured bandwidth, maximum bandwidth and other bandwidth QoS-specific requirements

- **Latency** - The description of link latency requirements within an NSI. 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 an NSI. A NST may request logical isolation which can be mapped to tunnelling technologies. It may also request explicitly a dedicated lambda or even physical link for specific services.

2.2. Computing for network slice instance

If an NST would like to host virtualized functions in an NSI, it may be interested in asking for specific computing resource including...
both bare metal common servers and virtual machines. This resource should also be specified considering the following characteristics.

- **CPU resources** - The physical and virtual CPU specifications a NST may request a NSP to provide.
- **GPU resources** - The GPU specifications a NST may request a NSP to provide.
- **RAM resources** - The RAM size associated with the requested computing resources in a NSI.

Instead of providing bare metal resources, NSP may also provide ready-to-used virtual machines and containers as part of the NSI. This virtual resources need also be specified with virtualization technology options, CPU/Virtual CPU requirements and etc.

### 2.3. Storage for network slice instance

It is necessary for NSP to provide storage components in an NSI 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 NSI. 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 an NSI.

### 2.4. Pre-defined function block for network slice instance

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 NSI, such as session management, mobility management and etc. NSP should be able to provide such pre-defined 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. The requirements of common information model for supervised heterogeneous network slice

As NSTs are not expected to be "network experts", the requirements injected to a NSP may be diversified in forms. NSP may have different preferences for the network slice service model provided to potential NSTs. However, there is a need for a common information model which explicitly describes the components and parameters within a NSI.
As seen in Figure 1. The common information model is used to describe a NSI according to the service model provided by NSTs. It is then further de-composited to models that are used by various management domain within the NSP’s network infrastructure.

3.1. Management of heterogeneous network slice

The network slice management include two levels. One is network-slice level management which is maintained by NSP, the other is intra-slice management which is maintained by NST but supervised by NSP.

o Network slice management agent - This is the NS-level management agent provided by NSP. Each created NSI should have a logical
entity serving as a network slice management agent. It executes the OAM messages received from the NSP network slice manager including life-cycle management, monitoring and etc. A profile of the created NSI should also be maintained within this agent, where the status of each element can be managed.

- Intra-slice management - As per agreement between NST and NSP, intra-slice management may be provide by NSP to oversee an given NSI as a general private network. NST are authorized to use this management capability to maintain the NSI. The NSI-level information is transparent to intra-slice management, which means the management system does not know the existence of network slice instances. The exposed management capability should be supervised by the NSP, so that the NSI will not violate NSI-level policies. Meanwhile, intra-slice management

4. IANA Considerations

This document makes no request of IANA.

5. Security Considerations

Each layer of the system has its own security requirements.

6. Acknowledgements

7. References

7.1. Normative References

[I-D.finn-detnet-architecture]

[I-D.qin-netslices-use-cases]
Qin, J., kiran.makhi@huawei.com, k., Dong, J., Qiang, L., and S. Peng, "Network Slicing Use Cases: Network Customization for Different Services", draft-qin-netslices-use-cases-00 (work in progress), March 2017.

7.2. Informative References

Authors’ Addresses

Liang Geng
China Mobile
Beijing
China

Email: gengliang@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