Network Slice Provision Models

draft-homma-slice-provision-models-01

Abstract

Network slicing is an approach to provide separate virtual network based on service requirements. It’s a fundamental concept of the 5G, and the architecture and specification is under standardization in several organizations. However, the definitions and scopes of network slicing vary to some degree from one organization to another. This document provides classification of provisioning models of network slice for clarifying the differences on the definitions and scopes.

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/.
This Internet-Draft will expire on January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction and Motivation ................................... 3
   1.1. Differentiated Roles in Network Slice Provisioning ........ 3
   1.2. High-level Problem Statement ............................. 4
2. Definition of Terms ............................................ 4
3. General Requirements for Network Slicing ........................ 7
   3.1. Requirements/Attributes for Network Slice ............... 7
4. Network Slice Structure ......................................... 8
   4.1. Resources for Structuring Network Slices ............... 8
   4.2. Basic Network Slice Structure ............................ 12
   4.3. Stakeholders in the Structuring Network Slices .......... 14
5. Variations of Network Slice Creation .......................... 15
   5.1. Ready-made Network Slice ................................ 15
   5.2. Custom-made Network Slice ................................. 15
   5.3. semi-Custom-made Network Slice ............................ 15
6. Network Slice Provision Models ................................ 15
   6.1. SaaS-like Model ........................................... 16
       6.1.1. Capability in SaaS-like Model ....................... 16
   6.2. PaaS-like Model .......................................... 16
       6.2.1. Capability in PaaS-like Model ....................... 17
   6.3. IaaS-like Model .......................................... 17
       6.3.1. Capability in IaaS-like Model ....................... 17
6.4. Mapping of NS Provision Models and Infrastructure Layering ............................................... 17
7. Security Considerations ....................................... 19
1. Introduction and Motivation

Network slicing is an approach to provide separate virtual networks depending on requirements of each service. Network slicing receives attention due to factors such as diversity of services and devices, and it is also a fundamental concept of the 5G for applying networks to such various types of requirements.

In addition, network slicing is expected to enable a business model to provide dedicated logical networks to 3rd parties or vertical customers on-demand, called NSaaS (Network Slice as a Service). For such usage, in network slicing, provision of networks able to guarantee communication characteristics end to end would be required. However, the definitions are not harmonized over several SDOs (Standards Developing Organizations).

This document clarifies provision patterns of network slice, and provides the definitions and scope of network slicing which are available over several organizations. Furthermore, the deliverables would be help for evaluating applicabilities of existing technologies/solutions to network slicing.

1.1. Differentiated Roles in Network Slice Provisioning

The widespread of system and network virtualization technologies has conducted to new business opportunities, enlarging the offer of IT resources in the form of Network Slices (NS). As a consequence, there is a clear differentiation between the owner of physical resources, the infrastructure operator, and the intermediary that conforms and delivers network services to the final customers, the Virtual Network Operator (VNO).

VNOs aim to exploit the virtualized infrastructures to deliver new and improved services to their customers. However, current NS techniques offer poor support for VNOs to control their resources. It has been considered that the infrastructure operator is responsible of the reliability of the NS elements but several situations advocate the VNO to gain a finer control on its resources. For instance, dynamic events, such as the identification of new requirements or the detection of incidents within the virtual system, might urge a VNO to quickly reform its virtual infrastructure and resource allocation. However, the interfaces offered by current
virtualization platforms do not offer the necessary functions for VNOs to perform the elastic adaptations they require to tackle with their dynamic operation environments.

1.2. High-level Problem Statement

Beyond their heterogeneity, which can be resolved by software adapters, NS platforms do not offer common methods and functions, so it is difficult for the virtual network controllers used by the VNOs to actually manage and control virtual resources instantiated on different platforms, not even considering different infrastructure operators. Therefore, it is necessary to reach a common definition of the functions that should be offered by underlying platforms to enable such overlay controllers with the possibility of allocate and deallocate resources dynamically and get monitoring data about them.

Such common methods should be offered by all underlying controllers, regardless of being network-oriented (e.g., ODL, ONOS, Ryu) or computing-oriented (e.g., OpenStack, OpenNebula, Eucalyptus). Furthermore, it is also important for those platforms to offer some "PUSH" function to report resource state, avoiding the need for the VNO’s controller to "POLL" for such data. A starting point to get proper notifications within current REST APIs could be to consider the protocol proposed by the \[WEBPUSH-WG\].

Finally, in order to establish a proper order and allow the coexistence and collaboration of different systems, a common ontology regarding network and system virtualization should be defined and agreed, so different and heterogeneous systems can understand each other without requiring to rely on specific adaptation mechanisms that might break with any update on any side of the relation.

2. Definition of Terms

This section lists definitions and terms related to network slicing. This document refers terms and view points on network slicing in some SDOs, such as 3GPP([TS.23.501-3GPP], [TS.28.530-3GPP], and [TS.28.801-3GPP]), and NGMN ([NGMN-5G-White-Paper]). However the scope of this document is not network slicing which is mobile specific but one for general networks, and thus some of definitions in this document may be different from ones of those documents.

Network Slicing: Network slicing indicates a technology, an approach, or a concept to create logical separate networks in support of services, depending on several requirements, on the same physical resources. This is possible by combinations of several network technologies.
Network Slice (NS): An NS is a logical separate network that provides specific network capabilities and characteristics. In 3GPP definitions, an NS potentially includes both data plane and control plane resources/functions.

Network Slice Instance (NSI): An NSI is a logical network instance composed with required infrastructure resources, including networking (WAN), computing (NFVI) resources, and some include additional network service functions such as firewall or load-balancer. It is composed of one or more Network Slice Subnet Instances.

Network Slice Subnet: A Network Slice Subnet is a representation of a set of required resources. It is composed and managed as a group of network elements.

Network Slice Subnet Instance (NSSI): An NSSI is a partial logical network instance represented as a network slice instance. It is a minimal unit managed or provided as a network slice. One or more NSSI structure an NSI or an E2E-NSI.

End-to-End Network Slice Instance (E2E-NSI): An E2E-NSI is a virtual network connecting among end points. It is composed of one or multiple NSSIs. This term is original of this document and is used when it should be emphasized that the target NSI provides connectivity from end to end. As an example, for providing an E2E-NSI on the 3GPP 5G network, combining three types of NSIs: RAN-, TRN-, and CN-NSIs would be required.

Transport (TRN)-NSSI: A set of connections between various network functions (VNF or PNF) with deterministic SLAs. They can be implemented (aka realized) with various technologies (e.g. IP, Optics, FN, Microwave) and various transport (e.g. RSVP, Segment routing, ODU, OCH etc). The overview of NSI composed with TRN-NSSI is shown in Appendix A.

RAN-NSSI: Regardless of RAN deployment (e.g. distributed-RAN, Centralized-RAN or Cloud-RAN), a RAN-NSSI creates a dedicate and logical resource on RAN for each NSI which are completely. The overview of NSI composed with RAN-NSSI is shown in Appendix A.

Core (CN)-NSSI: Regardless of Core deployment, a CN-NSI creates a dedicate and logical resource on Core network for each NSI which are completely. The overview of NSI composed with CN-NSSI is shown in Appendix A.

Network Slice as a Service (NSaaS): An NSaaS is a service delivery model in which a third-party provider or a vertical customer hosts
NSIs and makes them available to customers. In this model, there mainly two roles: NS provider and NS tenant.

Network Slice Provider (NS Provider): An NS provider is a person or group that designs and instantiates one or more NSIs/NSSIs, and provides them to NS tenants. In some cases, an NS provider is an infrastructure operator simultaneously. This includes NSI, NSSI, and E2E-NSI providers.

Network Slice Tenant (NS Tenant): An NS tenant is a person or group that rents and occupies NSIs from NS providers.

Network Slice Stakeholder (NS Stakeholder): An NS stakeholder is an actor in network slicing, and has roles of either NS provider or tenant.

Infrastructure Operator: An infrastructure operator is an organization who manages infrastructure networks or data centers for running NSIs. In the most of cases, infrastructure operators are initial NS providers on NSaaS. Also, some of them may be NS tenants simultaneously.

Vertical Customer: A vertical customer is an organization who provides some communicating services with using NSIs on NSaaS model. In many cases, a vertical customer become the final NS tenant on NSaaS. For example, video gaming companies or vehicle vendors will possibly be vertical customers.

Virtual Network Operator (VNO): A VNO is a person or group that operates virtual networks composed with resources or NSSIs rent from infrastructure operators and provides such virtual networks as NSIs to vertical customers who are final NS tenants. In some cases, infrastructure operators have this role in addition to operating their own infrastructure simultaneously.

Domain: A domain is a group of a network and devices administrated under a policy-based common set of rules and procedures.

Resource: A resource is an element used to create virtual networks. There are several types of resources, i.e., connectivity, computing and storage. The details are described Section 4.1

Virtual Network: A virtual network is a network running a number of virtual network functions.

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

Network Operation System: A network operation system is an entity or a group of entities for operating network nodes and functions as compositions of infrastructure network. For example, OSS/BSS, orchestrator, and EMS are considered to be network operation systems.

3. General Requirements for Network Slicing

On network slice operations, capabilities for dynamic instantiation, change, and deletion should be required because an NSI is established based on received orders from tenants in NSaaS. From this aspect, some mechanisms to design a network based on service requirements and to convert those to concrete configurations based on the design would be required.

In addition, each NS has to maintain concrete communication characteristics end to end, and resource reservations on data plane and isolation among NSIs would be required. Isolation is a concept to prevent the reduction of communication quality caused by disturbance from other NSs, and it may have some levels of enforcement, such as hard or soft isolations. In some cases, for providing appropriate communication between client and server, it would be allowed for NS tenants to put their applications as contents server on NSIs by using computing resources.

The required agility of slice operation and granularity of end to end communication quality requested can vary depending on provision model.

3.1. Requirements/Attributes for Network Slice

NS tenants will have specific requirements for network slices depending on the usages or service characteristics. Such requirements or the associated attributes are broken down into concrete design including network topology and configurations of infrastructure resources, and NS is established based on the design. The requirements or attributes on NSs are listed below:

- Requirements/Attributes of Network Resource
  - bandwidth
* latency
* jitter
* packet loss rate
* reliability (e.g., MTBF, MTTF)

Requirements/Attributes of Functionalities Resources

* function type (e.g., security, parental control)
* throughput
* packet error rate
* availability

4. Network Slice Structure

This section describes resources used for structuring NSs and the basic structure of E2E-NS.

4.1. Resources for Structuring Network Slices

A network slice is structured as combinations of the resources it uses. Such resources are mainly categorized into three classes: network/WAN, computing/NFVI, and functionality resources. Variations of each resource are described below. (Note that the lists are not exhaustive.)

Network(WAN) Resources:

* Connectivity:
  + (v)Link
    - Bandwidth per link/session
    - Connected area/end points
    - Forwarding route/path (e.g., for traffic engineering, redundancy)
    - Communication Priority (e.g., QoS class)
    - Range of jitter amount
+ Interface of vNode
  - QoS setting (e.g., Queue size, DSCP remarking, PIR/CIR)
  - Filter setting
+ vRouter/vSwitch (# Treated as a set of (v)links and interfaces of vNodes.)

* Multicast support
* Encryption support
* Authentication support
* Metadata conveyance (e.g., subscriber ID)

* Protocols for slice data plane:
  + VLAN
  + IPoE (IPv4 or IPv6)
  + MAP-E
  + DS-Lite
  + PPPoE
  + L2TP
  + GRE
  + MPLS
  + VxLAN
  + Geneve
  + GTP-U
  + Segment Routing MPLS
  + Segment Routing IPv6
  + NSH
  + Other
Computing (NFVI) Resources:

* (v)CPU core
* Storage
* Memory
* Disk
* vNIC
* Connectivity to VNF instances
* Virtual Deployment Unit:
  + Virtual Machine (VM)
  + container
  + micro kernel
* Resource Deployment Location (i.e., edge DC, central DC, public cloud, ..., etc.)

Functionality Resources:

* Image:
  + Data Plane (DP) NF:
    - GateWay (GW) function:
      o Access Point Type (e.g., for radio, Wi-Fi, and fixed accesses)
      o Slice Selection Setting
      o Terminate protocol
      o Authentication
    - Security Appliance:
      o IPS (Intrusion Prevention System)
      o IDS (Intrusion Detection System)
- WAF (Web Application Firewall)
  - DPI
  - Load Balancer
  - TCP Accelerator
  - Video Optimizer
  - Parental Control
  - Mobile DP functions (Ref. 3GPP 5GS)
    - gNB
    - UPF
    - Uplink Classifier

+ Control Plane(CP) NF:
  - DHCP
    - Fixed IP address allocation
    - Dynamic IP address allocation
    - The number of registered devices
  - DNS
  - VoIP (SBC, SIP server)
  - Mobile CP function (Ref. 3GPP 5GS)
    - AMF (Access and Mobility management Function)
    - SMF (Session Management Function)
    - PCF (Policy Control Function)
    - UDM (Unified Data Management)
    - NEF (Network Exposure Function)

* Provided VNF Type (e.g., open source, product of vendor#A, ...) etc.)
* Function location (e.g., edge DC, central DC, Public cloud, etc.)

In terms of security or usability for NS tenants, some abstraction on resource information would be required, however both setting parameters of underlay infrastructure and abstracted information may coexist in these lists.

For abstraction of parameters of underlay networks, some additional protocols or functions (like [RFC8453]) would be required. Moreover, for providing strict communication qualities, combinations of some technologies may be useful (ref. [I-D.dong-teas-enhanced-vpn]).

4.2. Basic Network Slice Structure

An E2E-NSI is constructed by stitching NSSIs instantiated on each participating domain. This includes the simplest case of a single NSSI as an E2E NS. Domain types where some NSSIs are established are described below:

- Fixed access network
- Mobile access network
- Transport network
- Fixed core network
- Mobile core network
- Data center (DC)
  - Edge DC
  - Central DC
- Private network
  - Enterprise
  - Factory
  - Utilities
  - Farming
  - Home/SOHO
* Other

Figure 1 describes the overview of this structure. Resources in each domain (e.g., access, core networks, and DC) are handled by management entities and constitute an NSSI. An E2E-NSI is established by stitching these NSSIs. Ways to stitch NS-subnets are described in [I-D.defoy-coms-subnet-interconnection] and [I-D.homma-nfvrg-slice-gateway].

---

Figure 1: Overview of NS Structure
Although it is shown that an NSSI belongs to just only one E2E-NSI in Figure 1, it may be allowed that multiple E2E-NSIs share an NSSI. Some resources may belong to multiple NSSIs as well.

In addition, structure on composition of NSI may be recursive. In other words, even though Figure 1 shows a case where NSSIs compose directly an E2E-NSI, in some cases, NSSIs compose an NSI which is a part of an E2E-NSI. The overview is shown in Figure 2. In this figure, NSI#4 is composed of NSSI#1 and NSSI#2, and it structures E2E-NSI#5 with NSSI#3.

---

**Figure 2: Overview of NS recursive structure**

### 4.3. Stakeholders in the Structuring Network Slices

Potential stakeholders in network slicing are described below:

- NSSI provider: infrastructure operator
- Intermediate-NSI provider: infrastructure operator, VNO
- E2E-NSI provider: infrastructure operator, VNO, service provider
- NS tenant: infrastructure operator, VNO, service provider, enterprise, mass user
- End customer: enterprise, mass user, etc.
5. Variations of Network Slice Creation

NSs can be classified according to their creation pattern into two types: ready-made (RM) NS, custom-made (CM), and semi-custom-made (sCM) NS. This section describes the features of these types.

5.1. Ready-made Network Slice

RM-NS is an NS creation pattern in which an infrastructure operator decides service requirements by itself, and established based on the requirements in advance. NS tenants select one of RM-NSs whose features are closer to their requirements.

This model doesn’t need immediacy on designing of NSI and enables to mitigate the difficulty of implementation compared with other models.

5.2. Custom-made Network Slice

CM-NS is an NS creation pattern in which an NS is established based on an order from a tenant and is provided to it. As examples of usage of CM-NS, an enterprise builds and operates a virtual private network for connecting several bases, or OTT (Over The Top) or other industrial service providers create NSs based on their own requirements and use them as a part of their own services (e.g., connected vehicles/drones, online video games, or remote surgery).

In this model, network operation system would be required to have incorporate intelligence for designing appropriate NSs on-demand.

5.3. semi-Custom-made Network Slice

sCM-NS is a derivation of a CM-NS. In sCM-NS, an NS provider designs the outline of NSs in advance, and a tenant tunes an NS with deciding some parameters or applications run on resources. For example, an infrastructure operator designs a logical network presenting connectivity, and tenants install their own applications on servers running on the logical network.

6. Network Slice Provision Models

This section classify NS provision models into three categories defined from aspect that granularity of information exposed to tenants. The provision models are categorized into three models: SaaS (Software as a Service) -like Model, PaaS (Platform as a Service) -like Model, and IaaS (Infrastructure as a Service) -like Model. The capabilities which NS tenants can have on management of NSs would vary depending on the selected provision model.
6.1. SaaS-like Model

In SaaS-like Model, underlay infrastructure is hidden from tenants, and tenants can receive desired communication environment without deep knowledge about network and servers. An NS tenant decides attribute values of its NS, such as bandwidth or latency, based on their requirements, and NS providers design and create NSIs which fulfill the values.

NS tenants need not to grasp detailed configurations in underlay networks in this model. However, it may not be possible to provide strictly desired NS to tenants because of abstraction of configurable parameters. Moreover, it may cause complexity on designing NS catalog due to quantities of selected attributes.

6.1.1. Capability in SaaS-like Model

In SaaS-like Model, an NS is represented for a tenant with attributes values listed in Section 3.1. In other words, an NS tenant never know the concrete configurations of components in underlay infrastructure.

An NS tenant chooses a value from the range presented by the NS provider in each attribute. The NS provider creates or changes a NS by configuring components in underlay infrastructures based on the decided attribute values.

In terms of telemetry for assurance of service qualities on a NS, a tenant can obtain telemetry information with unit of NSI, and never know ones of underlay components structuring the NS.

6.2. PaaS-like Model

In PaaS-like Model, an NS is represented with several components such as nodes and connectivities among them. An NS tenant can design and customize its desired NS with combining such components. NS providers breakdown the NS designed by the NS tenant to concrete configurations of their infrastructure, and create/change NSSIs by inputting the configurations. An NS tenant is also able to incorporate its own functions or applications into its NSI by using computing resources provided from NS providers.

This model potentially has high customizability of NS rather than SaaS-like model, but needs NS tenants to have some knowledge about network management. In terms of designing NS, the tenants provide outline of their NSs, and thus it would make creation of concrete configurations be easier.
6.2.1. Capability in PaaS-like Model

In PaaS-like model, an NS is represented with NF nodes and their connectivities. An NS tenant can indicate functionalities of NF nodes and their locations. Also, the tenant decides attribute values of connectivities. An NS provider creates or changes an NSI by configuring underlay nodes and links depending on the indication of the tenant. An NS tenant is also able to deploy its own NF as software with provided computing resources.

In terms of telemetry, an NS tenant can obtain telemetry information of NF nodes and connectivities structuring an NS, in addition to whole of NSI.

6.3. IaaS-like Model

In IaaS-like model, an NS is represented with concrete configurations of underlay infrastructure. NS tenants are able to structure or change their desired NS by controlling infrastructure resources directly.

This model potentially has high customizability of NS rather than other models, but needs NS tenants to have deep knowledge about network and server operation. Also, NS providers need not to recognize NSs on their infrastructure because NS tenants directly manage their NS. Meanwhile, in terms of security and prevention of disturbances among NSs, some limitations on expositions of resources to tenants would be needed.

6.3.1. Capability in IaaS-like Model

In IaaS-like Model, an NS is represented with configurations of (virtual) nodes and (virtual) links connecting the nodes. An NS tenant is able to configure nodes and links in underlay infrastructure. In short, an NS tenant directly design detailed NS and manages it. In addition, an NS tenant inserts its own functions or applications in the NS with using computing resources.

In terms of telemetry, an NS tenant can obtain telemetry information of nodes and links in addition of whole of NSI.

6.4. Mapping of NS Provision Models and Infrastructure Layering

An example of mapping of each NS provision model is shown in Figure 3.
Figure 3: Mapping of NS provision models

*Legends

- o: virtual/physical node
- -: virtual/physical link
- [AP]: Access point
- [APL]: Application owned by NS Tenant
- [FW]: Firewall Function
- [VM]: Virtual Machine Instance on Server
- [SV]: Server as Infrastructure
In some cases, NSIs provided based on IaaS- or PaaS-like models are coordinated to a form of SaaS-like model by an NS broker, and the NS broker or by the tenant, becoming a NS provider in a recursive manner. For example, a vertical customer sends its high-level requirements to an NS broker create an appropriate NSI with resources provided by infrastructure operators.

7. Security Considerations

In NSaaS, parts of controls of infrastructures are opened to externals, and thus some mechanisms, such as authentication for APIs, to prevent illegal access would be required.

Other considerations are TBD

8. IANA Considerations

This memo includes no request to IANA.

9. Acknowledgement

The author would like to thank Toru Okugawa for his kind review and valuable feedback.

10. Informative References

[I-D.defoy-coms-subnet-interconnection]
Foy, X., Rahman, A., Galis, A.,
kiran.makhijani@huawei.com, k., and L. Qiang,
"Interconnecting (or Stitching) Network Slice Subnets",
draft-defoy-coms-subnet-interconnection-01 (work in progress), October 2017.

[I-D.dong-teas-enhanced- vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Networks (VPN+) Service",
draft-dong-teas-enhanced- vpn-03 (work in progress), November 2018.

[I-D.homma-nfvrg-slice-gateway]
Homma, S., Foy, X., and A. Galis, "Gateway Function for Network Slicing",
draft-homma-nfvrg-slice-gateway-00 (work in progress), July 2018.

[NGMN-5G-White-Paper]
NGMN, "NGMN 5G White Paper", February 2015,
<https://www.ngmn.org/5g-white-paper/5g-white-paper.html>.
Appendix A. NS Structure in the 3GPP 5GS

The overview of structure of NS in the 3GPP 5GS is shown in Figure 4. The terms are described in the 3GPP documents (e.g., [TS.23.501-3GPP] and [TS.28.530-3GPP]).
Figure 4: Overview of Structure of NS in 3GPP 5GS

Authors’ Addresses

Shunsuke Homma  
NTT  
Japan  
Email: shunsuke.homma.fp@hco.ntt.co.jp

Hidetaka Nishihara  
NTT  
Japan  
Email: nishihara.hidetaka@lab.ntt.co.jp