MEF Standard

MEF 84

Subscriber Network Slice Service and Attributes

June 2021

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and MEF Forum (MEF) is not responsible for any errors. MEF does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by MEF concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by MEF as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this Standard. MEF is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this Standard or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any MEF member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any MEF members will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

c) any form of relationship between any MEF member and the recipient or user of this Standard.

Implementation or use of specific MEF standards or recommendations and MEF specifications will be voluntary, and no Member shall be obliged to implement them by virtue of participation in MEF Forum. MEF is a non-profit international organization to enable the development and worldwide adoption of agile, assured and orchestrated network services. MEF does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

List of Figures

List of Tables

1 List of Contributing Members

The following members of the MEF participated in the development of this Standard and have requested to be included in this list.

- AT&T
- Ciena
- Ericsson
- Ribbon Communications
- NEC/Netcracker
- Nokia
- NTT
- Verizon

2 Abstract

This Standard specifies Network Slicing in the context of MEF Lifecycle Service Orchestration (LSO) and MEF Services. Key concepts of Network Slicing, Network Slices and Network Services are described. Network Services as defined in this Standard enable Service Providers to offer Network Slices in the Service Provider domain as Services to Subscribers in the Customer domain.

3 Terminology and Abbreviations

This section defines the terms used in this Standard. In many cases, the normative definitions to terms are found in other Standards. In these cases, the third column is used to provide the reference that is controlling, in other MEF or external documents.

In this Standard, the term "Service" is used to describe any service that aligns with MEF-defined Standards and is specified using MEF-defined Service Attributes.

Term	Definition	Reference
Customer	A Customer is the organization purchasing, managing, and/or using Services from a Service Provider. This may be an end user business organization, mobile operator, cloud operator.	Adapted from MEF 55.1 [34]
EPL	Ethernet Private Line	MEF 6.3 [29]
EVC	Ethernet Virtual Connection	MEF 10.4 [30]
EVPL	Ethernet Virtual Private Line	MEF 6.3 [29]
LSO	Lifecycle Service Orchestration	MEF 55.1 [34]
Network Service	A Network Slice offered as a Service to one or more Subscribers.	This Standard
Network Service Internal Node Function	A function in the Topology View of a Network Service representing physical or virtual functionality.	This Standard
Network Service Link	A link in the Topology View of a Network Service representing the connectivity between Network Service UNIs, or a Network Service UNI and a Network Service Internal Node Function, or Network Service Internal Node Functions.	This Standard
Network Service UNI	The demarcation point between the responsibility of the Subscriber and the Service Provider of the Network Service.	This Standard
Network Slice	A subset of a Service Provider Network, which is used and managed independently of other subsets.	This Standard
Network Slicing	A means for a Service Provider to structure and organize subsets of its network into Network Slices.	This Standard
OTN	Optical Transport Network	ITU-T G.709 [27]
Partner	An organization providing Products and Services to the Service Provider in order to allow the Service Provider to instantiate and manage Service Components external to the Service Provider domain.	MEF 55.1 [34]
Resource	A physical or non-physical component (or some combination of these) within a Service Provider's infrastructure or inventory.	MEF 55.1 [34]

Term	Definition	Reference
Service	Represents the Customer experience of a Product Instance that has been realized within the Service Provider's infrastructure and when needed in the Partner's infrastructure.	Adapted from MEF 55.1 [34]
Service Agreement	The agreement between the Subscriber and Service Provider for the Network Service.	This Standard
Service Provider	An organization providing Services to Subscribers in exchange for payment.	This Standard
Service Provider Network	An interconnected network used by the Service Provider to provide services to one or more Subscribers.	MEF 10.4 [30] MEF 61.1 [35]
Subscriber	Synonymous for Customer.	This Standard
Topology View	Network Service topology information available to the Subscriber.	This Standard
UNI	User Network Interface	This Standard

Table 1 – Terminology and Abbreviations

4 Compliance Levels

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 (RFC 2119 [16], RFC 8174 [18]) when, and only when, they appear in all capitals, as shown here. All key words must be in bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as **[Dx]** for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as **[Ox]** for optional**.**

5 Introduction

This section outlines the scope of the Standard and introduces characteristics of Network Slicing, Network Slice and Network Service. Further, it provides information about the organization of the Standard.

5.1 Scope

This Standard describes the key concepts of Network Slicing, Network Slices and Network Services. The focus is on the Subscriber visible aspects of the Service Provider's internal Network Slices. This Standard defines a Network Service, Network Service attributes and requirements, such that the Service Provider can offer Network Slices as Services to Subscribers.

This Standard focuses on the terminology, the Subscriber and Service Provider relationship and Subscriber visible aspects of Network Slices in the Service Provider domain. The Service Provider and Partner relationships and Service Provider internal attributes of Network Slices are not covered.

5.2 Overview of Network Slicing, Network Slice and Network Service

Network Slicing is a means for a Service Provider to structure and organize subsets of its network into Network Slices. A Network Slice includes the capabilities to manage, control and orchestrate the functional elements in that subset independently from other Network Slices' subsets. The Service Provider may instantiate and use a Network Slice for a single Subscriber or for several Subscribers or for internal purposes.

When a Service Provider implements Network Slicing and offers a Network Slice as a Service to its Subscribers, i.e., a Network Service as defined in this Standard, the Service Provider makes aspects of the Network Slice and its associated Services visible and available to Subscribers. Services associated with a Network Slice are Services that the Subscriber can instantiate on the Network Slice or request the Service Provider to instantiate.

5.3 Organization of the Standard

Section 6 contains key concepts and definitions, information about the relationship of Services and Network Slices as well as the management of Network Slices.

Section 7 defines the attributes of a Network Service to be agreed upon by the Service Provider and the Subscriber. The attributes include the Topology View, the Services that can be instantiated on the Network Service, and the orchestration, control and management capabilities as specified in the Service Agreement.

Appendix A presents use cases.

Appendix B relates Network Slicing as defined in this Standard with Network Slicing efforts and specifications in other standards development organizations (SDOs).

6 Key Concepts and Definitions

This section provides key concepts and definitions for Network Slicing, Network Slices and Network Services in the context of MEF LSO and MEF Services.

6.1 Network Slicing

A Service Provider applies Network Slicing to its network, the Service Provider Network, by splitting it into subsets, the Network Slices. Network Slices may be used and managed independently of each other. Network Slices form physical and/or logical networks on a common infrastructure.

The number of instantiable Network Slices may be limited by the amount and capacity of Resources available in the Service Provider Network.

Examples of Network Slicing options are depicted in Figure 1 where the Service Provider Network contains five physical links which are sliced.

- Network Slicing option A: The Service Provider creates two subsets. Subset A.1 contains three physical links. Subset A.2 contains two physical links. Each physical link is assigned only to one subset. The two subsets do not share any physical links.

- Network Slicing option B: The Service Provider creates two subsets. Subset B.1 contains five virtual links with x% of the bandwidth available on the five physical links. Subset B.2 contains five virtual links with y% of the bandwidth available on the five physical links. The two subsets share the same physical links. The sum of x and y may be equal to, greater than or smaller than 1 (100%), while providing network isolation; see Section 6.2.3.

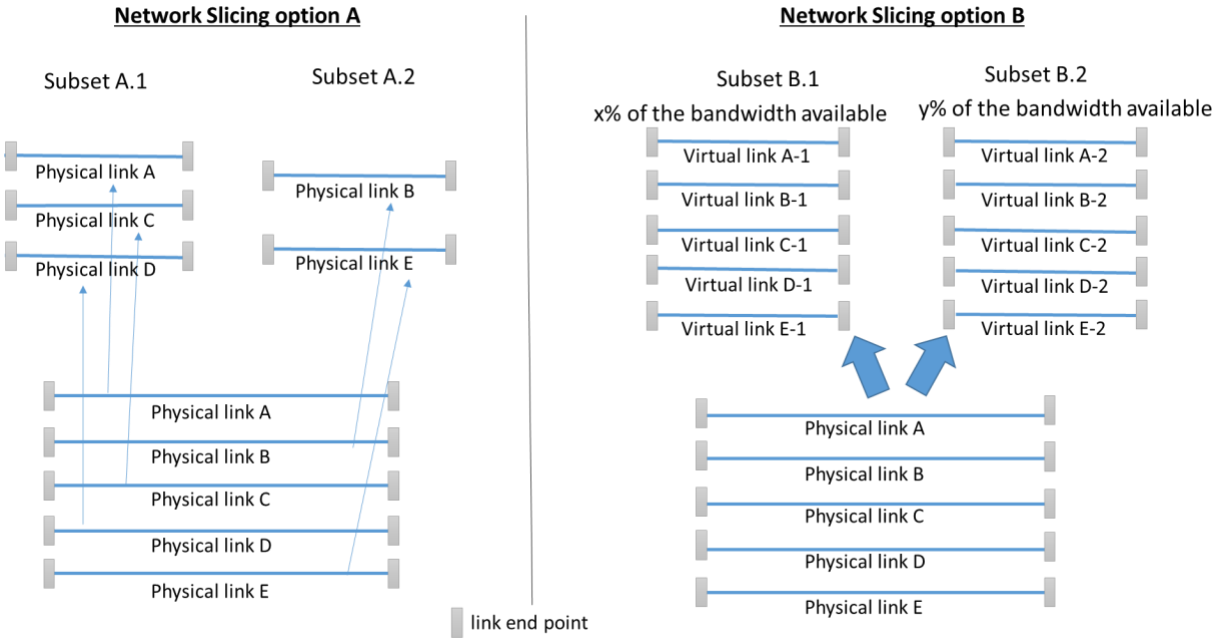


Figure 1 – Network Slicing Example Options A and B

Although the examples illustrated in Figure 1 only have connectivity Resources, subsets of the Service Provider Network may also contain other Resource types (e.g., applications such as in OCC 1.0 [42]) and any combination thereof.

6.2 Network Slices

A Network Slice is a subset of a Service Provider Network, which may be used and managed independently. Network Slices may be formed from physical as well as logical groupings of Resources. A Network Slice can be used to provide Services (see Section 6.3). In this case the Service Provider may provide topology information to a Subscriber via a Topology View. Resource abstraction allows the Service Provider to modify its network without changing a Subscriber's Topology View.

6.2.1 Dedicated or Shared Use

Network Slice Resources can be assigned and configured for either dedicated or shared use. Therefore, a Network Slice is classified for either dedicated or shared use.

- A Network Slice for dedicated use hosts Services provided to a single Subscriber.
- A Network Slice for shared use hosts Services provided to multiple Subscribers.

See Section 6.2.5 for examples of Network Slices instantiated for shared or dedicated use.

When Network Slices use shared Resources, the Service Provider ensures a sufficient amount of Resources is available.

6.2.2 Instantiation

A Network Slice may be instantiated for a single Subscriber (dedicated use) or for multiple Subscribers (shared use) or for the Service Provider's internal use. A Service Provider could offer a Service as a Product that will then be provisioned on an internal Network Slice.

The instantiation of a Network Slice may be triggered by a Subscriber ordering a Product from the Service Provider or the Service Provider preparing for potential Product Orders (e.g., in order to reduce the fulfilment time).

6.2.3 Isolation

Isolation of Network Slicing is required to guarantee the simultaneous existence of independent Network Slices on a common infrastructure. The Service Provider ensures that the Network Slices it creates are isolated from each other, such that information carried in one Network Slice does not spill over into another Network Slice and that events in one Network Slice do not impact other Network Slices.

[R1] The Service Provider **MUST** ensure the isolation of Network Slices instantiated on its network.

6.2.4 Recursion

Network Slices may be created recursively by combining and/or partitioning.

6.2.4.1 Composing a Network Slice Using Resources of Multiple Network Slices

Resources for a Network Slice could be provided by multiple Network Slices. An example could be an Ethernet Network Slice that uses Resources from an Ethernet Network Slice and an OTN Network Slice. Another example is a 3GPP 5G mobile network slice consisting of RAN, Transport and Core subnetwork slices (see also Appendix B.1).

6.2.4.2 Slicing a Network Slice

Slicing a Network Slice creates another set of Network Slices which need to be isolated from each other. The isolation requirement (see [R1]) applies to each set of Resources assigned to Network Slices.

When a Network Slice is provided as a Service (see Section 6.3) and the Subscriber wants to slice the network in the Topology View, there are two cases:

1. The Subscriber creates Network Slices based on the Resources in the Topology View without support from the Service Provider. The Subscriber assumes the role of a Service Provider for these new Network Slices. The Subscriber is responsible for the isolation of the Network Slices it created.

2. The Subscriber needs to request the Service Provider to slice the network in the Topology View. The Service Provider further slices the Network Slice and is responsible for the isolation of the new Network Slices it created.

An example of slicing a Network Slice is to create an Ethernet Network Slice from an Ethernet Network Slice (e.g., using Provider Bridging as in IEEE 802.1Q [9]).

6.2.5 Management of Network Slices

An instantiated Network Slice includes the functionality to orchestrate, control and manage Services instantiated on the Network Slice and their corresponding Resources.

Occasionally Network Slices may need to be modified for reasons such as:

- Service Provider Network internal changes to physical or virtual infrastructure.
- To scale Resources assigned to a Network Slice as required for instantiated Services.
- To reflect Network Service modifications that a Subscriber is permitted to request by the Service Agreement (see Section 6.3).

At the end of its lifecycle the Network Slice will be deleted from the management system and the associated Resources released.

[R2] The Service Provider **MUST** confine the Service orchestration, control and management to the corresponding Network Slice.

[R3] The Service Provider **MUST** confine the Resource orchestration, control and management to the corresponding Network Slice.

If a Network Slice is provided as a Service, the Service Provider continues to manage, control, configure and monitor the Network Slice it instantiated.

The LSO Reference Architecture Interface Reference Points for Network Slice related orchestration, control, management and business relationship interactions are:

- Cantata and Allegro for Subscriber and Service Provider interactions,
- Sonata and Interlude for Service Provider and Partner interactions,
- Legato and Presto for Service Provider internal handling of Network Slices.

6.3 Introduction to Network Service

The Service Provider can offer a Network Slice as a Network Service to one or more Subscribers, where:

- The Network Service is described as a Product in the Product Catalog
- Orchestration, control and management capabilities available to the Subscriber are part of the Network Service description

For example, a Service Provider can instantiate two different Network Slices and offer them as Services:

- One Network Slice is offered for shared use as Network Service 1. The Network Service 1 entry in the Product Catalog does not include a Topology View, nor orchestration, control and management capabilities. Network Service 1 supports EVPLs. Subscribers can order EVPL Services to be instantiated on Network Service 1.

- The other Network Slice is offered for dedicated use as Network Service 2. The Network Service 2 entry in the Product Catalog includes a Topology View. The Service Provider makes this Network Slice available with orchestration, control and management capabilities. As permitted by the Service Agreement, the one Subscriber can instantiate up to three EVPLs on Network Service 2 and can configure Resources in the Topology View.

- The Service Provider manages both Network Slices independently and enforces each instance to remain within their defined bounds of Resource usage.

- The Service Provider enforces each Subscriber's orchestration, control and management requests to remain within the bounds of their Service Agreement.

The Network Service is defined in Section 7.

7 Network Service – Providing a Network Slice as a Service

A Network Service is a Network Slice offered as a Service to a Subscriber by a Service Provider. The Network Service may include Subscriber orchestration, control and management capabilities.

The Subscriber is the organization that purchases, manages and uses a Network Service as defined in this Standard. There is no restriction on the type of organization that can act as a Subscriber, for example, a Subscriber can be an enterprise, a mobile operator, an IT system integrator, a governmental department, etc. When a Subscriber further slices the network in the Topology View of its Network Service and offers a Network Slice as a Network Service, it becomes a Service Provider to its own Subscribers.

Section 7.1 describes the Network Service.

Section 7.2 defines Network Service attributes to be agreed upon by the Service Provider and the Subscriber.

7.1 Network Service Description

The Network Service provides a network to the Subscriber based on Resources in a Network Slice instantiated in the Service Provider Network with a range of orchestration, control and management capabilities which depend on the Service Agreement. The Subscriber's Topology View of the Network Service can range from full abstraction to detailed topology. An example is illustrated in Figure 2.

In the example, the Service Provider's internal Network Slice used for the Network Service is illustrated by the orange parallelogram. The Subscriber's Network Service Topology View is illustrated by the blue network. The Topology View presents the Subscriber with an abstracted view of the Resources used by the Network Service. UNI-to-UNI connections can be established by the Subscriber ordering MEF connectivity services from the Service Provider or by setting them up on its own if the corresponding network management and configuration capabilities are included in the Service Agreement.

An example of the Topology View of a Network Service is a link connecting two UNIs. The Subscriber is allowed to request the instantiation of one EPL when the value of the Service Instantiation Capability Attribute is *TRUE* (see Section 7.2.6.1) and the value of the Supported Service Types Attribute includes the entry *Ethernet* in the list (see Section 7.2.4). See Appendix A for examples of other Topology Views.

APIs at the LSO Cantata and Allegro interface reference points are used for Service ordering, the Topology View and any orchestration, and control and management actions requested by the Subscriber on its Network Service.

The Product Catalog may list Product Offerings for Network Services with the following two categories of Service instantiation capability:

- Services that the Subscriber can order (as Products) via the LSO Cantata interface reference point to be established on the Network Service by the Service Provider.

- Services the Subscriber can request via the LSO Allegro interface reference point to be instantiated on the Network Service by the Service Provider.

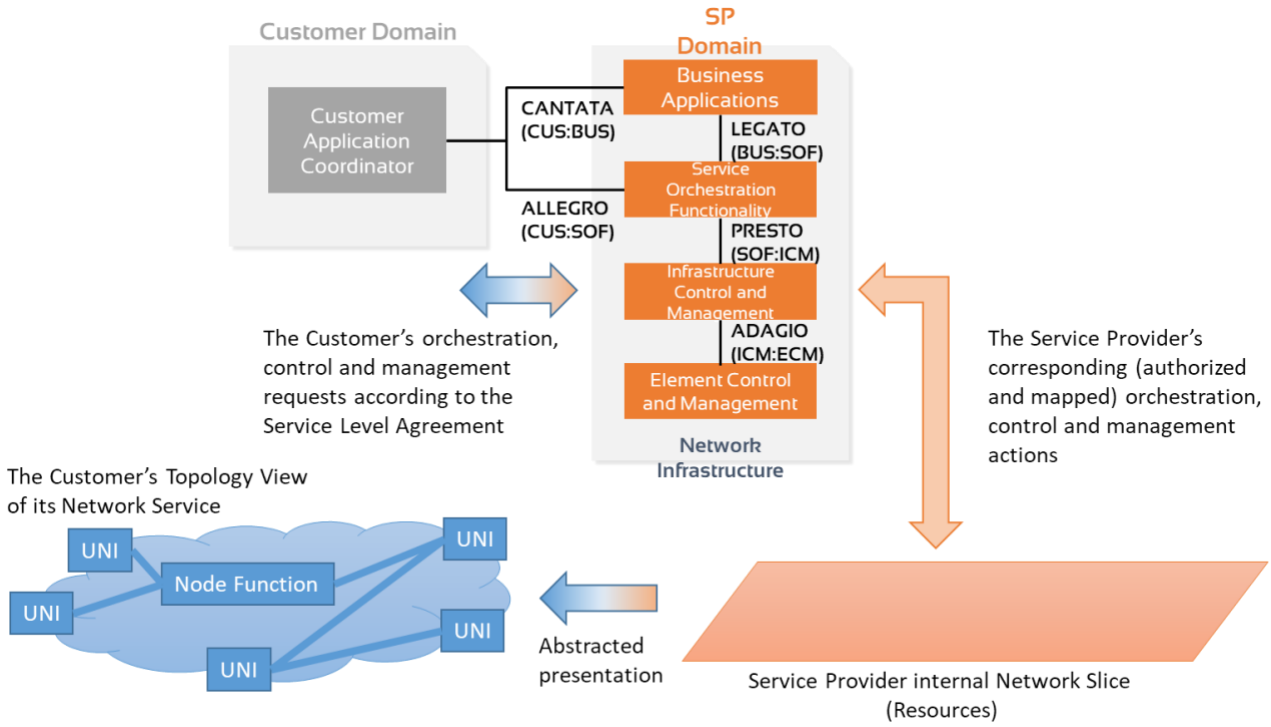


Figure 2 – Example of Network Service

The Subscriber can manage, configure and further slice the network in the Topology View of its Network Service and request instantiation of Services within the bounds agreed with the Service Provider. All orchestration, control and management actions on the Topology View by the Subscriber must be authorized and mapped to the Service Provider's internal Network Slice.

[R4] The Service Provider **MUST** confine the Subscriber's orchestration, control and management activities to the corresponding Topology View and within the bounds of the Service Agreement.

Examples of orchestration, control and management capabilities that the Subscriber can perform on the Topology View of its Network Service include:

- Applying Network Slicing to the Topology View for its own purposes (e.g., an enterprise providing individual Services for its departments).
- Configuring links and functions that are elements in the Topology View.
- Requesting instantiation of Services by the Service Provider using Resources in the Topology View.
- Modifying Services instantiated on the Topology View.

When permitted by the Service Agreement, the Subscriber requests the Service Provider to slice the network in the Topology View. The Service Provider implements the request accordingly for the Network Service and enforces the isolation of the Network Slices.

The Subscriber may offer Network Services as a reseller, thereby becoming a Service Provider to other Subscribers.

7.2 Network Service Attributes

This section defines the attributes of a Network Service to be agreed upon by the Service Provider and the Subscriber. The Network Service attributes are summarized in Table 2 and described in more detail in the following subsections.

Attribute Name	Summary Description	Possible Values
Network Service Identifier	The unique identifier of the Network Service.	String that is unique across the Service Provider´s network.
Network Profile Descriptor	A label to describe the category of Network Slice used for this Network Service	String, e.g., “URLLC” or “Robotic” or “for low bandwidth reliable IoT type traffic”
Network Profile	Describes the characteristics of the Network Slice used for this Network Service	*None* or a list of parameters as described in Section 7.2.3
Supported Service Types	List of Service types that are supported by the Network Slice	*Layer 1*, *Ethernet*, *IP*, *SD-WAN*, *Network Service*
Network Service Topology	Describes the Topology View	*None*, or a list of parameters as described in Section 7.2.5
Service Instantiation Capability	Indicates the Subscriber‘s ability to request instantiation of Services on its Network Service	*TRUE* or *FALSE* See Section 7.2.6.1.
Instantiated Services Configuration Capability	Indicates the Subscriber‘s ability to request modification of Services instantiated on its Network Service	*TRUE* or *FALSE* See Section 7.2.6.2.

Attribute Name	Summary Description	Possible Values
Network Configuration Capability	Indicates the Subscriber's ability to configure the Resources in its Topology View	*TRUE* or *FALSE* See Section 7.2.6.3.

Table 2 – Network Service attributes

The minimum set of attributes needed to order a Network Service is:

- Network Service Identifier Attribute, and
- Network Profile Descriptor Attribute, and
- Supported Service Types Attribute.

In this case, the values of the remaining service attributes are either *None* or *FALSE*.

The Service Provider should map the values of the Network Service attributes agreed with a Subscriber to the corresponding Service Provider internal Network Slice attribute values.

7.2.1 Network Service Identifier Attribute

The value of the Network Service Identifier Attribute is a unique string used by the Service Provider and the Subscriber to identify the Network Service.

[R5] The value of the Network Service Identifier **MUST** be unique among all such identifiers for Network Services supported by the Service Provider.

[R6] The Network Service Identifier **MUST** be less than or equal to 53 characters.

[R7] The Network Service Identifier **MUST** consist only of ASCII characters in the range 32-126 inclusive.

7.2.2 Network Profile Descriptor Attribute

The value of the Network Profile Descriptor Attribute is a string that a Service Provider can use as a label to describe the category of the Network Slice used for the Network Service.

[R8] The Network Profile Descriptor **MUST** be less than or equal to 255 characters.

[R9] The Network Profile Descriptor **MUST** consist only of ASCII characters in the range 32-126 inclusive.

As an example, the Service Provider might use "*provides stable, high data-rate connectivity"* as a Network Profile Descriptor.

7.2.3 Network Profile Attribute

The value of the Network Profile Attribute is a list of parameters describing the Network Slice used for the Network Service. Table 3 lists some example parameters.

Example Network Profile Attribute Parameter	Example Values
Profile Type	Class of Service Label similar to High, Medium, Low CoS Labels as defined in MEF 23.2 [32] 3GPP defined slice/service types eMBB, URLLC, MIoT [1]
Quality of service (QoS)	Bandwidth, latency, jitter
Security	Network functions (e.g., a firewall function) to be applied for the Network Slice
Failure safety	Required network redundancy

Table 3 – Examples of Network Profile Attribute parameters and values

7.2.4 Supported Service Types Attribute

The value of the Supported Service Types Attribute is a list of one or more Service types that are supported by the Network Slice used for this Network Service.

After a Subscriber has ordered a Network Service from the Service Provider's Product Catalog, and the value of the Service Instantiation Capability Attribute is *TRUE*, the Subscriber can request the instantiation of a Service via the LSO Allegro interface reference point. When the value of the Service Instantiation Capability Attribute is *FALSE*, the Subscriber can order a Service from the Service Provider's Product Catalog via the LSO Cantata interface reference point.

Table 4 lists the values for the Supported Service Types Attribute.

Supported Service Types Attribute values	MEF Standard
Layer 1	MEF 63/64 [36] [37]
Ethernet	MEF 6.3/51.1 [29] [33]
IP	MEF 69 [38]
SD-WAN	MEF 70 [39]
Network Service	MEF 84 [*This document*]

Table 4 – Supported Service Types Attribute Values

The instantiation of a new Network Service (MEF 84) corresponds to further slicing the current Network Service.

7.2.5 Network Service Topology Attribute

The value of the Network Service Topology Attribute is either *None* or a list of identifiers referring to Network Service UNIs (see Section 7.2.5.1), Network Service Links (see Section 7.2.5.2) and

Network Service Internal Node Functions (see Section 7.2.5.3) which describe the Topology View for the Network Service.

7.2.5.1 Network Service UNI

A Network Service UNI is the demarcation point between the responsibility of the Subscriber and the Service Provider of the Network Service. Each Network Service UNI has a Network Service UNI Identifier Attribute.

The value of the Network Service UNI Identifier Attribute is a unique string used by the Service Provider and the Subscriber to identify the Network Service UNI.

[R10] The value of the Network Service UNI Identifier **MUST** be unique among all such identifiers for Network Services supported by the Service Provider.

[R11] The Network Service UNI Identifier **MUST** be less than or equal to 53 characters.

[R12] The Network Service UNI Identifier **MUST** consist only of ASCII characters in the range 32-126 inclusive.

Examples of other Network Service UNI attributes are:

- A Network Service UNI type as one of the defined MEF virtual or physical UNI layers (e.g., MEF 63 for L1, MEF 10.4 for L2, MEF 61.1 for L3).
- A Network Service UNI interface rate (e.g., with a value of 100Gb/s).
- A Network Service UNI instantiable service type capability (e.g., a list of Supported Service Types; see Section 7.2.4).

7.2.5.2 Network Service Link

A Network Service Link is a link in the Topology View representing the connectivity between

- Network Service UNIs, or
- A Network Service UNI and a Network Service Internal Node Function, or
- Network Service Internal Node Functions.

Note that the Topology View is an abstracted representation of the Network Slice used for the Network Service (see Section 7.1), where a Network Service Internal Node Function could provide multi-point connectivity.

The value of the Network Service Link Identifier Attribute is a unique string used by the Service Provider and the Subscriber to identify the Network Service Link.

[R13] The value of the Network Service Link Identifier **MUST** be unique among all such identifiers for Network Services supported by the Service Provider.

[R14] The Network Service Link Identifier **MUST** be less than or equal to 53 characters.

[R15] The Network Service Link Identifier **MUST** consist only of ASCII characters in the range 32-126 inclusive.

A Network Service Link has one or more Network Service Link End Points, each of which has a Network Service Link End Point Identifier. The value of the Network Service Link End Point Identifier Attribute is a unique string used by the Service Provider and the Subscriber to identify the Network Service Link End Point.

[R16] The value of the Network Service Link End Point Identifier **MUST** be unique among all such identifiers for Network Services supported by the Service Provider.

[R17] The Network Service Link End Point Identifier **MUST** be less than or equal to 53 characters.

[R18] The Network Service Link End Point Identifier **MUST** consist only of ASCII characters in the range 32-126 inclusive.

Examples of other Network Service Link attributes are

- A Network Service Link type (e.g., with a value of one of Optical Transport Network, Ethernet, IP),
- A Network Service Link rate.

7.2.5.3 Network Service Internal Node Function

A Network Service Internal Node Function is a function in the Topology View representing physical or virtual functionality (e.g., an application, a cloud function, a forwarding function or firewall function) available in the Network Slice used for the Network Service. Each Network Service Internal Node Function has a Network Service Internal Node Function Identifier Attribute and a Network Service Internal Node Function Type Attribute.

The value of the Network Service Internal Node Function Identifier Attribute is a unique string used by the Service Provider and the Subscriber to identify the Network Service Internal Node Function.

[R19] The value of the Network Service Internal Node Function Identifier **MUST** be unique among all such identifiers for Network Services supported by the Service Provider.

[R20] The Network Service Internal Node Function Identifier **MUST** be less than or equal to 53 characters.

[R21] The Network Service Internal Node Function Identifier **MUST** consist only of ASCII characters in the range 32-126 inclusive.

The value of the Network Service Internal Node Function Type Attribute is a list of one or more of the following function types: *Connectivity Function, Compute Function, Storage Function, Security Function.*

Examples of parameters for Network Service Internal Node Function Type Attribute values are listed in Table 5.

Network Service Internal Node Function Type Attribute Value	Examples of parameters
Connectivity Function	Forwarding capability at a certain layer, capacity, number of ports
Compute Function	Processing capability, processor speed, memory
Storage Function	Storing capability, redundancy, capacity, speed of access (read/write speeds), storage time (persistency of information stored)
Security Function	Encryption, authentication, authorization

Table 5 – Examples of Network Service Internal Node Function Type parameters

7.2.6 Network Service Management Attributes

Network Service Management Attributes describe the Subscriber's management, orchestration and control capabilities for its Network Service and the Resources in its Topology View.

7.2.6.1 Service Instantiation Capability Attribute

The value of the Service Instantiation Capability Attribute indicates the Subscriber's ability to request the instantiation of Services (see Section 7.2.4) on its Network Service.

When the value is *FALSE*, the Subscriber would need to use the Product Ordering process via the LSO Cantata interface reference point to establish Services on its Network Service.

When the value of this attribute is *TRUE*, the Subscriber can request the instantiation of Services on its Network Service via the LSO Allegro interface reference point, rather than using the Product Ordering process.

The number of Services the Subscriber can have instantiated at the same time may be limited by the Service Agreement. In addition, the Service Provider may want to pre-define the maximum number of each Service type if more than one Service type is supported (e.g., with a matrix of allowed and forbidden combinations of Supported Service Types).

7.2.6.2 Instantiated Service Configuration Capability Attribute

The value of the Instantiated Service Configuration Capability Attribute indicates the Subscriber's ability to request modification of Services instantiated on its Network Service.

When the value of this attribute is *TRUE*, the Subscriber has the ability to request the modification of Services instantiated on its Network Service via the LSO Allegro interface reference point.

When the value is *FALSE*, the Subscriber does not have the ability to request the modification of Services instantiated on its Network Service.

7.2.6.3 Network Configuration Capability Attribute

The value of the Network Configuration Capability Attribute indicates the Subscriber's ability to configure the Resources in its Topology View.

It may include the capability to add or remove Resources in the Topology View; e.g., Network Service UNIs, Network Service Links and Network Service Internal Node Functions.

It may include the capability to configure Resources in the Topology View; e.g., forwarding rules for data traffic that can be transferred through the Network Slice, source and/or destination IP addresses, port numbers, etc.

When the value is *TRUE*, the Subscriber has the ability to configure Resources in its Topology View via the LSO Allegro interface reference point.

When the value is *FALSE*, the Subscriber has no ability to configure Resources in its Topology View.

8 References

[1] 3GPP TS 23.501 V15.10.0 (ETSI TS 123 501 V15.10.0), *System Architecture for the 5G System; Stage 2 (Release 15)*, July 2020

[2] 3GPP TS 28.530 V15.3.0 (ETSI TS 128 530 V15.3.0), *Management and orchestration; Concepts, use cases and requirements (Release 15)*, January 2020

[3] 3GPP TR 28.801 V15.1.0, *Study on management and orchestration of network slicing for next generation network (Release 15)*, January 2018

[4] ETSI GR NFV-EVE 012 V3.1.1, *Report on Network Slicing Support with ETSI NFV Architecture Framework*, December 2017

[5] ETSI GR NFV-IFA 024 V3.2.1, *Network Functions Virtualisation (NFV) Release 3; Information Modeling; Report on External Touchpoints related to NFV Information Model*, April 2019

[6] ETSI GS NFV-IFA 010 V3.4.1, *Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Functional requirements specification*, June 2020

[7] ETSI GS ZSM 003 V0.18.1, *Zero-touch Network and Service Management (ZSM); End to end management and orchestration of network slicing*, July 2020

[8] GSMA Official Document NG.116, *Generic Network Slice Template version 2.0*, October 2019

[9] IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks*, July 2018

[10] Internet Engineering Task Force Internet-Draft draft-king-teas-applicability-actn-slicing-04, *Applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to Network Slicing*, October 2018

[11] Internet Engineering Task Force Internet-Draft draft-rokui-5g-transport-slice-00, *5G Transport Slice Connectivity Interface*, July 2019

[12] Internet Engineering Task Force Internet-Draft draft-ietf-teas-enhanced-vpn-05, *A Framework for Enhanced Virtual Private Networks (VPN+) Services*, February 2020

[13] Internet Engineering Task Force Internet-Draft draft-nsdt-teas-ns-framework-03, *Framework for Transport Network Slices*, April 2020

[14] Internet Engineering Task Force Internet-Draft draft-nsdt-teas-transport-slice-definition-01, *Definition of Transport Slice*, April 2020

[15] Internet Engineering Task Force Internet-Draft draft-nsdt-teas-transport-slice-definition-02, *IETF Definition of Transport Slice*, April 2020

[16] Internet Engineering Task Force RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997

[17] Internet Engineering Task Force RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*, December 2001

[18] Internet Engineering Task Force RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, May 2017

[19] Internet Engineering Task Force RFC 8402, *Segment Routing Architecture*, July 2018

[20] Internet Engineering Task Force RFC 8453, *Framework for Abstraction and Control of TE Networks (ACTN)*, August 2018

[21] Internet Engineering Task Force RFC 8656, *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*, February 2020

[22] Internet Engineering Task Force RFC 8665, *OSPF Extensions for Segment Routing*, December 2019

[23] ITU-R Recommendation M.2083, *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, September 2015

[24] ITU-T Recommendation G.7702, *Architecture for SDN control of transport networks*, 2018

[25] ITU-T Recommendation Y.3100, *Terms and definitions for IMT-2020 network*, 2017

[26] ITU-T Technical Report GSTR-TN5G, *Transport network support of IMT-2020/5G*, October 2018

[27] ITU-T Recommendation G.709/Y.1331, *Interfaces for the optical transport network*, June 2020

[28] ITU-T Recommendation G.800, *Unified functional architecture of transport networks*, 2016

[29] MEF 6.3, *Subscriber Ethernet Service Definitions*, November 2019

[30] MEF 10.4, *Subscriber Ethernet Service Attributes*, December 2018

[31] MEF 22.3.1, *Amendment to MEF 22.3: Transport Services for Mobile Networks*, April 2020

[32] MEF 23.2, *Carrier Ethernet Class of Service – Phase 3*, Implementation Agreement, August 2016

[33] MEF 51.1, *Operator Ethernet Service Definitions*, December 2018

[34] MEF 55.1, *Lifecycle Service Orchestration (LSO): Reference Architecture and Framework,* 2021

[35] MEF 61.1, *IP Service Attributes*, May 2019

[36] MEF 63, *Subscriber Layer 1 Service Attributes*, August 2018

[37] MEF 64, *Operator Layer 1 Service Attributes and Services*, February 2020

[38] MEF 69, *Subscriber IP Service Definitions*, November 2019

[39] MEF 70, *SD-WAN Service Attributes and Services*, July 2019

[40] MEF White Paper, *Slicing for Shared 5G Fronthaul and Backhaul*, April 2020

[41] NGMN 5G White Paper, 2015

[42] Open Cloud Connect (OCC), *OCC 1.0 Reference Architecture*, December 2014

[43] Open Networking Foundation TR-521, *SDN Architecture 1.1*, 2016

[44] Open Networking Foundation TR-526, *Applying SDN Architecture to 5G Slicing*, 2016

[45] Open Networking Foundation *Transport Application Programming Interface*, https://wiki.opennetworking.org/display/OTCC/TAPI

Appendix A Use Cases (Informative)

This appendix provides example use cases for the concepts described in the body of this Standard. Further use cases are provided in the MEF White Paper on Slicing for Shared 5G Fronthaul and Backhaul [40].

A.1 Shared Fronthaul Use Case Example

Mobile Network Operators (MNOs) do not always have the network infrastructure necessary to provide the required mobile network coverage themselves. These coverage gaps are filled by utilizing services from other operators.

A.1.1 Basic Scenario and Preconditions

In this example, Provider-FH owns and operates a network that has edge fronthaul network elements (FH NEs) located near mobile network locations like Remote Radio Heads (RRH, 4G context), Radio Units (RU, 5G context) and in a co-location site with their corresponding Baseband Units (BBU, 4G) and/or Distributed Units (DU, 5G).

Figure 3 shows three mobile network operators (MNO-1, MNO-2, MNO-3) that use services from Provider-FH for their fronthaul connectivity, connecting each MNO's RRH/RUs to their corresponding BBU/DUs at the co-location site. Figure 3 only shows the fronthaul part of the mobile network operators; the rest of their networks is not illustrated (i.e., no mid/backhaul).

Note, at the radio tower locations there may be equipment from more than one MNO that share the cost of the tower, but the illustration only shows one MNO's radio equipment. Further, only one of each basic radio deployment type is shown. Typically the tower and hut are owned by a third party (e.g., Provider-XY).

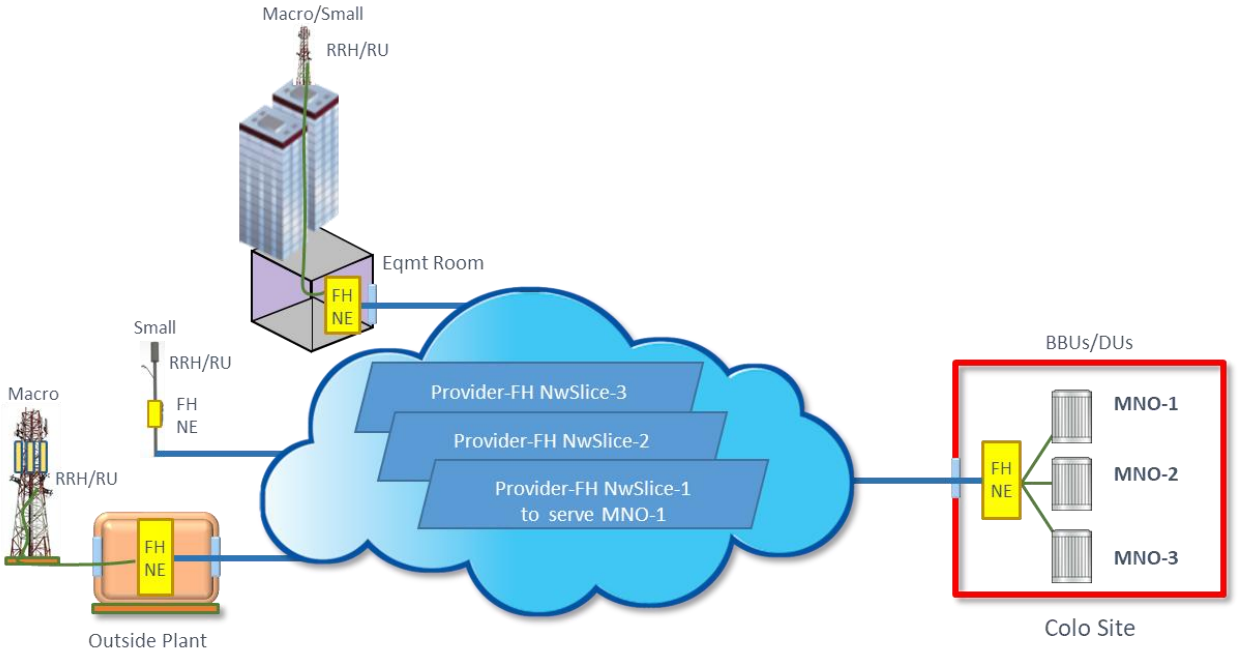


Figure 3 – Shared Fronthaul Example; basic scenario

In order to provide fronthaul networks and fronthaul connectivity services to the three MNOs, Provider-FH applies Network Slicing to its Shared Fronthaul Network creating three Network Slices (one per MNO: NwSlice-1, NwSlice-2, NwSlice-3). Although these three networks (Network Slices) are constructed on common infrastructure, they are isolated from each other and the Provider-FH network management enforces this isolation.

The three MNOs have entered business relationships with Provider-FH.

Internally, Provider-FH associates Network Slices to Subscribers in the following way:

- NwSlice-1 → MNO-1, and
- NwSlice-2 → MNO-2, and
- NwSlice-3 → MNO-3.

APIs at the LSO Cantata interface reference point are used for business related interactions like Product Ordering and billing.

APIs at the LSO Allegro interface reference point are used for configuration and control related management interactions as allowed by the respective Service Agreement, such as operational state queries, request updates to service parameters, or requests to instantiate other Services.

A.1.2 Example Service Scenarios

A.1.2.1 MNO-1: Connectivity Service to Connect Locations

In order to connect its remote locations with the co-location site, MNO-1 orders an Ethernet Virtual Private Line (EVPL) Service from Provider-FH.

The MNO-1 UNIs at each radio location are connected by FH NE ports to the corresponding co-location site FH NE port and MNO-1 UNI using the EVPL instantiated on NwSlice-1 by Provider-FH. This is visualized in Figure 4. For clarity, only one EVPL UNI is shown at each radio location.

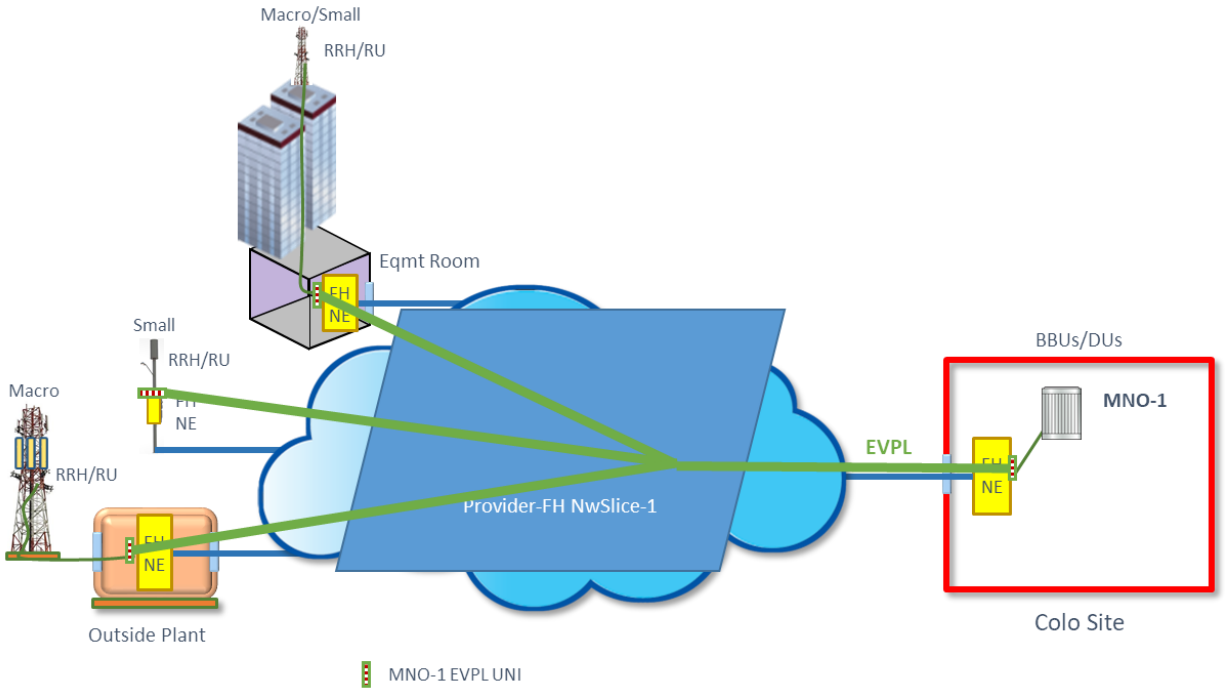


Figure 4 – Example Scenario MNO-1: Connectivity Service to connect locations

MNO-1 does not have the ability to manage and control Provider-FH resources associated with the Services obtained from Provider-FH.

MNO-1 has the ability to request, via an API at the LSO Allegro interface reference point, modifications of the values of EVPL service attributes within the scope of the Service Agreement with Provider-FH.

A.1.2.2 MNO-2: Network Service and Connectivity Services

In order to obtain a network connecting its radio locations and the co-location site, MNO-2 requests a Network Service from Provider-FH.

Provider-FH uses NwSlice-2 to realize the infrastructure for MNO-2. The Topology View presented in this example from Provider-FH to MNO-2 is shown in Figure 5. The MNO-2 Network Service UNIs demarcate connectivity between MNO-2's RRH/RUs and MNO-2's 5G DU. Each link in the Topology View has its individual capacity that may be different from the capacity of the other links.

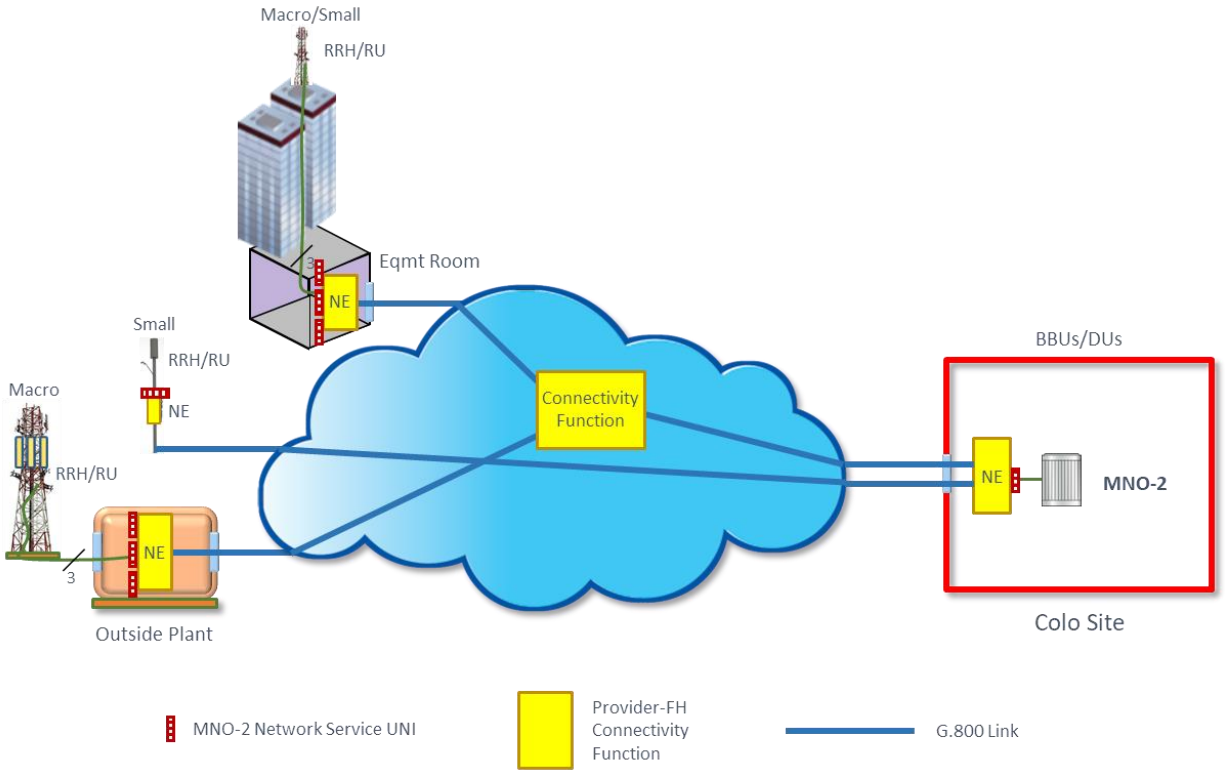


Figure 5 – Example Scenario MNO-2: Topology View presented from Provider-FH to MNO-2

By the Network Service agreement, MNO-2 in this example can request up to 2 Connectivity Service instances (e.g., 2 EVPLs with up to 7 EVCs each). Additional Service instances require either modification of the Network Service agreement or ordering a separate Connectivity Service.

The Topology View for MNO-2 (see Figure 5) includes:

- List of Network Service UNIs (see Section 7.2.5.1):
  - 3 UNIs at the NE in the Macro/Small site equipment room,
  - 1 UNI at the NE in the Small site,
  - 3 UNIs at the NE in the Outside Plant, and
  - 1 UNI at the NE in the co-location site.
- List of Network Service Links (see Section 7.2.5.2):
  - A link between the NE in the Small site and the NE in the co-location site, and
  - A link between each of the NEs at the Macro/Small site equipment room, Outside Plant, co-location site and the Connectivity Function.
- List of Network Service Internal Node Functions (see Section 7.2.5.3):
  - Five connectivity functions, each with capability to switch/multiplex Point-to-Point EVCs.

A link in the topology with direct connectivity between two Network Service UNIs is shown by the link connecting the NE at the Small site and the NE at the co-location site in Figure 5.

MNO-2 requests an EVPL Service composed of seven EVCs between the eight Network Service UNIs associated with the four NE Connectivity Functions: three EVCs between the Macro/Small site equipment room and co-location site, three EVCs between the Outside Plant and the co-location site and one EVC between the Small site and the co-location site. These EVCs are multiplexed at the three remote NE Connectivity Functions, the central Connectivity Function and the NE Connectivity Function at the co-location site. Figure 6 shows the Topology View with these EVCs.

If allowed by the Network Service agreement, MNO-2 may shift bandwidth between EVCs depending on the time of day. MNO-2 configures a full 25Gb/s per RU from the tower in the business district to the DU during office hours and some amount much less than that for the EVCs from the RUs in the suburbs. For the evening hours, MNO-2 configures the reverse bandwidth relationship.

Provider-FH checks any management and control actions by MNO-2 on the Topology View and makes any required changes to the Provider-FH resources associated with MNO-2's Network Service within the bounds of the Service Agreement.

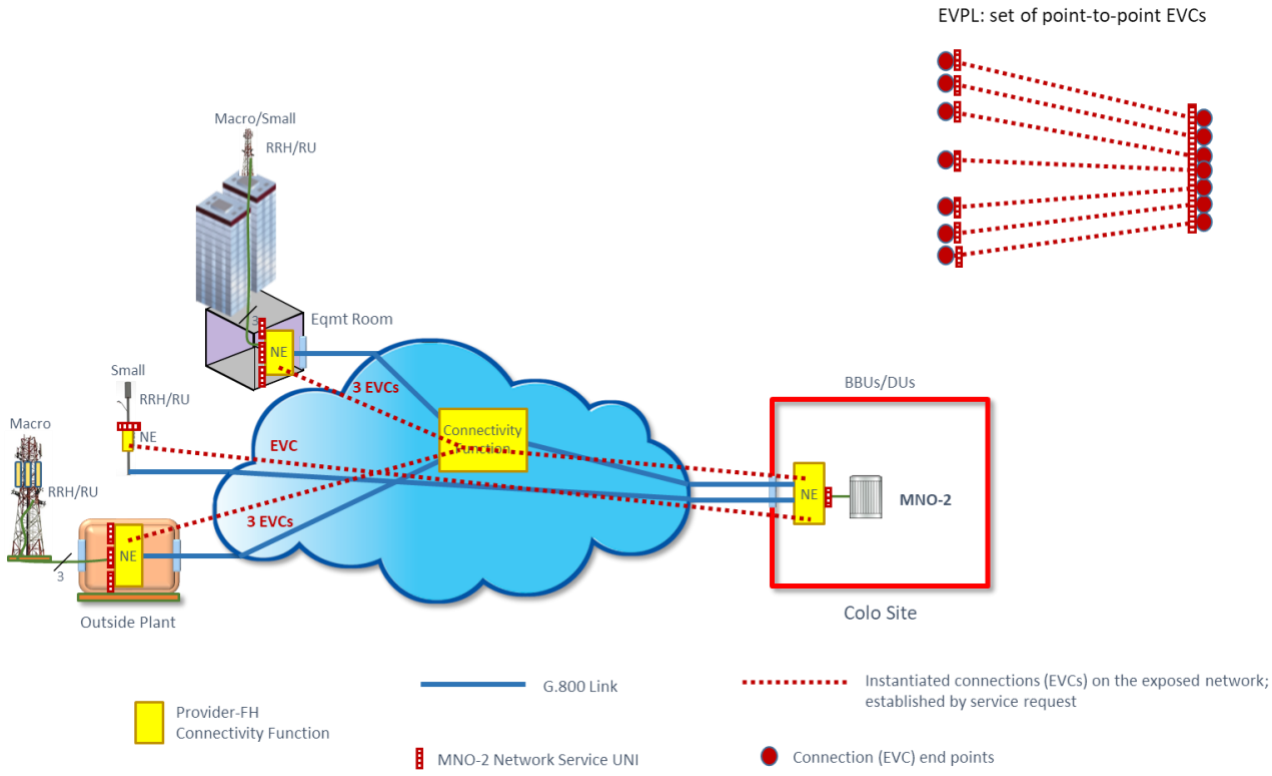


Figure 6 – Example Scenario MNO-2: EVCs in EVPL Service instantiated on the Network Service

A.1.2.3 MNO-3: Network Service and Ability to Slice the Network in the Topology View

In order to obtain a network connecting its radio locations and the co-location site, MNO-3 requests a Network Service from Provider-FH.

Provider-FH uses NwSlice-3 to realize the infrastructure for MNO-3. The Network Service Topology View has Network Service UNIs that correspond to MNO-3's radio locations and MNO-3's 5G DU location. Each link in the Topology View has its individual capacity that may be different from the capacity of the other links.

The Service Agreement includes the following capabilities for MNO-3:

- Slice the network in the Topology View (see Sections 7.2.6.1 and 7.2.4)
- Configure the Topology View (see Section 7.2.6.3)
- Instantiate Ethernet Connectivity Services and Cloud Services on the network in the Topology View (see Section 7.2.6.1)

A.1.3 Options for MNO 5G Network Slices

The MNOs in the previous use cases have several Provider-FH Service options for supporting the fronthaul segments of their 5G Network Slices (i.e., Network Slices as specified by 3GPP for 5G, c.f., Appendix section B.1), including:

- Obtaining a Connectivity Service (e.g., EVPL) per 5G Network Slice.
- Mapping several 5G Network Slices into a single Connectivity Service.
    - MNOs may use Service Classes to differentiate 5G Network Slices and need some means to coordinate data traffic enforcement accordingly.
    - Service Classes example: With a packet-based fronthaul network (eCPRI), if service frames have their Priority Code Point (PCP) set they can be mapped at ingress to a given Class of Service Name, as shown in Table 6.
- Obtaining a Network Service per 5G Network Slice type and using Connectivity Services on the Topology View for the 5G Network Slice Instances.

PCP Value	Class of Service Name	MNO 5G Service Category
Untagged, 0-2	mMTC	Massive Machine Type Communication, for applications such as the industrial or residential Internet of Things
3-5	eMBB	Enhanced Mobile Broadband, for higher bit rate support of, for example, streaming video
6-7	URLLC	Ultra-Reliable Low Latency Communication, for time-critical applications such as remote medical procedures

Table 6 – Example mapping of PCP values to Class of Service names

A.2 B2B2X Business Case: Network Slicing to Support OTT by Third Party Providers

Network Slicing can be a means to support network operators' "Business-to-Business-to-X" (B2B2X) business models, where the network operator acts as Service Provider enabling third Party Services for end users.

A.2.1 Basic Scenario

The Service Provider in this use case has the following B2B2X business model: with Network Services it provides dedicated networks to its Subscribers, for example an online gaming company, a car manufacturer and a rich-video streaming provider. The Service Provider internally realizes the dedicated networks by instantiating Network Slices and providing each Subscriber with a corresponding Topology View and management capabilities as defined by their respective Service Agreements. Each Subscriber uses its Network Service for end users with a subscription. This is illustrated in Figure 7.

The Network Slices are operated and managed by the Service Provider. Management and operational actions by a Subscriber on its Network Service are mapped by the Service Provider to the internal Network Slice for that Subscriber. Note that the Subscriber can manage and operate its Network Service only within the bounds defined in the Service Agreement.

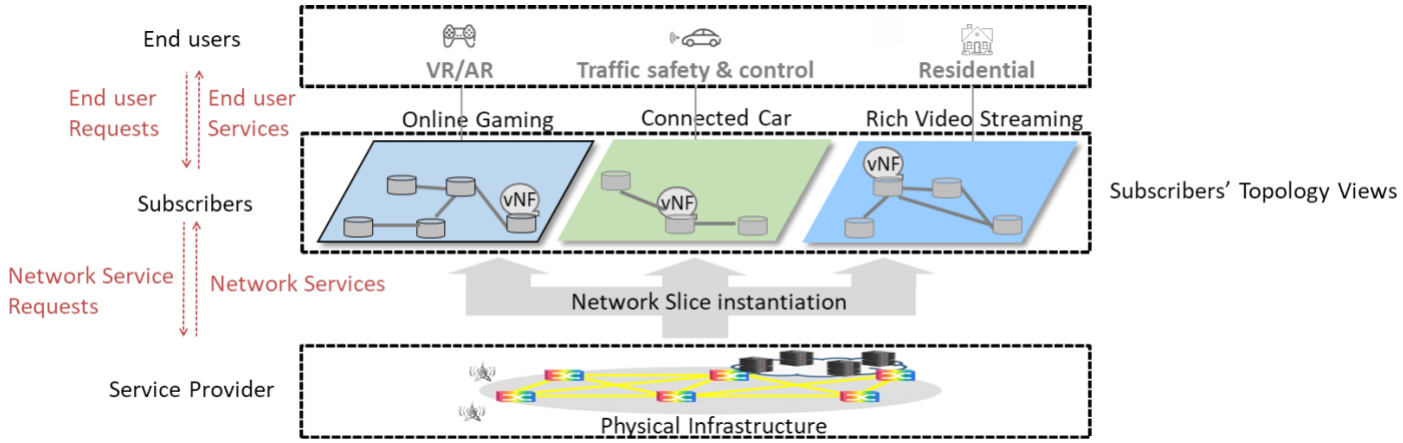


Figure 7 – Network Slice B2B2X service model

A.2.2 Network Provisioning Models

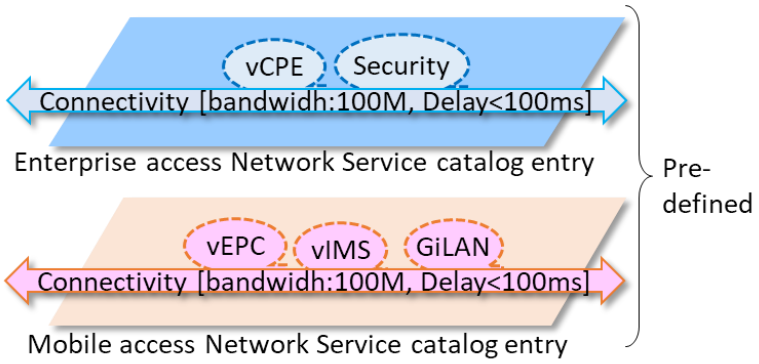
Network Slice requirements vary due to Subscriber infrastructure needs and Subscriber network technology expertise. Taking this into account, the Service Provider offers three types of network provisioning models: fully pre-defined, semi-customized and fully-customized.

A.2.2.1 Fully Pre-defined Network Provisioning Model

The fully pre-defined network provisioning model is offered to Subscribers with no interest in the network technology, infrastructure and operations. The Service Provider's Product Catalog lists different options for fully pre-defined networks that the Subscriber can choose from. A selected

Network Service option will be configured by the Service Provider based on the corresponding set of pre-defined attribute values.

A fully pre-defined Network Service catalog entry is linked to a set of pre-defined attribute values to be applied during Network Service instantiation. Pre-defined attribute values include quality of service (QoS), security, failure safety and possibly other functions. Two examples are illustrated in Figure 8.



vCPE	virtual Customer Premises Equipment
vEPC	virtual Evolved Packet Core
vIMS	virtualized IP Multimedia Services
GiLAN	SGi Local Area Network "Gi" is the name of the 3GPP reference point (it is SGi for LTE)

Figure 8 – Example Product Catalog entries for fully pre-defined Network Services

An example of a fully pre-defined Network Service Topology View is provided in Figure 9. Subscribers may initiate connectivity between specific groups of UNIs and each connection has pre-defined attribute values.

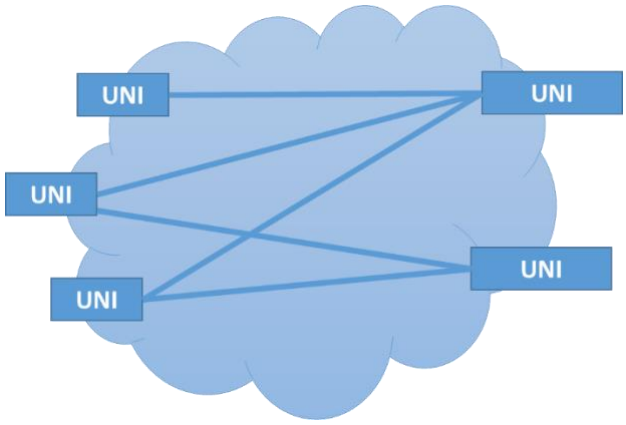
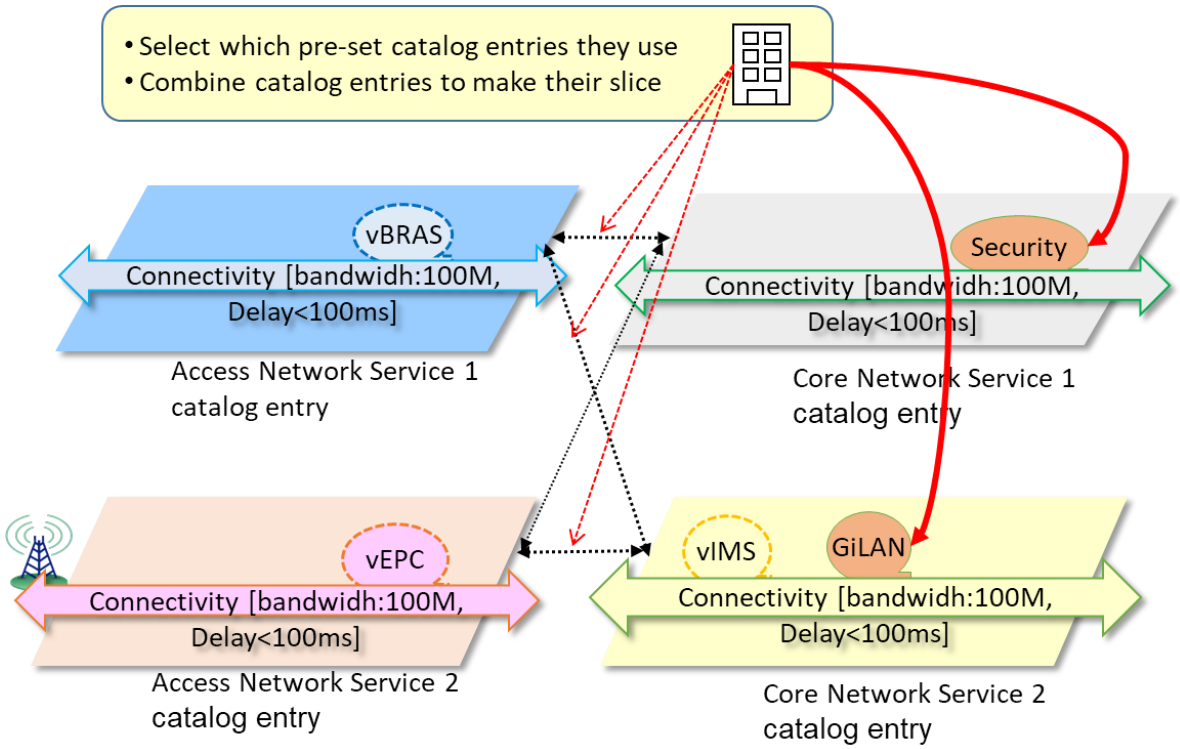


Figure 9 – Example of a fully pre-defined Network Service Topology View

A.2.2.2 Semi-customized Network Provisioning Model

The semi-customized network provisioning model is offered to Subscribers who want to choose and combine network components in their Network Service order. The Service Provider's Product Catalog lists different options of pre-defined networks and functions that the Subscriber can choose from and combine.

Each pre-defined Network Service catalog entry is linked to a Network Slice description with pre-defined attribute values to be applied during Network Service instantiation. The Subscriber may combine pre-defined Network Service catalog entries according to their requirements. The Subscriber can combine its own functions with the Network Service from the Service Provider. An example is illustrated in Figure 10 where a Subscriber adds a virtual Security function.



vBRAS	virtual Broadband Remote Access Server
vEPC	virtual Evolved Packet Core
vIMS	virtualized IP Multimedia Services
GiLAN	SGi Local Area Network; "Gi" is the name of the 3GPP reference point (it is SGi for LTE)

Figure 10 – Example Product Catalog selections for a semi-customized Network Service

The Service Provider internally instantiates a Network Slice dedicated to the Subscriber's Network Service. Examples of semi-customized Network Service Topology Views are provided in Figure 11, Figure 12 and Figure 13.

For its semi-customized Network Services the Service Provider also offers to the Subscriber the capability to control and operate the network in the Topology View and, if allowed by the Service Agreement, the option to install Subscriber owned applications or additional functions provided by the Service Provider.

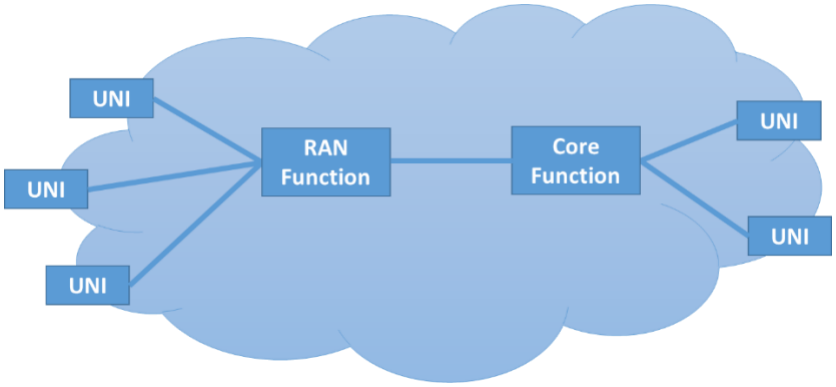


Figure 11 – Example 1 of a semi-customized Network Service Topology View

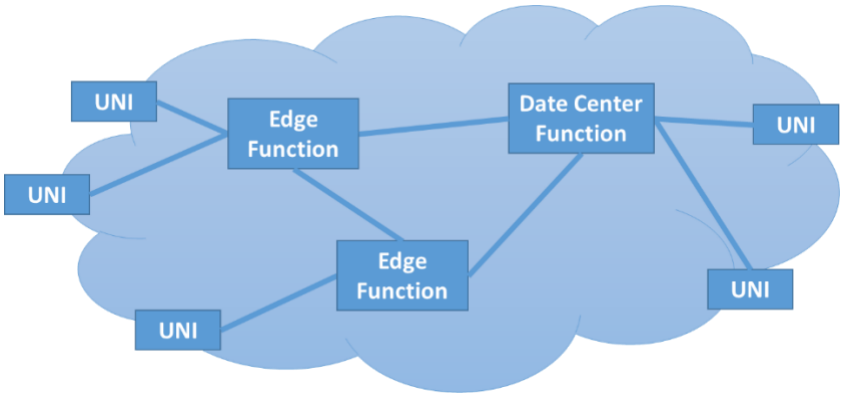


Figure 12 – Example 2 of a semi-customized Network Service Topology View

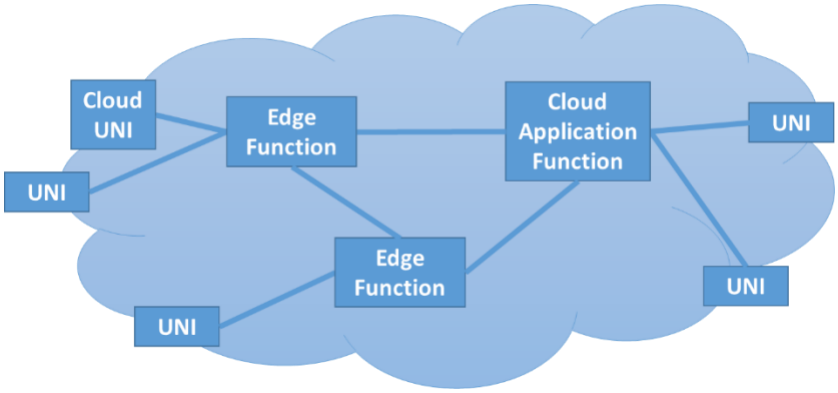
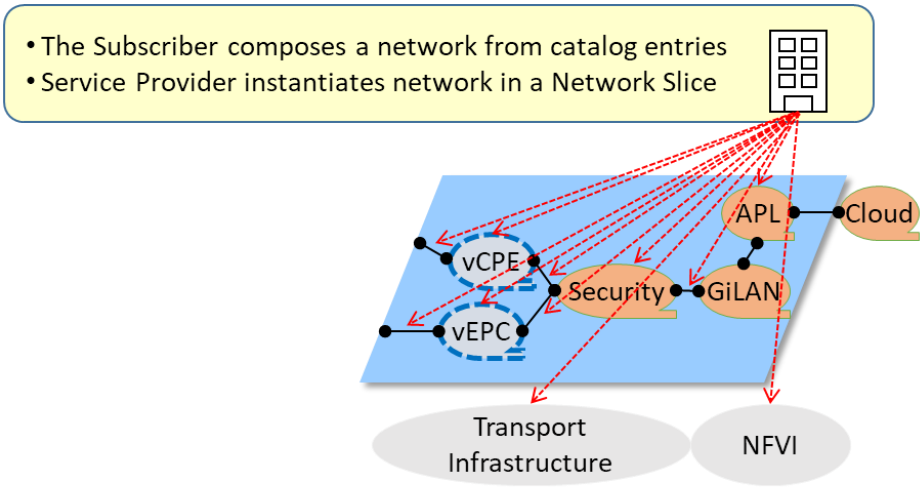


Figure 13 – Example 3 of a semi-customized Network Service Topology View

A.2.2.3 Fully-customized Network Provisioning Model

The fully-customized network provisioning model is offered to Subscribers who want to design their own Network Services. This means a Subscriber can configure attributes of the Network Service's topology, connectivity layers, redundancy, virtual link connections, capacity, routing, QoS policy, etc. In addition to selecting functions from the Service Provider's Product Catalog, the Subscriber can deploy its own virtual network functions (VNFs) as add-on components to the Network Slice on the Service Provider's network function virtualization (NFV) infrastructure. The Subscriber can also manage network performance, fault status and compute resources for VNFs via its Network Service Topology View. An example is illustrated in Figure 14.



APL	Application
GiLAN	SGi Local Area Network; "Gi" is the name of the 3GPP reference point (it is SGi for LTE)
vCPE	virtual Customer Premises Equipment
vEPC	virtual Evolved Packet Core
NFVI	Network Function Virtualization Infrastructure

Figure 14 – Example Product Catalog selections for a fully-customized Network Service

A.2.3 Configuration and Management Requirements

Table 7 summarizes configuration requirements for network provisioning models discussed in Sections A.2.2.1, A.2.2.2 and A.2.2.3.

Table 8 summarizes management requirements for network provisioning models discussed in Sections A.2.2.1, A.2.2.2 and A.2.2.3.

Major feature	Required Configuration Capabilities		
	Fully pre-defined network provisioning model	**Semi-customized network provisioning model**	**Fully-customized network provisioning model**
Connectivity	• IP reachability of Network Slice for delivering services on Network Service • L2 connection to Network Slice for delivering services on Network Service • IP address delivery for end-users • Multicast • Link aggregation	• IP reachability of Network Slice and the Resources in the Topology View • L2 connectivity to Network Slice or the Resource in the Topology View • IP address range for delivery to Subscribers • Multicast • Link aggregation	• Connectivity layer control from L1 to L3 • IP reachability of underlay equipment (physical and virtual resource) • L2 connectivity of underlay equipment (physical and virtual resource) • IP address delivery to underlay equipment (physical and virtual resource) • Multicast • Link aggregation
Session management	• Session creation and deletion of services on Network Service • Path creation and deletion for services on Network Service	• Session creation and deletion to connect to Network Slice • Path creation and deletion to connect to Network Slice • Equipment parameter exchange to connect Network Slice	• Session creation and deletion for configuring virtual link(VL) • Path creation and deletion for configuring virtual link • Parameter exchange between equipment for configuring virtual link
Authentica-tion	• Authentication of feature or application programming interface (API) access for Network Service Subscribers (Application service providers) • Authentication of feature or service delivery on Network Service for end-users	• Authentication of feature or API access for Network Service Subscribers	• Authentication of feature or API access for Network Service Subscriber
Policy control/ management	• Policy control/management feature of end-users	-	-
Mobility management	• Mobility management feature for end-users	-	-
Network Slice configuration	-	• Virtual resource (VNF/VL) configuration	• Configuration of underlay equipment(physical and virtual resource) • Topology • Redundancy • Connectivity layer

Table 7 – Configuration requirements for the different network provisioning models

Major feature	Required Management Capabilities		
	Fully pre-defined network provisioning model	**Semi-customized network provisioning model**	**Fully-customized network provisioning model**
Service ordering	• Service order and configuration of services on Network Service	• Order and configuration of virtual resource (VNF/VL) when creating or modifying Network Slice	• Service order configuration to underlay equipment (physical and virtual resource) on creation or deletion of Network Slice
Network/ equipment Informa-tion acquisition	• Information acquisition of VNF/VL used in service on a Network Slice	• Network Slice or Resource in the Topology View information acquisition	• Acquisition of underlay equipment (physical and virtual resource) information
Health check/Fault isolation	• Service health check/fault isolation on Network Slice	• Network Slice or Resource in the Topology View health check and fault isolation	• Health check and fault detection/isolation of underlay equipment (physical and virtual resource)
Resource manage-ment	• Virtual resource and physical resource management • Mapping resource and virtual resource	• Virtual resource and physical resource management • Mapping resource and virtual resource	-
Perform-ance monitoring	• UNI-to-UNI performance monitoring	• Performance monitoring per Network Slice or Resources in the Topology View	• Performance monitoring per each virtual link
Charging	• Charging information collection(data volume per end users)	• Charging information collection (utilization ratio per Network Slice or Resource in the Topology View, etc.)	• Charging information collection (physical or virtual resource usage ratio, etc.)
End users access manage-ment	• End users access management	• End users access management	• End users access management

Table 8 – Management requirements for the different network provisioning models

A.3 Enterprise Use Case Example

An enterprise in the banking business obtains two Network Services from a Service Provider.

The first Network Service will be used for highly secure financial transactions.

The second Network Service will be used for all the other enterprise internal communications. The second Network Service will be further sliced by the enterprise for document transfer, email transfer and video calls.

A.4 Manufacturer Use Case Example

A manufacturer obtains multiple Network Services from a Service Provider. Each of the Network Services is dedicated to a specific type of service (e.g., assembly line controls, business department communications).

A.5 IP Network Use Case Example

Enterprises need services of Service Providers to connect multiples sites. In this example IP-Provider owns and operates an IP network that has edge network elements (i.e., routers) located at the border of its network.

IP-Provider has applied Network Slicing on its IP network, resulting in three Network Slices named Provider-Slice-1, Provider-Slice-2 and Provider-Slice-3. They are illustrated as parallelograms in the IP-Provider network in Figure 15. The Network Slices are configured with different performance and traffic forwarding characteristics (e.g., routing paths, latency, bandwidth):

- Provider-Slice-1: A network suitable for IoT type traffic.
- Provider-Slice-2: A network suitable for ultra-reliable, very low-latency requirements (such as the URLLC slice defined in ITU-R M.2083 [23]).
- Provider-Slice-3: A network providing stable, high data-rate connectivity (such as eMBB defined in ITU-R M.2083 [23]).

IP-Provider offers these Network Slices as Network Services via its Product Catalog to Subscribers:

- Network-Service-1: Supports Ethernet type connectivity services using Provider-Slice-1
- Network-Service-2: Supports IP URLLC type connectivity services using Provider-Slice-2
- Network-Service-3: Supports IP eMBB type connectivity services using Provider-Slice-3

For these Network Service offers, Subscribers can establish connectivity Services through the corresponding Network Slices via requests at the LSO Allegro interface reference point, rather than having to use the Product Ordering process via the LSO Cantata interface reference point (i.e., the value of the Service Instantiation Capability Attribute is *TRUE*). Subscribers don't have the capability to manage the Service Provider's Network Slices (i.e., the value of the Network Configuration Capability Attribute is *FALSE* for, e.g., Network-Service-1 which uses Provider-Slice-1).

IP-Subscriber is a business with multiple sites as shown in Figure 15. In this example IP-Subscriber needs IP data transfer via tailored Network Slices between the four sites Data Center Edge 1, Cloud Edge 2, Branch Edge 3, Branch Edge 4 and places the following Product Orders:

- An Order for Network-Service-2 to support its internal, secure traffic between Cloud Edge 2 and Branch Edge 3.

- An Order for Network-Service-3 to support its general business or customer traffic between Data Center Edge 1 and Branch Edge 3 and Branch Edge 4.

To accommodate traffic connectivity needs between the different locations, IP-Subscriber requests the instantiation of the following IP Services via the LSO Allegro interface reference points:

- An IP Service on Network-Service-2, illustrated with the grey dashed line in Figure 15.
- An IP Service on Network-Service-3, illustrated with the black dotted line in Figure 15.

If IP-Subscriber had a need for another secure connection from Branch Edge 3 to Branch Edge 4, it could request the instantiation of a separate IP Service on Network-Service-3. The new IP Service would share the existing Network-Service-3 UNIs at Branch Edge 3 and Branch Edge 4. The relationship between IP Service UNIs and the Network Service UNI is n:1.

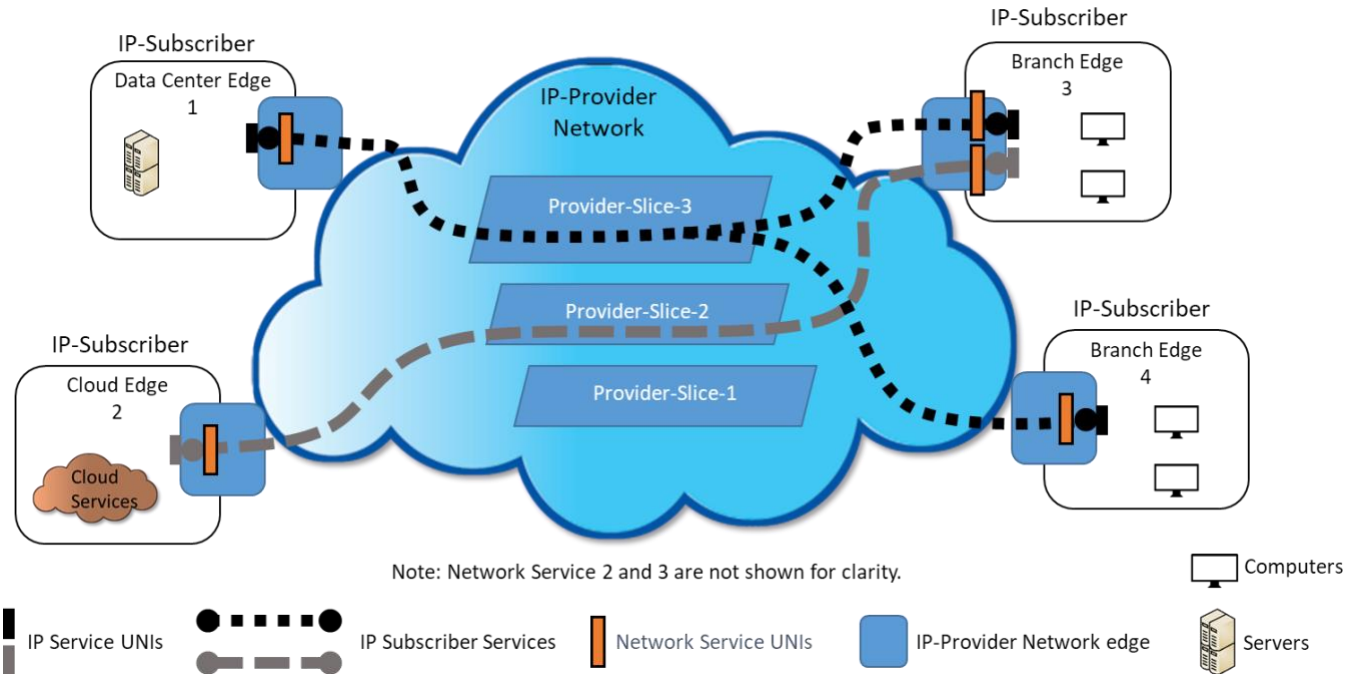


Figure 15 – IP network use case example

A.6 SD-WAN Use Case Example

Enterprises are adopting SD-WAN Services (MEF 70 [39]) to help simplify Enterprise networking. An SD-WAN Service Orchestration Function provides centralized configuration of SD-WAN Edge functions that implement Application Flow steering policies over Underlay Connectivity Services (UCSs). These UCSs may be instantiated on Network Slices. Figure 16 illustrates an example of an SD-WAN Service over IP UCSs which make use of two Network Slices.

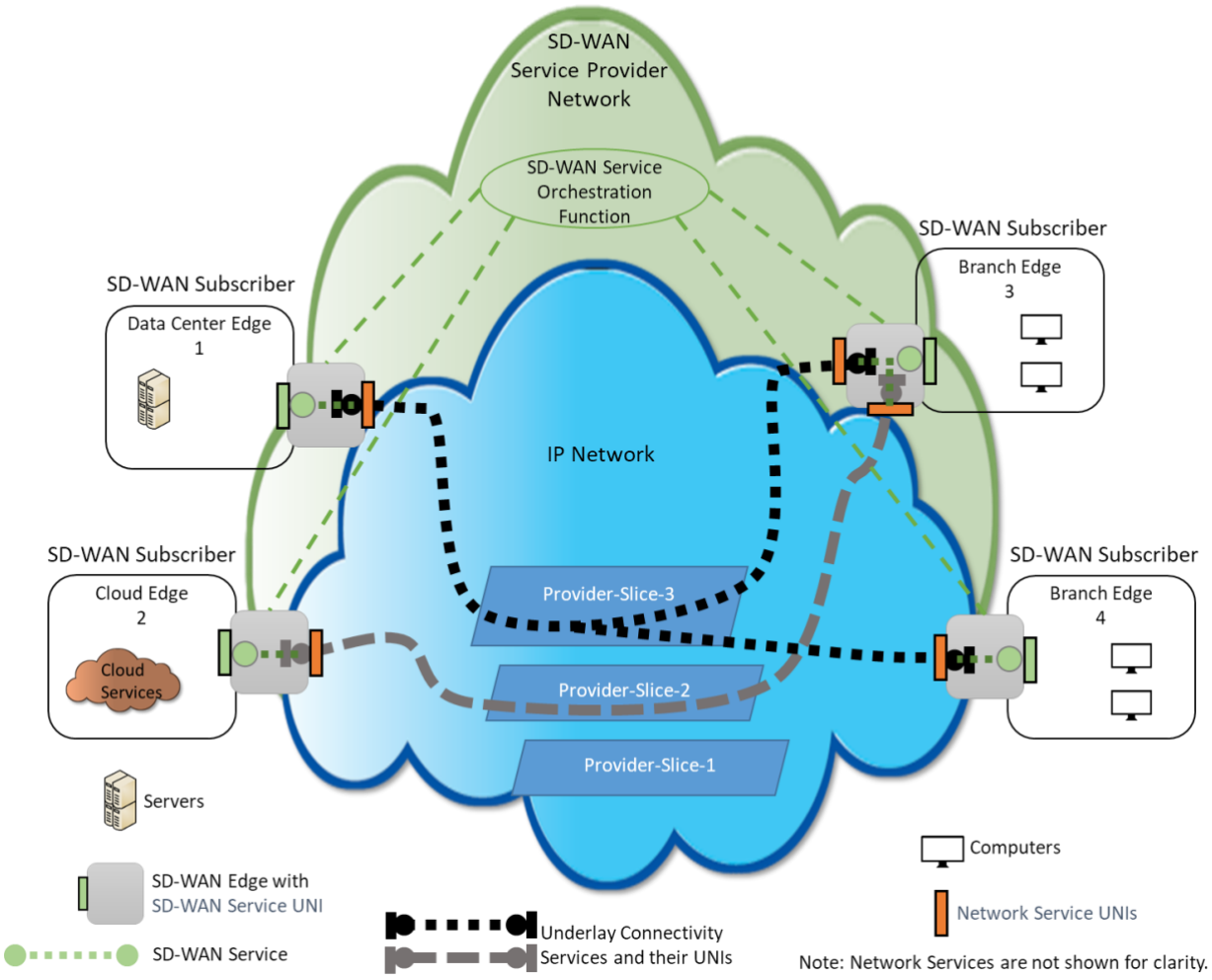


Figure 16 – SD-WAN use case example

Appendix B Relation to Network Slicing defined in other Organizations (Informative)

Network Slicing has received special attention since the NGMN 5G Vision White Paper [41] was published in 2015. Many organizations, including 3GPP, took up work on the topic.

With the discussion of "5G Network Slicing" originating in the mobile network operator domain, much of the work focused on mobile networks and mobile access technology. However, the 5G and network slicing visions and concepts have wider applicability and the terms "Network Slicing" or "Network Slice" are not always used. One common concept is that subsets of Resources from a common infrastructure are grouped and that these subsets (Network Slices) are used to provide services.

B.1 3GPP 5G

3GPP TS 23.501 [1] defines a "Network Slice" as "*A logical network that provides specific network capabilities and network characteristics*". A "Network Slice instance" is defined as "*A set of Network Function instances and the required resources (e.g., compute, storage and networking resources) which form a deployed Network Slice*".[1]

A 3GPP 5G Network Slice instantiated on a Public Land Mobile Network (PLMN) includes Core Network Control Plane and User Plane Network Functions and Next Generation Radio Access Network and/or non-3GPP Access Network.

3GPP TS 28.530 [2] specifies the concepts, use cases and requirements for management of network slicing in mobile networks. The 3GPP management system directly manages only the parts of the network that consist of network functions specified in 3GPP. The 3GPP 5G system consists of 5G Access Network (AN), 5G Core Network and UE.

Instances of 3GPP Network Slices may be used by Mobile Network Operators internally to provide communication services, or they may be provided "as service" to Subscribers from vertical industries. Different management capabilities and network slice instance provisioning procedures may be exposed for the customer.

Mapping to MEF:

- 3GPP Network Slice instance → (A component of a) MEF Network Slice
- 3GPP Network Slice provided "as service" → MEF Network Service
- The Transport Network part of a 3GPP Network Slice instance as defined in 3GPP TS 23.501 [1] can be mapped to a MEF Service (which itself may be instantiated on a Network Service as defined by this Standard) as described and illustrated in Appendix F of MEF 22.3.1 [31] for an EVC-based Ethernet Service.

[1] © 2020. 3GPP™ deliverables and material are the property of ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided to you "as is" for information purposes only. Further use is strictly prohibited.

B.2 ETSI ISG NFV

The relationship between Network Slicing and the NFV constructs was studied in ETSI GR NFV-EVE 012 [4]. The informative Annex D of ETSI GS NFV-IFA 010 [6] describes how NFV will support Network Slicing via NFV "Network Services"[2]:

"*The Network Slice management function is one of the sub-functions in the OSS. The Network Slice management is achieved via NFV Network Service management."*

"NFV MANO is not aware of the purpose for which the instantiation of a NFV Network Service has been requested (i.e. the context of Network Slicing is invisible to MANO)."

"The functions that are managing Network Slicing will use the NFV MANO (Os-Ma-Nfvo) reference point to request and manage NFV Network Service instances. The same reference point is used to control performance, privacy and other advanced functions needed for Network Slicing."

ETSI GR NFV-IFA 024 [5] shows the touchpoints between the information models defined by 3GPP and ETSI ISG NFV as illustrated in Figure 17[2].

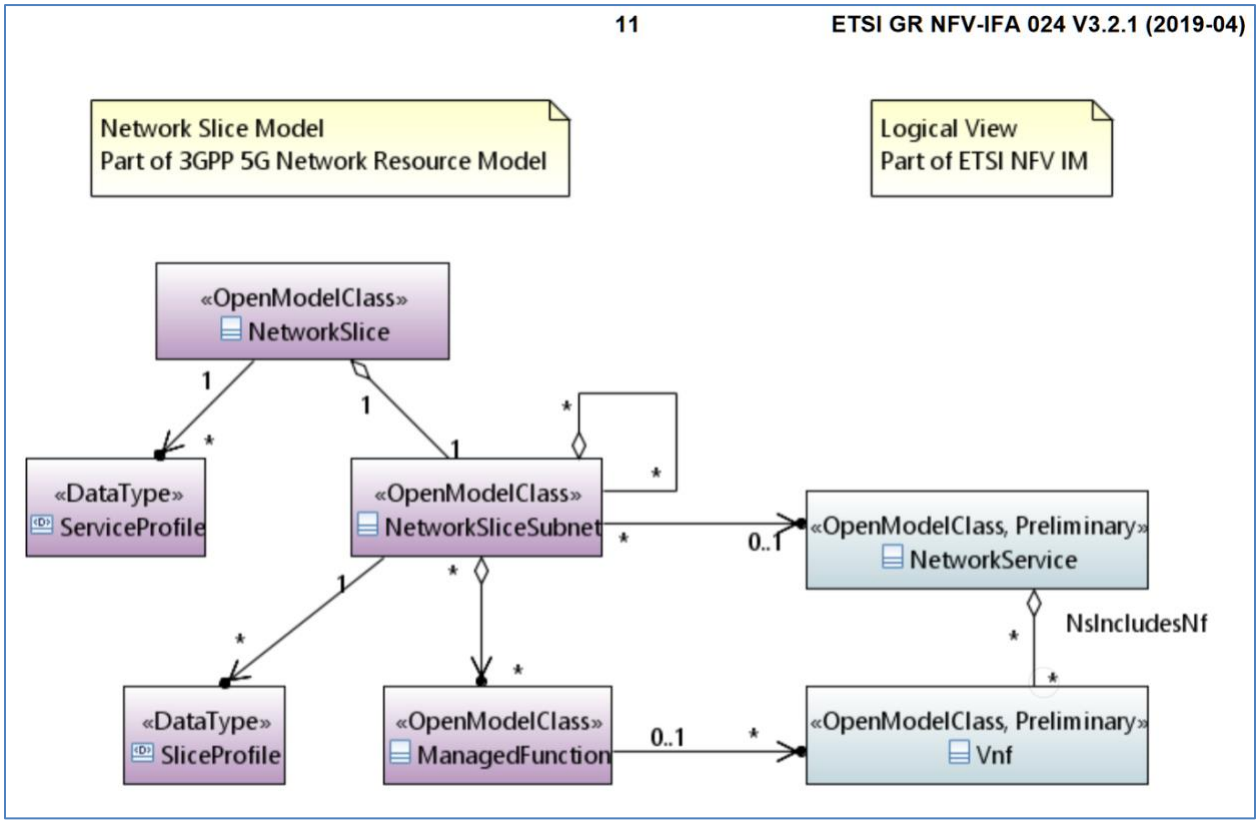


Figure 17 – Touchpoints between ETSI ISG NFV and 3GPP 5G information models

[2] © European Telecommunications Standards Institute 2020. Further use, modification, copy and/or distribution are strictly prohibited.

B.3 ETSI ISG ZSM

Based on documented business scenarios, the ETSI Zero-touch network and Service Management (ZSM) Industry Specification Group works on specifications for topics such as end-to-end management and orchestration of network slicing (ETSI GS ZSM 003 [7]); inter management domain lifecycle management; and closed-loop solutions for automation of E2E service and network management use cases.

B.4 GSMA

The GSMA represents the interests of mobile operators worldwide and, working with operators and vendors, has defined a Generic Slice Template (GST). In October 2019, version 2.0 of the GST was published [8], providing a standardized list of attributes that can characterize a type of network slice. The network slice attributes listed in the GST document are based on open and published 3GPP Release 15 specifications.

GSMA Document NG.116 [8] describes the following roles, illustrated in Figure 18[3]:

- "*Communication Service Customer: Uses communication services, e.g. end user, tenant, vertical.*
- *Communication Service Provider: Provides communication services. Designs, builds and operates its communication services. The Communication Service Provider provided communication service can be built with or without network slice.*
- *Network Operator: Provides network services. Designs, builds and operates its networks to offer such services.*
- *Network Slice Customer: The Communication Service Provider or Communication Service Customer who uses Network Slice as a Service.*
- *Network Slice Provider: The Communication Service Provider or Network Operator who provides Network Slice as a Service*."

[3] © GSM Association

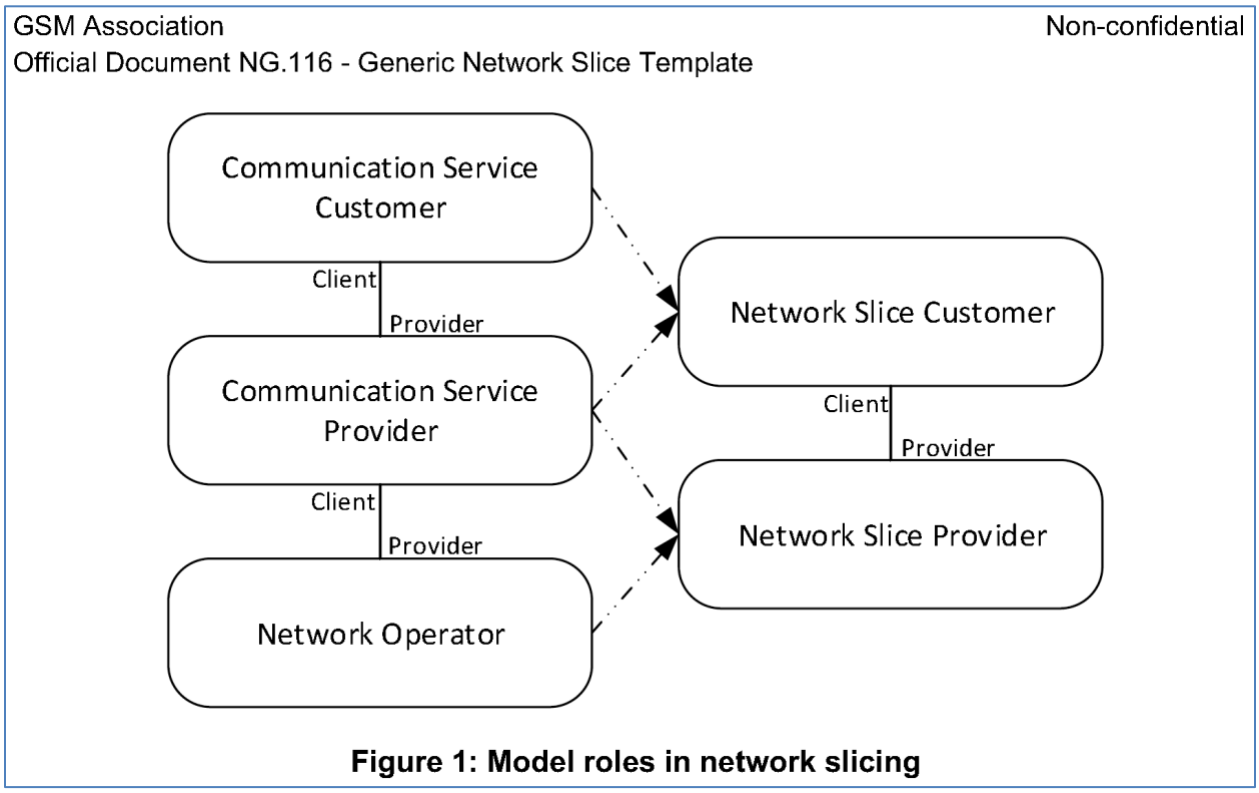


Figure 18 – GSMA model roles in network slicing

Mapping to MEF:

- GSMA Network Slice Customer → Subscriber of a MEF Network Service
- GSMA Network Slice Provider → Provider of a MEF Network Service

B.5 IETF

IETF has been standardizing several data plane techniques to logically separate IP based networks and convey traffic with fulfilling specific communication quality. For example, MPLS-TE (RFC3209 [17]) or Segment Routing (RFC8402 [19]) can provide paths whose intermediate route is decided. Also, deterministic networking (RFC8665 [22]) enables carrying data flows with extremely low data loss rates and bounded latency within an IP network domain.

In addition to the above data plane protocols, a framework called ACTN abstracts network resources on a single or multiple domains and provides traffic-engineered (TE) paths or virtual private networks to customers (RFC8453 [20]).

Some of these techniques are expected to be used for network slicing use cases. For meeting advanced requirements for networks, the VPN+ framework provides more enhanced virtual private network (VPN) services by combining several IETF techniques/protocols (I-D.ietf-teas-enhanced-vpn-05 [12]). However, those were not specifically designed for network slicing, and there are no unified definitions of network slicing and its characteristics. For example, definitions of network slicing described in RFC8453 [20] and RFC8656 [21] are a bit different.

Recently a Network Slicing Design Team (NS-DT) was formed and started discussion in response to demands for network slicing. The role of the NS-DT is development of a framework for delivering network slicing using existing IETF technologies, and if and where needed, possible extensions to those technologies. The NS-DT has been proceeding to make definition and framework for network slices in transport networks (e.g., IP, Ethernet, Optics, TDM, etc.). Early drafts about the definition (I-D.nsdt-teas-transport-slice-definition-02 [15]) and framework (I-D.nsdt-teas-ns-framework-03 [13]) were published in April 2020.

B.6 ITU-T

ITU-T defines in Recommendation Y.3100 [25] the term "Network slice" as "*A logical network that provides specific network capabilities and network characteristics*" and notes "*Network slices enable the creation of customized networks to provide flexible solutions for different market scenarios which have diverse requirements, with respect to functionalities, performance and resource allocation*"[4]. Virtualization is defined in ITU-T Recommendation G.7702 [24] as "*an abstraction and subset whose selection criterion is dedication of resources to a particular client or application*"[4]. A virtual network is a virtualization of ITU-T G.800 [28] layer network resources. The virtual network is a part of the information contained in a client context or a server context. Transport network resources are assigned to a virtual network by administrative or other means. Note that a virtual network in the server context of a client controller is the same as the virtual network in the corresponding client context of its server controller. In ITU-T GSTR-TNGG [26], Section 8 describes how a virtual network in a transport network supports a 3GPP network slice, including management aspects.

The client and server contexts referred to in the above paragraph are defined in ONF TR-521 [43] and in ITU-T G.7702 [24].

B.7 ONF SDN Architecture

Although the SDN Architecture specification in ONF TR-521 [43] does not use the term slice or network slice, ONF TR-526 [44] shows that a 5G slice is comparable to, if not the same as, an SDN client context.

The view and functionality provided by the SDN Architecture's "client context" in a controller corresponds to the network presented to a Subscriber and the corresponding Subscriber's orchestration, control and management capabilities provided by the Service Provider.

Mapping ONF SDN Architecture to MEF

- Network Slice corresponds to "client-context" of ONF SDN Architecture and maps to LSO SOF and ICM functionalities.

[4] © ITU All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

B.8 Harmonized View for Network Slice Management with MEF LSO

This section examines how a harmonized architectural view can be derived from network slicing-related developments in the aforementioned SDOs and taking MEF LSO as a reference for managing the orchestration of Network Slices.

This harmonized architectural view takes as a reference the abstraction layers specified in MEF 55.1 [34]. Similar concepts are specified in other SDOs like TM Forum where abstraction layers are classified into more granular levels in terms of technology, vendor-specific or agnostic domains. The combination of these concepts with the MEF LSO architecture is illustrated in Figure 19.

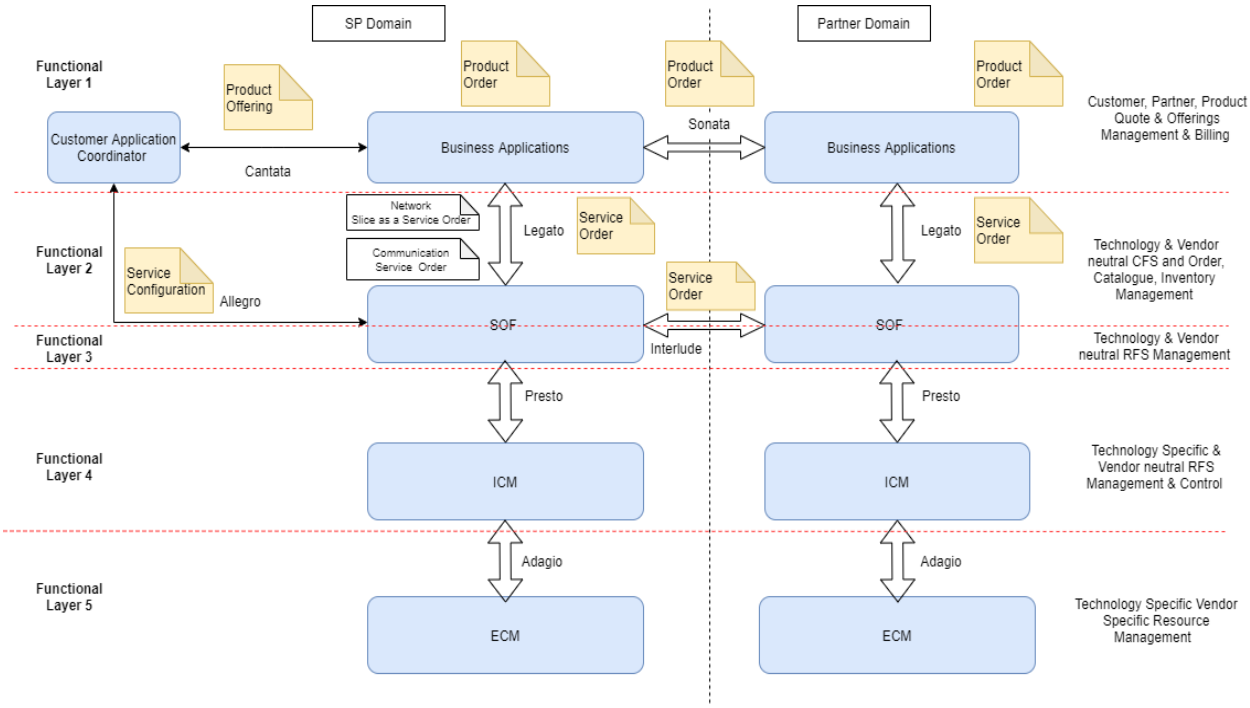


Figure 19 – Combination of LSO Abstraction Layers and TM Forum Functional Layers

Referring to MEF 55.1, the service orchestration functionality (SOF) mainly carries out service orchestration and management. Broadly it can be assumed that in the SOF, there is an internal functional layer which operates on the Subscriber/Customer facing service (CFS) and the resource facing service (RFS). Additionally the SOF provides a technology and vendor agnostic Service view to the upper layers. Similarly infrastructure control and management (ICM) operates on the technology specific and vendor agnostic RFS and further coordinates with element control and management (ECM) which is focused on the technology and vendor specific resource Management.

Section 6.2.2 discussed two flavors of Subscriber orders that is possible with Network Slicing – a) Network Slice offered as a Network Service to the Subscriber and b) another (communication or connectivity) Service provisioned on a Network Slice.

In both cases a) and b), depending on the deployment scenario the order can be fulfilled by the Service Provider domain alone or coordinated between Service Provider and Partner domain LSO functions.

In case a), the order expresses Subscriber requirements for a Network Slice with a specific set of characteristics which can be managed and tuned by the Subscriber on demand (see also Section 6.2.5). Based on the Service Agreement with the Service Provider, Resources may be presented to the Subscriber as well as corresponding parameters to manage the presented Resources.

In case b), the order expresses the Subscriber requirements in terms of the Service characteristics (such as the Service Level Specification (SLS), Quality of Service, end point properties, service controls) and internally this is translated to a profile that is used to allocate right-sized Network Slice instances to support the CFS. This means that the existence of the Network Slice is not exposed to the Subscriber, but indirectly the Subscriber's requirements are translated to requirements on a Network Slice.

The diagram in Figure 19 also shows five functional layers that are roughly classified based on the logic discussed earlier in this section. Note that these functional layers are used as an aid for identifying the functionality impact of Network Slicing and not necessarily to define new capabilities.

- Functional Layer 1: operates on and manages the business entities.
- Functional Layer 2: operates on and manages the Service order and CFS which is technology and vendor agnostic.
- Functional Layer 3: operates on and manages the technology and vendor neutral RFS.
- Functional Layer 4: operates on and manages the technology specific RFS.
- Functional Layer 5: operates on and manages the technology specific and vendor specific resources.

The functional layers identified above can be mapped to different SDO defined functional blocks as in Table 9. Note that Functional Layer 5 is omitted as there is a high possibility of vendor specialization which is outside the scope of this Appendix section.

Logical layers to identify Network Slice related management functionality	Mapped LSO Functional Block	Mapped SDO Function	Mapped Open Source Implementation Functions (e.g., Open Networking Automation Platform (ONAP), Open Source MANO (OSM) etc.)
Functional Layer 1	Business Applications	TM Forum Open Digital Architecture (ODA) Core Commerce Management	TM Forum Business Operating System (BOS)
Functional Layer 2	SOF (CFS handling)	MEF Service Orchestration Function (SOF), TM Forum ODA Production, ETSI Zero Touch network & Service Management (ZSM) E2E Service Management, 3GPP Communication Service Management Function (CSMF)	Open Networking Automation Platform (ONAP) External API (Ext-API), ONAP Service Orchestrator (SO)
Functional Layer 3	SOF (RFS handling)	MEF SOF, ODA Production, ZSM E2E Service Management, 3GPP NSMF, 3GPP NSSMF (Optional)	ONAP SO, Open Source MANO (OSM) Service Orchestrator(SO)
Functional Layer 4	ICM	IETF draft-nsdt-teas-transport-slice-definition-01 Transport Slice Controller, MEF ICM, ODA Production, IETF Abstraction and Control of Traffic Engineered Networks (ACTN) MDSC, 3GPP Network Slice Subnet Management Function (NSSMF) (Optional), ETSI Network Function Virtualization (NFV) Management and Orchestration (MANO), ZSM Management Domain, ONF Transport API (TAPI) VNS Controllers, ONF SDN Controller	ONAP SO, ONAP Virtual Function Controller (VFC), ONAP Software Defined Network Controller (SDNC), OSM Service or Resource Orchestrator (SO/RO)

Table 9 – Functional Layers Mapped to Different SDO Defined Functional Blocks

The diagram in Figure 20 represents Table 9 with a business scenario where 5G mobile network slicing is realized by a Service Provider using relevant SDO functions mapped to the LSO functional blocks and transport Network Slice segments (for fronthaul, midhaul and backhaul) realized by a Partner LSO function.

As stated above two flavors of Subscriber orders are possible with Network Slicing:

a) Network Slice offered as Network Service to the Subscriber which presents the Network Slice requirements and controllable parameters.

b) Another (communication or connectivity) Service to be instantiated/provisioned on a Network Slice. The visibility of the underlying Network Slice depends on Service Provider policy/strategy and ranges from no visibility to a fully transparent presentation.

The following 3GPP management functions (defined in 3GPP TR 28.801 [3]) are logically mapped to SOF in MEF LSO: communication service management function (CSMF), network slice management function (NSMF) and network slice subnet management function (NSSMF). These management functions are mapped to the operations support systems (OSS) in ETSI GR NFV EVE 012 [4]. For mobile network slicing there may be many partner domains coordinating with a Service Provider i.e., application vendors, edge service providers, value-added service providers, roaming network providers, etc. MEF LSO already has Sonata and Interlude reference points defined for east-west connectivity.

Considering a scenario where the Subscriber places an order for a communication service, the SOF functional layer that operates on the CFS receives the communication service-related requirements from the Order management functions and composes the Service profile. Depending on the Service orchestration logic, the Service profile is shared with the NSMF or a new request is sent to the Partner domain to realize the required constituent RFS, leading to constituent Network Slice instances being created.

The ICM functional layer consists of multiple functions. Each ICM could have some combination of all the white blocks shown in Figure 20. However, for clarity of the diagram some functional white blocks are shown on the Service Provider ICM and others on the Partner ICM.

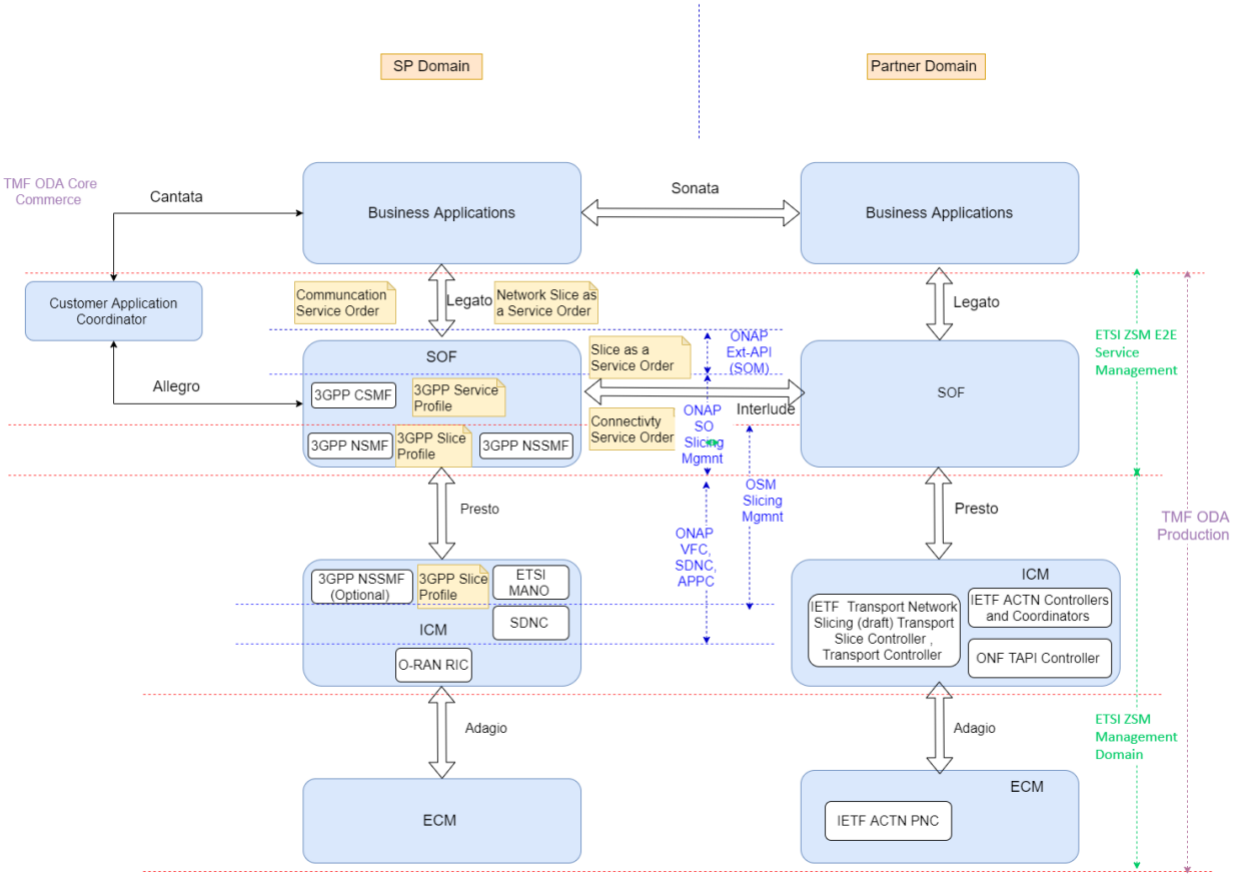


Figure 20 – Example for functional mapping of management functions across different SDOs to MEF LSO to support Network Slicing

The NSSMF function can optionally be mapped to the SOF or ICM blocks depending on the deployment scenario. This is due to the fact that NSSMF along with other ICM blocks may be logically grouped as a separate logical domain in certain deployments thereby appearing as cross-domain SOF. Such a logical domain may be composed based on technology or geographic proximity or other business level criteria.

NSMF to NSSMF interaction is beyond the scope of this Appendix section and covered in 3GPP specifications. This Appendix section does not elaborate on the MANO and SDNC mapping as these are well defined in Section 9.1.1 of MEF 55.1 [34].

In the business scenario depicted in Figure 20, a transport Network Slice segment is realized by the Partner domain. While transport network slicing related standardization activities are in the initial stage, there are early drafts like draft-rokui-5g-transport-slice-00 [11], draft-nsdt-teas-transport-slice-definition-01 [14] or, in the context of IETF ACTN specification, draft-king-teas-applicability-actn-slicing-04 [10]. All these drafts define enhancements or additional capabilities on the controller functions to support transport Network Slicing.

MEF already supports the Presto reference point for infrastructure control and management. The Presto reference point realized through the T-API [45] supports the management and control of connectivity Service, virtual network service, and topology service, etc. The early work being done in IETF to realize transport network slicing can functionally map to the ICM reference block in the MEF LSO Reference Architecture.

Figure 20 also depicts the functional mapping to ONAP and OSM open source implementations. Both ONAP and OSM are either in early stages of supporting network slicing or have reference proof of concepts available for further development.

In ONAP Frankfurt Release (Release 6) early support for slicing the 5G core network was introduced. This was realized by developing the communication service management function and network slice management function as part of the service orchestrator component. The network slice subnet management function is expected to be implemented externally to ONAP. This is aligned with the harmonization view depicted above, with an exception that the NSSMF is realized as an external function and not part of SOF. In this case NSSMF positioning in the ICM functional block in MEF LSO is more suitable as this is realized through a separate technology specific (5G core) domain controller.

In OSM Release 7, there are some early activities on modelling templates for network slices and mapping those to network services connected by virtual links. The OSM Release 7 documentation mainly focusses on the “network slice” and “network slice subnet” orchestration functionality by onboarding associated network slice templates and network service descriptors, and instantiation of shared and standalone network slice instances.