Draft

MEF 84 (R1)

Network Slicing

July 2020

Caution – this draft represents MEF work in progress and is subject to change.

This draft document represents MEF work in progress; it has not achieved full MEF standardization and is subject to change. Changes are likely before this becomes a fully endorsed MEF Standard. The reader is strongly encouraged to keep this in mind and review the Release Notes (if applicable) when making a decision on adoption. Additionally, because this document has not been adopted as a Final Specification in accordance with MEF's Bylaws, Members are not obligated to license patent claims that are essential to implementation of this document under MEF's Bylaws.

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.

Editor Note 1. This list will be finalized before Letter Ballot. Any member that comments in at least one CfC is eligible to be included by opting in before the Letter Ballot is initiated. Note it is the MEF member that is listed here (typically a company or organization), not their individual representatives.

- ABC Networks
- XYZ Communications

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.

Editor Note 2. Ensure to add all abbreviations to the table

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, or a partner network operator.	MEF w55.1 or This Standard
EVC	Ethernet Virtual Connection	MEF 10.4
EVPL	Ethernet Virtual Private Line	MEF 6.3
Network Service	A Network Slice offered as a Service to one or more Subscribers	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 infrastructure into Network Slices	This Standard
Resource	A physical or non-physical component (or some combination of these) within a Service Provider's infrastructure or inventory	MEF 55 [TMF GB922]
Service	Represents the Customer experience of a Product Instance that has been realized within the Service Provider's and / or Partner's infrastructure	MEF 55 [TMF GB922]
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 MEF 61
Subscriber	Synonymous for Customer	This Standard
UNI	User Network Interface	This Standard
User Network Interface	The demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber	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 [1], RFC 8174 [2]) 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**.**

Editor Note 3. The following paragraph will be deleted if no conditional requirements are used in the document.

A paragraph preceded by **[CRa]<** specifies a conditional mandatory requirement that **MUST** be followed if the condition(s) following the "<" have been met. For example, "**[CR1]<**[D38]" indicates that Conditional Mandatory Requirement 1 must be followed if Desirable Requirement 38 has been met. A paragraph preceded by **[CDb]<** specifies a Conditional Desirable Requirement that **SHOULD** be followed if the condition(s) following the "<" have been met. A paragraph preceded by **[COc]<** specifies a Conditional Optional Requirement that **MAY** be followed if the condition(s) following the "<" have been met.

5 Introduction

This section informs about 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 put on what is required for external visibility of Service Provider domain internal Network Slice instances in the Subscriber domain. This Standard defines a Network Service and provides information about Network Service attributes and requirements, through which the Service Provider can provide Network Slices as Services to Subscribers.

This Standard focuses on the terminology and descriptions for the Subscriber and Service Provider relationship; details of Service Provider and Partner relationships are excluded.

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 infrastructure into Network Slices. Network Slices have capabilities to manage, control and orchestrate the functional elements in their subset independently from other Network Slices' subsets.

When a Service Provider applies Network Slicing, the Service Provider has the option to either use a Network Slice for its own internal purpose only, or to make the Network Slice and its associated possible services visible and available to Subscribers as a Network Service.

A Service Provider may decide to make only some aspects of Network Slices visible to Subscribers. A Network Slice offered by a Service Provider to a Subscriber is referred to as a Network Service in this Standard.

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 6.4 informs about Network Service attributes that describe a network and related orchestration, control and management capabilities presented to the Subscriber from a Network Slice instantiated in the Service Provider domain.

The informative Appendix A presents use cases.

The informative Appendix B relates Network Slicing as defined in this Standard with other 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 infrastructure.

Examples of Network Slicing where the Service Provider has infrastructure containing five physical links and could slice these as follows, which is illustrated in Figure 1.

- Network Slicing option A: create two subsets
    - Subset A.1: three physical links
    - Subset A.2: 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: create two subsets
  - Subset B.1: five virtual links with x% of the bandwidth available on the five physical links
  - Subset B.2: 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%)

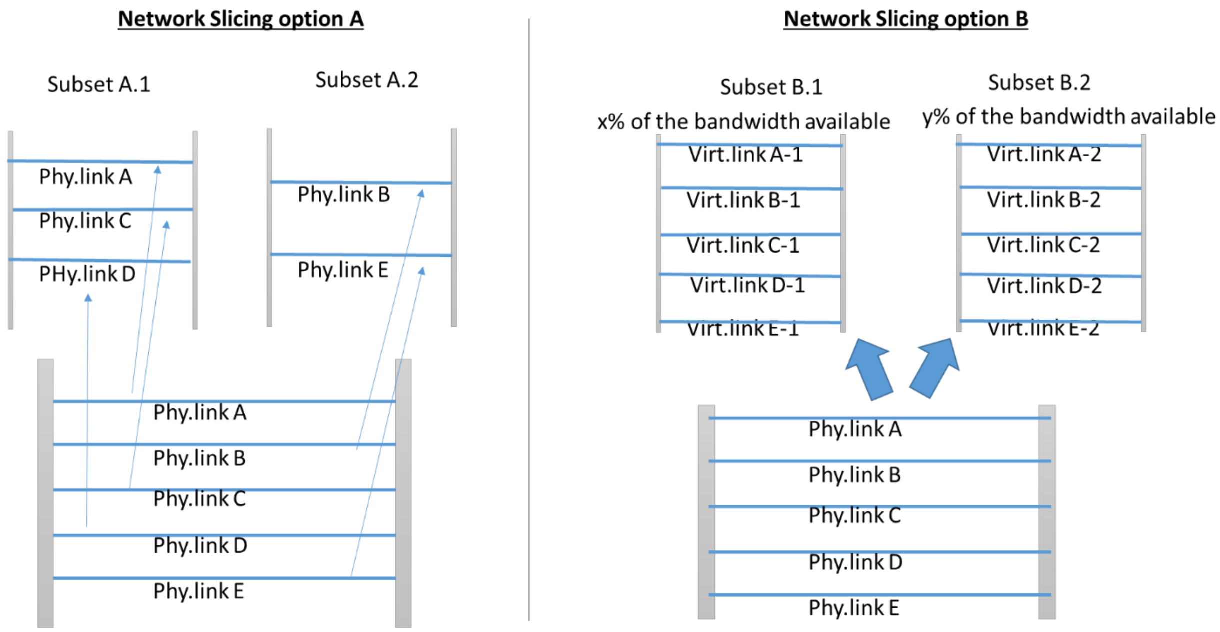


Figure 1: Network Slicing Example Options A and B

6.2 Network Slices and Services

A Network Slice is a subset of a Service Provider Network, which may be used and managed independently. Network Slices can result from physical as well as logical grouping of infrastructure.

A Network Slice consists of infrastructure and resources for Services.

As Network Slices are formed on a common underlying infrastructure, resources can be assigned and configured for either dedicated or shared use. Therefore, Network Slices are instantiated either for dedicated or shared use.

A Service can be instantiated on a Network Slice and offered as a Product to a Subscriber or provided by a Partner to a Service Provider.

[R1] A Network Slice **MUST** be instantiated prior to being used to provide Services.

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 a Product Order from a Subscriber.

The Product Order from a Subscriber may be for

- A Network Service (see sections 6.3 and 7), or
- Another Service to be instantiated/provisioned on a Network Slice.

A Network Slice can host one or more Services.

As Network Slices are instantiated on common underlying infrastructure, Network Slice resources can be assigned and configured for either dedicated or shared use.

A Network Slice created to serve a specific Subscriber is dedicated to that Subscriber.

A Network Slice for shared use hosts Services provided to several Subscribers.

Isolation is an important feature of Network Slicing. The Service Provider ensures Network Slices are isolated from each other, such that information carried in a Network Slice does not spill over into another Network Slice.

[R2] The Service Provider **MUST** enforce the isolation of Network Slices instantiated on its infrastructure.

6.3 Network Services

The Service Provider can offer Network Slices as Network Services to one or more Subscribers with

- The Network Service description to be used for Product Orders
- Orchestration, control and management capabilities available to the Subscriber(s) as part of the Network Service offer

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

- One Network Slice, named Network-1, is offered for shared use as Network Service 1. It contains subset 1 of the Service Provider Network. Only the existence of Network-1 is made visible, i.e. no topology information is presented to Subscribers from Network-1. Network Service 1 supports EVPL connectivity. Subscribers can order EVPL Services on Network-1, but they have no orchestration, control and management capabilities for Network-1 (opaque view).

- The other Network Slice, named Network-2, is offered for dedicated use as Network Service 2. It contains subset 2 of the Service Provider Network. The Service Provider makes this Network Slice available to one Subscriber by presenting more details of Network-2 than in the example with Network-1. The Subscriber can order up to three EVPL on Network-2 and orchestration, control and management capabilities are extended to the presented network.

- The Service Provider manages both Network Slices independently from each other, and enforces that each instance remains within its defined bounds of resource usage.

- The Service Provider enforces that Subscriber orchestration, control and management requests remain within the bounds of the agreement with the Subscriber

The Network Service is defined in section 7.

6.4 Management of Network Slices

After a Network Slice has been instantiated it needs to be managed, controlled, configured and monitored.

After the Service Provider has instantiated a Network Slice for a Network Service, the Service Provider continues to manage, control, configure and monitor the Network Slice.

From time to time Network Slices may need to be updated or modified.

From time to time, the Service Provider may need to update or modify the Network Slice to reflect Network Service modifications by the Subscriber(s).

Finally, at the end of its lifecycle the Network Slice will be deleted from the management system and the associated resources made available.

An instantiated Network Slice includes the capability to orchestrate, control and manage Services and their corresponding resources.

[R1] The Service Provider **MUST** confine the Service orchestration, control and management to the corresponding Network Slice.

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

7 Network Service – Providing a Network Slice as Service

A Network Service is a Network Slice offered as a Service to a Subscriber. The Service Provider is the organization that provides this Service.

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.

This section describes the Network Service in section 7.1.

Section 7.2 provides attributes to describe/define the Network Service.

7.1 Network Service Description

The Network Service presents a network to the Subscriber, based on resources in a Network Slice which is instantiated in the Service Provider Network. The presentation of the Network Slice (i.e. the presented network) can range from full abstraction to actual resources. The degree of the Subscriber's management capability for the presented network depends on the service agreement. An example is illustrated in Figure 2.

In the example, the Service Provider internal Network Slice that is used for the Network Service is symbolized by the orange parallelogram. The network presented to the Subscriber is visualized by the blue network. The presented network provides infrastructure (resources) to the Subscriber. UNI-to-UNI connections can be established by the Subscriber either by ordering (MEF defined) connectivity services from the Service Provider; or on its own, if the corresponding network management and configuration capabilities are included in the Network Service.

The LSO Cantata and Allegro interfaces are used for Service ordering, network presentation to the Subscriber and any orchestration, control and management actions (requested) by the Subscriber on the presented network.

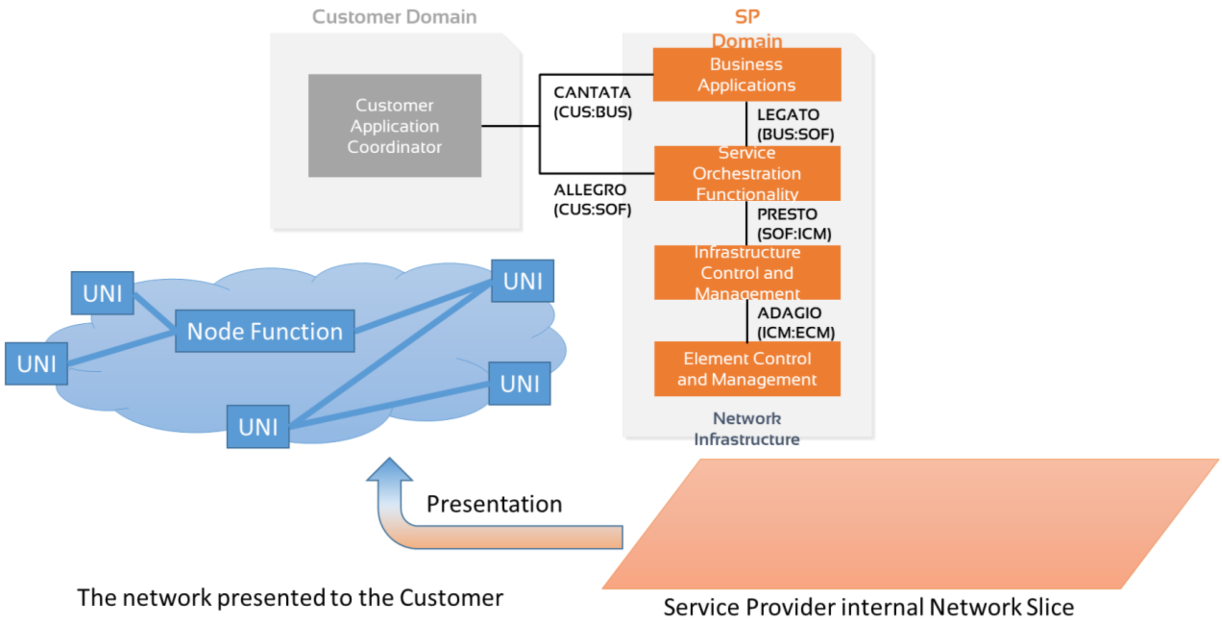


Figure 2: Example of Network Service

The Subscriber can manage, configure and further slice the presented network and instantiate Services within the bounds agreed with the Service Provider. All orchestration, control and management actions on the presented network by the Subscriber must be authorized and mapped to the SP internal Network Slice.

[R3] The Service Provider MUST confine the Subscribers orchestration, control and management activities on the network presented by a Network Service to the corresponding service agreement and utilized Network Slice.

Examples of orchestration, control and management capabilities that the Subscriber can perform include:

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

With regard to further slicing the presented network, there are two cases:

1. Slicing is applied to the presented network and enforced by the Subscriber. This is not visible to the Service Provider.

2. Slicing of the presented network is requested by the Subscriber from the Service Provider and enforced by the Service Provider.

Combinations of items 1 and 2 are also possible. For example, the Subscriber requests the Service Provider to slice the presented network into the subsets A and B. Then the Subscriber further splits (creates subsets) of subset A, without asking the Service Provider for its support.

The Subscriber’s orchestration, control and management capabilities apply to the Network Service for that Subscriber. When Network Slices use shared resources, the Service Provider ensures a sufficient amount of resources is available.

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

At its most basic, a Network Service provides the Subscriber a network presentation connecting two UNIs with a single, direct link and the Subscriber is enabled to instantiate Services on that presented network. For example, the Network Service exposes a network topology with two UNIs connected by a link and the Subscriber is allowed to request instantiation of one EPL.

Please refer to Appendix A for examples of other variants of presented networks and topologies.

7.2 Network Service Attributes

This section provides a list of Network Service attributes that can be used to describe a Network Service. Network Service attributes are grouped into Resource attributes (see 7.2.1), attributes describing instantiable Services (see 7.2.2) and Management attributes (see 7.2.3).

Editor Note 1. MEF Network Service Attributes standardization should take into account GSMA, 3GPP list of attributes to enable MEF Services over 3GPP 5G Network Slices.

7.2.1 Network Service Resource Attributes

Network Service Resource attributes describe aspects of the Network Slice which are presented to the Subscriber, such as:

- Network Service Topology
    - List of Network Service UNIs
    - List of Network Service Internal Node Functions
    - List of Network Service Links

- Network Service UNI
    - Network Service UNI Identifier
    - Interface type (e.g. ETH)
    - Rate (e.g. 100G)
    - Instantiable Service type capability (e.g. L2,L3)
        - There can be a unique association with an existing MEF Standard (e.g. MEF 6.3 for L2, MEF69 for L3)
        - There may be several instantiated Service UNIs on a Network Service UNI resource
- Network Service Link
    - Network Service Link Identifier
    - Link type
    - Link rate
    - Network Service Link End Points (set of 2 or more)
- Network Service Internal Node Function
    - Network Service Internal Node Function Identifier
    - Characteristic (e.g. physical or virtual)
    - Function type (one or more of the following are possible)
        - Connectivity Function
            - Forwarding capability (will have e.g. a certain capacity and number of ports)
        - Compute Function
            - Processing capability (e.g. processor speed, memory)
        - Storage Function
            - Storing capability (e.g. redundancy, capacity)
            - Speed of access

            - Storage time (persistency of information stored)
        - Security Function (e.g. Encryption, AAA)
        - Other

7.2.2 Instantiable Services Attributes

Instantiable Services attributes describe Services that the Subscriber can request the Service Provider to instantiate on the presented network.

- Supported Service Types
    - Supported Services (for example MEF 63/64, MEF 6.3/51.1, MEF 69, MEF 70)
    - Max. number of instantiated services supported
        - Limiting the overall number of supported Service instances on the presented network
        - In addition Service Provider may want to pre-define the max number per service type if more than one service type is supported
- Matrix of allowed and forbidden combinations of supported Service type instantiation

7.2.3 Network Service Management Attributes

Management attributes describe the Subscriber's management and control capabilities for the network presented to the Subscriber, such as:

- Network Service Identifier
    - The unique identifier of the Network Service
- Network Identifier
    - The unique identifier of the Network Slice utilized for this Network Service
- Network Slice Profile
    - The Service Provider can use this as label to describe the kind of Network Slice used for this Network Service
    - Examples a Service Provider may use are 3GPP slice type, MEF 23 performance metric objective for high, medium, low classes of service
- Slicing Capability – Ability to further slice the presented network

- Configuration Capability – Ability to configure the presented network and its Resources (Network Service UNIs, Network Service Links and Network Service Internal Node Functions)
    - May include the capability to add/remove resources (e.g. UNI, Link)
- Service Instantiation Capability– Ability to instantiate Services or request instantiation of Services
- Service Configuration Capability – Ability to modify Services instantiated by the Service Provider
- Other

8 References

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

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

[3] MEF Service Operations Specification MEF 55 *Lifecycle Service Orchestration (LSO): Reference Architecture and Framework*

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

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

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

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

[8] NGMN 5G White Paper, 2015

[9] 3GPP TS 23.501 V15.4.0 (2018-12), *System Architecture for the 5G System; Stage 2 (Release 15), December 2018*

[10] ETSI GR NFV-EVE 012 V3.1.1 (2017-12), *Report on Network Slicing Support with ETSI NFV Architecture Framework*, December 2017

[11] ETSI GS NFV-IFA 010 V3.1.7 (2019-2), *Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Functional requirements specification*, February 2019

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

[13] GSMA Official Document NG.116, "*Generic Network Slice Template version 2.0*, October 2010

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

[15] 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

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

[17] 3GPP TR 28.801 V15.1.0 (2018-01), *Study on management and orchestration of network slicing for next generation network (Release 15)*, January 2018

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

Appendix A Use Cases (Informative)

This appendix provides example use cases for the concepts described in the previous sections of this Standard. Further use cases are provided in the MEF White Paper on Slicing for Shared 5G Fronthaul and Backhaul [18].

A.1 Shared Fronthaul 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 network elements located in a co-location site and near mobile network locations like Remote Radio Heads (RRH, 4G context), Radio Units (RU, 5G context) 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 MNOs 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).

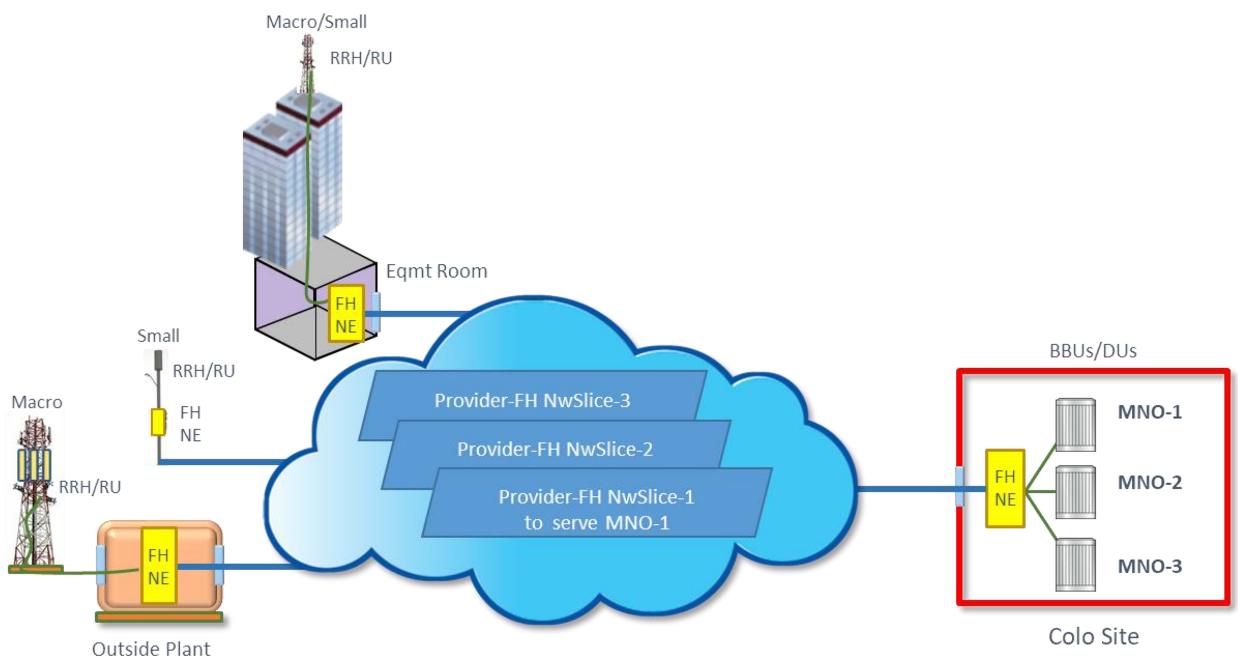


Figure 3: Shared Fronthaul Example; basic scenario

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

The LSO Cantata interface is used for business related interactions like ordering and billing.

The LSO Allegro interface is used for configuration and control related management interactions which are allowed by the respective Service agreement; like 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 UNIs to be connected are MNO-1 Fronthaul NE ports and the corresponding MNO-1 5G DU port.

Provider-FH instantiates the EVPL on NwSlice-1. This is visualized in Figure 4.

For clarity, only one UNI port is shown at each radio location.

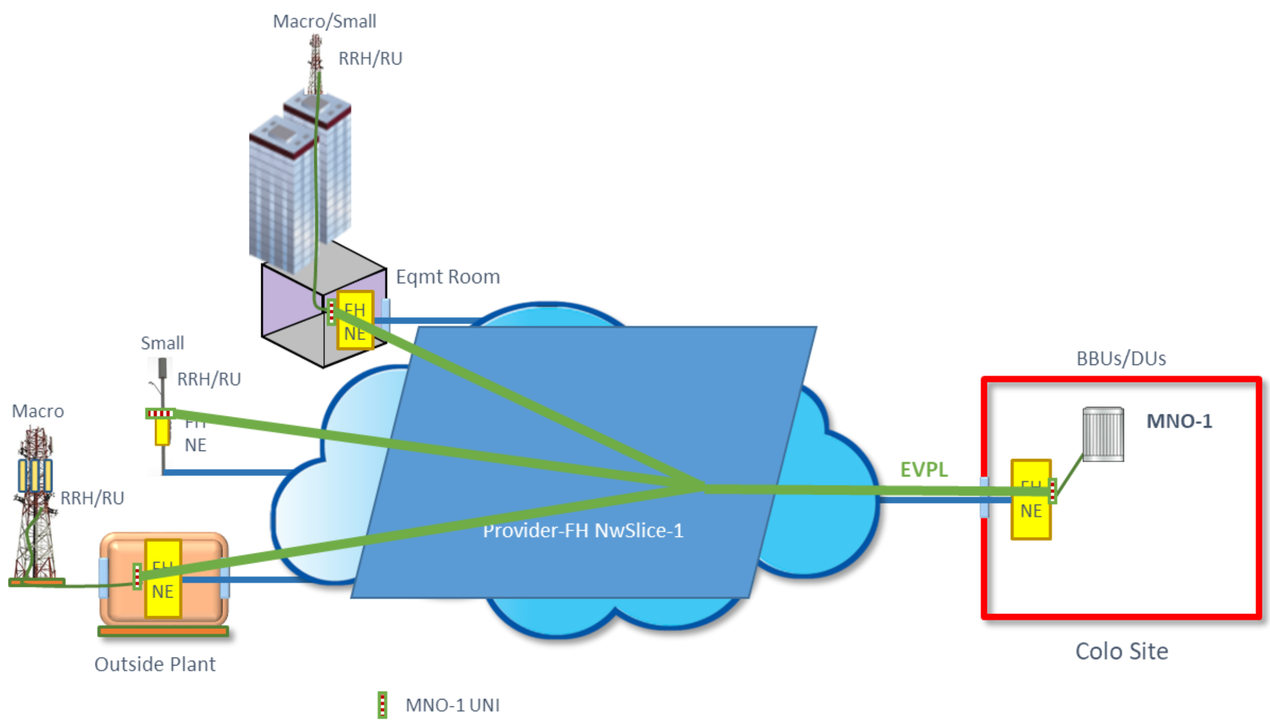


Figure 4: Example Scenario MNO-1: Connectivity Service to connect locations

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 LSO Allegro interface, modifications of the values of EVPL service attributes as 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 network topology presented in this example from Provider-FH to MNO-2 is shown in Figure 5. The UNIs support connections from MNO-2's RRH/RUs and MNO-2's 5G DU. Each link in the presented topology has its individual capacity that may be different from the capacity of the other links.

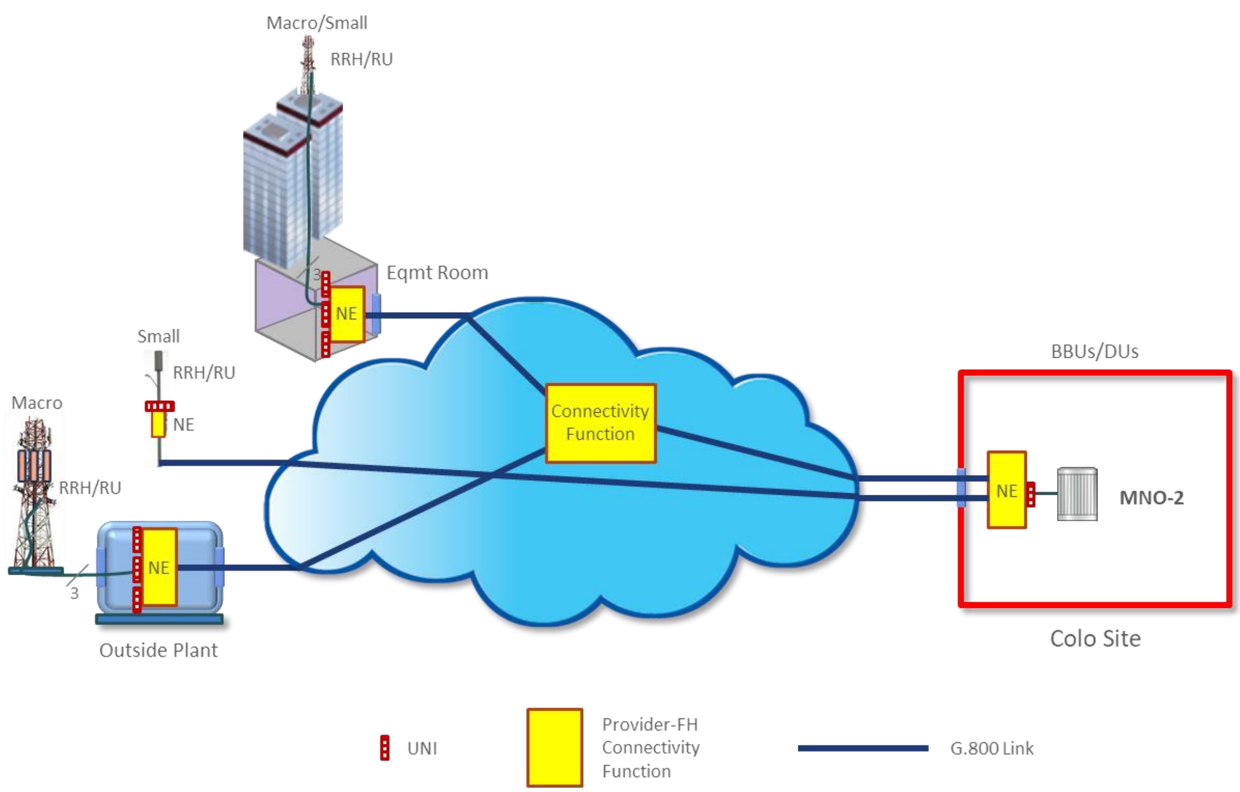


Figure 5: Example Scenario MNO-2: Network topology presented from Provider-FH

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 presented to MNO-2 (see Figure 5) includes:

- List of UNIs:
  - 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 Links:
  - 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 internal Functions:
  - Five connectivity functions with capability to switch/multiplex Point-to-Point EVCs.

A link in the topology with direct connectivity between two UNIs is shown like 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 UNIs associated with the four NEs: 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 NEs, the Connectivity Function and the NE at the co-location site. Figure 6 shows the topology 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 office tower 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.

Since MNO-2 does not have the ability to manage and control Provider-FH resources associated with its Network Service, Provider-FH checks any management and control actions by MNO-2 on the presented network and makes any required changes to the Provider-FH resources associated with MNO-2's Network Service within the bounds of the Service Agreement.

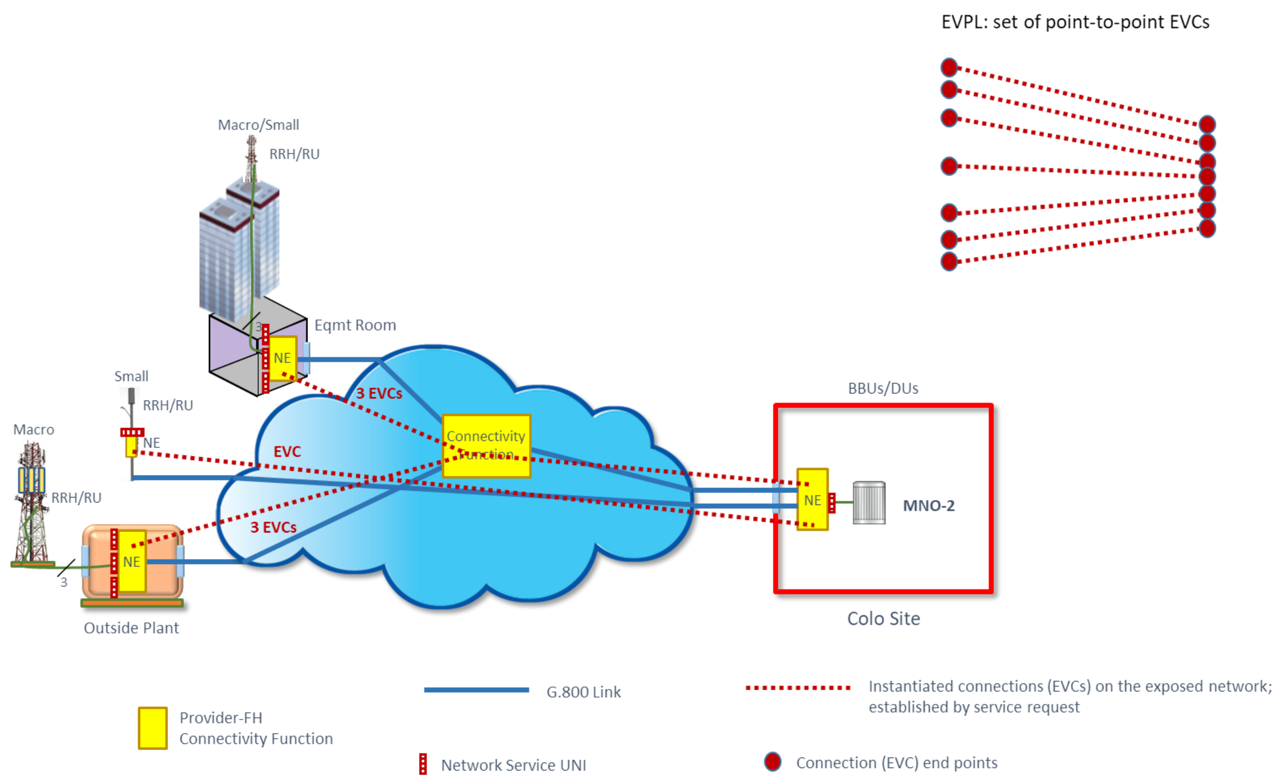


Figure 6: Example Scenario MNO-2: EVCs in EVPL Service instantiated on the presented network

A.1.2.3 MNO-3: Network Service and Ability to Slice the Presented Network

In order to obtain a network connecting its fronthaul network elements, MNO-3 uses a Network Service from Provider-FH.

Provider-FH uses NwSlice-3 to realize the infrastructure for MNO-3. The network topology exposed has UNIs that correspond to MNO-3's Fronthaul NE ports and MNO-3's 5G DU port. Each link in the presented topology 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 presented network
    - Configure the presented network
    - Instantiate Ethernet Connectivity Services and Cloud Services on the presented network

A.1.3 Options for MNO 5G Network Slices

The MNOs in this use case have different options to use Provider-FH Services for the fronthaul parts of their 5G Network Slices, including:

- Obtaining a Connectivity Service 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 2.
- Obtaining a Network Service per 5G Network Slice type and using Connectivity Services on the presented network for 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 2 – 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: it provides dedicated networks to its Subscribers that, in this example, are an online gaming company, a car manufacturer and a rich-video streaming provider. The Service Provider internally realizes the dedicated networks with instantiating Network Slices and presenting to each Subscriber a network with the corresponding topology and management capabilities as defined by their respective Service Agreements. Each Subscriber uses its dedicated network for end users having a subscription with them. 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 dedicated network (i.e. the network presented from a Network Slice to that Subscriber), are mapped by the Service Provider to the internal Network Slice for that Subscriber. Note that the Subscriber can manage and operate its presented dedicated network only within the bounds defined in the Service Agreement.

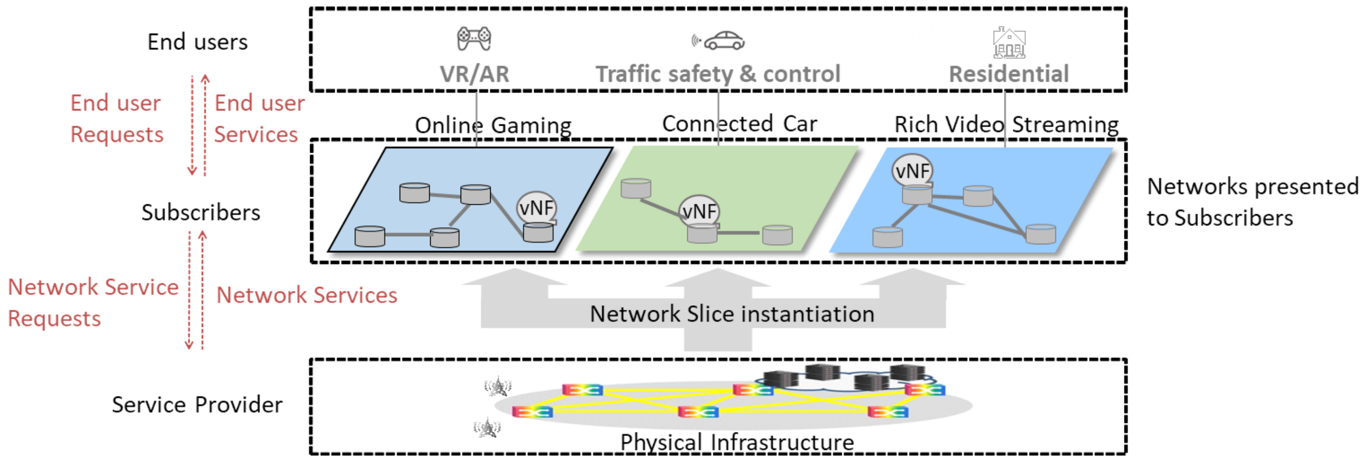


Figure 7: Network Slice B2B2X service model

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 without interest in insights to or knowledge of network technology, infrastructure and operations. The Service Provider's network catalog lists different options for fully pre-defined networks that the Subscriber can choose from. The Network Service to be ordered (and thus the network to be presented to the Subscriber) will be configured based on the chosen network catalog entry.

A fully pre-defined Network Service catalog entry is linked to a Network Slice description and pre-defined parameters to be applied during Network Slice instantiation. Pre-defined parameters include parameters covering QoS, security, failure safety and possibly other functions. Two examples are illustrated in Figure 8.

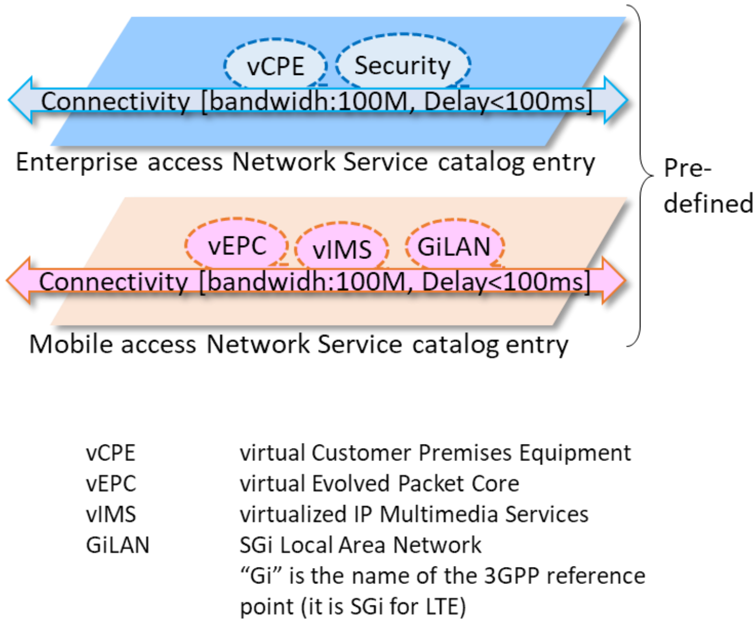


Figure 8: Example of catalog list options for fully pre-defined networks

An example of a network presented to the Subscriber under the fully pre-defined network provisioning model is provided in Figure 9. Subscribers may initiate connectivity between specific groups of UNIs and each connection has pre-defined parameters and functions.

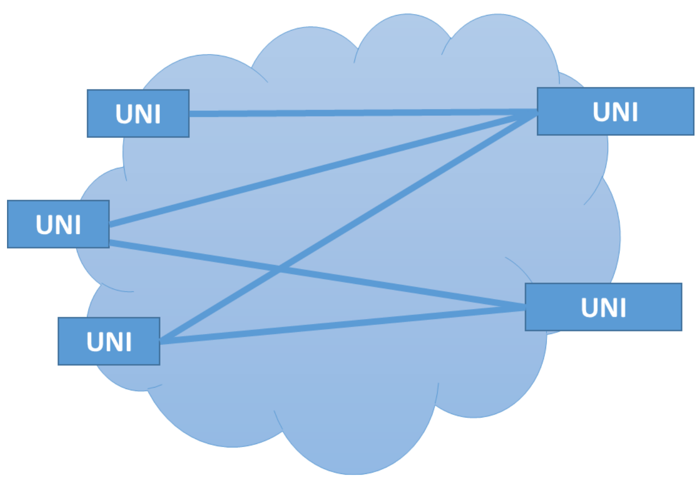


Figure 9: Example of a network presented to a Subscriber under the fully pre-defined network provisioning model

A.2.2.2 Semi-customized Network Provisioning Model

The semi-customized network provisioning model is offered to Subscribers who want to choose from and combine network components in their Network Service Order. The Service Provider’s 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 and has some pre-defined parameters to be applied during Network Slice instantiation. The Subscriber may combine pre-defined Network Service catalog entries according to their requirements. In addition, the Subscriber may be offered additional functions (either their own or Catalog-listed) for some pre-defined networks. An example is illustrated in Figure 10.

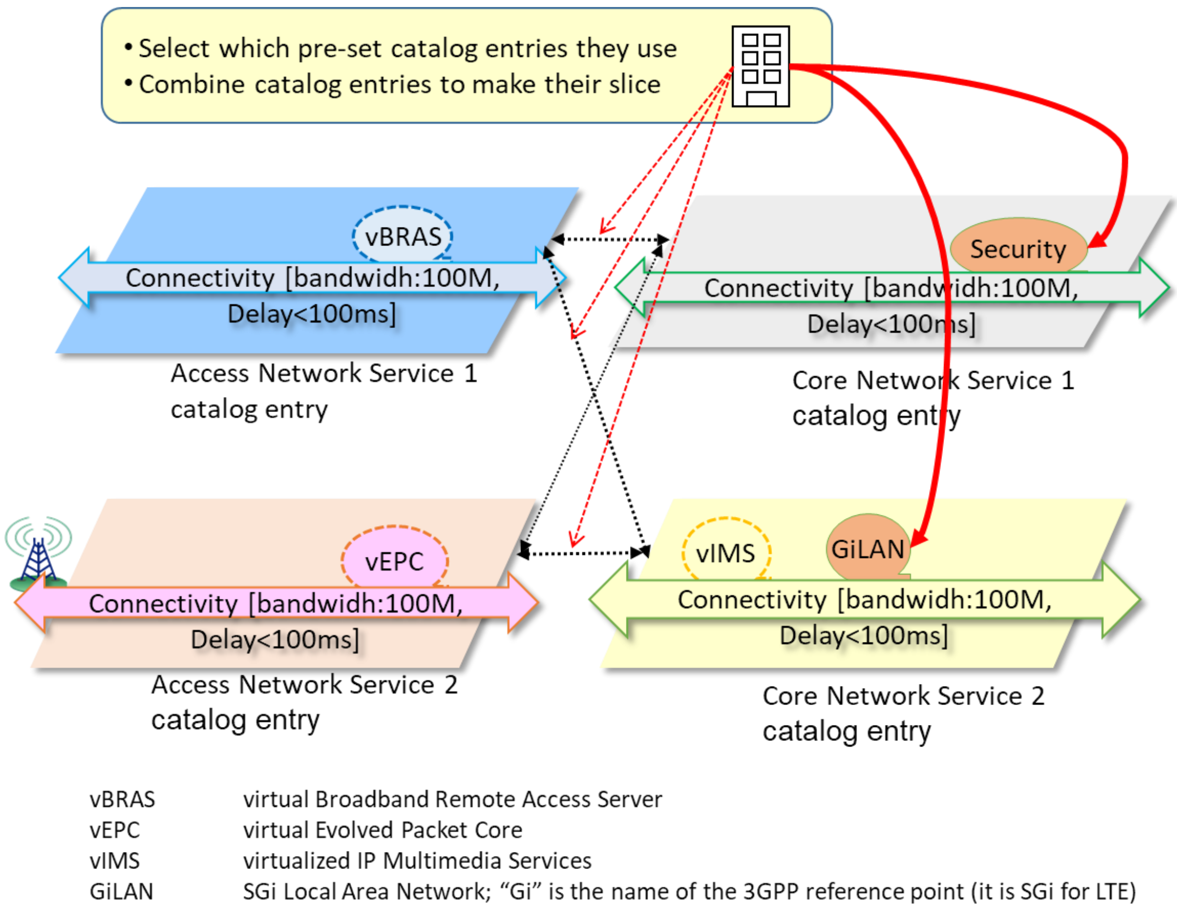


Figure 10: Example of a selection from catalog list options for semi-customized networks

The Service Provider internally instantiates a Network Slice dedicated to the Subscriber’s Network Service.

Examples of networks presented to the Subscriber from a semi-customized Network Service are provided in Figure 11, Figure 12 and Figure 13.

For its semi-customized Network Services the Service Provider also offers to the Subscriber a tool to control and operate the presented network, and, if covered by the Service Agreement (Order), the possibility to install own functions.

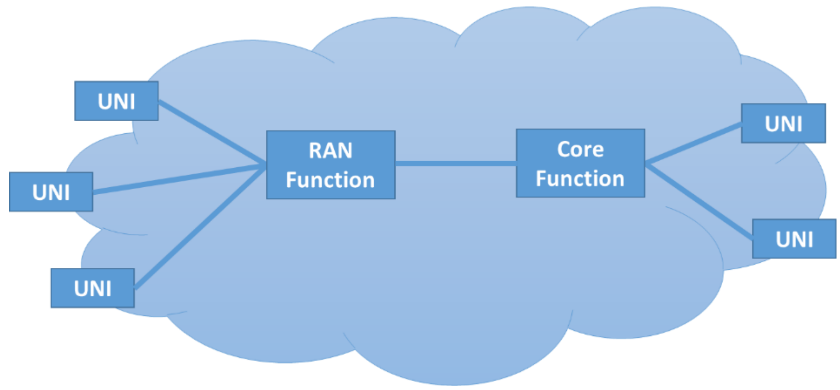


Figure 11: Example 1 of a network presented to a Subscriber under the semi-customized network provisioning model

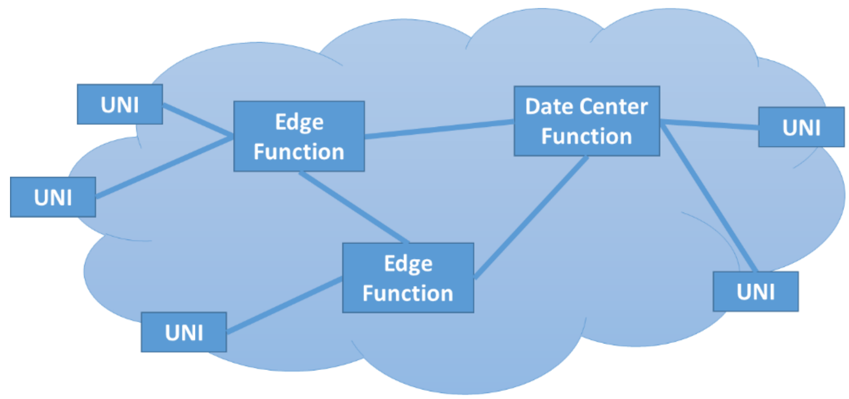


Figure 12: Example 2 of a network presented to a Subscriber under the semi-customized network provisioning model

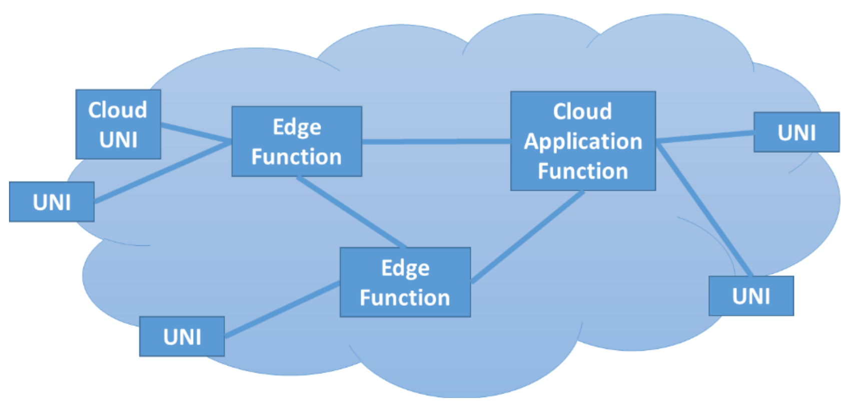
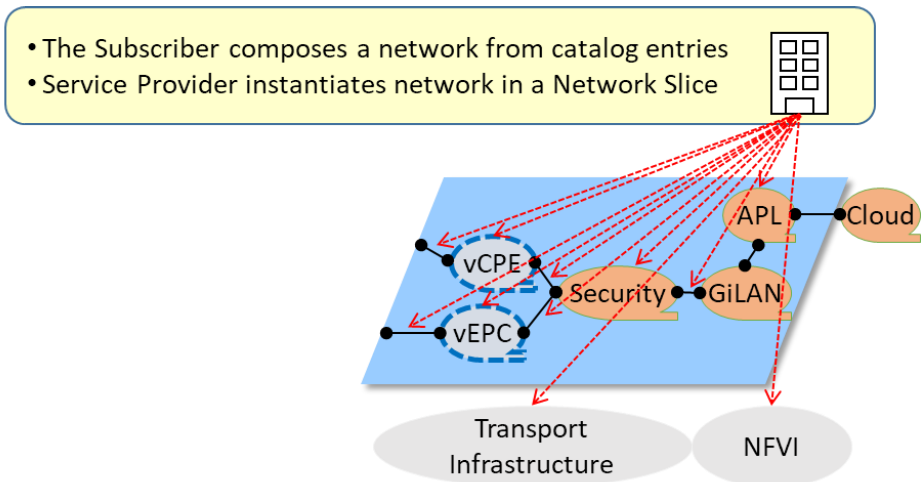


Figure 13: Example 3 of a network presented to a Subscriber under the semi-customized network provisioning model

A.2.3 Fully-customized Network Provisioning Model

The fully-customized network provisioning model is offered to Subscribers that want to design their own Network Slices. This means a Subscriber can configure the presented network's topology, connectivity layers, redundancy, virtual link connections, capacity, routing, QoS policy etc. In addition to selecting functions from the Service Provider Catalog, the Subscriber can deploy own virtual network functions (VNFs) as components of the Network Slice, on the Service Provider's network function virtualization (NFV) infrastructure. The Subscriber can also manage the presented network performance, fault status and compute resources for VNFs. 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 of a selection from catalog list options for fully-customized networks

A.2.4 Control and Management Interface Requirements

Table 3 summarizes configuration requirements for network provisioning models as provided in sections A.2.1, A.2.2 and A.2.3.

Table 4 summarizes management requirements for network provisioning models as provided in sections A.2.1, A.2.2 and A.2.3.

Major feature	Detailed feature		
	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 Slice • L2 connectivity to Network Slice for delivering services on Network Slice • IP address delivery for end-users • Multicast • Link aggregation	• IP reachability of Network Slice and the Resources in the presented network • L2 connectivity to Network Slice or the Resource in the presented network • 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 Slice • Path creation and deletion for services on Network Slice	• 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
Authentication	• Authentication of feature or application programming interface (API) access for Network Slice Subscribers (Application service providers) • Authentication of feature or service delivery on Network Slice for end-users	• Authentication of feature or API access for Network Slice Subscribers	• Authentication of feature or API access for Network Slice 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 3 – Configuration requirements for the different network provisioning models

Major feature	Detailed feature		
	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 Slice	• 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 Information acquisition	• Information acquisition of VNF/VL used in service on a Network Slice	• Network Slice or Resource in the presented network 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 presented network health check and fault isolation	• Health check and fault detection/isolation of underlay equipment (physical and virtual resource)
Resource management	• Virtual resource and physical resource management • Mapping resource and virtual resource	• Virtual resource and physical resource management • Mapping resource and virtual resource	• -
Performance monitoring	• UNI-to-UNI performance monitoring	• Performance monitoring per Network Slice or Resources in the presented network	• 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 presented network etc.)	• Charging information collection (physical or virtual resource usage ratio etc.)
End users access management	• End users access management	• End users access management	• End users access management

Table 4 – Management requirements for the different network provisioning models

A.3 Enterprise Use Case Example

Enterprise in the banking business obtains 2 Network Services from a Service Provider.

The network presented to the enterprise from one Network Service will be used for financial transactions.

The network presented to the enterprise from the other Network Service will be used for all other enterprise internal communications. This network will be 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 networks exposed by the Network Services is dedicated to a specific type of service.

A.5 IP Network Use Case Example

Editor Note 2. Content in this section is still subject for discussion and will be updated if needed

Business or enterprises need services of network operators to connect multiples sites.

In this example IP-Provider owns and operates an IP aware network that has edge network elements (i.e. routers) located at the border of the IP-Provider’s network and potentially at customer premise locations. It is also possible that customers provide their own edge network elements at their location, or that IP-Provider and customer edge network elements are located at a co-location facility.

IP-Provider applied Network Slicing on its IP aware 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 or bandwidth):

- Provider Slice 1: network suiting IoT type traffic
- Provider Slice 2: ….
- Provider Slice 3: ….

IP-Provider makes the existence of these Network Slices and their respective network characteristics visible/known to Customers via its Product Catalog

IP-Customer is a Business with multiple sites as shown in Figure 15. In this example IP-Customer needs IP data transfer between the four sites and purchases the following two IP connectivity services:

- IP Service 1 for internal, secure traffic, connecting Cloud Edge 2 with Site Edge 3 through Provider Slice 2, illustrated with the green dotted line in Figure 15
- IP Service 2 for general business or customer traffic, connecting Data Center Edge 1 with Site Edge 3 and Site Edge 4 through Provider Slice 3, illustrated with the red dotted line in Figure 15

Figure 16 illustrates IP-Customer’s perspective on the scenario. IP-Customer has no insight to the network of IP-Provider. The IP-Provider Network Slices appear as different IP networks.

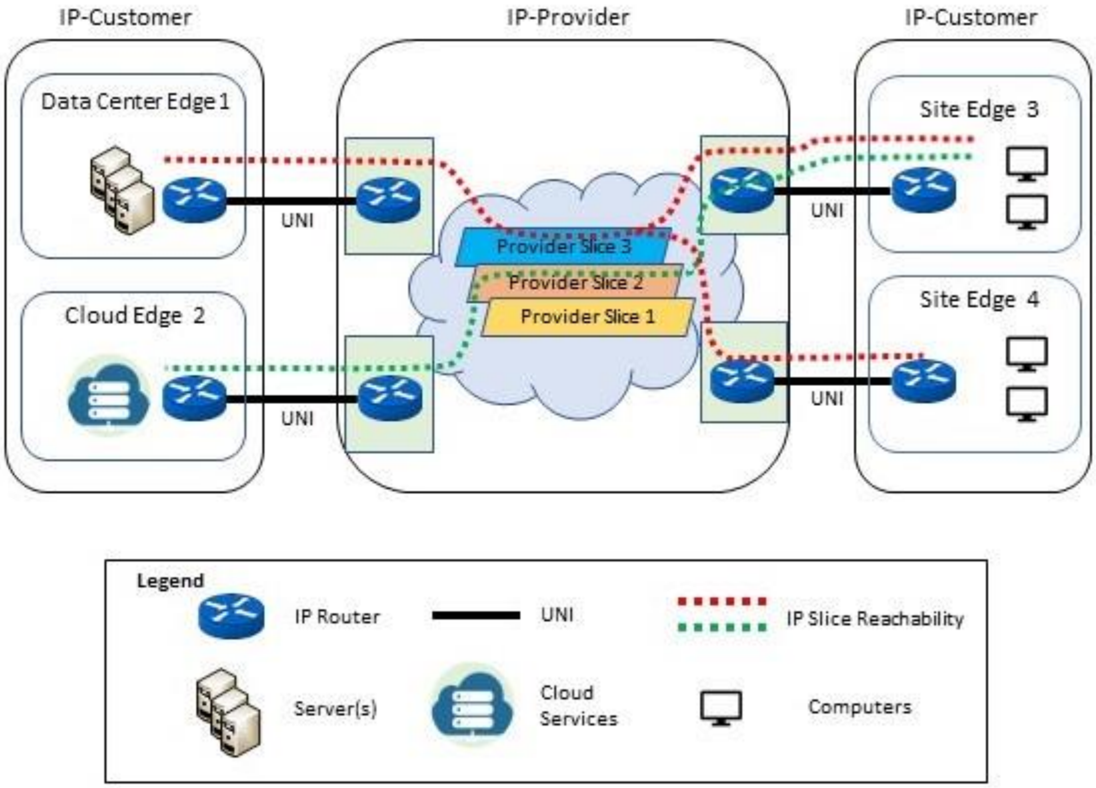


Figure 15: IP network use case example

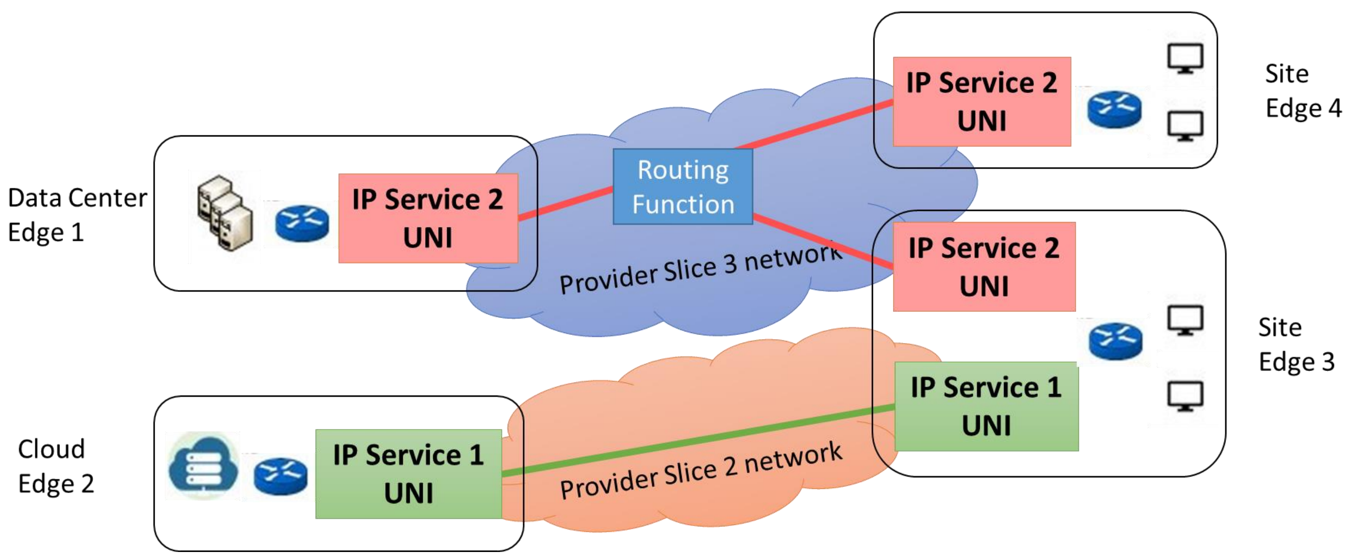


Figure 16: IP-Customer IP Services on networks presented by IP-Provider

The topology presented to IP-Customer (see Figure 16) includes:

- For IP Service 1
  - IP Service UNIs at Cloud Edge 2 and Site Edge 3
  - Link connecting the two IP Service UNIs
- For IP Service 2
  - IP Service UNIs at Data Center Edge 1, Site Edge 3 and Site Edge 4
  - Routing Function
  - Links connecting the three IP Service UNIs with the Routing Function

The two service agreements include for IP-Customer the following orchestration, control and management capabilities on the presented networks:

- For IP Service 1
  - Increase and decrease the bandwidth available to the Service UNIs and the link.
- For IP Service 2
  - Increase and decrease the bandwidth available to the Service UNIs and the corresponding links connecting them to the Routing Function
  - Question: does IP-Customer have some routing configuration control capability for the Routing Function?
  - Question: does IP-Customer have the capability to add/remove additional sites, i.e. Service UNIs and corresponding links? If not, the service agreement needs to be updated/changed to add/remove sites.

IP-Customer will order additional IP Services if needed to map specific additional or separate applications to specific networks (i.e. IP-Provider Network Slices).

A.6 SD-WAN Use Case Example

Editor Note 3. Content in this section is still subject for discussion and will be updated if needed

Enterprises are adopting SD WAN to help simplify Enterprise networking. SD WAN uses an Orchestrator to enable centralized configuration/visibility and Edges that implement Application Flow steering policies on an SD WAN Overlay configured via the Orchestrator.

A.6.1 Description

SD WAN can use one or more Network Slices as the Enterprise WAN and facilitate mapping of Application Flows to the appropriate network slice. SD WAN can also be deployed at both the Enterprise DataCenter and Cloud to provide SD WAN connectivity between devices and users at the Enterprise branches to Enterprise Applications/Services located at the DataCenter or the Cloud.

A.6.2 Topology Example

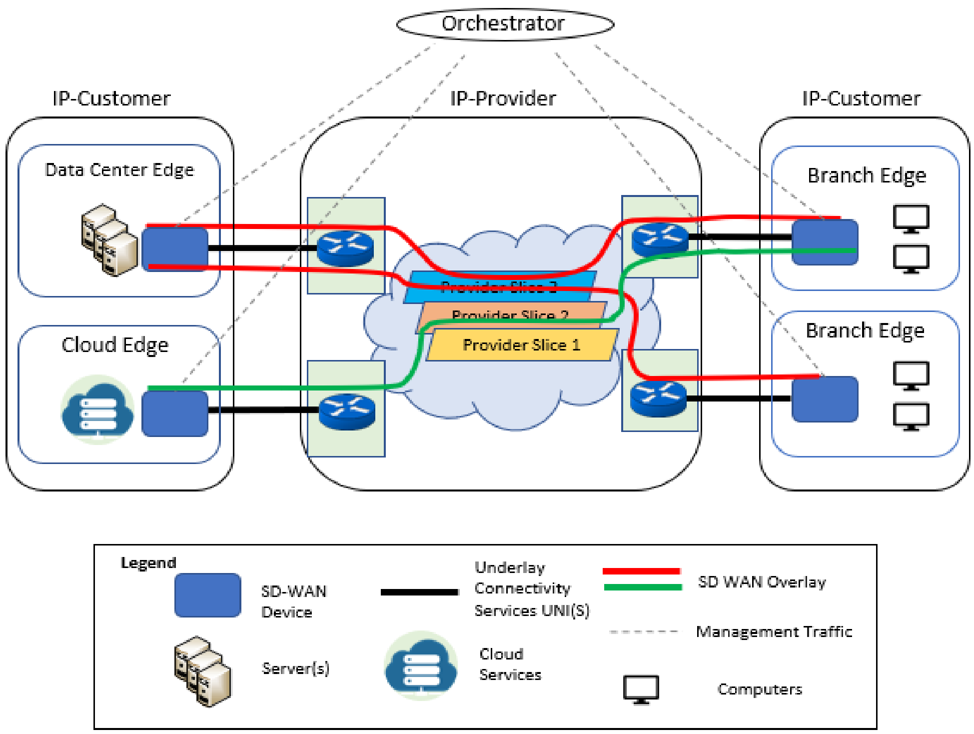


Figure 17: Topology Example for SD-WAN use case

A.6.3 Allowed Services Example

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

Network Slicing has received special attention since the NGMN 5G Vision White Paper [8] was published in 2015. Many groups and organizations took up work on the topic, with 3GPP being a prominent one.

With the discussion of “5G Network Slicing” originating in the mobile network operator domain, much of the work and discussion 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 (slices) are used to provide services. These subsets (slices) are isolated from each other on their level, although the resources in the underlying infrastructure may have been assigned with dedicated or shared characteristics.

Any interaction (e.g., business, orchestration, control or management interaction) between a Service Provider and a Partner, of any network technology, is via APIs at the Sonata and Interlude LSO Management Interface Reference Points.

Any interaction (e.g., business, orchestration, control or management interaction) between a Service Provider and a Subscriber, of any network technology, is via APIs at the Cantata and Allegro LSO Management Interface Reference Points.

B.1 ITU-T

ITU-T defines in Recommendation Y.3100 [5] the term Network Slice as ”A logical network that provides specific network capabilities and network characteristics”. 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. Virtualization is defined in ITU-T Recommendation G.7702 [4] as “an abstraction and subset whose selection criterion is dedication of resources to a particular client or application“. A virtual network is a virtualisation of ITU-T G.800 [14] 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-TN5G [12], 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 [6].

B.2 ONF SDN Architecture

Although the SDN Architecture specification in ONF TR-521 [6] does not use the term slice or network slice, ONF TR-526 [7] 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

B.3 3GPP 5G

3GPP in [9] 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.

A 3GPP 5G Network Slice Instance composed on a Public Land Mobile Network (PLMN) shall include:

- the Core Network Control Plane and User Plane Network Functions

and, in the serving PLMN, at least one of the following:

- the NG Radio Access Network
- the N3IWF functions to the non-3GPP Access Network.

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.

Note – A "Network Slice" defined by 3GPP TS 23.501 can be mapped to a Service (itself instantiable in a Network Slice as defined by this Standard) as described and illustrated in Appendix F of MEF 22.3.1 for an EVC-based Ethernet Service.

B.4 ETSI ISG NFV

The relationship between Network Slicing and the NFV constructs was studied in [10]. Annex D.3 of [11] describes how NFV will support Network Slicing via NFV "Network Services".

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.

B.5 GSMA

In October 2019 the GSMA published their version 2.0 of the Generic Network Slice Template [13], providing a standardized list of attributes that can characterize a type of network slice.

The purpose of this Standard is to provide the standardised list of attributes that can characterise a type of network slice.

The attributes listed in this Standard are based on the open and published 3GPP specifications as listed in the Section 1.6. 3GPP Release 15. This first release supporting 5G and network slicing, is taken as basis.

Roles (specified in 3GPP TS 28.530):

- 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.

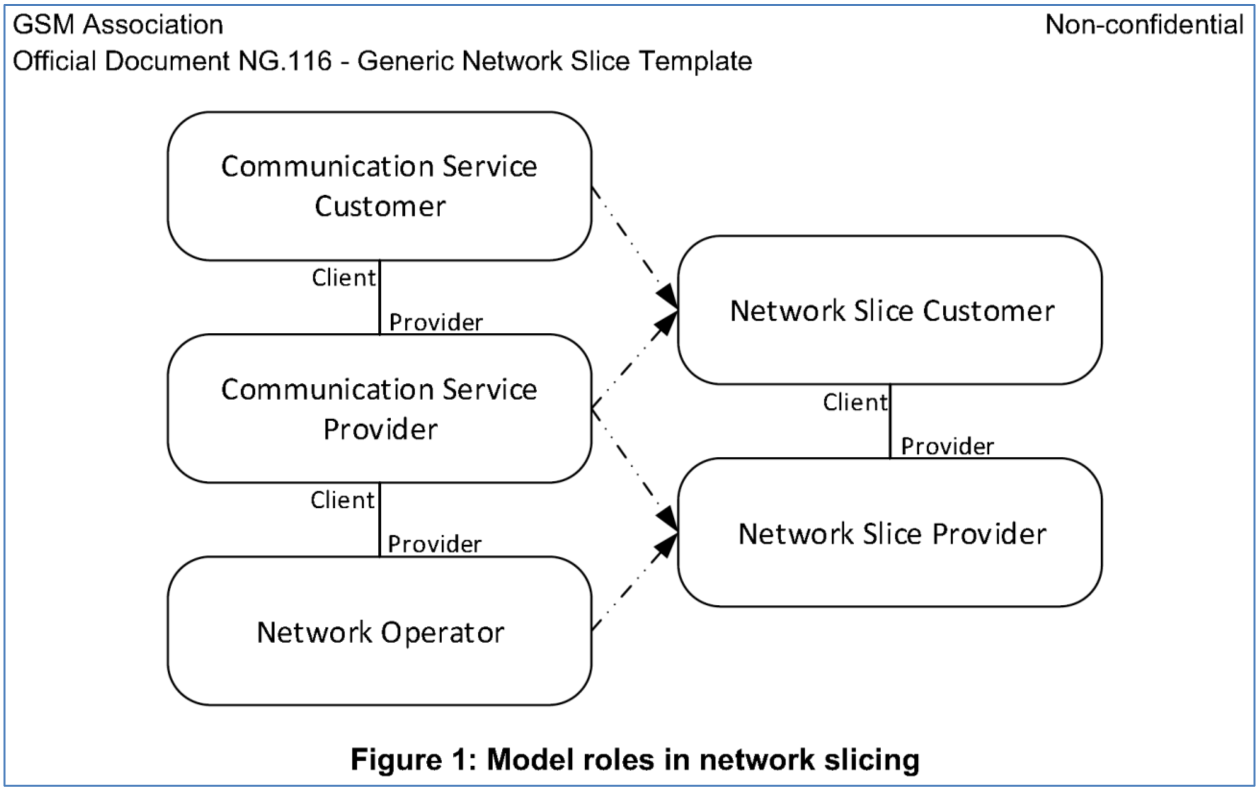


Figure 18: GSMA model roles in network slicing

Mapping to MEF:

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

B.6 IETF

Editor Note 4. Content in this section is still subject for discussion and will be updated if needed

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) or Segment Routing (RFC8402) can provide paths whose intermediate route is decided. Also, deterministic networking (RFC8665) enables to carry 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, to abstract network resources on a single or multiple domains and provide TE paths or virtual private networks to customers (RFC8453).

Some of these techniques are expected to be used for network slicing use cases. For meeting advanced requirements for networks, a framework to provide more enhanced VPN services by combing several IETF techniques/protocols (I-D.ietf-teas-enhanced-vpn-05). However, those were not dedicatedly de-signed for network slicing, and there are no unified definitions of network slicing and its characteristics. For example, definitions of network slicing described in RFC8453 and RFC8656 are bit different.

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

B.7 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 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 [3]. 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.

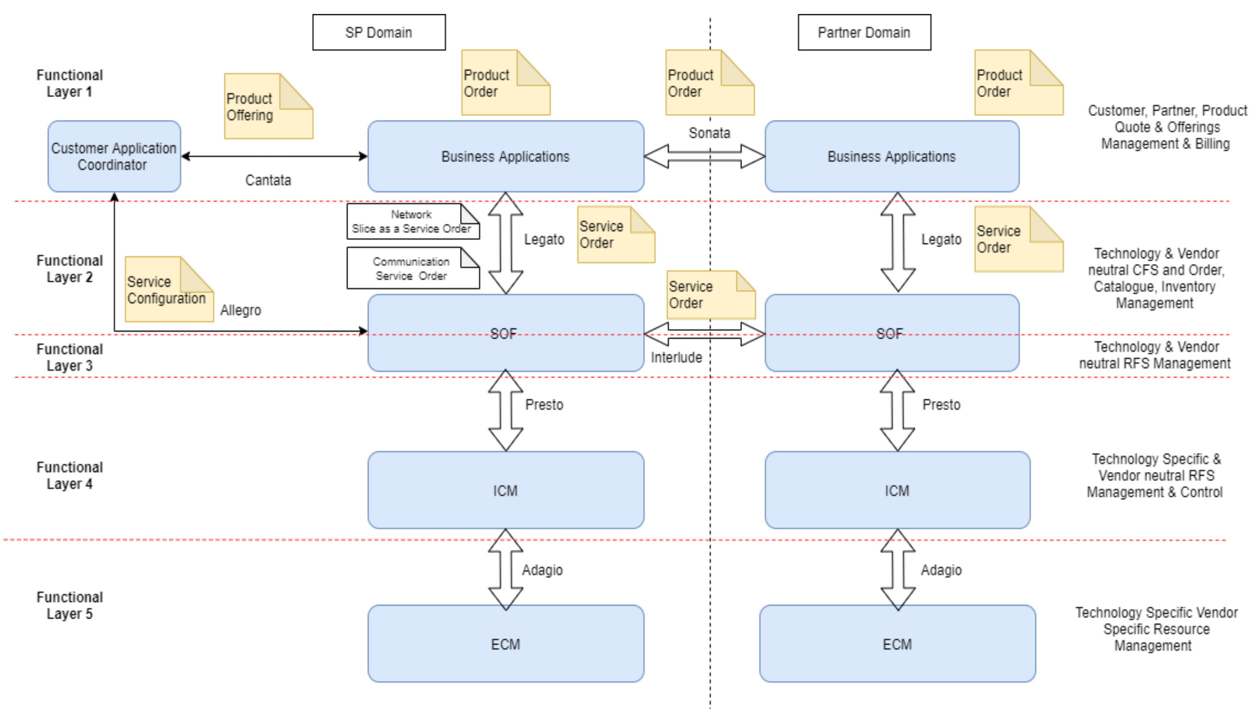


Figure 19: Combination of LSO Abstraction Layers and TM Forum Functional Layers

Referring to MEF 55, 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 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 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. 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 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 in the initial part of 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 5. Note that Functional Layer 5 is omitted as there is 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. ONAP, OSM etc.)**
Functional Layer 1	Business Applications	TM Forum ODA Core Commerce Management	TM Forum BOS
Functional Layer 2	SOF (CFS handling)	MEF SOF, TM Forum ODA Production, ZSM E2E Service Management, 3GPP CSMF	ONAP Ext-API, ONAP SO
Functional Layer 3	SOF (RFS handling)	MEF SOF, ODA Production, ZSM E2E Service Management, IETF draft-rokui-5G-transport-slice E2E Network Slice Controller, 3GPP NSMF, 3GPP NSSMF (Optional)	ONAP SO, OSM SO
Functional Layer 4	ICM	IETF draft-rokui-5G-transport-slice Specific Controllers, MEF ICM, ODA Production, IETF ACTN MDSC, 3GPP NSSMF (Optional), ETSI NFV MANO, ZSM Management Domain, ONF TAPI VNS Controllers	ONAP SO, ONAP VFC, ONAP SDNC, OSM SO/RO

Table 5 – Functional Layers Mapped to Different SDO Defined Functional Blocks

The diagram in Figure 20 represents Table 5with a business scenario where 3GPP 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.

3GPP management functions CSMF, NSMF and NSSMF ((acronyms expanded in 3GPP TR 28.801 [17]) are logically mapped to SOF in MEF LSO. These management functions are mapped to the operations support systems (OSS) in ETSI GR NFV EVE 012 [10]. For mobile network slicing there may be many partner domains coordinating with a Service Provider i.e. ~~network slice providers,~~ 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, hence it is well aligned to support practical requirements for interworking between Service Provider and Partner domains.

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 functional white blocks in the Partner ICM could also be in the Service Provider ICM, but are not shown for clarity. Similarly, the functional white blocks in the Service Provider ICM could also be in the Partner ICM.

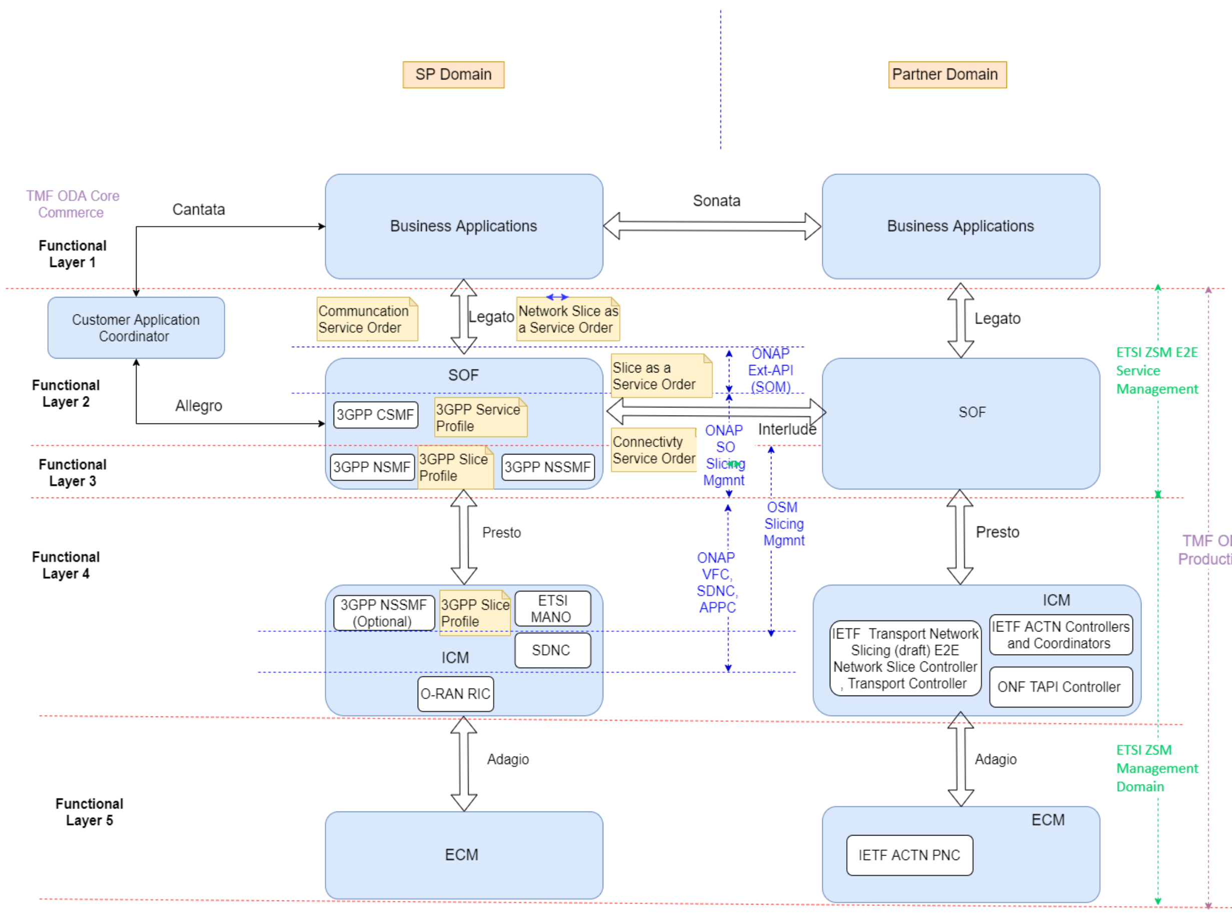


Figure 20: Example for functional mapping of management functions across different SDOs to MEF LSO to support Network Slicing

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 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 document and covered in 3GPP specifications. This document does not elaborate on the MANO and SDNC mapping as these are well defined in section 9.1.1 of MEF 55 [3].

In the business scenario depicted in Figure 20, 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 [16], or, in the context of IETF ACTN specification, draft-king-teas-applicability-actn-slicing-04 [15]. 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 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 stage of supporting network slicing or have reference proof of concepts available for further development.

In ONAP Frankfurt Release 6 support for slicing the 5G core is under development. This is realized by developing CSMF, NSMF as part of the SO component and NSSMF is expected to be implemented externally to ONAP. This is aligned with the harmonization view depicted above, with an exception that the NSSMF SOF in the SOF is not available and instead it is realized as an external function. In this case NSSMF alignment in the ICM is more suitable as this is realized through a separate technology specific (5G core) domain controller. Similar model is expected for the RAN controller as well in future.

In OSM there are some early work items on modelling network slices as network slice templates and mapping those to network service descriptions and VNF descriptions is documented. The current documentation mainly focusses on the network slice and slice subnet management functionality and does not depict clearly the Subscriber facing communication, connectivity or slice as a service mappings.

Appendix C Release Notes

This section contains information on comments not yet resolved.

Section	Comment	Comment resolution status
3	Change the "Network Service" definition from "…a Subscriber" to "… one or more Subscribers	The change has been applied, but will be checked again
3	On the definition of the term "Network Slice": independently of other subsets → independently is not true for all other subsets	Need to add text in later sections about the recursion
8, B	Several versions of referenced documents are outdated, citations	The references should be updated
7.1, 7.2.3, A.1.1	On the use of the LSO Allegro interface: Should add orchestration related management interactions which are required to request instantiation of a Service on and manage the presented network of a Network Service	This is related to the Network Service management capabilities that the Service Provider grants a Subscriber Network Service management attributes discussion has not yet concluded and attributes listed in this document are still subject to change
Global	There are comments about wording, use of terms	These need to be discussed/resolved