broadband forum

Technical Report

TR-522

Mobile-transport network slice instance Management Interfaces

Issue: 1

Issue Date: June 2022

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is owned and copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be owned and/or copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER'S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE Technical Report IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE Technical Report, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

All copies of this Technical Report (or any portion hereof) must include the notices, legends, and other provisions set forth on this page.

Issue History

Issue Number	Issue Date	Issue Editors	Changes
1	24 June 2022	Xueyan Song, ZTE Reza Rokui, Nokia	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editors: Reza Rokui, Nokia

                Xueyan Song, ZTE

Work Area Director: David Sinicrope, Ericsson

Project Stream Leader: David Sinicrope, Ericsson

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This document specifies the Mobile-transport network slice instance Management Interface (MMI) between a 3GPP network slice management system and transport network slice controller in support of 5G network slices. The transport network slice controller, through MMI interfaces, receives the requests for network slice creation, modification or deletion of network slices with specific requirements and maps the requests to appropriate network resources and provides network slice services using specific technologies.

This document defines service and functional requirements on MMI interfaces for the provision of network slices, operational attributes for network slice enablement, and data models for MMI interfaces.

1 Purpose and Scope

1.1 Purpose

5G network slicing (specified in 3GPP TS 28.530 [18]) facilitates multiple logical self-contained networks on the top of a common physical infrastructure platform enabling a flexible stakeholder ecosystem that allows technical and business innovation. In realizing a 5G network slice the 3GPP management System needs to be aligned with the corresponding transport network management in order to ensure that the desired performance, functionality, and connectivity is fulfilled.

BBF TR-221 [1] has specified multiple solutions for mobile backhaul transport networks: L2VPN, L3VPN, and IP over LSP; other candidate packet switching solutions may further include E-VPN, TSN, DetNet, Segment Routing, and etc.

This document intends to fill the gap that exists in the 3GPP specifications on the missing interfaces between 3GPP Management System and the Transport Network (TN) Manager; that is, some interfaces are specified between the 3GPP Management System and the Transport Network (TN) Manager to provide:

    (i) Transport network capability exposure information towards the mobile network and

    (ii) Resource mapping and life-cycle management of network slices, as identified by 3GPP SA5 (in 3GPP TS 28.531 [19]), to the underlying transport network.

This new suite of interfaces (may consist of one or more interfaces) are denoted overall as Mobile – transport network slice instance Management Interfaces (MMI). The focus of this document is on how to support 5G network slices in the BBF broadband networks as specified in TR-221 [1].

The document has the following objectives:

- Identify the service requirements related to the MMI interfaces for various slice types, for example 3GPP Standard Slice Type (STT) defined in TS 23.501 [16].

- Analyze operations that the MMI interfaces need to support for fulfilling the 3GPP life-cycle management of network slices

  Study existing work on network slice management and related service interfaces of other industry bodies such as ITU-T, IETF, MEF, etc.

- Specify the interfaces and data models to support 5G network slices in the BBF broadband networks; the data models will refer to existing models in other SDOs (such as IETF and MEF) whenever possible.

1.2 Scope

This document defines the requirements, functions, and interfaces in support of 5G network slices in the BBF broadband network. It includes:

- Specify functional and service requirements
- Specify requirements to be supported by MMI interfaces
- Specify the parameters that the MMI interfaces need to support as are related to the 3GPP life-cycle management of network slices

- Specify an abstract transport network capability exposure for enabling transport network slice that can be mapped to existing packet switching technologies (e.g., L2VPN, L3VPN, E-VPN, VLAN, and etc.)
- Specify interfaces to support the configuration, assurance/monitoring and reconfiguration of 5G network slices in the BBF broadband networks.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [2]

MUST	This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term "RECOMMENDED", means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document		Title	Source	Year
[1]	TR-221	Technical Specifications for MPLS in Mobile Backhaul Networks	BBF	2011
[2]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[3]	RFC 3393	IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)	IETF	2002
[4]	RFC 5481	Packet Delay Variation Applicability Statement	IETF	2009
[5]	RFC 6241	Network Configuration Protocol (NETCONF)	IETF	2011
[6]	RFC 7950	The YANG 1.1 Data Modeling Language	IETF	2016

[7]	RFC 7951	JSON Encoding of Data Modeled with YANG	IETF	2016
[8]	RFC 8040	RESTCONF Protocol	IETF	2017
[9]	RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3	IETF	2018
[10]	RFC 9020	YANG Data Model for Segment Routing	IETF	2021
[11]	RFC 9182	A YANG Network Data Model for Layer 3 VPNs	IETF	2022
[12]	draft-ietf-teas-ietf-network-slices-10	Framework for IETF Network Slices	IETF	2022
[13]	draft-ietf-teas-yang-path-computation-18	YANG Data Model for requesting Path Computation	IETF	2022
[14]	draft-ietf-spring-sr-policy-yang-01	YANG Data Model for Segment Routing Policy	IETF	2021
[15]	draft-ietf-opsawg-l2nm-15	A YANG Network Data Model for Layer 2 VPNs	IETF	2022
[16]	TS 23.501	System architecture for the 5G System (5GS)	3GPP	2020
[17]	TS 23.502	Procedures for the 5G System (5GS)	3GPP	For R16
[18]	TS 28.530	Management and orchestration; Concepts, use cases and requirements	3GPP	For R16
[19]	TS 28.531	Management and orchestration; Provisioning	3GPP	For R16
[20]	TS 28.532	Management and orchestration; Generic management services	3GPP	For R16
[21]	TS 28.533	Management and orchestration; Architecture framework	3GPP	For R16
[22]	TS 28.540	Management and orchestration; 5G Network Resource Model (NRM); Stage 1	3GPP	For R16
[23]	TS 28.541	Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3	3GPP	For R16
[24]	TS 33.501	Security architecture and procedures for 5G System	3GPP	For R16

2.3 Definitions

The following terminology is used throughout this Technical Report.

Network Slicing	A technology that creates multiple logical networks on demand, providing differentiate or dedicated services to customers with a shared or dedicated network resource.
Network Slice	See definition from 3GPP TS 28.530 [18].
Network Slice Instance (NSI)	See definition from 3GPP TS 28.530 [18].
Network Slice Subnet Instance (NSSI)	See definition from 3GPP TS 28.530 [18].

5G Network Slice	A logical network with specific SLA requirements from customers. From the 3GPP specifications, a 5G Network Slice may cross multi-domains and consists of RAN, TN, CN Slice subnets. This document uses IETF Network Slice for TN Slice Subnet.
RAN slice subnet	See definition from 3GPP TS 28.530 [18].
CN slice subnet	See definition from 3GPP TS 28.530 [18].
IETF Network Slice	See definition from IETF draft-ietf-teas-ietf-network-slices [12].
Mobile-transport network slice instance Management Interface (MMI)	A set of interfaces that provide communication between 3GPP network slice management system and IETF Network Slice Controller responsible for automation and service management of IETF network slices.
IETF Network Slice Controller (NSC)	See definition from IETF draft-ietf-teas-ietf-network-slices [12].
Service Demarcation Point (SDP)	See definition from IETF draft-ietf-teas-ietf-network-slices [12].
Service Level Expectation (SLE)	See definition from IETF draft-ietf-teas-ietf-network-slices [12].
Service Level Objective (SLO)	See definition from IETF draft-ietf-teas-ietf-network-slices [12].

2.4 Abbreviations

This Technical Report uses the following abbreviations:

5QI	5G QoS Identifier
ACTN	Abstraction and Control of Traffic-engineering Networks
AMF	Access and mobility Management Function
BBU	Baseband unit
CCTV	closed-circuit television
CN	Core Network
C-RAN	Cloud RAN
CSG	Cell Site Gateway
DCI	Data Centre Interconnection
D-RAN	Distributed RAN
DSCP	Differentiated Services Code Point
DU	Distributed Unit
eCPRI	Enhanced Common Public Radio Interface
eMBB	Enhanced Mobile Broadband
EVPN	Ethernet Virtual Private Network
FlexE	Flexible Ethernet
MMI	Mobile-transport network slice Management Interface

NETCONF	Network Configuration Protocol
NSC	Network Slice Controller
NSI	Network Slice Instance
NSSI	Network Slice Subnet Instance
NSS	Network Slice Subnet
NSSAI	Network Slice Selection Assistance Information
PCP	Priority Code Point
QFI	QoS Flow Identifier
RAN	Radio Access Network
RSVP	Resource ReServation Protocol
RU	Radio Unit
SD	Slice Differentiator
SDP	Service Demarcation Point
SFC	Service Function Chaining
SLA	Service Level Agreement
SLE	Service Level Expectation
SLO	Service Level Objectives
SMF	Session Management Function
S-NSSAI	Single – Network Slice Selection Assistance Information
SST	Slice/Service Type
TLS	Transport Layer Security
TN	Transport Network
TR	Technical Report
TS	Technical Specification
UE	User Equipment
UPF	User Plane Function
VLAN	Virtual LAN
VN	Virtual Network
VPN	Virtual Private Network
WA	Work Area
WT	Working Text

3 Technical Report Impact

3.1 Energy Efficiency

This document has no impact on energy efficiency.

3.2 IPv6

This document specifies MMI interfaces to support 5G Network Slice in broadband network. The MMI for network slice realization is technology-agnostic, has no impact on IPv6.

3.3 Security

The 5G network slice management system performs differentiated data protection policies based on the specific network security and network capability requirements from service, customer, and network endpoints, etc. This section identifies a few of the security aspects for the MMI specification of this document:

- Security request: the network slice customer requests for the instantiation of transport network slice (refers to "IETF Network Slice") may carry specific security requirements along with SLO/SLE parameters and these requests will be sent to transport network slice controller (refers to "IETF Network Slice Controller (NSC)") through MMI interface. Different industries may require differentiated security service guarantee.

- Security authentication: IETF Network Slice customer needs to perform authentication implementation before communicating with the producer for the network slice operation; the detailed authenticated requirements is referred to in section 11.2 of this document.

- Data integrity protection: the data carried for instantiation of IETF network slice through MMI should implement data integrity protection, to ensure the data is authorized and has not been changed.

- Data confidentiality protection, when the network slice provider performs enablement or operation of network slice required by a customer, it protects the customer's data using encryption to prevent unnecessary access or change by other customers.

For detailed security considerations, see section 11.

3.4 Privacy

The SLO/SLE parameters and operations over the MMI may themselves reveal information about the end customers. Therefore, the MMI should provide privacy protection for this information.

Network Slice customers may have some privacy considerations when requesting during the implementation of network slice instance. In case of IETF network slice, the privacy constraint attributes (maybe including tenant identity information, some sensitive information, etc.) are carried with SLO/SLE parameters through MMI when instantiation of IETF network slice.

4 Architecture of 5G Network Slice

This section introduces the architecture of a Network Slice, based on 3GPP TS 28.530 [18]. It describes the role of various domains RAN, Core, and Transport, along with their associated controllers and how they relate to a 5G Network Slice.

4.1 5G Network Slicing

5G network slicing is a fundamental technology for concurrent delivery of differentiated 5G services. It will be a key for moving 5G use cases toward a service-driven evolution that supports meeting unprecedented SLAs deterministically across network resources of different domains.

The simplest definition of a network slice is an independent and logical self-contained network on top of common physical or virtual infrastructure network. It extends from the end devices to the application servers and includes all intermediate functions and domains. The concept of network slicing is applicable to various applications that can benefit from network slicing. Some of these applications are:

- 5G network slicing
- Wholesale business VPNs
- Network sharing among operators
- Data Center connectivity (DCI)

This section focuses on 5G applications as per 3GPP Release 15. A Network Slice may include virtual and physical network functions, cloud infrastructure, transport/connectivity, augmented services (e.g., network analytics and security services), as well as application functions. Network slices are orchestrated to form service-specific logical networks running on the same physical network that meet certain service level objective (SLO) attributes (such as data speed, capacity, latency, reliability, availability, coverage and security) and service level expectation (SLE) attributes (e.g., diversity, isolation, and geographical restrictions).
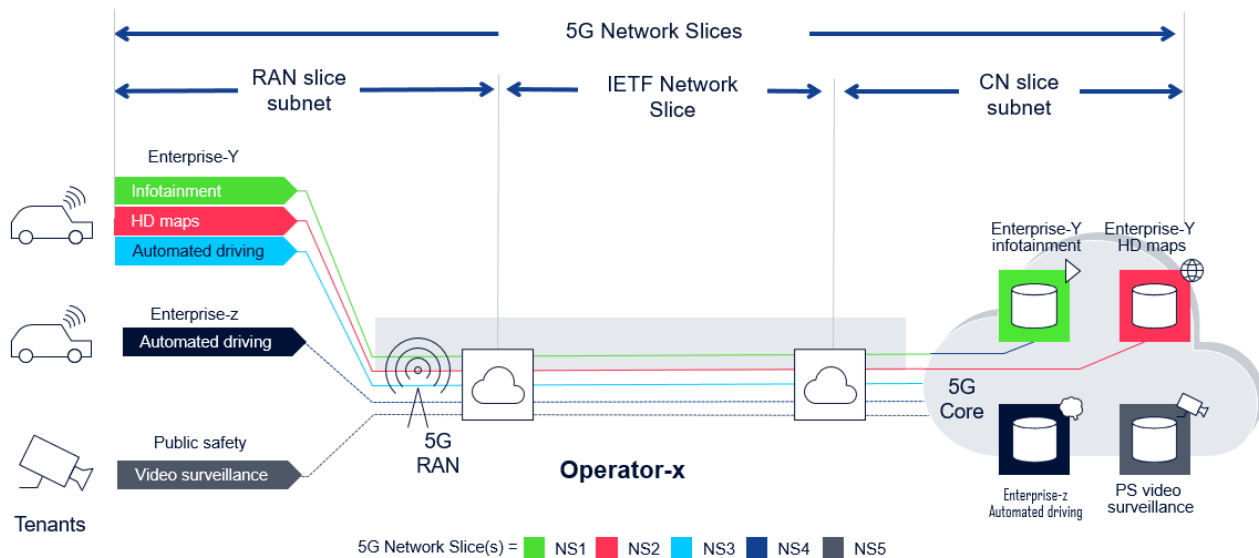

Figure 1 A typical 5G Network Slice from Operator-X perspective

To better demonstrate the concept of 5G network slicing, Figure 1 shows a typical network from a mobile network operator (MNO) Operator-X, which supports 5G network slicing. The operator has three customers (a.k.a. tenants): Public Safety, Enterprise-Y and Enterprise-Z. Each of these customers asks Operator-X to create one or more logical independent networks within its common or shared network infrastructure with specific Service Level Objectives and/or Expectations. Each of these logical networks is called a "5G network slice". In this network, Operator-X has created five network slices, NS1 to NS5, each with certain SLO/SLE marked as different colors (e.g., SLO/SLE red, green, etc.).

Network slicing is required since 5G services and devices have their own specific SLO/SLE requirements, many of which vary diversely depending on the application. As shown in the Figure 1, each 5G Network Slice consists of one RAN slice subnet, one CN slice subnet, and one or more IETF Network Slices.

> **Note:** The term "sub-slice" or "slice subnet" is also used by some standard organizations to refer to RAN, Core and IETF Network Slices (e.g., IETF Network sub-slice or IETF Network Slice-subnet). From BBF point of view, these terms are all equivalent. We will use the term "slice subnet" in this document to be aligned with IETF i.e., IETF Network Slice (see draft-ietf-teas-ietf-network-slices [12]). The RAN slice subnet is the logical context that is created for a specific 5G Network Slice on RAN network elements (e.g., eNB, gNB, DU, CU). In other words, the RAN slice subnet is the network slice context that is programmed on RAN network for a certain SLO/SLE. For instance, in Figure 1, the RAN network elements will have the contexts for all or a subset of the network slices NS1 to NS5. The actual RAN slice subnet configuration depends on RAN deployment such as distributed RAN, centralized RAN, or cloud RAN, but in general it involves the configuration of network slice ID (i.e., S-NSSAI), air interface, RAN scheduling, various policies, etc.

Similar to the RAN slice subnet, the CN slice subnet is the logical context created for a specific 5G Network Slice on CN network (e.g., AMF, SMF, and UPF). The concept of the CN slice subnet is very similar to RAN slice subnet but on CN network elements. In Figure 1, the CN network elements will have the contexts for all or a subset of the network slices NS1 to NS5. In practice, the CN slice subnet involves the configuration of CN network elements for network slice ID (S-NSSAI), various policies, etc.

Unlike RAN and CN slice subnets, the IETF Network Slices address the connectivity between various network functions, applications, etc. In Figure 1, the IETF Network Slice provides the connectivity needed within and between RAN and CN slice subnets. Such IETF Network Slices have deterministic SLO/SLEs in order to achieve the 5G Network Slice SLA. The concept of IETF Network Slices for various access RAN deployment will be covered in next section.

In the network shown in Figure 1, customer Enterprise-Y has three 5G Network Slices for services "Infotainment", "HD maps" and "Autonomous driving", each with its own SLO/SLE. Similarly, customers Enterprise-Z and Public Safety each have one 5G Network Slice (i.e., NS4 and NS5) for services "Autonomous driving" and "Video Surveillance", respectively. For instance, NS1 is created by Operator-X for customer Enterprise-Y for service "Infotainment" where the SLO/SLE is bandwidth (SLO/SLE green) whereas the NS3 is created for the same customer but for service "Autonomous driving" where the SLO/SLE is the combination of latency and reliability (SLO/SLE blue).

Referring to Figure 1, the following important facts should be considered:

- The 5G Network Slice is different from RAN slice subnet, IETF Network Slice(s) and CN slice subnet. To have a 5G Network Slice, a set of RAN and CN slice subnets, and IETF Network Slices will be constructed first and then are associated together to form a single 5G Network Slice.

- The 5Gcontext is only visible to the top layer 5G Network Slice Orchestrator. None of the domain controllers have 5G visibility.

- A single tenant can have more than one 5G Network Slice, each of them is logically isolated and independent from other slices.

- Multiple 5G Network Slices can exist for the same service type but for different customers. These 5G Network Slices are completely independent of each other. For instance, Figure 1 shows that there are two 5G Network Slices for service type "Autonomous driving" for customers Enterprise-Y and Enterprise-Z with different SLO/SLEs. These two 5G Network Slices are completely independent of each other.

4.2 IETF Network Slice in Different RAN Deployments

Since the MMI interfaces deal with life cycle of the IETF Network Slices, this section covers the IETF Network Slices in different RAN access deployment. The definition of "IETF Network Slice" in this document is aligned with IETF draft-ietf-teas-ietf-network-slices [12] and is as follows:

"An IETF Network Slice enables connectivity between a set of Service Demarcation Points (SDPs) with specific Service Level Objectives (SLOs) and Service Level Expectations (SLEs) over a common underlay network."

An IETF Network Slice consists of a set of connectivity constructs between multiple SDPs with a specified connectivity type and one or more SLO/SLEs, which   are used to describe different network resources associated with the service delivered and corresponding parameters necessary to realize the IETF Network Slice. In specific in 5G network slicing, there are one or multiple IETF Network Slices for various RAN access deployments, which are covered in this section. In all the scenarios in this section, the IETF Network Slices will be created for following 5G network slice:

- 5G network slice ID (a.k.a. S-NSSAI): 02222222
- Customer: Public Safety
- Service type: CCTV

4.2.1 IETF Network Slice in Distributed-RAN Deployment

Figure 2 illustrates a typical Distributed-RAN (D-RAN) deployment where the RAN access network elements, gNBs, are responsible for all aspects of the radio access functions such as signaling processing, radio interface and scheduling. This deployment is basically equivalent of today's 4G network where the eNB network elements are responsible for all aspects of 4G radio access functions. In this deployment the RAN network elements are interfacing the transport network through Cell Site Gateway network elements and might have one or more contexts for various 5G network slices. In other words, each gNB network element might have one or more RAN slice subnets.
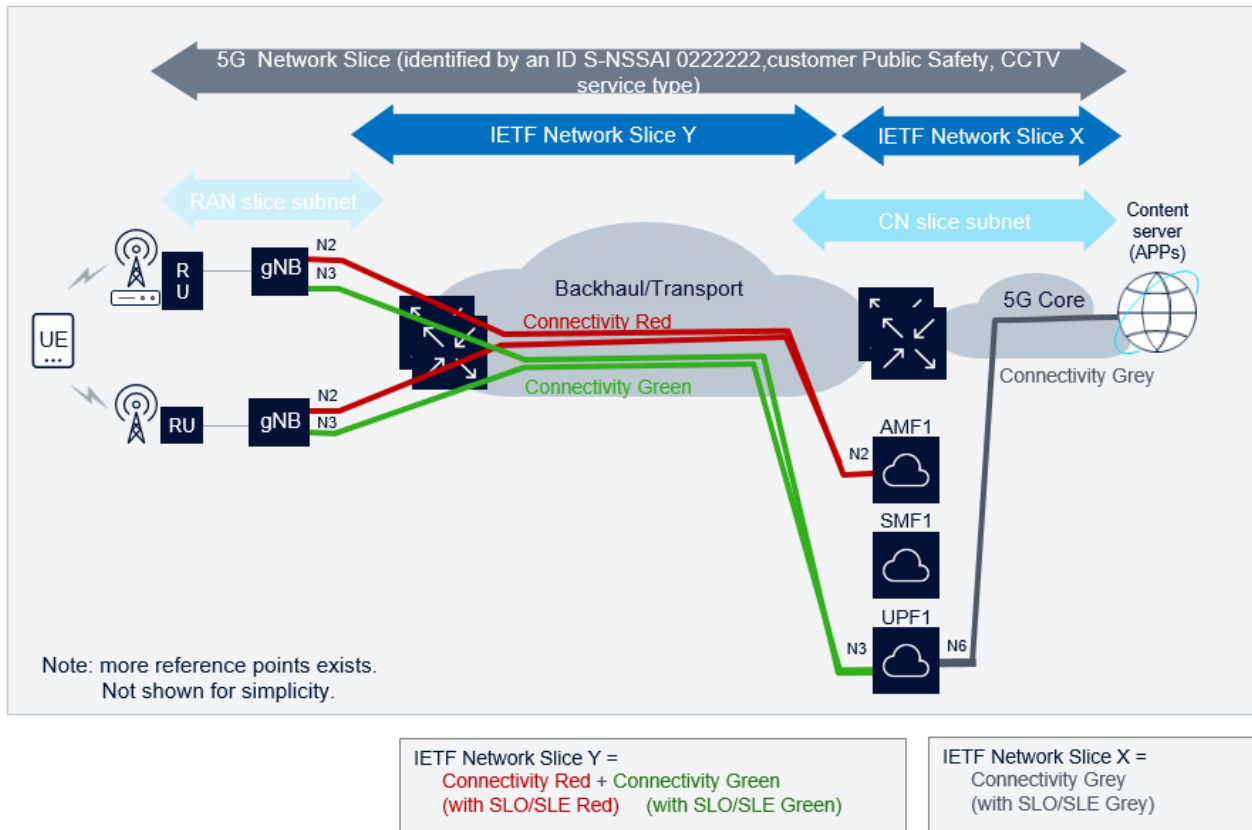
Figure 2 IETF Network Slices in Distribute RAN (D-RAN)

Within the context of 5G network slice, there is "IETF Network Slice Y" between gNB network elements and 5G Core network functions. IETF Network Slice Y contains "Connectivity Red" and "Connectivity Green" to connect N2 and N3 interfaces of RAN to Core nodes, respectively. Note that each connectivity in the IETF Network Slice Y has its own SLO/SLEs. For example, the SLO/SLEs for Connectivity Red might be the Reliability whereas the SLO/SLEs for Connectivity Green might be Bandwidth or Latency. In case the application content server is not collocated with Core network functions, there might be "IETF Network Slice X" to connect the Core N6 interfaces to application servers.

4.2.2 IETF Network Slice in Centralized-RAN Deployment

Figure 3 illustrates a Centralized RAN deployment where signal processing units (BBU) of the RAN nodes are transferred to a centralized center to simplify the network management and to enhance the computation capabilities. As a result, a new network called "fronthaul network" is introduced to provide the transport connectivity between the radio unit (RU) and the signal processing unit (BBU).

Figure 3 shows the same 5G Network Slice, created in Figure 2 where the RAN deployment is Centralized RAN instead of Distributed RAN. Comparing Figure 2 with Figure 3 reveals that in addition to IETF Network Slices X and Y, a new IETF Network Slice Z is needed to provide the connectivity between RU network elements and BBU nodes. The new IETF Network Slice Z contains "Connectivity Blue" which has strict latency requirements. The IETF Network Slice Z in the fronthaul domain is based on CPRI or eCPRI and sensitive to latency.
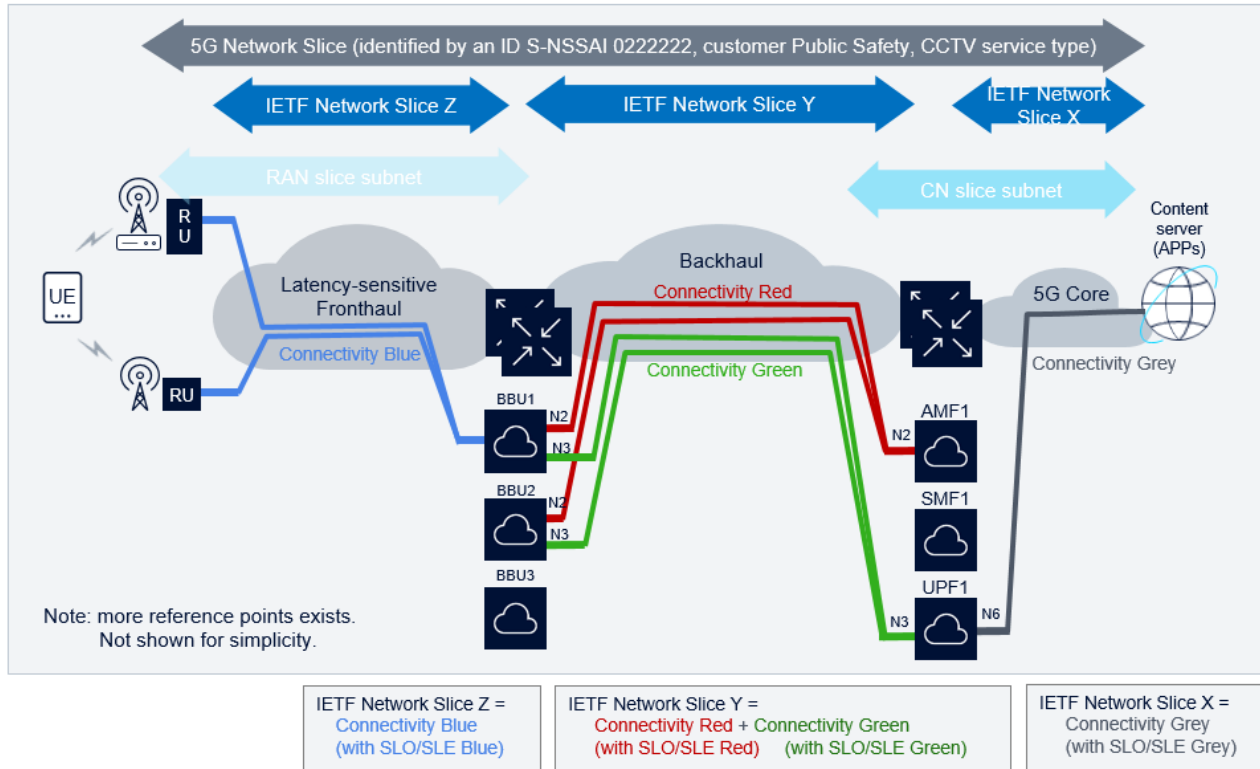
Figure 3 IETF Network Slices in Centralized RAN

4.2.3 IETF Network Slice in Cloud RAN (C-RAN) Deployment

In a Cloud RAN deployment (C-RAN), the BBU network element can be distributed even further into Distributed Unit (DU) and Central Unit (CU). In such a scenario, a new interface (F1) is introduced to provide the transport connectivity between DUs and CUs. As Figure 4 shows, a new "IETF Network Slice W" will be required to interconnect the DU with the CU function using the new midhaul transport network.

As shown in Figure 4, in C-RAN deployment, the scope of IETF Network Slices is across all domains, including fronthaul, midhaul, and backhaul domains. Within these different domains, the concept being used for IETF Network Slicing is always the same, i.e., to connect various network functions and application servers together for specific SLO/SLEs.
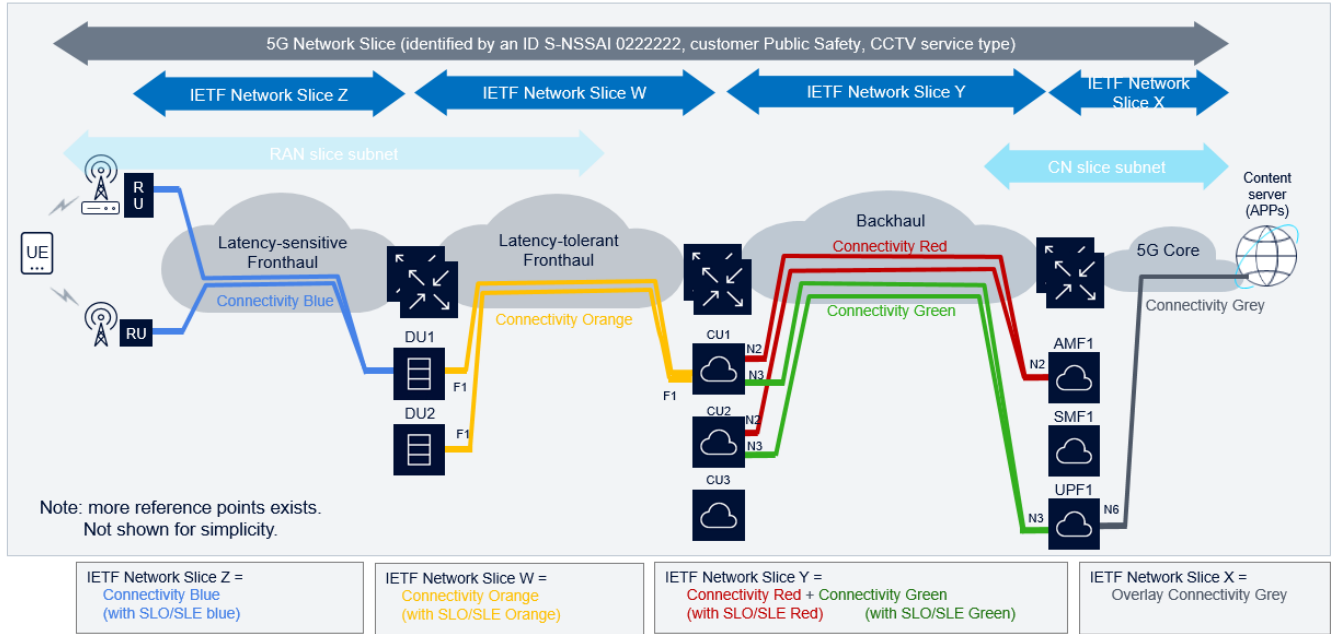
Figure 4 IETF Network Slices in Cloud RAN (C-RAN)

4.3 Reference Architecture of Network Slice Management Function

The section specifies the functions and interfaces related to network slice management.

This document uses IETF terms "5G Network Slice Orchestrator" for "NSMF" and "IETF Network Slice Controller" for "NSSMF". For RAN Slice Controller and CN Slice Controller refers to "Other External Controllers". This term is similar to the informally used industry term {NSMF, NSSMF}. For an informative example of industry usage of those terms, see 3GPP TR 28.801. Figure 5 is the reference architecture for management of a 5G Network Slice and shows the multiple interfaces between 5G Network Slice Orchestrator and other External Controllers with IETF NSC:
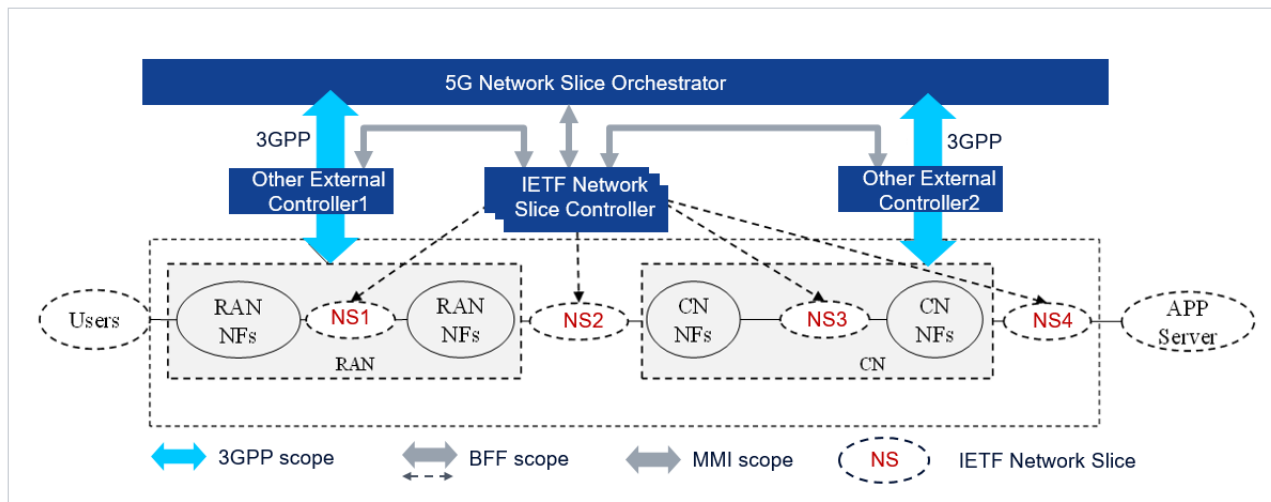
Figure 5 Reference architecture of IETF Network Slice Management

The Orchestrator is responsible for the management of Network Slice Instance (NSI), which is in the context of 5G. The 5G Network Slice Orchestrator sends network service requests to the Access, Core and Transport Network Slice Subnet Management Functions (i.e., IETF NSC and other external controller) based on the preparation needs of 5G Network Slice, indicating the transport network parameters to satisfy specific objectives.

According to the requirements for creation of a 5G Network Slice and per request from the 5G Network Slice Orchestrator, various domain controller create multiple NSSIs (i.e., RAN and CN slice subnet instances RAN and CN NSSI). Refer to 3GPP TS 28.530 [18] Figure 4.1.3.1 and Section 4.7.

The IETF Network Slice Controller is responsible for the management of IETF Network Slices, including transport network preparation and life-cycle management of IETF Network Slices, where the phases include creation, activation, and termination of IETF Network Slice and relationship set up with specific network slice and other IETF Network Slices that belong to the same NSI. Depending on the deployment of the 5G network slicing, it is possible to have multiple IETF Network Slice Controllers as shown in Figure 5.

The IETF Network Slice Controller establishes, when needed, the IETF Network Slice based on the service requirements derived from the 5G Network Slice Orchestrator (may also be some other external Controllers in RAN or CN) and maps the IETF Network Slice onto network resources (e.g., VPN, SR, etc.). At the same time, considering the transport network as connection of RAN and CN NSSI, the IETF Network Slice Controller needs to support the mapping management used for stitching of IETF Network Slice Instance with RAN and CN slice subnet instance.

The IETF Network Slice Controller might follow a hierarchical relationship that would provide a hierarchy of IETF Network Slices. In this case, IETF Network Slice realization contains other IETF Network Slices that are created for a particular technology. The IETF Network Slice will be decomposed to multiple IETF Network Slices, which are realized by IETF Network Slice Controllers.

The Other External Controller1 shown in Figure 5 is responsible for the life-cycle management of RAN slice subnet instances. The interface between 5G Network Slice Orchestrator and this Controller is defined in various 3GPP technical documents (See 3GPP TS 28.531 [19] and 3GPP 28.532 [18]).

The controller for RAN slice management might send requests for topology and connectivity parameters of transport network within 5G Radio Access Network to IETF Network Slice Controller when preparing the Access NSSI for certain 5G RAN. This case is needed for Cloud RAN and Centralized RAN deployments (Refer to Section 5.1) when multiple IETF Network Slices are needed between various RAN network functions for midhaul and fronthaul networks. Figure 5 shows these IETF Network Slice Instance1 between RAN NFs. Note that it might also be possible to manage the IETF Network Slice Instance1 directly from 5G Network Slice Orchestrator via the interface between 5G Network Slice Orchestrator and IETF Network Slice Controller.

The Other External Controller2 shown in Figure 5 is responsible for the life-cycle management of CN slice subnet. The interface between 5G Network Slice Orchestrator and this Controller is defined in various 3GPP technical documents (See 3GPP TS 28.531 [19] and 3GPP TS 28.532 [20]).

The controller for CN slice management might send requests for topology and connectivity parameters of transport network within 5G Core Network to IETF Network Slice Controller for certain 5G Core topologies. This case might be needed for cases when the core network elements are virtualized in different datacenters and need underlying transport connectivity. Figure 5 shows these IETF Network Slice Instance3 between CN NFs. Note that it might also be possible to manage the IETF Network Slice Instance3 directly from 5G Network Slice Orchestrator via the interface between 5G Network Slice Orchestrator and IETF Network Slice Controller.

The Mobile-transport network slice Management Interfaces (MMI) deal with the coordination between 5G Network Slice Orchestrator, or other external Controllers to IETF Network Slice Controller and are responsible for obtaining specific transport network service requirements, providing capability exposure of transport network and providing the monitoring and reporting of the IETF Network Slices to the 3GPP mobile network management functions. Figure 6 presents IETF Network Slice Controller from the perspective of the architecture reference model of management services, as specified in clause 5.1.1 3GPP TS 28.533 [21]. From its northbound, the IETF Network Slice Controller can be considered as producer that exposing transport network capability to the Orchestrator, which is viewed as a consumer of transport network service requesting the parameters related to transport network to prepare instantiation of a 5G Network Slice. In its southbound, the IETF Network Slice Controller can be considered as a consumer of IETF Network Slice Instance, the Network Resources as IETF Network Slice Instance producer providing a dedicated logical network with appropriate isolation to satisfy the requests of life-cycle management of IETF Network Slice Instance.
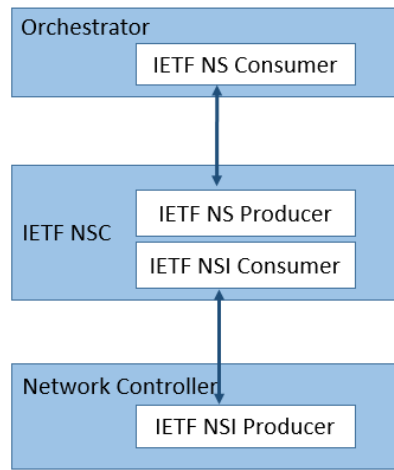

Figure 6 Producer and consumer of IETF network slice management

5 Service and Functional Requirements on MMI Interfaces

5.1 What are MMI Interfaces?

This section defines Mobile – transport network slice Management Interfaces (MMI) and identifies the service requirements to be supported by these interfaces for various 5G network slice types.

Referring to Figure 5, the Other External Controller functional blocks have interfaces to 5G Network Slice Orchestrator to perform the life-cycle management of RAN and CN slice subnets.

Various 3GPP technical specifications describe these operations and the interface requirements between 5G Network Slice Orchestrator and Controllers including the data model, attributes, and functional behavior. (such as 3GPP TS 28.530 [18], TS 28.531 [19], TS 28.532 [20], TS 28.541 [23]).

However, the interfaces between 5G Network Slice Orchestrator (may also be external Controller) and IETF Network Slice Controller are currently not defined or standardized. The goal of this document is to specify the requirements of these interfaces for various services provided by these interfaces.

The suite of interfaces between 5G Network Slice Orchestrator and IETF Network Slice Controller is denoted as Mobile-transport network slice instance Management Interfaces (MMI). The focus of this section is to identify the service requirements related to the MMI interfaces for various supported services.

Section 6 covers the attributes and parameters needed to be supported by MMI for automation and assurance of various services. Section 7 analyzes the necessary operations that the MMI interfaces need to support for IETF Network Slices to maintain continuity of the 5G Network Slice service, including attributes mapping/binding, SLA decomposition, etc. Service requirements on MMI interfaces.

The MMI interfaces deal with capabilities to manage and control the IETF Network Slices including:

1. Processing of IETF Network Slice automation requests from 5G Network Slice Orchestrator for enablement of IETF Network Slices including creation, deletion, and modification of IETF Network Slices

2. Exposure of transport network capabilities towards the 5G Network Slice Orchestrator including the transport network abstract topology

3. Exposure of IETF Network Slice monitoring data towards the 5G Network Slice Orchestrator

Figure 7 shows the various steps needed for lifecycle management of an IETF Network Slice and how they are related to MMI interfaces. These steps are:

Steps 1-3 show how the abstract topology of transport network will be discovered by 5G Network Slice Orchestrator via MMI interfaces.

Steps 4-7 show how the 5G Network Slice Orchestrator will request enablement (i.e., creation, modification, deletion) of IETF Network Slices via MMI interfaces.

Steps 8-11 show how the IETF Network Slice monitoring data will be exposed to 5G Network Slice Orchestrator via MMI interfaces.
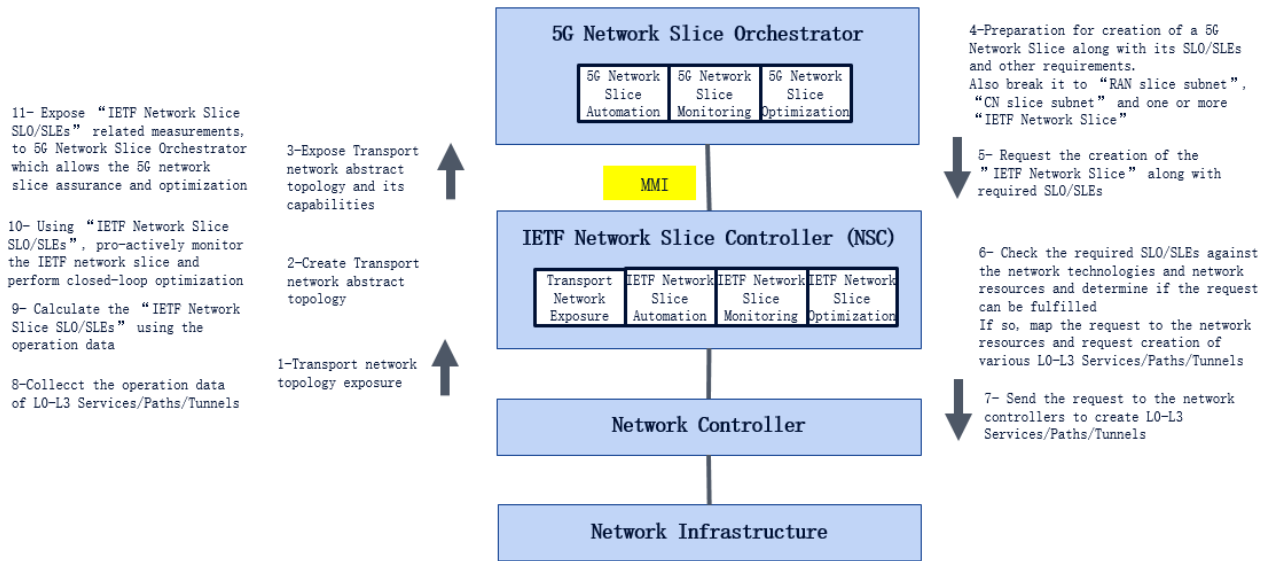
Figure 7 High-level functions for MMI interfaces

The IETF Network Slice Controller via its MMI interfaces receives various IETF Network Slice requests for following operations on an IETF Network Slice. Note that these requests will be received in context of a 5G Network Slice as explained in section 4.2:

- Create a new IETF Network Slice

- Disassociate an IETF Network Slice from certain 5G Network Slice

- Modify an IETF Network Slice

- Terminate an IETF Network Slice

The IETF Network Slice attributes needed to be supported by MMI interfaces for these requests are covered in Section 6.1.

The IETF Network Slice Controller via its MMI interfaces should also support the run-time aspects of the IETF Network Slices by collecting the real-time telemetry data on resources of the IETF Network Slices and exposing the IETF Network Slice SLO/SLEs to the high layer 5G Network Slice Orchestrator. In other words, IETF Network Slice Controller collects certain performance parameters related to the allocated resources of an IETF Network Slice and exposing them to 5G Network Slice Orchestrator for assurance on IETF Network Slices. The IETF Network Slice attributes needed to be supported by MMI interfaces in support of assurance are covered in Section 6.2 .

In addition, the IETF Network Slice Controller via its MMI interfaces should expose the transport network abstract topology to higher layer 5G Network Slice Orchestrator. This allows 5G Network Slice Orchestrator to form the abstract topology. These IETF Network Slice attributes needed to be supported by MMI interfaces are covered in Section 6.3.

5.2 Functional Requirements on MMI Interface

5.2.1 General

According to section 4.3 of this document, 5G Network Slice Orchestrator communicates with IETF Network Slice Controller through the MMI interface, which is also implemented between the 3GPP mobile network slice management subnet system and IETF Network Slice Controller. When the IETF Network Slice Controller receives IETF Network Slice requests, the MMI interface needs to process data objects to provide IETF Network Slice service functions, such as creation, modification, and termination of IETF Network Slice instance, as well as monitoring of resource occupancy or reporting of the IETF Network Slice instance operation to provide the necessary network slice service to the upper IETF Network Slice consumer. Refer to section 5.2.2 for the functional requirements on MMI interface.

This section provides some functional requirements for the MMI interface.

5.2.2 Functional Requirements for MMI interface

[R-1]   The MMI interface MUST support the processing of data objects for requests and responses of IETF Network Slice instance creation.

[R-2]   The MMI interface MUST support the processing of data objects for requests and responses of IETF Network Slice instance de-creation.

[R-3]   The MMI interface MUST support the processing of data objects for requests and responses of IETF Network Slice instance modification.

[R-4]   The MMI interface MUST support the processing of data objects for requests and responses of IETF Network Slice instance termination.

[R-5]   The MMI interface MUST support querying or notifying the network topology and network resource of the IETF Network Slice instance.

[R-6]   The MMI interface MUST support interaction between an IETF Network Slice consumer (e.g., 5G Network Slice Orchestrator) and an IETF Network Slice Provider (i.e., IETF NSC) based on YANG data model operational data.

5.3 IETF Network Slice mapping

A NSI is viewed as a set of network function instances and the required network resources. In the 5G context network functions across radio access network (RAN), transport network (TN), and core network (CN). AN slice subnets and CN slice subnets are managed by the 3GPP management system, IETF Network Slices are considered as a set of connectivity constructs within and between RAN and CN slice subnets and managed by the transport management system (i.e., IETF Network Slice Controller).

The upper network slice management system (i.e., Orchestrator), refer to Figure 5 in Section 4.3, creates a 5G Network Slice identified by its NSI ID, as specified in clause 5.1.1 of 3GPP TS 28.531 [19]. NSI ID, in turn, is associated with NSSI IDs of related subnets for slicing dependency management. A NSI provides specific network features and capacities for required services. The SST and SD values identify the service type provided for particular customers. The standardized values of SST are specified in clause 5.15 of 3GPP TS 23.501 [16]. An Operator is not required to support all standardized SST values and can provide

customized services with non-standardized SST values. The S-NSSAI parameter includes SST and SD information. When creating a subnet slice of a 5G NSI:

1. The 5G Network Slice Orchestrator solicits the network slice SLO/SLEs into each subnet slice;

2. The Controller located in different domain (e.g., RAN, CN, TN) receives the RAN/CN slice creation request from the 5G Network Slice Orchestrator with a specific SLA, allocates suitable network resources to realize RAN/CN NSSI which identified as RAN/CN NSSI ID;

3. The IETF Network Slice Controller receives the IETF Network Slice creation request with a specific SLO/SLE and maps the request to the suitable network resources and provides network slice services using some technologies.

The IETF Network Slice instance is identified by IETF Network Slice ID, which may be generated by IETF Network Slice Controller. The instantiation of the IETF Network Slice is a mapping of the underlying infrastructure. IETF Network Slice Instance may be achieved through VPNs, a variety of tunneling and supporting technologies, such as segment routing, SFC, EVPN, or FlexE among others. The identifier (e.g., VPN-id, EVPN-id, etc.) may be varied with no definitive identification in IETF Network Slice packets. As a result, the mapping between the identifier of technologies and IETF Network Slice instance is non-deterministic and requires additional consideration. Furthermore, in the management plane, the IETF Network Slice Controller associates IETF Network Slice Instance with NSI ID binding IETF Network Slice and 5G Network Slice. Also, the IETF Network Slice Controller sets the relationship of IETF Network Slice ID with IETF Network Slice specific technology identifier realizing the bound of IETF Network Slice with its related network resources.

6 IETF Network Slice Attributes and Parameters

This section covers the parameters that the MMI interfaces need to support as are related to the life-cycle management of "IETF Network Slice". As per Section 5.2, the IETF Network Slice Controller via its MMI interfaces receives various requests for following operations on an IETF network slice:

- Create a new "IETF network slice"
- Activate an "IETF network slice" and associate them with 5G Network Slice(s)
- Disassociate an "IETF network slice" from certain 5G Network Slice
- De-active an "IETF network slice"
- Modify an "IETF network slice"
- Terminate an "IETF network slice"

To support all these operations, incoming requests via MMI interface to IETF Network Slice Controller should include the following attributes:

- "IETF Network Slice" attributes:
    - These attributes specify the "IETF Network Slice" and include attributes such as identification, description, and SDPs of an "IETF Network Slice"
- "IETF Network Slice" SLO/SLE attributes:
    - Performance requirements on IETF network slice such as capacity, latency, and jitter
- IETF Network Slice assurance attributes: These attributes indicate 5G Network Slice Orchestrator (or some other external controllers) desired on how to perform the monitoring on IETF network slices. Using these attributes, the IETF Network Slice Controller will process the received monitoring attributes from the transport network and performs the monitoring on "IETF Network Slices" which in turn will be propagated to 5G Network Slice Orchestrator.

After creation of an "IETF Network Slice", its operational state should be visible to 5G Network Slice Orchestrator. To support that, IETF Network Slice Controller should keep a set of operational state per IETF Network Slice.

Section 6.1 covers the attributes should be supported by MMI for "IETF Network Slice" fulfillment in more detail.

Section 6.2 covers the operational attributes of "IETF Network Slice" supported by MMI interfaces.

6.1 Attributes for IETF Network Slice Enablement

This section specifies the IETF network slice attributes, which should be supported by MMI interfaces towards IETF Network Slice Controller. This allows 5G Network Slice Orchestrator to request fulfillment of "IETF network slices".

To be consistent with 3GPP "Slice Profile term defined in 3GPP TS 28.541 [23] section 6.3.4 for RAN and CN slice subnets, BBF will introduce the following term:

- **IETF Network Slice Profile**: It contains all attributes of IETF network slices which 5G Network Slice Orchestrator communicates with IETF Network Slice Controller via MMI interfaces when requesting Creation, Modification, Activation, De-activation, and Termination of an IETF network slice.

Table 1 shows the content of the "IETF Network Slice Profile":

Table 1 - Content of IETF Network Slice Profile

IETF Network Slice Profile	Description
IETF Network Slice Profile ID	Identification of the IETF Network Slice Profile
IETF Network Slice Identification Attributes	These attributes identify the IETF Network Slice
IETF Network Slice SLO/SLE Attributes	IETF Network slice Service Level Objectives and/or Expectations
IETF Network Slice SDP Attributes	These attributes specify the IETF Network Slice Service Demarcation Points (SDPs)
List of IETF Network Slice connectivity constructs	This is the list of all connectivity constructs belong to an IETF Network slice and are between multiple SDPs.
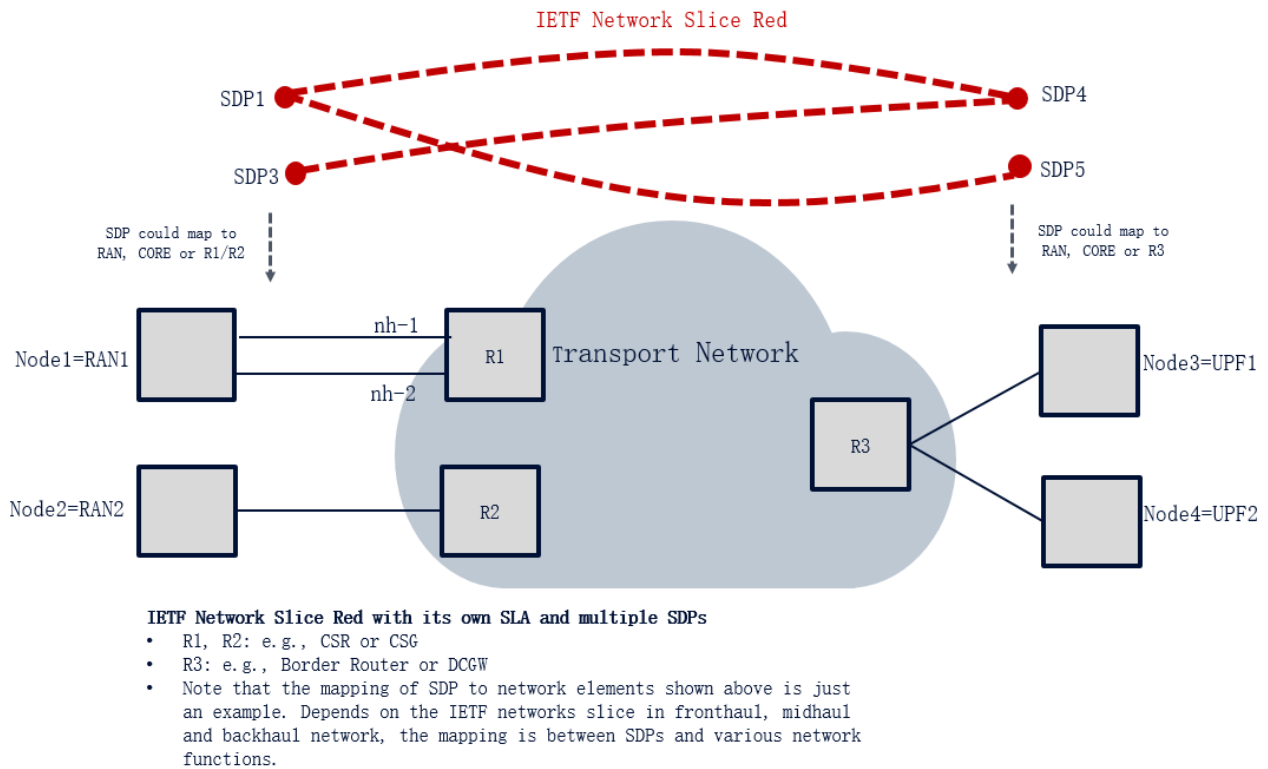
Figure 8 A Transport network with one IETF network slice

Figure 8 shows a typical IETF network slice with multiple connectivity constructs with its own SLO/SLE. It also has multiple IETF network slice SDPs. This figure can be used to provide examples for content of Table 2 to Table 5.

Table 2 to Table 5 describe the detail of all "IETF Network Slice Profile" attributes defined in Table 1.

Table 2 specifies the details of IETF Network Slice Identification attributes:

Table 2 - List of IETF Network Slice attributes

IETF Network Slice SDPs	Description	Property
ins_id	IETF network slice identification. This attribute specifies a unique identifier of the IETF network slice. This is assigned by IETF Network Slice Controller in response to creation request from 5G Network Slice Orchestrator. This can be used in subsequent modification, activation, de-activation, and termination request	type: String multiplicity: 1 default Value: None mandatory
ins_description	Description of an IETF network slice	type: String multiplicity: 1 default Value: None optional
ins_correlation_id	Used by higher layer 5G Network Slice Orchestrator for correlation, notification etc.	type: String multiplicity: 1 default Value: None mandatory

Table 3 includes the attributes of IETF Network Slice SDPs. The number of SDPs could or 2 or more (i.e., at least there should be two SDPs). This table uses 3GPP transport slice endpoint (i.e., EP Transport) attributes described in TS 28.541 [23], the term "endpoint" is replaced with SDP to align with IETF draft-ietf-teas-ietf-network-slices [12], and augment them with other attributes. Figure 8 shows various potential cases for IETF network slice SDPs (e.g., SDP-1, SDP-2, and SDP-3).

Table 3 - IETF Network slice SDP attributes

IETF Network Slice SDPs	Description	Property
sdp_id	This attribute specifies an identification for IETF network slice SDP. This attribute is unique per system	type: uint32 multiplicity: 1 default Value: None mandatory
sdp_description	Description of the IETF network slice SDP	type: String multiplicity: 1 default Value: None optional

sdp_node_id	This attribute specifies an identification the node. This attribute is unique among all nodes.	type: String multiplicity: 1 default Value: None optional
sdp_ip	This attribute specifies the IP address assigned to IETF network slice SDP. It can be an IPv4 or an IPv6 addresses. This attribute is unique among all nodes.	type: String multiplicity: 1 default Value: None mandatory

Table 4 specifies the details of IETF network slice SLO/SLE attributes. The number of IETF network slice SLO/SLEs could be one or more.

Note: All attributes must be supported by all implementations. The "Mandatory" and "Optional" mean that whether that attribute is required in any specific instance.

Table 4 - IETF Network Slice Service Level Objectives and/or Expectation Attributes

IETF Network Slice SLO	Description	Property
ins_SLO/SLE_id	This attribute specifies the SLO/SLE identification	type: Integer multiplicity: 1 default Value: None mandatory
max_guaranteed_latency	Upper bound of desire latency when transmitting between SDPs of IETF network slice	type: Integer multiplicity: 1 default Value: None optional
min_guaranteed_bandwidth	Guaranteed Minimum bandwidth between SDPs at any time	type: Integer multiplicity: 1 default Value: None optional

max_guaranteed_jitter	Upper bound of packet delay variation (aka Jitter PDV) as defined in IETF RFC 3393 [3]	type: Integer multiplicity: 1 default Value: None optional
max_packet_loss_rate	Ratio of packets dropped to packets transmitted between any two IETF network slice SDPs.	type: Integer multiplicity: 1 default Value: None optional

Table 5 specifies the list of attributes of IETF network slice connectivity constructs. Each connectivity construct may be between two or more SDPs with specific SLO/SLEs. An IETF network slice can contain one or more connectivity constructs.

Note that Table 5 covers connectivity constructs and their associated SLO/SLEs. This model is also aligned with IETF.

Table 5 - Attributes of IETF Network Slice connectivity construct

IETF Network Slice connectivity constructs	Description	Property
IETF network slice connectivity construct id	This attribute specifies the identifier of an IETF network slice connectivity construct between a group of SDPs. The details of the SDP is identified in Table 3.	type: string multiplicity: 1 default Value: None mandatory
IETF network slice connectivity construct SLO/SLEs	This attribute specifies the name of SLO-SLE-policy associated with the connectivity construct.	type: string multiplicity: 1 default Value: None mandatory

6.2 Assurance Attributes of IETF Network Slice

The MMI interface should support the monitoring of the IETF network slices during enablement of the IETF network slices. In addition, the MMI interface should also support the retrieval of the monitoring and assurance data from the IETF Network Slice Controller towards the 5G Network Slice Orchestrator. This section specifies the IETF network slice attributes, which should be supported by MMI interfaces. This allows 5G Network Slice Orchestrator) to request the monitoring of "IETF network slices" and also to receive the current SLAs of IETF network slices.

Table 1 specifies the list of monitoring attributes of IETF network slice which should be supported by MMI interfaces. Table 4 specifies the list of Service Level Objectives and/or Expectations which should be

supported by MMI interfaces when 5G Network Slice Orchestrator requests IETF Network Slice Controller for creation/modification of an IETF network slice.

Note that for any specific IETF network slice, MMI interfaces should report only those SLO/SLEs which are include during the enablement request. In other words, the MMI interfaces should support all monitoring attributes of Table 6. However, for any specific IETF network slice, a subset of monitoring attributes will be reported to 5G Network Slice Orchestrator.

Table 6 - Assurance Attributes of IETF Network Slice

IETF Network Slice Monitoring Attributes	Description	Property
Ins_monitoring_enabled	This attribute is sent from 5G Network Slice Orchestrator to IETF Network Slice Controller during the enablement of IETF Network Slices. It allows the IETF Network Slice Controller to collect the Telemetry data from the network in context of the IETF network slice. If this attribute is TRUE, IETF Network Slice Controller will also send the IETF network slice SLAs to 5G Network Slice Orchestrator	type: Binary multiplicity: 1 defaultValue: TRUE optional
Ins_monitoring_frequency	If attribute "ins_monitoring_enabled" is TRUE, this attribute specifies how often IETF Network Slice Controller should send the IETF network slice telemetry data to 5G Network Slice Orchestrator	type: Integer (in Second) multiplicity: 1 defaultValue: 300 [sec] optional
Is_on_sla	If attribute "ins_monitoring_enabled" is TRUE, this attributes indicate if the IETF network slice is on SLA, i.e., the IETF network slice SLA is still valid	type: Binary multiplicity: 1 defaultValue: None optional
Ins_used_bandwidth	This attribute is related to **Table 4** attribute "min_guaranteed_bandwidth". If attribute "ins_monitoring_enabled" is TRUE, this attribute specifies the median/percentile of IETF network slice used bandwidth.	type: Integer multiplicity: 1 defaultValue: None optional
Ins_latency	This attribute is related to **Table 4** attribute "max_guaranteed_latency". If attribute "ins_monitoring_enabled" is TRUE, this attribute specifies the median/percentile of IETF network	type: Integer multiplicity: 1 defaultValue: None optional

	slice latency. If this value is below requested value "max_guaranteed_latency", the IETF network slice is marked as "on-sla".	
In_jitter	This attribute is related to **Table 4** attribute "max_guaranteed_jitter". If attribute "ins_monitoring_enabled" is TRUE, this attribute specifies the current median/percentile of IETF network slice jitter. If this value is below requested value "max_guaranteed_jitter", the IETF network slice is marked as "on-sla". For details of Packet Delay Variation, see RFC 5481 [4].	type: Integer multiplicity: 1 defaultValue: None optional
Ins_packet_loss_rate	This attribute is related to **Table 4** attribute "max_packet_loss_rate". If attribute "ins_monitoring_enabled" is TRUE, this attribute specifies the median/percentile of IETF network slice packet loss rate. If this value is below requested value "max_packet_loss_rate", the IETF network slice is marked as "on-sla".	type: Integer multiplicity: 1 defaultValue: None optional

6.3 Operational Attributes for IETF Network Slice

6.3.1 Creation Operation

6.3.1.1 Description

The IETF Network Slice Instance Consumer (including 5G Network Slice Orchestrator, Controller) sends the creation request of IETF Network Slice Instance to the IETF Network Slice Provider (i.e., IETF Network Slice Controller). The IETF Network Slice Provider decides whether to create a new IETF Network Slice Instance or reuse an existing instance to meet the network topology and network resource requirements, and responds with the IETF Network Slice Instance creation result to the IETF Network Slice Instance Consumer.

6.3.1.2 Input Parameters

Table 7 - Input parameters for IETF Network Slice creation

Attributes	Property	Description
Attribute List	Type: List <attribute name, attribute value> Mandatory support	The list of IETF Network Slice Instance attributes is specified in Section 6.1, which include network profile attributes, network connectivity constructs, SLO/SLEs, security requirements, etc.

6.3.1.3 Output Parameters

Table 8 - Output parameters for IETF Network Slice creation

Attributes	Property	Description
Ins_id	Type: String Mandatory support	The unique identifier of an IETF Network Slice Instance. **Note 1:** The IETF Network Slice Controller is expected to automatically allocate the identifier of the IETF Network Slice instance when receiving the creation request of IETF Network Slice Instance. How the instance id is allocated by the IETF Network Slice Controller is out of the scope of this document. **Note 2:** The IETF Network Slice instance as a part of a 5G Network Slice instance, the instance id of IETF Network Slice is used for the life-cycle management of subnet transport network slice and its binding relationship management with 5G Network Slice instance.
Status_code	Type: Boolean Mandatory support	The parameter is to notify whether the operation is succeeded or failed. True means success.
Status_info	Type: Boolean Mandatory support	The parameter is to notify the necessary supplementary information for the result of the operation. If the operation is successful the attribute indicates its corresponding job identifier, if failed the attribute indicates error message or error code to identify failure cause.

6.3.2   Deletion Operation

6.3.2.1   Description

The IETF Network Slice Consumer sends a deletion request of an IETF Network Slice Instance to the IETF Network Slice Provider, when there is no need for the IETF Network Slice provision, which responds to the deletion result to the IETF Network Slice Consumer and may correspondingly release the IETF Network Slice Instance related resources, delete the binding with other subnet or 5G Network Slice instance, and terminate services.

6.3.2.2   Input Parameters

Table 9 - Input parameters for IETF Network Slice deletion

Attributes	Property	Description
Ins_id	Type: String Mandatory support	The unique identifier of an IETF Network Slice Instance.

6.3.2.3   Output Parameters

Table 10 - Output parameters for IETF Network Slice deletion

Attributes	Property	Description
Status_code	Type: Boolean Mandatory support	The parameter is to notify whether the operation is succeeded or failed. True means success.
Status_info	Type: String Mandatory support	The parameter is to notify the necessary supplementary information for the result of the operation. If the operation is successful the attribute indicates its corresponding job identifier, if failed the attribute indicates error message or error code to identify failure cause.

6.3.3   Modification Operation

6.3.3.1   Description

The IETF Network Slice Consumer sends modification request of an IETF Network Slice Instance to the IETF Network Slice Provider with the change of network capability requirements, such as network slice SDP, SLO/SLE requirements, NSI binding, etc. The IETF Network Slice Provider decides whether the IETF Network Slice Instance modification requirements can be satisfied and executes and then responds with the corresponding result to the IETF Network Slice Instance Consumer.

Note: When the IETF Network Slice Instance is un-available, the network slice SDP may be required for change, and when the network load exceeds the support of transport network, it may bring the change to network slice related SLO/SLE requirements and binding with other NSI.

6.3.3.2 Input Parameters

Table 11 - Input parameters for IETF Network Slice modification

Attributes	Property	Description
Attribute List	Type: List <attribute name, attribute value> Mandatory support	A list of attributes contained in a specific IETF Network Slice Instance.
Ins_id	Type: String Mandatory support	The unique identifier of an IETF Network Slice Instance.

6.3.3.3 Output Parameters

The output parameters for IETF Network Slice modification are the same as the deletion operation; refer to section 6.3.2.3.

6.3.4 Query Operation

6.3.4.1 Description

The IETF Network Slice Consumer sends network capability query request of an IETF Network Slice Instance to the IETF Network Slice Provider, such as latency, bandwidth, jitter, etc. to monitor and determine whether the network capability requirements are met.

6.3.4.2 Input Parameters

Table 12 - Input parameters for IETF Network Slice query

Attributes	Property	Description
Ins_id	Type: String Mandatory support	The unique identifier of an IETF Network Slice Instance.

6.3.4.3 Output Parameters

Table 13 - Output parameters for IETF Network Slice query

Attributes	Property	Description
Attribute List	Type: List <attribute name, attribute value> Mandatory support	A list of attributes contained in a specific IETF Network Slice Instance.
Status_code	Type: Boolean Mandatory support	The parameter is to notify whether the operation is succeeded or failed. True means success.
Status_info	Type: String Mandatory support	The parameter is to notify the necessary supplementary information for the result of the operation. If the operation is successful the attribute indicates its corresponding job identifier, if failed the attribute indicates error message or error code to identify failure cause.

6.4 Abstract Transport Network Exposure

6.4.1 General

In the 5G Network Slice management system, the transport network slice provider is triggered to expose abstract transport network capability to its upper network slice consumer during the lifecycle management of IETF Network Slice Instance. The exposure data may include provision data, monitoring data, etc. The agreement should be reached between IETF Network Slice Controller with the third trusted party (i.e., 5G Network Slice Orchestrator, Controller) through MMI interface(s) before abstract transport network capability is exposed. The authorization information is part of the advertised information.

The provision capability exposure is supported during the lifecycle management of an IETF Network Slice instance. For example, in the creation phase, the IETF Network Slice Controller needs:

- Provide the abstract transport network capability data for the IETF Network Slice instance preparation to 5G Network Slice Orchestrator. The provision information may include network resource occupation, network topology, network connectivity, etc.

- Provide the IETF Network Slice instance provision result and report to the 5G Network Slice Orchestrator through MMI interface(s). The provision information may include: IETF Network Slice Instance identifier, SLO/SLE parameters configured, etc.

The monitoring capability exposure is supported by the IETF Network Slice provider (i.e., IETF Network Slice Controller) for monitoring the operating condition of an IETF Network Slice instance. Transport network uses telemetry technologies to calculate whether the IETF Network Slice instance SLO/SLE requirements are satisfied and reports context to the 5G Network Slice Orchestrator used for 5G Network Slice management and optimization.

6.4.2 Requirements

This section provides some abstract transport network capability exposure requirements for the MMI interface.

[R-7]   The MMI interface MUST support the exposure of abstract transport network capability.

[R-8]   The MMI interface MUST support the exposure of provisioning of an IETF Network Slice instance, including enablement and operation, as specified in section 6.1 and 6.2.

[R-9]   The MMI interface MUST support the exposure of provisioning report of an IETF Network Slice instance.

[R-10]   The MMI interfaces MUST support the exposure of measurement of an IETF Network Slice instance.

7 Operations for MMI Interfaces in Support of 5G Network Slices

7.1 General

Network slicing is a 5G communication technology that can provide users with specific network service guarantee. A network slice provider provisions an instance of 5G Network Slice when Orchestrator receives a request from the consumer. The 5G Network Slice instance is a network (dedicated or shared) reaching across multiple network domains (from RAN, TN to CN). The corresponding 5G NSI is comprised of RAN NSSI, CN NSSI, and IETF Network Slice Instance. An IETF Network Slice Instance provides the connectivity with specific SLO/SLE requirements between RAN and CN NSSIs. For example, IETF Network Slice Instance provides reachability within or between from RAN to CN with low latency, high reliability, or best effort.

5G Network Slice across domains using different technologies and encapsulations, in order to concatenate subnet slices, it's necessary to build a mapping or binding between network subnet slice instance and 5G NSI (may through network slice identifier), and QoS mapping from 5G QoS (i.e., 5QI) with transport QoS (e.g., DSCP/PCP) to maintain continuity of network slicing service, as specified in section 5.3. The 5G NSI management system (5G Network Slice Orchestrator) should be responsible for the mapping provisions to communicate with the transport network slice manager (i.e., IETF Network Slice Controller) through the MMI interface. The mapping creation to transport network nodes and packet encapsulation processing are out of the scope of this document.

7.2 SLA Parameters Mapping and Decomposition

Service Level Agreement (SLA) agreed upon by a network slice consumer and provider includes: service type, resource creation, and service duration, guarantee level, etc. As described in clause 6.3.3 of 3GPP TS 28.541 [23], a 5G network slice provider (i.e., 5G Network Slice Orchestrator) maps SLA requirements to a service profile as input for network slice requirements and decomposes service profile attributes into subnet slice requirements.   It then sends these requirements to the subnet slice management system correspondingly. For example, the CN slice profile is used to specify core network slice requirements. The

RAN slice profile is used to specify radio access network slice requirements. The IETF Network Slice profile is used to specify transport network slice requirements.

For 5G network service requirements, the service profile is defined in section 6.3.3 of 3GPP TS 28.541 [23], RAN slice profile and CN slice profile is defined in section 6.3.4 of 3GPP TS 28.541 [23], TN slice profile (i.e., IETF Network Slice profile) is defined in section 6.1 of this document.

In order to support 5G SLA monitoring requirements, the IETF Network Slice Controller should support to expose transport network capability to 5G Network Slice Orchestrator through MMI interface, for example, the IETF Network Slice Controller calculates IETF Network Slice Instance SLO/SLE compliance using Telemetry technology and reports results to 5G Network Slice Orchestrator to achieve 5G Network Slice instance assurance and optimization, as described in section 6.4.

The mapping of IETF Network Slice Instance SLO/SLE with 3GPP service profile is listed in Table 14 below.

Table 14 - Mapping of IETF Network Slice SLO/SLE with 3GPP service profile

IETF Network Slice SLO/SLE Attributes	Mandatory/Optional	3GPP service profile Attributes
Max_guaranteed_latency	O	Latency
min_guaranteed_bandwidth	O	dLThptPerSlice uLThptPerSlice
max_guaranteed_jitter	O	Jitter

7.3 Requirements

[R-11]   The MMI interface MUST be able to enable of IETF Network Slice Instance, as described in section 6.1.

[R-12]   The MMI interface MUST support the operation of IETF Network Slice Instance, as described in section 6.2.

[R-13]   The MMI interface MUST support binding an IETF Network Slice Instance to one or more 5G NSI(s).

[R-14]   The MMI interface MUST support unbinding an IETF Network Slice Instance to 5G NSI(s).

[R-15]   The MMI MUST support mapping between 5G QoS (i.e., 5QI) and transport QoS (e.g., DSCP, PCP).

[R-16]   The 5G Network Slice Orchestrator MUST support mapping of a 3GPP service profile to an IETF Network Slice profile SLO/SLE.

8 Interfaces of the BBF Broadband Networks in Support 5G Network Slices

8.1 Related Work on Network Slice Management and Related Service Interfaces of Other SDOs

As an essential technology for 5G, network slicing attracts wide-spread attention in industrial and standard organizations. For example, 3GPP SA2 and SA5 have released many related study reports and technical specifications, such as: TS 23.501 [16] and TS 23.502 [17] specify the identification, processing of network slice.

Additionally, 3GPP SA5 released a list of specifications on network slice management, such as: TS 28.530 [18], TS 28.531 [19], TS 28.533 [21], TS 28.540 [22], and TS 28.541 [23] specifies use cases, requirements and management services and processing for 5G network slicing.

Unlike 3GPP, whose work is all about network slicing in a mobile network, IETF discusses network slice management in a transport network. The discussion topics include the IETF network slice framework, network slice service management interfaces, technology realization for IETF network slice. The draft-ietf-teas-ietf-network-slices [12] provides the definition and framework for IETF network slice.

9 Data Models for MMI Interface in Support of 5G Network Slices

YANG is a data modeling language used to model configuration and state data of network management protocols, procedures, and notifications; refer to IETF RFC 7950 [6]. YANG can be used for Network Configuration Protocol (NETCONF) (see IETF RFC 6241 [5]), RESTCONF (see IETF RFC 8040 [8]), and JSON (see IETF RFC 7951 [7]), providing programmatic interface for accessing data. YANG data models can be used to configure on service managed components (i.e., service model) or directly configure on network elements (i.e., configuration model), bringing modularity and efficiency of function realization. Of which service model provides an abstract service delivery while configuration model provides a visualized function configuration on network elements.

The data model for MMI interface is an IETF Network Slice service model and allows IETF Network Slice Controller to expose abstract network connectivity capability with SLO/SLE requirements in support of 5G Network Slice delivery for consumer. The MMI interface data model for an IETF Network Slice instantiation involves MMI reference architecture, as described in section 4.3.

- 5G Network Slice Orchestrator as IETF Network Slice consumer requests guaranteed network connectivity service within and between RAN and CN slice.

- IETF Network Slice Controller, as IETF Network Slice provider, provides network slice as a service with SLO/SLE requirements assurance.

- MMI interfaces that support communication between 5G Network Slice Orchestrator and IETF Network Slice Controller allow a network slice consumer to request for network slice service delivery and facilitate modification and monitoring of the IETF network slice instance by the IETF Network Slice consumer in support of 5G Network Slice life-cycle management.

The MMI data model should align with the IETF Network Slice service YANG model.

9.1 Requirements

[R-17]   The MMI interface MUST support operation (including configuration, modification, and termination) of an IETF Network Slice instance based on a YANG data model.

[R-18]   The MMI interface SHOULD support operation of an IETF Network Slice instance in XML via NETCONF.

[R-19]   The MMI interface MUST support operation of an IETF Network Slice instance in JSON via RESTCONF.

[R-20]   The MMI interface MUST support operational state retrieval of an IETF Network Slice instance based on a YANG data model.

[R-21]   The MMI interface MUST support operational state retrieval of an IETF Network Slice instance in JSON via RESTCONF.

[R-22]   The MMI interface SHOULD support operational state retrieval of an IETF Network Slice instance in XML via NETCONF.

[R-23]   HTTPS MUST be supported if RESTCONF is supported on the MMI interface.

10 Mapping of the MMI Data Models to Exiting Packet Switching Technologies

As defined in IETF draft-ietf-teas-ietf-network-slices [12], the IETF Network Slice is an abstract topology connecting a set of SDPs using shared or dedicated network resources (including network, compute, and storage resource) to satisfy customer's SLO/SLE requirements. The IETF Network Slice is technology agnostic.

The IETF Network Slice controller (NSC) is located between the IETF Network Slice customer (i.e., 5G Network Slice Orchestrator, Other External Controller) and the transport network controller, IETF network slice is a part of 5G Network Slice, the framework for MMI is showed as the Figure 9 below.
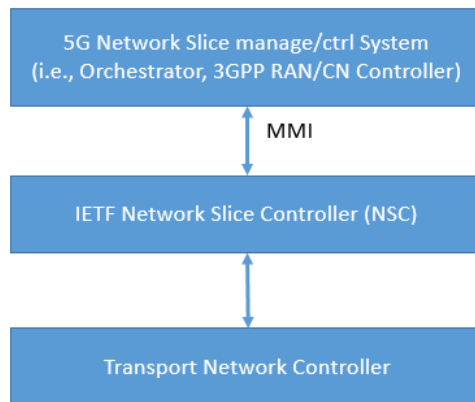

Figure 9 IETF NSC used for 5G network slice scenario

IETF NSC is responsible for mapping the MMI data model to specific network technology and completes the IETF Network Slice instantiation in the underlying physical network. This document assumes the solution is YANG-based (RFC 7950 [6]), such as RESTCONF (see IETF RFC 8040 [8]) or NETCONF (see IETF RFC 6241 [5]). The specific protocol data model MAY include, for example, VPN YANG (see RFC 9182 [11], draft-ietf-opsawg-l2nm [15], etc.), MPLS-TE YANG (see IETF draft-ietf-teas-yang-path-computation [13]), SR YANG (see IETF RFC 9020 [10]), SR policy YANG (see IETF draft-ietf-spring-sr-policy-yang [14]), etc. The underlying network abstracts physical network resources into virtual network nodes and network connectivity to form an abstract network topology with SLO/SLE requirements satisfaction and export to the IETF network slice controller.

The IETF NSC uses a specific packet switching technology to provide network resources and divides the underlying network into separate logical networks.

11 Security Considerations

11.1 General

In the 5G Network Slice management scenario, the IETF Network Slice Provider (i.e., IETF Network Slice Controller) is outside of 3GPP trusted domain. Upon receiving an IETF Network Slice consumer's request from 3GPP mobile network slice management system (including 5G Network Slice Orchestrator, external Controller), the IETF Network Slice Provider (i.e., IETF Network Slice Controller) needs to authenticate the slice request of a resource. After successful mutual authentication, the IETF Network Slice Controller would authorize the slice consumer before processing the IETF Network Slice service request. The MMI interface as the transmission channel interface between IETF Network Slice consumer (e.g., 5G Network Slice Orchestrator) and IETF Network Slice Provider (i.e., IETF Network Slice Controller), needs to support mutual authentication and authorization mechanism to the IETF Network Slice consumer. At the same time, the MMI interface should support confidentiality protection and integrity protection of data objects.

11.2 Requirements for MMI Interface

Clause 15 of 3GPP TS 33.501 [24] requires that a transport service request between the 3GPP network slice management system and an external untrusted domain (e.g., IETF Network Slice Controller) can be authenticated. Hence the requirement for the MMI:

[R-24]   The MMI interface MUST support TLS (Transport Layer Security) authentication mechanism, refer to RFC 8446 [9].

[R-25]   The MMI interface MUST support data integrity protection.

[R-26]   The MMI interface MUST support data confidentiality protection.

[R-27]   The MMI interface MUST support authorization mechanism.

For example, authorization can be provided using principles and mechanisms specified in the OAuth 2.0 Authorization framework (reference to RFC 6749 [13]), or a local management policy to control the authorization of IETF Network Slice consumers who request an IETF Network Slice service.

End of Broadband Forum Technical Report WT-522