Network Working Group
Internet-Draft
Intended status: Informational
Expires: October 16, 2021

A. Farrel, Ed.
Old Dog Consulting
E. Gray
Ericsson
J. Drake
Juniper Networks
R. Rokui
Nokia
S. Homma
NTT
K. Makhijani
Futurewei
LM. Contreras
Telefonica
J. Tantsura
Juniper Networks

April 14, 2021

Framework for IETF Network Slices
draft-ietf-teas-ietf-network-slices-00

Abstract

<FAb>

This memo discusses setting up special-purpose network connections using existing IETF technologies. These connections are called IETF network slices for the purposes of this memo. The memo discusses the general framework for this setup, the necessary system components and interfaces, and how abstract requests can be mapped to more specific technologies. The memo also discusses related considerations with monitoring and security.

This memo is intended for discussing interfaces and technologies. It is not intended to be a new set of concrete interfaces or technologies. Rather, it should be seen as an explanation of how some existing, concrete IETF VPN and traffic-engineering technologies can be used to create IETF network slices. Note that there are a number of these technologies, and new technologies or capabilities keep being added. This memo is also not intended presume any particular technology choice.

<DAb>

This document provides a definition of the term "IETF Network Slice" for use within the IETF and specifically as a reference for other IETF documents that describe or use aspects of network slices.

The document also describes the characteristics of an IETF network slice, related terms and their meanings, and explains how IETF network slices can be used in combination with end-to-end network slices or independent of them.

Status of This Memo

This Internet-Draft will expire on October 16, 2021.

Copyright Notice

Table of Contents

1. Introduction

===================== EDITOR'S NOTE =====================

This document is a merge of the text in [I-D.ietf-teas-ietf-network-slice-definition] and [I-D.ietf-teas-ietf-network-slice-framework]. In this version, the text is presented as a simple inclusion of all text from the contributing documents. The only work performed by the Editor in this revision is the assignment of text to the sections of the document, and the marking of the text to indicate its origin, as well as simple editorial fixes to resolve the most basic typographic and formatting issues.

For this purpose, the text in this revision is tagged to show its origin using the format <D1.3> or <F2.4> where the letters 'D' and 'F' indicate the definitions draft [I-D.ietf-teas-ietf-network-slice-definition] and the framework draft

[I-D.ietf-teas-ietf-network-slice-framework] respectively, and the subsequent numbers indicate the the section of the source document.

In the case that the source text is not used within the document, it is presented in Appendix A.

It is expected that this is a short term measure and that later revisions will be presented as text in its own right.

=================== END EDITOR'S NOTE ===================

<D1.>

A number of use cases benefit from network connections that along with the connectivity provide assurance of meeting a specific set of objectives wrt network resources use. In this document, as detailed in the subsequent sections, we refer to this connectivity and resource commitment as an IETF Network Slice. Services that might benefit from the network slices include but not limited to:

o 5G services (e.g. eMBB, URLLC, mMTC)(See [TS23501])

o Network wholesale services

o Network infrastructure sharing among operators

o NFV connectivity and Data Center Interconnect

The use cases are further described in [I-D.ietf-teas-ietf-network-slice-framework].

This document defines the concept of IETF network slices that provide connectivity coupled with a set of specific commitments of network resources between a number of endpoints over a shared network infrastructure. Since the term network slice is rather generic, the qualifying term 'IETF' is used in this document to limit the scope of network slice to network technologies described and standardized by the IETF.

IETF network slices are created and managed within the scope of one or more network technologies (e.g., IP, MPLS, optical). They are intended to enable a diverse set of applications that have different requirements to coexist on the shared network infrastructure. A request for an IETF network slice is technology-agnostic so as to allow a consumer to describe their network connectivity objectives in a common format, independent of the underlying technologies used.

<F1.>

This document provides a framework for discussing IETF network slices, as defined in [I-D.ietf-teas-ietf-network-slice-definition]. It is the intention in this document to use terminology consistent with this and other definitions provided in that document.

In particular, this document uses the following terminology defined in the definitions document:

- IETF Network Slice

- IETF Network Slice Controller (NSC)

- Network Controller (NC)

- Northbound Interface (NBI)

- Southbound Interface (SBI)

This framework is intended as a structure for discussing interfaces and technologies. It is not intended to specify a new set of concrete interfaces or technologies. Rather, the idea is that existing or under-development IETF technologies (plural) can be used to realize the concepts expressed herein.

For example, virtual private networks (VPNs) have served the industry well as a means of providing different groups of users with logically isolated access to a common network. The common or base network that is used to provide the VPNs is often referred to as an underlay network, and the VPN is often called an overlay network. As an example technology, a VPN may in turn serve as an underlay network for IETF network slices.

Note: It is conceivable that extensions to these IETF technologies are needed in order to fully support all the ideas that can be implemented with slices, but at least in the beginning there is no plan for the creation of new protocols or interfaces.

Driven largely by needs surfacing from 5G, the concept of network slicing has gained traction ([NGMN-NS-Concept], [TS23501], [TS28530], and [BBF-SD406]). In [TS23501], Network Slice is defined as "a logical network that provides specific network capabilities and network characteristics", and 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." According to [TS28530], an end-to-end network slice consists of three major types of network segments: Radio Access Network (RAN), Transport Network (TN) and Core Network (CN). IETF network slice provides the required connectivity between different

entities in RAN and CN segments of an end-to-end network slice, with a specific performance commitment. For each end-to-end network slice, the topology and performance requirement on a consumer's use of IETF network slice can be very different, which requires the underlay network to have the capability of supporting multiple different IETF network slices.

While network slices are commonly discussed in the context of 5G, it is important to note that IETF network slices are a narrower concept, and focus primarily on particular network connectivity aspects. Other systems, including 5G deployments, may use IETF network slices as a component to create entire systems and concatenated constructs that match their needs, including end-to-end connectivity.

A IETF network slice could span multiple technologies and multiple administrative domains. Depending on the IETF network slice consumer's requirements, an IETF network slice could be isolated from other, often concurrent IETF network slices in terms of data, control and management planes.

The consumer expresses requirements for a particular IETF network slice by specifying what is required rather than how the requirement is to be fulfilled. That is, the IETF network slice consumer's view of a IETF network slice is an abstract one.

Thus, there is a need to create logical network structures with required characteristics. The consumer of such a logical network can require a degree of isolation and performance that previously might not have been satisfied by traditional overlay VPNs. Additionally, the IETF network slice consumer might ask for some level of control of their virtual networks, e.g., to customize the service paths in a network slice.

This document specifies a framework for the use of existing technologies as components to provide a IETF network slice service, and might also discuss (or reference) modified and potential new technologies, as they develop (such as candidate technologies described in section 5 of [I-D.ietf-teas-enhanced-vpn]).

2. Terms and Abbreviations

<D2.>

The terms and abbreviations used in this document are listed below.

o NS: Network Slice

o NSC: Network Slice Controller

- NBI: NorthBound Interface

- SBI: SouthBound Interface

- SLI: Service Level Indicator

- SLO: Service Level Objective

- SLA: Service Level Agreement

The above terminology is defined in greater details in the remainder of this document.

3. IETF Network Slice Objectives

<F2.>

It is intended that IETF network slices can be created to meet specific requirements, typically expressed as bandwidth, latency, latency variation, and other desired or required characteristics. Creation is initiated by a management system or other application used to specify network-related conditions for particular traffic flows.

And it is intended that, once created, these slices can be monitored, modified, deleted, and otherwise managed.

It is also intended that applications and components will be able to use these IETF network slices to move packets between the specified end-points in accordance with specified characteristics.

As an example of requirements that might apply to IETF network slices, see [I-D.ietf-teas-enhanced-vpn] (in particular, section 3).

3.1. Definition and Scope of IETF Network Slice

<D3.>

The definition of a network slice in IETF context is as follows:

An IETF network slice is a logical network topology connecting a number of endpoints using a set of shared or dedicated network resources that are used to satisfy specific Service Level Objectives (SLOs).

An IETF network slice combines the connectivity resource requirements and associated network behaviors such as bandwidth, latency, jitter, and network functions with other resource behaviors such as compute

and storage availability. IETF network slices are independent of the underlying infrastructure connectivity and technologies used. This is to allow an IETF network slice consumer to describe their network connectivity and relevant objectives in a common format, independent of the underlying technologies used.

IETF network slices may be combined hierarchically, so that a network slice may itself be sliced. They may also be combined sequentially so that various different networks can each be sliced and the network slices placed into a sequence to provide an end-to-end service. This form of sequential combination is utilized in some services such as in 3GPP's 5G network [TS23501].

An IETF network slice is technology-agnostic, and the means for IETF network slice realization can be chosen depending on several factors such as: service requirements, specifications or capabilities of underlying infrastructure. The structure and different characteristics of IETF network slices are described in the following sections.

Term "Slice" refers to a set of characteristics and behaviours that separate one type of user-traffic from another. IETF network slice assumes that an underlying network is capable of changing the configurations of the network devices on demand, through in-band signaling or via controller(s) and fulfilling all or some of SLOs to all of the traffic in the slice or to specific flows.

4. IETF Network Slice System Characteristics

<D4.>

The following subsections describe the characteristics of IETF network slices.

4.1. Objectives for IETF Network Slices

<D4.1.>

An IETF network slice is defined in terms of several quantifiable characteristics or service level objectives (SLOs). SLOs along with terms Service Level Indicator (SLI) and Service Level Agreement (SLA) are used to define the performance of a service at different levels.

A Service Level Indicator (SLI) is a quantifiable measure of an aspect of the performance of a network. For example, it may be a measure of throughput in bits per second, or it may be a measure of latency in milliseconds.

A Service Level Objective (SLO) is a target value or range for the measurements returned by observation of an SLI. For example, an SLO may be expressed as "SLI <= target", or "lower bound <= SLI <= upper bound". A network slice is expressed in terms of the set of SLOs that are to be delivered for the different connections between endpoints.

A Service Level Agreement (SLA) is an explicit or implicit contract between the consumer of an IETF network slice and the provider of the slice. The SLA is expressed in terms of a set of SLOs and may include commercial terms as well as the consequences of missing/ violating the SLOs they contain.

Additional descriptions of IETF network slice attributes is covered in [I-D.contreras-teas-slice-nbi].

4.1.1. Service Level Objectives

<D4.1.1.>

SLOs define a set of network attributes and characteristics that describe an IETF network slice. SLOs do not describe 'how' the IETF network slices are implemented or realized in the underlying network layers. Instead, they are defined in terms of dimensions of operation (time, capacity, etc.), availability, and other attributes. An IETF network slice can have one or more SLOs associated with it. The SLOs are combined in an SLA. The SLOs are defined for sets of two or more endpoints and apply to specific directions of traffic flow. That is, they apply to specific source endpoints and specific connections between endpoints within the set of endpoints and connections in the network slice.

4.1.2. Minimal Set of SLOs

<D4.1.2.>

This document defines a minimal set of SLOs and later systems or standards could extend this set as per Section 4.1.3.

SLOs can be categorized in to 'Directly Measurable Objectives' or 'Indirectly Measurable Objectives'. Objectives such as guaranteed minimum bandwidth, guaranteed maximum latency, maximum permissible delay variation, maximum permissible packet loss rate, and availability are 'Directly Measurable Objectives'. While 'Indirectly Measurable Objectives' include security, geographical restrictions, maximum occupancy level objectives. The later standard might define other SLOs as needed.

Editor's Note TODO: replace Minimal set to most commonly used objectives to describe network behavior. Other directly or indirectly measurable objectives may be requested by that consumer of an IETF network slice.

The definition of these objectives are as follows:

Guaranteed Minimum Bandwidth

Minimum guaranteed bandwidth between two endpoints at any time. The bandwidth is measured in data rate units of bits per second and is measured unidirectionally.

Guaranteed Maximum Latency

Upper bound of network latency when transmitting between two endpoints. The latency is measured in terms of network characteristics (excluding application-level latency). [RFC2681] and [RFC7679] discuss round trip times and one-way metrics, respectively.

Maximum Permissible Delay Variation

Packet delay variation (PDV) as defined by [RFC3393], is the difference in the one-way delay between sequential packets in a flow. This SLO sets a maximum value PDV for packets between two endpoints.

Maximum permissible packet loss rate

The ratio of packets dropped to packets transmitted between two endpoints over a period of time. See [RFC7680].

Availability

The ratio of uptime to the sum of uptime and downtime, where uptime is the time the IETF network slice is available in accordance with the SLOs associated with it.

Security

An IETF network slice consumer may request that the network applies encryption or other security techniques to traffic flowing between endpoints.

Note that the use of security or the violation of this SLO is not directly observable by the IETF network slice consumer and cannot be measured as a quantifiable metric.

Also note that the objective may include request for encryption (e.g., [RFC4303]) between the two endpoints explicitly to meet architecture recommendations as in [TS33.210] or for compliance with [HIPAA] and/or [PCI].

Editor's Note: Please see more discussion on security in Section 9.

4.1.3. Other Objectives

<D4.1.3.>

Additional SLOs may be defined to provide additional description of the IETF network slice that a consumer requests.

If the IETF network slice consumer service is traffic aware, other traffic specific characteristics may be valuable including MTU, traffic-type (e.g., IPv4, IPv6, Ethernet or unstructured), or a higher-level behavior to process traffic according to user-application (which may be realized using network functions).

Maximal occupancy for an IETF network slice should be provided. Since it carries traffic for multiple flows between the two endpoints, the objectives should also say if they are for the entire connection, group of flows or on per flow basis. Maximal occupancy should specify the scale of the flows (i.e., maximum number of flows to be admitted) and optionally a maximum number of countable resource units, e.g., IP or MAC addresses a slice might consume.

4.2. IETF Network Slice Endpoints

<D4.2.>

As noted in Section 3.1, an IETF network slice describes connectivity between multiple endpoints across the underlying network. These connectivity types are: point-to-point, point-to-multipoint, multipoint-to-point multipoint-to-point, or multipoint-to-multipoint.

Figure 1 shows an IETF network slice along with its NSEs.

The characteristics of IETF network slice endpoints (NSEs) are as follows:

- The IETF network slice endpoints (NSEs) are conceptual points of connection to IETF network slice. As such, they serve as the IETF network slice ingress/egress points.

- Each endpoint could map to a device, application or a network function. A non-exhaustive list of devices, applications or network functions might include but not limited to: routers, switches, firewalls, WAN, 4G/5G RAN nodes, 4G/5G Core nodes, application acceleration, Deep Packet Inspection (DPI), server load balancers, NAT44 [RFC3022], NAT64 [RFC6146], HTTP header enrichment functions, and TCP optimizers.

- An NSE should be identified by a unique ID in the context of an IETF network slice consumer.

- In addition to an identifier, each NSE should contain a subset of attributes such as IPv4/IPv6 addresses, encapsulation type (i.e., VLAN tag, MPLS Label etc.), interface/port numbers, node ID etc.

- A combination of NSE unique ID and NSE attributes defines an NSE in the context of the IETF network slice controller.

- During the realization of the IETF network slice, in addition to SLOs, all or subset of IETF NSE attributes will be utilized by IETF network slice controller (NSC) to find the optimal realization in the IETF network.

- Similarly to IETF network slices, the IETF network slice endpoints are logical entities that are mapped to services/tunnels/paths endpoints in IETF network slice during its initialization and realization.

Note that there are various IETF TE terms such as access points (AP) defined in [RFC8453], Termination Point (TP) defined in [RFC8345], and Link Termination Point (LTP) defined in [RFC8795] which are tightly coupled with TE network type and various realization techniques. At the time of realization of the IETF network slice, the NSE could be mapped to one or more of these based on the network slice realization technique in use.

```
                        |----------------------------------|
                   NSE1 |                                  | NSE2
                  O.....|                                  |.....O
                    .   |                                  |  .
                    .   |                                  |  .
                    .   |                                  |  .
                        |                                  |
                   NSEm |                                  | NSEn
                  O.....|                                  |.....O
                        |                                  |
                        |----------------------------------|

                  <------------ IETF Network Slice -------------->
                           between endpoints NSE1 to NSEn

            Legend:
                 NSE: IETF Network Slice Endpoint
                   O: Represents IETF Network Slice Endpoints
```

Figure 1: An IETF Network Slice Endpoints (NSE)

4.2.1. IETF Network Slice Connectivity Types

<D4.2.1.>

The IETF Network Slice connection types can be point to point (P2P), point to multipoint (P2MP), multi-point to point (MP2P), or multi-point to multi-point (MP2MP). They will requested by the higher level operation system.

4.3. IETF Network Slice Composition

<D4.3.>

Operationally, an IETF network slice may be decomposed in two or more IETF network slices as specified below. Decomposed network slices are then independently realized and managed.

- Hierarchical (i.e., recursive) composition: An IETF network slice can be further sliced into other network slices. Recursive composition allows an IETF network slice at one layer to be used by the other layers. This type of multi-layer vertical IETF network slice associates resources at different layers.

- Sequential composition: Different IETF network slices can be placed into a sequence to provide an end-to-end service. In

sequential composition, each IETF network slice would potentially support different dataplanes that need to be stitched together.

5. Framework

<F3.>

A number of IETF network slice services will typically be provided over a shared underlying network infrastructure. Each IETF network slice consists of both the overlay connectivity and a specific set of dedicated network resources and/or functions allocated in a shared underlay network to satisfy the needs of the IETF network slice consumer. In at least some examples of underlying network technologies, the integration between the overlay and various underlay resources is needed to ensure the guaranteed performance requested for different IETF network slices.

IETF Network Slice Definition ([I-D.ietf-teas-ietf-network-slice-definition] defines the role of a Customer (or User) and a IETF Network Slice Controller. That document also defines a NSC Northbound Interface (NBI).

A IETF network slice user is served by the IETF Network Slice Controller (NSC), as follows:

- The NSC takes requests from a management system or other application, which are then communicated via an NBI. This interface carries data objects the IETF network slice user provides, describing the needed IETF network slices in terms of topology, applicable service level objectives (SLO), and any monitoring and reporting requirements that may apply. Note that - in this context - "topology" means what the IETF network slice connectivity is meant to look like from the user's perspective; it may be as simple as a list of mutually (and symmetrically) connected end points, or it may be complicated by details of connection asymmetry, per-connection SLO requirements, etc.

- These requests are assumed to be translated by one or more underlying systems, which are used to establish specific IETF network slice instances on top of an underlying network infrastructure.

- The NSC maintains a record of the mapping from user requests to slice instantiations, as needed to allow for subsequent control functions (such as modification or deletion of the requested slices), and as needed for any requested monitoring and reporting functions.

Section 3 of [I-D.ietf-teas-enhanced-vpn] provides an example architecture that might apply in using the technology described in that document.

5.1. IETF Network Slice Stakeholders

<D6.>

An IETF network slice and its realization involves the following stakeholders and it is relevant to define them for consistent terminology.

Consumer: A consumer is the requester of an IETF network slice. Consumers may request monitoring of SLOs. A consumer may manage the IETF network slice service directly by interfacing with the IETF network slice controller or indirectly through an orchestrator.

Orchestrator: An orchestrator is an entity that composes different services, resource and network requirements. It interfaces with the IETF network slice controllers.

IETF Network Slice Controller (NSC): It realizes an IETF network lice in the underlying network, maintains and monitors the run-time state of resources and topologies associated with it. A well-defined interface is needed between different types of IETF network slice controllers and different types of orchestrators. An IETF network slice operator (or slice operator for short) manages one or more IETF network slices using the IETF network slice Controller(s).

Network Controller: is a form of network infrastructure controller that offers network resources to NSC to realize a particular network slice. These may be existing network controllers associated with one or more specific technologies that may be adapted to the function of realizing IETF network slices in a network.

5.2. Management Systems or Other Applications

<F3.1.>

The IETF network slice system is used by a management system or other application. These systems and applications may also be a part of a higher level function in the system, e.g., putting together network functions, access equipment, application specific components, as well as the IETF network slices.

5.3. Expressing Connectivity Intents

<F3.2.>

The IETF Network Slice Controller (NSC) northbound interface (NBI) can be used to communicate between IETF network slice users (or consumers) and the NSC.

A IETF network slice user may be a network operator who, in turn, provides the IETF network slice to another IETF network slice user or consumer.

Using the NBI, a consumer expresses requirements for a particular slice by specifying what is required rather than how that is to be achieved. That is, the consumer's view of a slice is an abstract one. Consumers normally have limited (or no) visibility into the provider network's actual topology and resource availability information.

This should be true even if both the consumer and provider are associated with a single administrative domain, in order to reduce the potential for adverse interactions between IETF network slice consumers and other users of the underlay network infrastructure.

The benefits of this model can include:

- Security: because the underlay network (or network operator) does not need to expose network details (topology, capacity, etc.) to IETF network slice consumers the underlay network components are less exposed to attack;

- Layered Implementation: the underlay network comprises network elements that belong to a different layer network than consumer applications, and network information (advertisements, protocols, etc.) that a consumer cannot interpret or respond to (note - a consumer should not use network information not exposed via the NSC NBI, even if that information is available);

- Scalability: consumers do not need to know any information beyond that which is exposed via the NBI.

The general issues of abstraction in a TE network is described more fully in [RFC7926].

This framework document does not assume any particular layer at which IETF network slices operate as a number of layers (including virtual L2, Ethernet or IP connectivity) could be employed.

Data models and interfaces are of course needed to set up IETF network slices, and specific interfaces may have capabilities that allow creation of specific layers.

Layered virtual connections are comprehensively discussed in IETF documents and are widely supported. See, for instance, GMPLS-based networks ([RFC5212] and [RFC4397]), or ACTN ([RFC8453] and [RFC8454]). The principles and mechanisms associated with layered networking are applicable to IETF network slices.

There are several IETF-defined mechanisms for expressing the need for a desired logical network. The NBI carries data either in a protocol-defined format, or in a formalism associated with a modeling language.

For instance:

- Path Computation Element (PCE) Communication Protocol (PCEP) [RFC5440] and GMPLS User-Network Interface (UNI) using RSVP-TE [RFC4208] use a TLV-based binary encoding to transmit data.

- Network Configuration Protocol (NETCONF) [RFC6241] and RESTCONF Protocol [RFC8040] use XML abnd JSON encoding.

- gRPC/GNMI [I-D.openconfig-rtgwg-gnmi-spec] uses a binary encoded programmable interface;

- SNMP ([RFC3417], [RFC3412] and [RFC3414] uses binary encoding (ASN.1).

- For data modeling, YANG ([RFC6020] and [RFC7950]) may be used to model configuration and other data for NETCONF, RESTCONF, and GNMI - among others; ProtoBufs can be used to model gRPC and GNMI data; Structure of Management Information (SMI) [RFC2578] may be used to define Management Information Base (MIB) modules for SNMP, using an adapted subset of OSI's Abstract Syntax Notation One (ASN.1, 1988).

While several generic formats and data models for specific purposes exist, it is expected that IETF network slice management may require enhancement or augmentation of existing data models.

5.4. IETF Network Slice Structure

<D5.>

Editor's note: This content of this section merged with Relationship with E2E slice discussion.

An IETF network slice is a set of connections among various endpoints to form a logical network that meets the SLOs agreed upon.

```
                 |------------------------------------------|
       NSE1 O....|                                          |....O NSE2
         .       |                                          |    .
         .       |             IETF Network  Slice          |    .
         .       |  (SLOs e.g.  B/W > x bps, Delay < y ms)  |    .
       NSEm O....|                                          |....O NSEn
                 |------------------------------------------|

       == == == == == == == == == == == == == == == == == == == == == ==

                         .--.               .--.
               [EP1]    (    )- .          (    )- .    [EP2]
                 .    .' IETF    '  SLO  .'  IETF   '     .
                 .   (  Network-1 ) ... (  Network-p )    .
                     `-----------'      `-----------'
               [EPm]                                    [EPn]

       Legend
         NSE: IETF Network Slice Endpoints
         EP:  Serivce/tunnels/path Endpoints used to realize the
              IETF Network Slice
```

Figure 2: IETF Network slice

Figure 2 illustrates a case where an IETF network slice provides connectivity between a set of IEFT network slice endpoints (NSE) pairs with specific SLOs (e.g., guaranteed minimum bandwidth of x bps and guaranteed delay of no more than y ms). The IETF network slice endpoints are mapped to the underlay IETF networks endpoints (EP). Also, the IETF network slice endpoints on the same IETF network slice may belong to the same or different address spaces.

IETF Network slice structure fits into a broader concept of end-to-end network slices. A network operator may be responsible for delivering services over a number of technologies (such as radio networks) and for providing specific and fine-grained services (such as CCTV feed or High definition realtime traffic data). That operator may need to combine slices of various networks to produce an end-to-end network service. Each of these networks may include multiple physical or virtual nodes and may also provide network functions beyond simply carrying of technology-specific protocol data units. An end-to-end network slice is defined by the 3GPP as a

complete logical network that provides a service in its entirety with a specific assurance to the consumer [TS23501].

An end-to-end network slice may be composed from other network slices that include IETF network slices. This composition may include the hierarchical (or recursive) use of underlying network slices and the sequential (or stitched) combination of slices of different networks.

5.5. IETF Network Slice Controller (NSC)

<F3.3.>

The IETF Network Slice Controller takes abstract requests for IETF network slices and implements them using a suitable underlying technology. A IETF Network Slice Controller is the key building block for control and management of the IETF network slice. It provides the creation/modification/deletion, monitoring and optimization of IETF network slices in a multi-domain, a multi-technology and multi-vendor environment.

A NSC northbound interface (NBI) is needed for communicating details of a IETF network slice (configuration, selected policies, operational state, etc.), as well as providing information to a slice requester/consumer about IETF network slice status and performance. The details for this NBI are not in scope for this document.

The controller provides the following functions:

- Provides a technology-agnostic NBI for creation/modification/deletion of the IETF network slices. The API exposed by this NBI communicates the endpoints of the IETF network slice, IETF network slice SLO parameters (and possibly monitoring thresholds), applicable input selection (filtering) and various policies, and provides a way to monitor the slice.

- Determines an abstract topology connecting the endpoints of the IETF network slice that meets criteria specified via the NBI.The NSC also retains information about the mapping of this abstract topology to underlying components of the IETF network slice as necessary to monitor IETF network slice status and performance.

- Provides "Mapping Functions" for the realization of IETF network slices. In other words, it will use the mapping functions that:

  * map technology-agnostic NBI request to technology-specific SBIs

  * map filtering/selection information as necessary to entities in the underlay network.

- Via an SBI, the controller collects telemetry data (e.g., OAM results, statistics, states etc.) for all elements in the abstract topology used to realize the IETF network slice.

- Using the telemetry data from the underlying realization of a IETF network slice (i.e. services/paths/tunnels), evaluates the current performance against IETF network slice SLO parameters and exposes them to the IETF network slice consumer via the NBI. The NSC NBI may also include a capability to provide notification in case the IETF network slice performance reaches threshold values defined by the IETF network slice consumer.

5.5.1. IETF Network Slice Controller Interfaces

<D7.>

The interworking and interoperability among the different stakeholders to provide common means of provisioning, operating and monitoring the IETF network slices is enabled by the following communication interfaces (see Figure 3).

NSC Northbound Interface (NBI): The NSC Northbound Interface is an interface between a consumer's higher level operation system (e.g., a network slice orchestrator) and the NSC. It is a technology agnostic interface. The consumer can use this interface to communicate the requested characteristics and other requirements (i.e., the SLOs) for the IETF network slice, and the NSC can use the interface to report the operational state of an IETF network slice to the consumer.

NSC Southbound Interface (SBI): The NSC Southbound Interface is an interface between the NSC and network controllers. It is technology-specific and may be built around the many network models defined within the IETF.

```
        +------------------------------------------+
        | Consumer higher level operation system   |
        |   (e.g E2E network slice orchestrator)   |
        +------------------------------------------+
                             A
                             | NSC NBI
                             V
        +------------------------------------------+
        |    IETF Network Slice Controller (NSC)   |
        +------------------------------------------+
                             A
                             | NSC SBI
                             V
        +------------------------------------------+
        |           Network Controllers            |
        +------------------------------------------+
```

Figure 3: Interface of IETF Network Slice Controller

5.5.2. Northbound Interface (NBI)

<F3.3.1.>

The IETF Network Slice Controller provides a Northbound Interface (NBI) that allows consumers of network slices to request and monitor IETF network slices. Consumers operate on abstract IETF network slices, with details related to their realization hidden.

The NBI complements various IETF services, tunnels, path models by providing an abstract layer on top of these models.

The NBI is independent of type of network functions or services that need to be connected, i.e., it is independent of any specific storage, software, protocol, or platform used to realize physical or virtual network connectivity or functions in support of IETF network slices.

The NBI uses protocol mechanisms and information passed over those mechanisms to convey desired attributes for IETF network slices and their status. The information is expected to be represented as a well-defined data model, and should include at least endpoint and connectivity information, SLO specification, and status information.

To accomplish this, the NBI needs to convey information needed to support communication across the NBI, in terms of identifying the IETF network slices, as well providing the above model information.

5.6. Mapping

<F3.4.>

The main task of the IETF network slice controller is to map abstract IETF network slice requirements to concrete technologies and establish required connectivity, and ensuring that required resources are allocated to the IETF network slice.

5.7. Realizing IETF Network Slice

<D8.>

Realization of IETF network slices is out of scope of this document. It is a mapping of the definition of the IETF network slice to the underlying infrastructure and is necessarily technology-specific and achieved by the NSC over the SBI.

The realization can be achieved in a form of either physical or logical connectivity through VPNs (see, for example, [I-D.ietf-teas-enhanced-vpn], a variety of tunneling technologies such as Segment Routing, MPLS, etc. Accordingly, endpoints may be realized as physical or logical service or network functions.

5.7.1. Underlying Technology

<F3.5.>

There are a number of different technologies that can be used, including physical connections, MPLS, TSN, Flex-E, etc.

See Section 5 of [I-D.ietf-teas-enhanced-vpn] for instance, for example underlying technologies.

Also, as outlined in "applicability of ACTN to IETF Network Slices" below, ACTN ([RFC8453]) offers a framework that is used elsewhere in IETF specifications to create virtual network (VN) services similar to IETF network slices.

A IETF network slice can be realized in a network, using specific underlying technology or technologies. The creation of a new IETF network slice will be initiated with following three steps:

- Step 1: A higher level system requests connections with specific characteristics via NBI.

- Step 2: This request will be processed by a IETF Network Slice Controller which specifies a mapping between northbound request to any IETF Services, Tunnels, and paths models.

- Step 3: A series of requests for creation of services, tunnels and paths will be sent to the network to realize the trasport slice.

It is very clear that regardless of how IETF network slice is realized in the network (i.e., using tunnels of type RSVP or SR), the definition of IETF network slice does not change at all but rather its realization.

6. Applicability of ACTN to IETF Network Slices

<F4.>

Abstraction and Control of TE Networks (ACTN - [RFC8453]) is an example of similar IETF work. ACTN defines three controllers to support virtual network (VN) services -

- Customer Network Controller (CNC),

- Multi-Domain Service Coordinator (MDSC) and

- Provisioning Network Controller (PNC).

A CNC is responsible for communicating a customer's VN requirements.

A MDSC is responsible for multi-domain coordination, virtualization (or abstraction), customer mapping/translation and virtual service coordination to realize the VN requirement. Its key role is to detach the network/service requirements from the underlying technology.

A PNC oversees the configuration, monitoring and collection of the network topology. The PNC is a underlay technology specific controller.

While the ACTN framework is a generic VN framework that is used for various VN service beyond the IETF network slice, it is still a suitable basis to understand how the various controllers interact to realize a IETF network slice.

One possible mapping between the IETF network slice, and ACTN, definitions is as shown in Figure 4.

```
                   IETF Network Slice                |   ACTN analogous
                 Terminology / Concepts                  Terminology
                                                     |    and Concepts
          +--------------------------------------+
          |Consumer higher level operation system|   |    +-----+
          | (e.g E2E network slice orchestrator) | =====> | CNC |
          +--------------------------------------+   |    +-----+
                            ^                                ^
                            | NSC NBI                |       | CMI
                            v                                v
          +-------------------------------------+    |    +-------+
          | IETF Network Slice Controller (NSC) |  =====> | MDSC |
          +-------------------------------------+    |    +-------+
                            ^                                ^
                            | NSC SBI                |       | MPI
                            v                                v
          +-------------------------------------+    |    +-----+
          |        Network Controller(s)        |  =====> | PNC |
          +-------------------------------------+    |    +-----+
```

Figure 4: Mapping between IETF network slices and ACTN

Note that the left-hand side of this figure comes from IETF Network Slice Definition ([I-D.ietf-teas-ietf-network-slice-definition]).

The NSC NBI conveys the generic IETF network slice requirements. These may then be realized using an SBI within the NSC.

As per [RFC8453] and [I-D.ietf-teas-actn-yang], the CNC-MDSC Interface (CMI) is used to convey the virtual network service requirements along with the service models and the MDSC-PNC Interface (MPI) is used to realize the service along network configuration models. [I-D.ietf-teas-te-service-mapping-yang] further describe how the VPN services can be mapped to the underlying TE resources.

The Network Controller is depicted as a single block, analogous to a Provisioning Network Controller (PNC - in this example). In the ACTN framework, however, it is also possible that the NC function is decomposed into MDSC and PNC - that is, the NC may comprise hierarchy as needed to handle the multiple domains and various underlay technologies, whereas a PNC in ACTN is intended to be specific to at most a single underlay technology and (likely) to individual devices (or functional components).

Note that the details of potential implementations of everything that is below the NSC in Section 6 are out of scope in this document - hence the specifics of the relationship between NC and PNC, and the

possibility that the MDSC and PNC may be combined are at most academically interesting in this context. Another way to view this is that, in the same way that ACTN might combine MDSC and PNC, the NSC might also directly include NC functionality.

[RFC8453] also describes TE Network Slicing in the context of ACTN as a collection of resources that is used to establish a logically dedicated virtual network over one or more TE networks. In case of TE enabled underlying network, ACTN VN can be used as a base to realize the IETF network slicing by coordination among multiple peer domains as well as underlay technology domains.

Section 6 shows only one possible mapping as each ACTN component (or interface) in the figure may be a composed differently in other mappings, and the exact role of both components and subcomponents will not be always an exact analogy between the concepts used in this document and those defined in ACTN.

This is - in part - shown in a previous paragraph in this section where it is pointed out that the NC may actually subsume some aspects of both the MDSC and PNC.

Similarly, in part depending on how "customer" is interpreted, CNC might merge some aspects of the higher level system and the NSC. As in the NC/PNC case, this way of comparing ACTN to this work is not useful as the NSC and NSC NBI are the focus on this document.

7. Isolation in IETF Network Slices

<D9.>

An IETF network slice consumer may request, that the IETF Network Slice delivered to them is isolated from any other network slices of services delivered to any other consumers. It is expected that the changes to the other network slices of services do not have any negative impact on the delivery of the IETF network slice.

7.1. Isolation as a Service Requirement

<D9.1.>

Isolation may be an important requirement of IETF network slices for some critical services. A consumer may express this request as an SLO.

This requirement can be met by simple conformance with other SLOs. For example, traffic congestion (interference from other services) might impact on the latency experienced by an IETF network slice.

Thus, in this example, conformance to a latency SLO would be the primary requirement for delivery of the IETF network slice service, and isolation from other services might be only a means to that end.

It should be noted that some aspects of isolation may be measurable by a consumer who have the information about the traffic on a number of IETF network slices or other services.

7.2. Isolation in IETF Network Slice Realization

<D9.2.>

Delivery of isolation is achieved in the realization of IETF network slices, with existing, in-development, and potential new technologies in IETF. It depends on how a network operator decides to operate their network and deliver services.

Isolation may be achieved in the underlying network by various forms of resource partitioning ranging from dedicated allocation of resources for a specific IETF network slice, to sharing or resources with safeguards. For example, traffic separation between different IETF network slices may be achieved using VPN technologies, such as L3VPN, L2VPN, EVPN, etc. Interference avoidance may be achieved by network capacity planning, allocating dedicated network resources, traffic policing or shaping, prioritizing in using shared network resources, etc. Finally, service continuity may be ensured by reserving backup paths for critical traffic, dedicating specific network resources for a selected number of network slices, etc.

8. Management Considerations

<F5.1.>

IETF network slice realization needs to be instrumented in order to track how it is working, and it might be necessary to modify the IETF network slice as requirements change. Dynamic reconfiguration might be needed.

9. Security Considerations

<D10.>

This document specifies terminology and has no direct effect on the security of implementations or deployments. In this section, a few of the security aspects are identified.

- Conformance to security constraints: Specific security requests from consumer defined IETF network slices will be mapped to their

realization in the unerlay networks. It will be required by underlay networks to have capabilities to conform to consumer's requests as some aspects of security may be expressed in SLOs.

- IETF network slice controller authentication: Unerlying networks need to be protected against the attacks from an adversary NSC as they can destablize overall network operations. It is particularly critical since an IETF network slice may span across different networks, therefore, IETF NSC should have strong authentication with each those networks. Futhermore, both SBI and NBI need to be secured.

- Specific isolation criteria: The nature of conformance to isolation requests means that it should not be possible to attack an IETF network slice service by varying the traffic on other services or slices carried by the same underlay network. In general, isolation is expected to strengthen the IETF network slice security.

- Data Integrity of an IETF network slice: A consumer wanting to secure their data and keep it private will be responsible for applying appropriate security measures to their traffic and not depending on the network operator that provides the IETF network slice. It is expected that for data integrity, a consumer is responsible for end-to-end encryption of its own traffic.

Note: see NGMN document[NGMN_SEC] on 5G network slice security for discussion relevant to this section.

<F5.2.>

IETF network slices might use underlying virtualized networking. All types of virtual networking require special consideration to be given to the separation of traffic between distinct virtual networks, as well as some degree of protection from effects of traffic use of underlying network (and other) resources from other virtual networks sharing those resources.

For example, if a service requires a specific upper bound of latency, then that service can be degraded by added delay in transmission of service packets through the activities of another service or application using the same resources.

Similarly, in a network with virtual functions, noticeably impeding access to a function used by another IETF network slice (for instance, compute resources) can be just as service degrading as delaying physical transmission of associated packet in the network.

While a IETF network slice might include encryption and other security features as part of the service, consumers might be well advised to take responsibility for their own security needs, possibly by encrypting traffic before hand-off to a service provider.

9.1. Privacy Considerations

<F5.3.>

Privacy of IETF network slice service consumers must be preserved. It should not be possible for one IETF network slice consumer to discover the presence of other consumers, nor should sites that are members of one IETF network slice be visible outside the context of that IETF network slice.

In this sense, it is of paramount importance that the system use the privacy protection mechanism defined for the specific underlying technologies used, including in particular those mechanisms designed to preclude acquiring identifying information associated with any IETF network slice consumer.

10. IANA Considerations

<F5.4.>

There are no requests to IANA in this framework document.

11. Acknowledgments

<D12.>

The entire TEAS NS design team and everyone participating in those discussion has contributed to this draft. Particularly, Eric Gray, Xufeng Liu, Jie Dong, Adrian Farrel, and Jari Arkko for a thorough review among other contributions.

<F6.>

The entire TEAS NS design team and everyone participating in related discussions has contributed to this document. Some text fragments in the document have been copied from the [I-D.ietf-teas-enhanced-vpn], for which we are grateful.

Significant contributions to this document were gratefully received from the contributing authors listed in the "Contributors" section. In addition we would like to also thank those others who have attended one or more of the design team meetings, including:

- Aihua Guo

- Bo Wu

- Greg Mirsky

- Jeff Tantsura

- Kiran Makhijani

- Lou Berger

- Luis M. Contreras

- Rakesh Gandhi

- Ran Chen

- Sergio Belotti

- Shunsuke Homma

- Stewart Bryant

- Tomonobu Niwa

- Xuesong Geng

12. Contributors

The following authors contributed significantly to this document:

Jari Arkko
Ericsson
Email: jari.arkko@piuha.net

Dhruv Dhody
Huawei, India
Email: dhruv.ietf@gmail.com

Jie Dong
Huawei
Email: jie.dong@huawei.com

Xufeng Liu
Volta Networks
Email: xufeng.liu.ietf@gmail.com

13. References

13.1. Normative References

[I-D.ietf-teas-ietf-network-slice-definition]
Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "Definition of IETF Network Slices", draft-ietf-teas-ietf-network-slice-definition-00 (work in progress), January 2021.

[I-D.ietf-teas-ietf-network-slice-framework]
Gray, E. and J. Drake, "Framework for IETF Network Slices", draft-ietf-teas-ietf-network-slice-framework-00 (work in progress), March 2021.

13.2. Informative References

[BBF-SD406]
Broadband Forum, ., "End-to-end network slicing", BBF SD-406 , n.d..

[HIPAA] HHS, "Health Insurance Portability and Accountability Act - The Security Rule", February 2003, <https://www.hhs.gov/hipaa/for-professionals/security/index.html>.

[I-D.contreras-teas-slice-nbi]
Contreras, L., Homma, S., and J. Ordonez-Lucena, "IETF Network Slice use cases and attributes for Northbound Interface of controller", draft-contreras-teas-slice-nbi-03 (work in progress), October 2020.

[I-D.ietf-teas-actn-yang]
Lee, Y., Zheng, H., Ceccarelli, D., Yoon, B., Dios, O., Shin, J., and S. Belotti, "Applicability of YANG models for Abstraction and Control of Traffic Engineered Networks", draft-ietf-teas-actn-yang-06 (work in progress), August 2020.

[I-D.ietf-teas-enhanced-vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Networks (VPN+) Service", draft-ietf-teas-enhanced-vpn-06 (work in progress), July 2020.

[I-D.ietf-teas-te-service-mapping-yang]
Lee, Y., Dhody, D., Fioccola, G., WU, Q., Ceccarelli, D., and J. Tantsura, "Traffic Engineering (TE) and Service Mapping Yang Model", draft-ietf-teas-te-service-mapping-yang-05 (work in progress), November 2020.

[I-D.openconfig-rtgwg-gnmi-spec]
Shakir, R., Shaikh, A., Borman, P., Hines, M., Lebsack, C., and C. Morrow, "gRPC Network Management Interface (gNMI)", draft-openconfig-rtgwg-gnmi-spec-01 (work in progress), March 2018.

[NGMN-NS-Concept]
NGMN Alliance, ., "Description of Network Slicing Concept", https://www.ngmn.org/uploads/media/161010_NGMN_Network_Slicing_framework_v1.0.8.pdf , 2016.

[NGMN_SEC]
NGMN Alliance, "NGMN 5G Security - Network Slicing", April 2016, <https://www.ngmn.org/wp-content/uploads/Publications/2016/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf>.

[PCI] PCI Security Standards Council, "PCI DSS", May 2018, <https://www.pcisecuritystandards.org>.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, DOI 10.17487/RFC2578, April 1999, <https://www.rfc-editor.org/info/rfc2578>.

[RFC2681] Almes, G., Kalidindi, S., and M. Zekauskas, "A Round-trip Delay Metric for IPPM", RFC 2681, DOI 10.17487/RFC2681, September 1999, <https://www.rfc-editor.org/info/rfc2681>.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, DOI 10.17487/RFC3022, January 2001, <https://www.rfc-editor.org/info/rfc3022>.

[RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", RFC 3393, DOI 10.17487/RFC3393, November 2002, <https://www.rfc-editor.org/info/rfc3393>.

[RFC3412] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, DOI 10.17487/RFC3412, December 2002, <https://www.rfc-editor.org/info/rfc3412>.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, DOI 10.17487/RFC3414, December 2002, <https://www.rfc-editor.org/info/rfc3414>.

[RFC3417] Presuhn, R., Ed., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, DOI 10.17487/RFC3417, December 2002, <https://www.rfc-editor.org/info/rfc3417>.

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and Y. Rekhter, "Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, DOI 10.17487/RFC4208, October 2005, <https://www.rfc-editor.org/info/rfc4208>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC4397] Bryskin, I. and A. Farrel, "A Lexicography for the Interpretation of Generalized Multiprotocol Label Switching (GMPLS) Terminology within the Context of the ITU-T's Automatically Switched Optical Network (ASON) Architecture", RFC 4397, DOI 10.17487/RFC4397, February 2006, <https://www.rfc-editor.org/info/rfc4397>.

[RFC5212] Shiomoto, K., Papadimitriou, D., Le Roux, JL., Vigoureux, M., and D. Brungard, "Requirements for GMPLS-Based Multi-Region and Multi-Layer Networks (MRN/MLN)", RFC 5212, DOI 10.17487/RFC5212, July 2008, <https://www.rfc-editor.org/info/rfc5212>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7679] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton, Ed., "A One-Way Delay Metric for IP Performance Metrics (IPPM)", STD 81, RFC 7679, DOI 10.17487/RFC7679, January 2016, <https://www.rfc-editor.org/info/rfc7679>.

[RFC7680] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton, Ed., "A One-Way Loss Metric for IP Performance Metrics (IPPM)", STD 82, RFC 7680, DOI 10.17487/RFC7680, January 2016, <https://www.rfc-editor.org/info/rfc7680>.

[RFC7926] Farrel, A., Ed., Drake, J., Bitar, N., Swallow, G., Ceccarelli, D., and X. Zhang, "Problem Statement and Architecture for Information Exchange between Interconnected Traffic-Engineered Networks", BCP 206, RFC 7926, DOI 10.17487/RFC7926, July 2016, <https://www.rfc-editor.org/info/rfc7926>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8345] Clemm, A., Medved, J., Varga, R., Bahadur, N., Ananthakrishnan, H., and X. Liu, "A YANG Data Model for Network Topologies", RFC 8345, DOI 10.17487/RFC8345, March 2018, <https://www.rfc-editor.org/info/rfc8345>.

[RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453, DOI 10.17487/RFC8453, August 2018, <https://www.rfc-editor.org/info/rfc8453>.

[RFC8454] Lee, Y., Belotti, S., Dhody, D., Ceccarelli, D., and B. Yoon, "Information Model for Abstraction and Control of TE Networks (ACTN)", RFC 8454, DOI 10.17487/RFC8454, September 2018, <https://www.rfc-editor.org/info/rfc8454>.

[RFC8795] Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Gonzalez de Dios, "YANG Data Model for Traffic Engineering (TE) Topologies", RFC 8795, DOI 10.17487/RFC8795, August 2020, <https://www.rfc-editor.org/info/rfc8795>.

[TS23501] 3GPP, ., "System architecture for the 5G System (5GS)", 3GPP TS 23.501 , 2019.

[TS28530] 3GPP, ., "Management and orchestration; Concepts, use cases and requirements", 3GPP TS 28.530 , 2019.

[TS33.210] 3GPP, "3G security; Network Domain Security (NDS); IP network layer security (Release 14).", December 2016, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279>.

Appendix A. Unused Material

This section includes material from the source documents that is not used in the body of this document. It is intended for deletion.

Authors' Addresses

Adrian Farrel (editor)
Old Dog Consulting

Email: adrian@olddog.co.uk

Eric Gray
Ericsson

Email: ewgray@graiymage.com

John Drake
Juniper Networks

Email: jdrake@juniper.net

Reza Rokui
Nokia

Email: reza.rokui@nokia.com

Shunsuke Homma
NTT

Email: shunsuke.homma.ietf@gmail.com

Kiran Makhijani
Futurewei

Email: kiranm@futurewei.com

Luis M. Contreras
Telefonica
Spain

Email: luismiguel.contrerasmurillo@telefonica.com

Jeff Tantsura
Juniper Networks

Email: jefftant.ietf@gmail.com