Network Working Group S. Barguil
Internet-Draft L.M. Contreras
Intended status: Informational Telefonica
Expires: 10 January 2022 V. Lopez
R. Rokui
Nokia
O. Gonzalez de Dios
Telefonica
9 July 2021

Instantiation of IETF Network Slices in service providers networks
draft-barguil-teas-network-slices-instantation-01

Abstract

The IETF has produced several YANG data models to support the Software-Defined Networking and Network Slice Architecture. This document describes the relationship between IETF Network Slice models utilized for requesting the IETF Network Slices and the Network Models (e.g. L3NM, L2NM) used during their realizations. This document describes the communication between the IETF Network Slice Controller and the network controllers for realization of IETF network slices.

The IETF Network Slice YANG model provides the customer-oriented view of the network slice. Thus, once the IETF Network Slice controller (NSC) receives a request, it needs to map it to accomplish the specific parameters expected by the network controllers. The network models are analyzed in terms of how they can satisfy the IETF Network Slice requirements. Identified gaps on existing models are reported.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The IETF has produced several YANG data models to support the Software-Defined Networking and Network Slice Architecture. This document describes the relationship between the IETF Network Slice models utilized for requesting the IETF Network Slices and the Network Models (e.g. L3NM, L2NM) used during their realizations. This document describes the communication between the IETF Network Slice Controller and the network controllers for realization of IETF network slices.

The IETF Network Slice YANG service model provides the customer-oriented view of the network slice. Once the IETF Network Slice controller (NSC)receives a request, it needs to map it to accomplish the specific parameters expected by the network controller. The network models are analyzed in terms of how they can satisfy the IETF Network Slice requirements. Identified gaps on existing models are reported.

Editor's Note: the terminology in this draft will be aligned with the final terminology selected for describing the notion of IETF Network Slice when applied to IETF technologies, which is currently under discussion. By now same terminology as used in [I-D.ietf-teas-ietf-network-slice-definition] and [I-D.nsdt-teas-ns-framework] is primarily used here. Consensus to use "IETF Network Slice" term has been reached.

1.1. Terminology

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

2. Reference architecture

As described in [I-D.ietf-teas-ietf-network-slice-definition], the IETF Network Slice Controller (NSC) is a functional entity for control and management of IETF network slices. As shown in Figure A, NSC from its Norht Bound Interface (NBI exposes set of APIs that allow a higher level system to request an IETF network slice. The NSC NBI supports the request for enablement of an IETF Network Slice (i.e., creation, modification or deletion). Upon receiving a request from its NBI, NSC finds the resources needed for realization of the IETF Network Slice and in turn interfaces from its South Bound Interface (SBI) with one or more Network Controllers for the realization of the requested IETF Network Slice.

This document focuses on how IETF Network Slice Controller (NSC) can be implemented in operator's network.

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

Figure 1 Network Slice Controller as a module of the Hierarchical SDN controller.

Several architectural definitions have arisen on the IETF to support SDN and network slicing deployments. The architectural proposal defined in [I-D.ietf-teas-ietf-network-slice-definition] includes a three-level hierarchy and expresses how each level relates with the ACTN architecture framework.

Figure 2 defines depicts a possible architecture using those concepts. It starts from a top consumer or high-level operational systems. Next, the IETF Network Slice Controller function migth be part of the Hierarchical network controller (e.g., as the MDSC in the ACTN context [RFC8453]) as a modular function. At the bottom, two network controllers, each one can handle multiple or single underlay technologies.

```
                  +------------------------------+
                  | High-level operation system. |
                  +--------------+---------------+
                                 |IETF Network Slice Request
                                 |
             +-------------------v------------------+
             |                                      |
             |    Hierarchical Network              |
             |    Controller/Orchestrator           |
             |                                      |
             |   +-------------------------------+  |
             |   | IETF Network Slice Controller |  |
             |   +-------------------------------+  |
             |                                      |
             +-------------------+------------------+
                                 |
                                 |
                  +--------------+---------------+
                  |                              |
                  v                              v
    +-------------+----------+     +-------------+----------+
    |   Network Controller   |     |   Network Controller   |
    +-------------+----------+     +-------------+----------+
                  |                              |
                  |                              |
                  v                              v
           Network Elements                Network Elements
```

Figure 2 IETF Network Slice Controller as a module of the Hierarchical SDN controller.

In other implementations, the IETF Network Slice Controller can be a stand-alone element and directly interact with the network controller, as depicted in Figure 2. In this scenario, the services request follows a data-enrichment path, where each entity adds more information to the service request. This document describes how the available service models and network models interact to deliver the network slices in a service provider environment.

```
              +-------------------------------+
              |  High-level operation system  |
              +-------------+-----------------+
                            |IETF Network Slice Request
                            |
              +-------------v-----------------+
              | IETF Network Slice Controller |
              +-------------+-----------------+
                            |
                            |
              +-------------v-----------------+
              |       Network Controller      |
              +-------------+-----------------+
                            |
                            |
                            v
                    Network Elements
```

Figure 3 The IETF Network Slice Controller as a stand-alone entity.

As another implementation possibility, the IETF Network Slice Controller can be integrated with the Network controller and directly realize the network slice using device data models to configure the network devices. The sample architecture is depicted in Figure 4.

```
              +-------------------------------+
              |  High-level operation system  |
              +-------------+-----------------+
                            |IETF Network Slice Request
                            |
              +-------------v----------------+
              |      Network Controller      |
              |                              |
              |+----------------------------+|
              ||   Network Slice Controller ||
              |+----------------------------+|
              |                              |
              +-------------+----------------+
                            |
                            |
                            v
                    Network Elements
```

Figure 4 IETF Network Slice Controller as a module of the Network controller.

3. IETF Network Slice: requirements and data models

The main set of requirements for the IETF Slice, based on the high-level slice requirements from multiple organizations and use cases, are compiled in [I-D.contreras-teas-slice-nbi] and reproduced bellow the slice use cases reported:

Network Slice Requirements for 5G service
Availability
Deterministic communication
Downlink throughput per network slice
Energy efficiency
Group communication support
Isolation level
Maximum supported packet size
Mission critical support
Performance monitoring
Slice quality of service parameters
Support for non-IP traffic
Uplink throughput per network slice
User data access
Delay tolerance

NFV-based services
Incoming and outgoing bandwidth
Qos metrics
Directionality
MTU
Protection scheme
Connectivity mode

Network sharing
Maximum and Guaranteed Bit Rate
Bounded latency
Packet loss rate
IP addressing
L2/L3 reachability
Recovery time
Secure connection

To accomplish those requirements, a set of YANG data models have been proposed. Those Yang models, summarized in table xx, could be used by an IETF Network Slice Controller to manage CRUD operations on the IETF Network Slice. That is, these models aim capturing the requirements from the consumer of the slice point of view and avoid entering into the detail of how the slice is actually created.

* [draft-wd-teas-ietf-network-slice-nbi-yang]: A Yang Data Model for IETF Network Slice NBI.

* [draft-liu-teas-transport-network-slice-yang]: Transport Network Slice YANG Data Model.

4. Yang Models for Network Controllers

As a functional entity responsible for managing a network domain, the network controller, can expose its northbound interface based on YANG models. The IETF Network Slice Controller can use the network controller's NBI during the realization of IETF Network Slice. The following network models can be used for realization of IETF Network slices:

* LxVPN Network models:

  - These models describe a VPN service from the network point of view. It supports the creation of Layer 3 and Layer 2 services using several control planes.

* Traffic Engineering models:

  - These models allow to manipulate Traffic Engineering tunnels within the network segment. Technology-specific extensions allow to work with a desired technology (e.g. MPLS RSVP-TE tunnels, Segment Routing paths, OTN tunnels, etc.)

* TE Service Mapping extensions:

  - These extensions allow to specify for LxVPN the details of an underlay based on TE.

* ACLs and routing policies models:

  - Even though ACLs and routing policies are device models, it's exposure in the NBI of a domain controller allows to provide an additional granularity that the network domain controller is not able to infer on its own.

4.1. LxVPN Network Models

The framework defined in [RFC8969] compiles a set of YANG data models for automating network services. The data models can be used during the service and network management life cycle (e.g., service instantiation, service provisioning, service optimization, service monitoring, service diagnosing, and service assurance). The so called Network models could be reused for the realization of Network slice requests.

The following models are examples of Network models that describe services.

- [I-D.ietf-opsawg-l3sm-l3nm]: A Layer 3 VPN Network YANG Model

- [I-D.ietf-opsawg-l2nm]: A Layer 2 VPN Network YANG Model

4.2. Traffic Engineering Models

TEAS has defined a collection of models to allow the management of Traffic Engineering tunnels.

- [I-D.ietf-teas-yang-te]: A YANG Data Model for Traffic Engineering Tunnels, Label Switched Paths and Interfaces. The model allows to instantiate paths in a TE enabled network. Note that technology augmented models are require to particular per-technology instantiations.

4.3. Traffic Engineering Service Mapping

The IETF has defined a YANG model to set up the procedure to map VPN service/network models to the TE models. This model, known as service mapping, allows the network controller to assign/retrieve transport resources allocated to specific services. At the moment there is just one service mapping model [I-D.ietf-teas-te-service-mapping-yang]. The "Traffic Engineering (TE) and Service Mapping Yang Model" augments the VPN service and network models.

5. Compliance of Network Controller models with IETF Network Slice Requirements.

Section 3 presented the requirements of the IETF Network slices. This section analyses how YANG models used by a Network Controller can satisfy those requirements and identifies the potencial gaps.

5.1. Availability

As per [draft-ietf-teas-te-service-mapping-yang], Availability is a probabilistic measure of the length of time that a VPN/VN instance functions without a network failure. As per RFC 8330, The parameter "availability", as described in [G.827], [F.1703], and [P.530], is often used to describe the link capacity. The availability is a time scale, representing a proportion of the operating time that the requested bandwidth is ensured".

The calculation of the availability is not trivial and would need to be clearly scoped to avoid misunderstandings.

The set of Yang models proposed today allow to request tunnels/paths with different resiliency requirements in terms of protection and restoration. However, none of them include the possibility of requesting a specific availability (e.g. 99.9999%).

5.2. Downlink throughput / Uplink throughput.

The LxVPN Models ([I-D.ietf-opsawg-l3sm-l3nm] and [I-D.ietf-opsawg-l2nm]) allow to specify the bandwdidth at the interface level between the slice and the customer. In addition, the Service Mapping model [draft-ietf-teas-te-service-mapping-yang] allows to bind a VPN to a given LSP, which have its bandwidth requirements. Additionally, TE models can force a give bandwidth in the connection between Provider Edges.

Previous comment applies to the incoming and outgoing bandwidth parameters required for the NFV-based services use case in [I-D.contreras-teas-slice-nbi]. The Network sharing use case has Maximum and Guaranteed Bit Rate parameters. These parameters can be mapped to the TE tunnel models when setting up LSPs [draft-ietf-teas-yang-te].

5.3. Protection scheme

Protection schemes are mechanisms to define how to setup resources for a given connection. TE tunnel models [draft-ietf-teas-yang-te] includes protection and restoration as two main attributes. The parameters included in the containers for protection and restoration cover the requirements of the IETF NS related with protection schemes. Similarly, TE models cover the parameter 'recovery time' for the network sharing use case.

5.4. Delay

Delay is a critical parameter for several IETF NS types. Every use-case defined in [I-D.contreras-teas-slice-nbi] contains delay constraints. 5G use cases require 'delay tolerance', NFV-based services have the delay information within 'QoS metrics' and 'Bounded latency' in the network sharing use case.

During the realization of the IETF Network Slice, these parameters are part of the requirements of a TE tunnel configuration [draft-ietf-teas-yang-te]. They can be included within the 'path-metric-bounds' parameter, so the created LSP fulfils the given metrics bounds like 'path-metric-delay-average' or 'path-metric-delay-minimum'.

5.5. Packet loss rate

The packet loss rate indicates the maximum rate for lost packets that the service tolerates in the link. During the realization of the IETF Network Slice, this attribute will influence the tunnel selection and the value is included in the [draft-ietf-teas-yang-te] document as the 'path-metric-loss". The 'path-metric-loss' is a metric type, which measures the percentage of packet loss of all links traversed by a P2P path. This parameter is required for 5G services and network sharing use-case, while it is part of the 'QoS metrics' for the NFV-based services.

6. Interactions

Draft [draft-contreras-teas-slice-controller-models] shows the internal structure of an IETF Network Slice Controller which can be divided into two components:

* IETF Network Slice Mapper: this high-level component processes the customer request, putting it into the context of the overall IETF Network Slices in the network.

* IETF Network Slice Realizer: this high-level component processes the complete view of transport slices including the one requested by the customer, decides the proper technologies for realizing the IETF Network Slice and triggers its realization.

```
                             Higher Level System
                                      |
                                      | NSC NBI
                         +-------------------------+
                         | NSC        |            |
                         |            v            |
                         |   +-----------------+   |
                         |   |                 |   |
                         |   |    NS Mapper    |   |
                         |   |                 |   |
                         |   +-----------------+   |
                         |            |            |
                         |            v            |
                         |   +-----------------+   |
                         |   |                 |   |
                         |   |    NS Realizer  |   |
                         |   |                 |   |
                         |   +-----------------+   |
                         |            |            |
                         +-------------------------+
                                      | NSC SBI
                                      v
                             Network Controllers
```

Figure 8: IETF Network Slice Controller Structure

The details of IETF network slice mapper and realize are provided below for various implementation of NCS.

6.1. IETF Network Slice requested to Hierarchical Network Controller

Referring to Figure 1 in an integrated architecture, the IETF Network Slice Controller (NCS) is part of a Hierarchical SDN controller module, the NSC's and the Hierarchical Network Controller should share the same internal data and the same NBI. Thus, the H-SDN module must be able to:

* Map: The customer request received using the [draft-wd-teas-ietf-network-slice-nbi-yang] must be processed by the NCS. The mapping process takes the network-slice SLAs selected by the customer to available Routing Policies and Forwarding policies.

- Realize: Create necessary network requests. The slice's realization can be translated into one or several LXNM Network requests, depending on the number of underlay controllers. Thus, the NCS must have a complete view of the network to map the orders and distribute them across domains. The realization should include the expansion/selection of Forwarding Policies, Routing Policies, VPN policies, and Underlay transport preference.

To maintain the data coherence between the control layers, the IETF Network Slice ID "ns-id" used of the [draft-wd-teas-ietf-network-slice-nbi-yang] must be directly mapped to the "transport-instance-id" at the VPN-Node level.

```
                              +
                              |
                              | IETF Network Slice Request:
                  draft-wd-teas-ietf-network-slice-nbi-yang
                              | * network-slice-id
                              |
          +-------------------v------------------+
          |                                      |
          |    Hierarchical Network              |
          |    Controller/Orchestrator           |
          |                                      |
          |   +-------------------------------+  |
          |   | IETF Network Slice Controller |  |
          |   +-------------------------------+  |
          |                                      |
          +-------------------+------------------+
      IETF Network Slice Realizer: LXNM
        VPN-id                |
     * transport-instance-id  |
                              |
               +--------------+---------------+
               |                              |
               v                              v
 +-------------+----------+     +-------------+----------+
 |   Network Controller   |     |   Network Controller   |
 +-------------+----------+     +-------------+----------+
               |                              |
               |                              |
               v                              v
        Network Elements                Network Elements
```

Figure 9 Workflow for the slice request in an integrated architecture.

6.2. IETF Network Slice requested to Network Slice Controller

Referring to Figure 2 when the Network Slice Controller is a stand-alone controller module, the NSC's should perform the same two tasks described in section 6.1:

* Map: Process the customer request. The customer request can be sent using the [draft-liu-teas-transport-network-slice-yang]. This draft allows the topology mapping of the Slice request.

* Realize: Create necessary network requests. The slice's realization will be translated into one LXNM Network request. As the NCS has a topological view of the network, the realization can include the customer's traffic engineering transport preferences and policies.

```
                               +
                               |IETF Network Slice Request
                draft-liu-teas-transport-network-slice-yang
                network-id
                               |
                 +-------------v-----------------+
                 | IETF Network Slice Controller |
                 +-------------+-----------------+
                               |
                    IETF Network Slice Realizer: LXNM
                      VPN-id   |
                      * Underlay-transport
                      * transport-instance-id
                               |
                 +-------------v----------------+
                 |       Network Controller     |
                 +-------------+----------------+
                               |
                               |
                               v
                       Network Elements
```

Figure 10 Workflow for the slice request in an stand-alone architecture.

6.3. Network Slice Controller as part of the domain controller

The Network Slice Controller can be a module of the Network controller. In that case, two options are available. One is to share the same device data model in the NBI and SBI of the SDN controller. The direct translation would reduce the service logic implemented at the SDN controller level, grouping the mapping and translation into a single task:

- Realize: As the device models are part of the network controller's NBI thus, the realization can be done by the network controller applying a simple service logic to send the Network elements.

```
                                   +
                                   | Slice Request based on
                                   |   Device Models
                                   |
                                   |
                +------------------v------------------+
                |                                     |
                |    Network                          |
                |    Controller                       |
                |                                     |
                |   +------------------------------+  |
                |   |   Network Slice Controller   |  |
                |   +------------------------------+  |
                |                                     |
                +------------------+------------------+
                                   | Device Models
                                   |
                                   v
                           Network Elements
```

Figure 11 Workflow for the slice request in an stand-alone architecture.

A second option introduces a more complex logic in the network controller and creates an abstraction layer to process the transport slices. In that case, the controller should receive network slices creation requests and maintain the whole set of implemented slices:

- Map & Realize: The mapping and realization can be done by the Domain controller applying the service logic to create policies directly on the Network elements.

```
                               +
                               |Slice Request
                draft-liu-teas-transport-network-slice-yang-01
                network-id
                               |
                               |
            +------------------v------------------+
            |                                     |
            |    Network                          |
            |    Controller                       |
            |                                     |
            |   +------------------------------+  |
            |   |   Network Slice Controller   |  |
            |   +------------------------------+  |
            |                                     |
            +------------------+------------------+
                               |
                               |
                               v
                       Network Elements
```

Figure 12 Workflow for the slice request in an stand-alone architecture.

7. Security Considerations

There are two main aspects to consider. On the one hand, the IETF Network Slice has a set of security related requirements, such as hard isolation of the slice, or encryption of the communications through the slice. All those requirements need to be analyzed in detailed and clearly mapped to the Network Controller and device interfaces.

On the other hand, the communication between the IETF network slicer and the network controller (or controllers or hierarchy of controllers) need to follow the same security considerations as with the network models.

The network YANG modules defines schemas for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC8466]. The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

The following summarizes the foreseen risks of using the Network Models to instantiate IETF network Slices:

* Malicious clients attempting to delete or modify VPN services that implements an IETF network slice. The malicious client could manipulate security related aspects of the network configuration that impact the requirements of the slice, failing to satisfy the customer requirement.

* Unauthorized clients attempting to create/modify/delete a VPN hat implements an IETF network slice service.

* Unauthorized clients attempting to read VPN services related information hat implements an IETF network slice

* Malicious clients attempting to leak traffic of the slice.

8. IANA Considerations

This document is informational and does not require IANA allocations.

9. Conclusions

A wide variety of yang models are currently under definition in IETF that can be used by Network Controllers to instantiate IETF network slices. Some of the IETF slice requirements can be satisfied by multiple means, as there are multiple choices available. However, other requirements are still not covered by the existing models. A more detailed definition of those uncovered requirements would be needed. Finally a consensus on the set of models to be exposed by Network Controllers would facilitate the deployment of IETF network slices.

10. Normative References

[I-D.contreras-teas-slice-nbi]
Contreras, L. M., Homma, S., and J. A. Ordonez-Lucena, "IETF Network Slice Use Cases and Attributes for Northbound Interface of IETF Network Slice Controllers", Work in Progress, Internet-Draft, draft-contreras-teas-slice-nbi-04, 22 February 2021, <https://datatracker.ietf.org/doc/html/draft-contreras-teas-slice-nbi-04>.

[I-D.ietf-opsawg-l2nm]
Barguil, S., Dios, O. G. D., Boucadair, M., and L. A. Munoz, "A Layer 2 VPN Network YANG Model", Work in Progress, Internet-Draft, draft-ietf-opsawg-l2nm-02, 30 April 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-l2nm-02>.

[I-D.ietf-opsawg-l3sm-l3nm]
Barguil, S., Dios, O. G. D., Boucadair, M., Munoz, L. A., and A. Aguado, "A Layer 3 VPN Network YANG Model", Work in Progress, Internet-Draft, draft-ietf-opsawg-l3sm-l3nm-08, 22 April 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-l3sm-l3nm-08>.

[I-D.ietf-teas-ietf-network-slice-definition]
Rokui, R., Homma, S., Makhijani, K., Contreras, L. M., and J. Tantsura, "Definition of IETF Network Slices", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slice-definition-01, 22 February 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-definition-01>.

[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", Work in Progress, Internet-Draft, draft-ietf-teas-te-service-mapping-yang-07, 21 February 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-te-service-mapping-yang-07>.

[I-D.ietf-teas-yang-te]
Saad, T., Gandhi, R., Liu, X., Beeram, V. P., Bryskin, I., and O. G. D. Dios, "A YANG Data Model for Traffic Engineering Tunnels, Label Switched Paths and Interfaces", Work in Progress, Internet-Draft, draft-ietf-teas-yang-te-26, 22 February 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-yang-te-26>.

[I-D.nsdt-teas-ns-framework]
Gray, E. and J. Drake, "Framework for IETF Network Slices", Work in Progress, Internet-Draft, draft-nsdt-teas-ns-framework-05, 2 February 2021, <https://datatracker.ietf.org/doc/html/draft-nsdt-teas-ns-framework-05>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[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>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[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>.

[RFC8466] Wen, B., Fioccola, G., Ed., Xie, C., and L. Jalil, "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery", RFC 8466, DOI 10.17487/RFC8466, October 2018, <https://www.rfc-editor.org/info/rfc8466>.

[RFC8969] Wu, Q., Ed., Boucadair, M., Ed., Lopez, D., Xie, C., and L. Geng, "A Framework for Automating Service and Network Management with YANG", RFC 8969, DOI 10.17487/RFC8969, January 2021, <https://www.rfc-editor.org/info/rfc8969>.

Authors' Addresses

Samier Barguil
Telefonica
Distrito T
28050 Madrid
Spain

Email: samier.barguilgiraldo.ext@telefonica.com

Luis Miguel Contreras
Telefonica
Distrito T
28050 Madrid
Spain

Email: luismiguel.contrerasmurillo@telefonica.com

Victor Lopez
Nokia
Calle de María Tubau, 9
28050 Madrid
Spain

Email: victor.lopez@nokia.com

Reza Rokui
Nokia
Canada

Email: reza.rokui@nokia.com

Oscar Gonzalez de Dios
Telefonica
Distrito T
28050 Madrid
Spain

Email: oscar.gonzalezdedios@telefonica.com