TEAS WG
Internet Draft
Intended status: standard track
Expires: March 18, 2019

Young Lee
Dhruv Dhody
Huawei

Daniele Ceccarelli
Ericsson

Jeff Tantsura
Nuage

Giuseppe Fioccola
Telecom Italia

Qin Wu
Huawei

September 18, 2018

Traffic Engineering and Service Mapping Yang Model

draft-lee-teas-te-service-mapping-yang-11

Abstract

This document provides a YANG data model to map customer service models (e.g., the L3VPM Service Model) to Traffic Engineering (TE) models (e.g., the TE Tunnel or the Abstraction and Control of Traffic Engineered Networks Virtual Network model). This model is referred to as TE Service Mapping Model and is applicable to the operator's need for seamless control and management of their VPN services with TE tunnel support.

The model is principally used to allow monitoring and diagnostics of the management systems to show how the service requests are mapped onto underlying network resource and TE models.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Copyright Notice

Table of Contents

1. Introduction

Data models are a representation of objects that can be configured or monitored within a system. Within the IETF, YANG [RFC6020] is the language of choice for documenting data models, and YANG models have been produced to allow configuration or modeling of a variety of network devices, protocol instances, and network services. YANG data models have been classified in [RFC8199] and [RFC8309].

[RFC8299] provides a L3VPN service delivery YANG model for PE-based VPNs. The scope of that draft is limited to a set of domains under control of the same network operator to deliver services requiring TE tunnels.

Framework for Abstraction and Control of Traffic Engineered Networks (ACTN) [RFC8453] introduces an architecture to support virtual network services and connectivity services. [ACTN-VN-YANG] defines a YANG model and describes how customers or end-to-end orchestrators can request and/or instantiate a generic virtual network service. [ACTN-Applicability] describes the way IETF YANG models of different classifications can be applied to the ACTN interfaces. In particular, it describes how customer service models can be mapped into the CNC-MDSC Interface (CMI) of the ACTN architecture.

While the IP/MPLS Provisioning Network Controller (PNC) is responsible for provisioning the VPN service on the Provider Edge (PE) nodes, the Multi-Domain Service Coordinator (MDSC) can coordinate how to map the VPN services onto Traffic Engineering (TE) tunnels. This is consistent with the two of the core functions of the MDSC specified in [RFC8453]:

. Customer mapping/translation function: This function is to map customer requests/commands into network provisioning requests that can be sent to the PNC according to the business policies that have been provisioned statically or dynamically.

Specifically, it provides mapping and translation of a customer's service request into a set of parameters that are specific to a network type and technology such that the network configuration process is made possible.

. Virtual service coordination function: This function translates customer service-related information into virtual network service operations in order to seamlessly operate virtual networks while meeting a customer's service requirements. In the context of ACTN, service/virtual service coordination includes a number of service orchestration functions such as

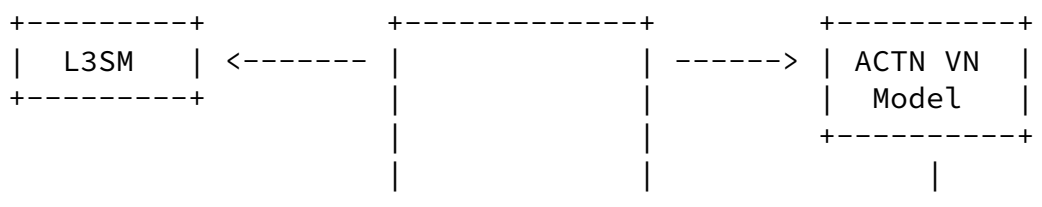
multi-destination load balancing, guarantees of service quality, bandwidth and throughput. It also includes notifications for service fault and performance degradation and so forth.

The YANG model described in this document provides an ACTN TE-service mapping model that encodes the mapping of services (L1/2/3 VPN, ACTN VN) to TE-Topology/TE-tunnel models at the MDSC.

2. TE-Service Mapping Model

The role of the TE-service Mapping model is to expose the mapping relationship between service models and TE models so that VN/VPN service instantiations provided by the underlying TE networks can be viewed outside of the MDSC, for example by an operator who is diagnosing the behavior of the network. It also allows for the customers to access operational state information about how their services are instantiated with the underlying TE topology or TE tunnels provided that the MDSC operator is willing to share that information. This mapping will facilitate a seamless service management operation with underlay-TE network visibility.

Figure 1 shows the scope of the TE-Service Mapping Model. The arrow-heads show a reference from one model to another.



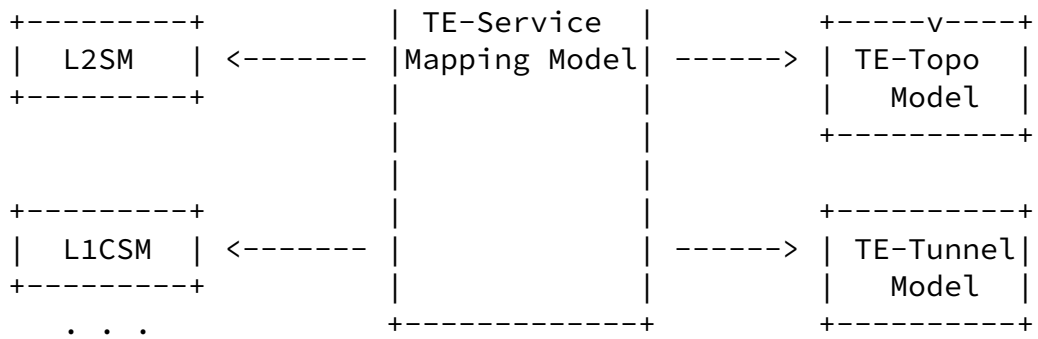


Figure 1. TE-Service Mapping

As seen in Figure 1, the TE-Service Mapping Model records a mapping between the customer service models and the ACTN VN YANG model. Thus, when the MDSC receives a service request it creates a VN that

meets the customer's service objectives with various constraints via TE-topology model [TE-topo], and this relationship is recorded by the Te-Service Mapping Model. The model also supports a mapping between a service model and TE-topology or a TE-tunnel.

The TE-service model described in this document can also be extended to support other services beyond L3SM, L2SM and L1CSM.

Moreover, the TE-Service Mapping model provides additional service parameters and policies that are not included in the respective service models such as L3SM [RFC8299], L2SM [L2SM-YANG] and L1CSM [L1CSM-YANG]. For example, how VN/TE tunnel should be created (e.g., with an isolation level) for a certain service instance is described in the TE-Service Mapping model.

2.1. VN/Tunnel Selection Requirements

In some cases, the service requirements may need addition TE tunnels to be established. This may occur when there are no suitable existing TE tunnels that can support the service requirements, or when the operator would like to dynamically create and bind tunnels to the VPN such that they are not shared by other VPNs, for example, for network slicing. The establishment of TE tunnels is subject to the network operator's policies.

To summarize, there are three modes of VN/Tunnel selection

operations to be supported as follows. Additional modes may be defined in the future.

- New VN/Tunnel Binding - A customer could request a VPN service based on VN/Tunnels that are not shared with other existing or future services. This might be to meet VPN isolation requirements. Further, the YANG model described in Section 5 of this document can be used to describe the mapping between the VPN service and the ACTN VN. The VN (and TE tunnels) could be bound to the VPN and not used for any other VPN.

  Under this mode, the following sub-categories can be supported:

  1. Hard Isolation with deterministic characteristics: A customer could request a VPN service using a set of TE Tunnels with deterministic characteristics requirements (e.g., no latency variation) and where that set of TE Tunnels must not be shared with other VPN services and

     must not compete for bandwidth or other network resources with other TE Tunnels.

  2. Hard Isolation: This is similar to the above case but without the deterministic characteristics requirements.

  3. Soft Isolation: The customer requests a VPN service using a set of TE tunnels which can be shared with other VPN services.

- VN/Tunnel Sharing - A customer could request a VPN service where new tunnels (or a VN) do not need to be created for each VPN and can be shared across multiple VPNs. Further, the mapping YANG model described in Section 5 of this document can be used to describe the mapping between the VPN service and the tunnels in use. No modification of the properties of a tunnel (or VN) is allowed in this mode: an existing tunnel can only be selected.

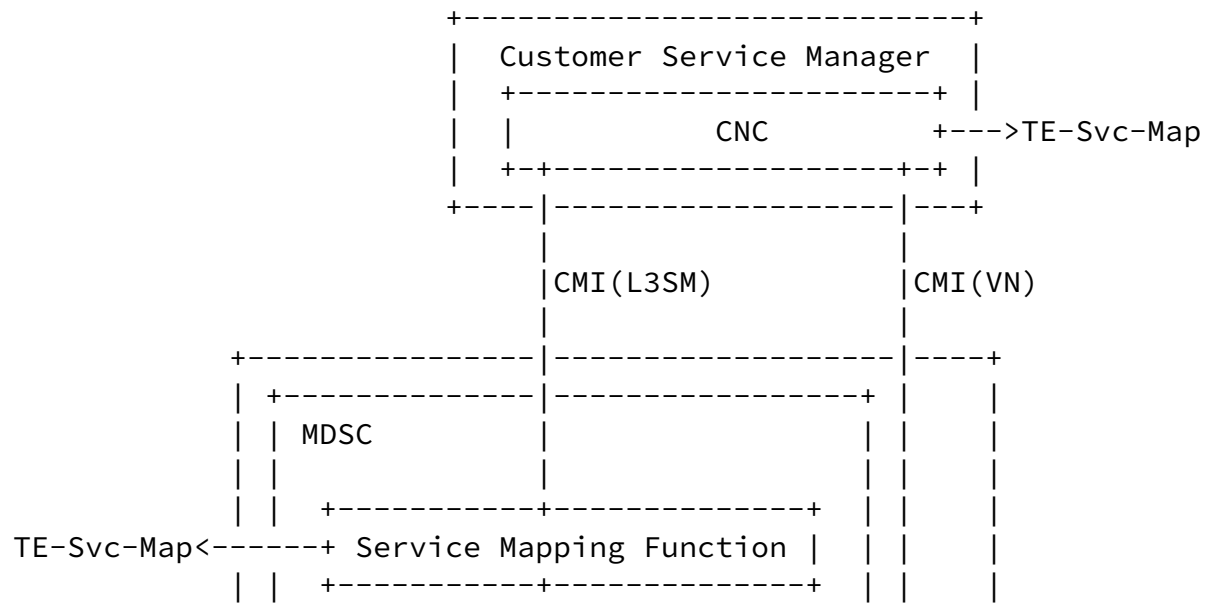
- VN/Tunnel Modify - This mode allows the modification of the properties of the existing VN/tunnel (e.g., bandwidth).

2.2. Availability Requirement

Availability is another service requirement or intent that may influence the selection or provisioning of TE tunnels or a VN to support the requested service. Availability is a probabilistic measure of the length of time that a VPN/VN instance functions without a network failure.
The availability level will need to be translated into network specific policies such as the protection/reroute policy associated with a VN or Tunnel. The means by which this is achieved is not in the scope of this draft.

3. L3VPN Architecture in the ACTN Context

Figure 2 shows the architectural context of this document referencing the ACTN components and interfaces.



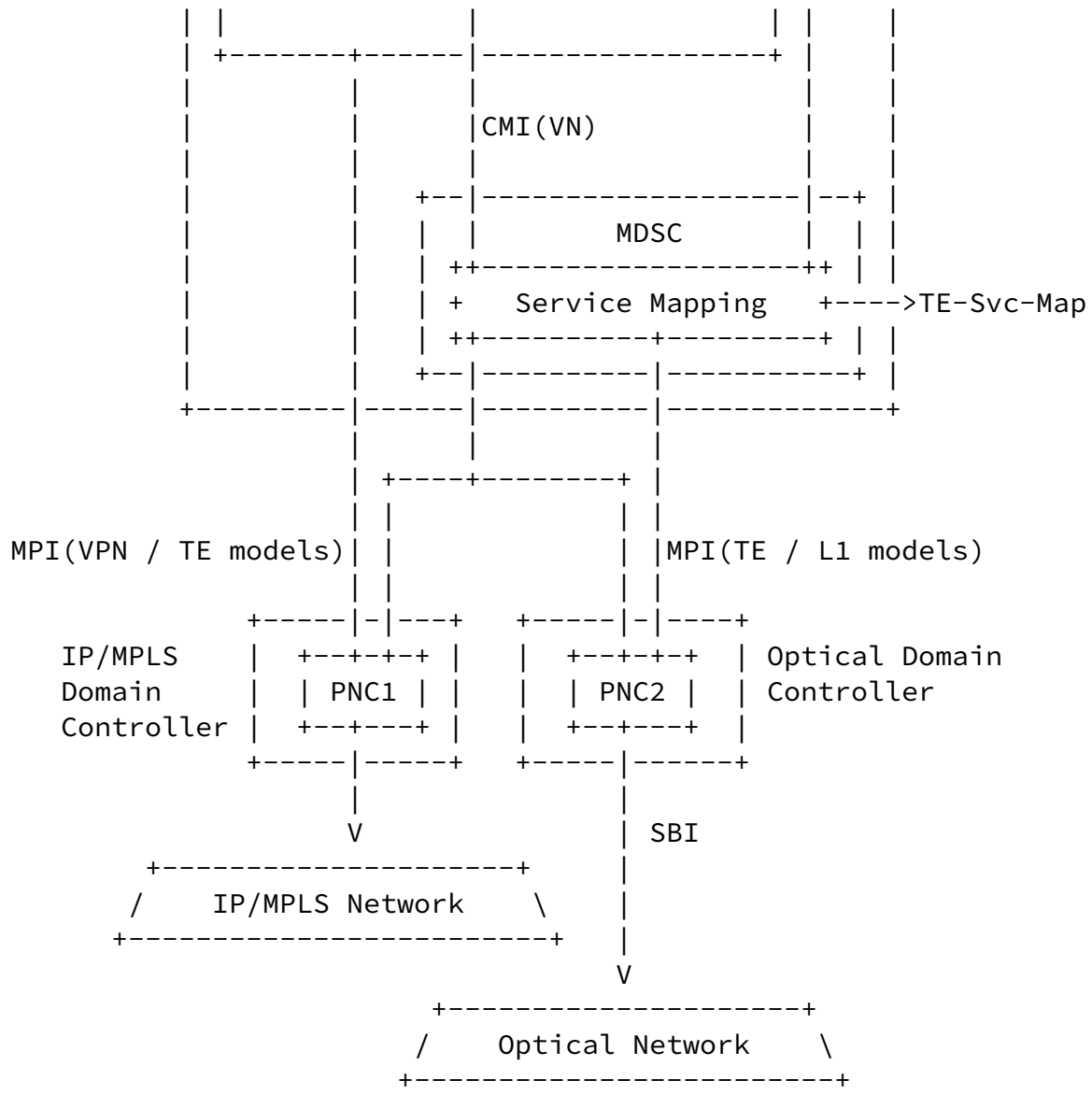


Figure 2: L3VPN Architecture from the IP+Optical Network Perspective

There are three main entities in the ACTN architecture and shown in Figure 2.

. CNC: The Customer Network Controller is responsible for generating service requests. In the context of an L3VPN, the CNC uses the L3SM to express the service request and communicate it to the network operator.
. MDSC: This entity is responsible for coordinating a L3VPN service

request (expressed via the L3SM) with the IP/MPLS PNC and the Transport PNC. For TE services, one of the key responsibilities of the MDSC is to coordinate with both the IP PNC and the Transport PNC for the mapping of the L3VPN Service Model to the ACTN VN model. In the VN/TE-tunnel binding case, the MDSC will need to coordinate with the Transport PNC to dynamically create the TE-tunnels in the transport network as needed. These tunnels are added as links in the IP/MPLS Layer topology. The MDSC coordinates with IP/MPLS PNC to create the TE-tunnels in the IP/MPLS layer, as part of the ACTN VN creation.

. PNC: The Provisioning Network Controller is responsible for configuring and operating the network devices. Figure 2 shows two distinct PNCs.
  - o IP/MPLS PNC (PNC1): This entity is responsible for device configuration to create PE-PE L3VPN tunnels for the VPN customer and for the configuration of the L3VPN VRF on the PE nodes. Each network element would select a tunnel based on the configuration.
  - o Transport PNC (PNC2): This entity is responsible for device configuration for TE tunnels in the transport networks.

There are four main interfaces shown in Figure 2.

. CMI: The CNC-MDSC Interface is used to communicate service requests from the customer to the operator. The requests may be expressed as VPN service requests (L2SM, L3SM), as connectivity requests (L1CSM), or as virtual network requests (ACTN VN).
. MPI: The MDSC-PNC Interface is used by the MDSC to orchestrate networks under the control of PNCs. The requests on this interface may use TE tunnel models, TE topology models, VPN network configuration models or layer one connectivity models.
. SBI: The Southbound Interface is used by the PNC to control network devices and is out of scope for this document.
. The TE Service Mapping Model as described in this document can be used to see the mapping between service models and VN models and TE Tunnel/Topology models. That mapping may occur in the CNC if a

service request is mapped to a VN request. Or it may occur in the MDSC where a service request is mapped to a TE tunnel, TE topology, or VPN network configuration model. The TE Service Mapping Model may be read from the CNC or MDSC to understand how the mapping has been made and to see the purpose for which network resources are used.

As shown in Figure 2, the MDSC may be used recursively. For example, the CNC might map a L3SM request to a VN request that it sends to a recursive MDSC.

The high-level control flows for one example are as follows:

1. A customer asks for an L3VPN between CE1 and CE2 using the L3SM model.

2. The MDSC considers the service request and local policy to determine if it needs to create a new VN or any TE Topology, and if that is the case, ACTN VN YANG [ACTN-VN-YANG] is used to configure a new VN based on this VPN and map the VPN service to the ACTN VN. In case an existing tunnel is to be used, each device will select which tunnel to use and populate this mapping information.

3. The MDSC interacts with both the IP/MPLS PNC and the Transport PNC to create a PE-PE tunnel in the IP network mapped to a TE tunnel in the transport network by providing the inter-layer access points and tunnel requirements. The specific service information is passed to the IP/MPLS PNC for the actual VPN configuration and activation.

    a. The Transport PNC creates the corresponding TE tunnel matching with the access point and egress point.
    b. The IP/MPLS PNC maps the VPN ID with the corresponding TE tunnel ID to bind these two IDs.

4. The IP/MPLS PNC creates/updates a VRF instance for this VPN customer. This is not in the scope of this document.

3.1. Service Mapping

L3SM and L2SM can be used to request VPN service creation including the creation of sites and corresponding site network access connection between CE and PE. A VPN-ID is used to identify each VPN service ordered by the customer. The ACTN VN can be used further to establish PE-to-PE connectivity between VPN sites belonging to the

same VPN service. A VN-ID is used to identify each virtual network

established between VPN sites.

Once the ACTN VN has been established over the TE network (maybe a new VN, maybe modification of an existing VN, or maybe the use of an unmodified existing VN), the mapping between the VPN service and the ACTN VN service can be created.

3.2. Site Mapping

The elements in L3SM and L2SM define site location parameters and constraints such as distance and access diversity that can influence the placement of network attachment points (i.e, virtual network access points (VNAP)). To achieve this, a central directory can be set up to establish the mapping between location parameters and constraints and network attachment point location. Suppose multiple attachment points are matched, the management system can use constraints or other local policy to select the best candidate network attachment points.

After a network attachment point is selected, the mapping between VPN site and VNAP can be established as shown in Table 1.

Site	Site Network Access	Location (Address, Postal Code, State, City,Country Code)	Access Diversity (Constraint-Type, Group-id,Target Group-id)	PE
SITE1	ACCESS1	(,,US,NewYork,)	(10,PE-Diverse,10)	PE1
SITE2	ACCESS2	(,,CN,Beijing,)	(10,PE-Diverse,10)	PE2
SITE3	ACCESS3	(,,UK,London,)	(12,same-PE,12)	PE4
SITE4	ACCESS4	(,,FR,Paris,)	(20,Bearer-Diverse,20)	PE7

Table 1 : Mapping Between VPN Site and VNAP

4. YANG Data Tree

```
module: ietf-te-service-mapping
+--rw te-service-mapping
```

```
   +--rw service-mapping
   |  +--rw mapping-list* [map-id]
   |     +--rw map-id            uint32
   |     +--rw map-type?         map-type
   |     +--rw (service)?
   |     |  +--:(l3vpn)
   |     |  |  +--rw l3vpn-ref?    -> /l3:l3vpn-svc/vpn-services/vpn-service/vp
   |     |  +--:(l2vpn)
   |     |  |  +--rw l2vpn-ref?    -> /l2:l2vpn-svc/vpn-services/vpn-service/vp
   |     |  +--:(l1vpn)
   |     |     +--rw l1vpn-ref?    -> /l1:l1-connectivity/services/service/serv
   |     +--rw (te)?
   |        +--:(actn-vn)
   |        |  +--rw actn-vn-ref?    -> /vn:actn/vn/vn-list/vn-id
   |        +--:(te-topo)
   |        |  +--rw vn-topology-id?   te-types:te-topology-id
   |        |  +--rw abstract-node?    -> /nw:networks/network/node/node-id
   |        +--:(te-tunnel)
   |           +--rw te-tunnel-list*   te:tunnel-ref
   +--rw site-mapping
      +--rw mapping-list* [map-id]
         +--rw map-id         uint32
         +--rw (service)?
         |  +--:(l3vpn)
         |  |  +--rw l3vpn-ref?    -> /l3:l3vpn-svc/sites/site/site-id
         |  +--:(l2vpn)
         |  |  +--rw l2vpn-ref?    -> /l2:l2vpn-svc/sites/site/site-id
         |  +--:(l1vpn)
         |     +--rw l1vpn-ref?    -> /l1:l1-connectivity/access/unis/uni/id
         +--rw (te)?
            +--:(actn-vn)
            |  +--rw actn-vn-ref?    -> /vn:actn/ap/access-point-list/access-po
            +--:(te)
               +--rw ltp?           te-types:te-tp-id
```

5. YANG Data Model

The YANG code is as follows:

<CODE BEGINS> file "ietf-te-service-mapping@2018-09-18.yang"

```
   module ietf-te-service-mapping {

       namespace "urn:ietf:params:xml:ns:yang:ietf-te-service-mapping";
```

```
        prefix "tm";
```



```
        import ietf-l3vpn-svc {
            prefix "l3";
        }

        import ietf-l2vpn-svc {
            prefix "l2";
        }

        import ietf-l1csm {
            prefix "l1";
        }

        import ietf-te-types {
            prefix "te-types";
        }

        import ietf-network {
            prefix "nw";
        }

        import ietf-te {
            prefix "te";
        }

        import ietf-actn-vn {
            prefix "vn";
        }

        organization
            "IETF Traffic Engineering Architecture and Signaling (TEAS)
            Working Group";

        contact
            "Editor: Young Lee <leeyoung@huawei.com>
                     Dhruv Dhody <dhruv.ietf@gmail.com>
                   Qin Wu <bill.wu@huawei.com>";
        description
            "This module contains a YANG module for the mapping of
            service (e.g. L3VPN) to the TE tunnels or ACTN VN.";
```

```
        revision 2018-09-18 {
            description
                "initial version.";
            reference
                "TBD";
        }

        /*
         * Identities
```



```
         */
        identity service-type {
            description
                "Base identity from which specific service types are
                derived.";
        }

        identity l3vpn-service {
            base service-type;
            description
                "L3VPN service type.";
        }

        identity l2vpn-service {
            base service-type;
            description
                "L2VPN service type.";
        }

        identity l1vpn-service {
            base service-type;
            description
                "L1VPN connectivity service type.";
        }
        /*
         * Enum
         */
        identity map-type {
          description
          "Base identity from which specific map types are
           derived.";
       }
```

```
        identity new {
           base map-type;
           description
             "The new VN/tunnels are binded to the service.";
        }

        identity detnet-hard-isolation {
           base new;
           description
             "Hard isolation with deterministic characteristics.";
        }

        identity hard-isolation {
           base new;
           description
             "Hard isolation.";
```



```
        }

        identity soft-isolation {
          base new;
          description
            "Soft-isolation.";
        }

        identity select {
           base map-type;
           description
             "The VPN service selects an existing tunnel with no
              modification.";
        }

        identity modify {
           base map-type;
           description
             "The VPN service selects an existing tunnel and allows
              to modify the properties of the tunnel (e.g., b/w)";
        }


         /*
```

```
 * Groupings
 */
grouping service-ref{
    description
        "The reference to the service.";
     choice service {
        description
            "The service";
        case l3vpn {
            leaf l3vpn-ref {
                type leafref {
                    path "/l3:l3vpn-svc/l3:vpn-services/"
                    + "l3:vpn-service/l3:vpn-id";
                }
                description
                    "The reference to L3VPN Service Yang Model";
            }
        }
        case l2vpn {
            leaf l2vpn-ref {
                type leafref {
                    path "/l2:l2vpn-svc/l2:vpn-services/"
                    + "l2:vpn-service/l2:vpn-id";
                }
                description
```



```
                    "The reference to L2VPN Service Yang Model";
            }

        }
        case l1vpn {
            leaf l1vpn-ref {
                type leafref {
                    path "/l1:l1-connectivity/l1:services/"
                    + "l1:service/l1:service-id";
                }
                description
                    "The reference to L1VPN Service Yang Model";
            }

        }
     }
```

```
        }

        grouping site-ref {
            description
                "The reference to the site.";
             choice service {
                description
                    "The service choice";
                case l3vpn {
                    leaf l3vpn-ref{
                        type leafref {
                            path "/l3:l3vpn-svc/l3:sites/l3:site/"
                            + "l3:site-id";
                        }
                        description
                            "The reference to L3VPN Service Yang Model";
                    }
                }
                case l2vpn {
                    leaf l2vpn-ref{
                        type leafref {
                            path "/l2:l2vpn-svc/l2:sites/l2:site/"
                            + "l2:site-id";
                        }
                        description
                            "The reference to L2VPN Service Yang Model";
                    }

                }
                case l1vpn {
                    leaf l1vpn-ref{
                        type leafref {
                            path "/l1:l1-connectivity/l1:access/l1:unis/"
```



```
                            + "l1:uni/l1:id";
                        }
                        description
                            "The reference to L1VPN Connectivity Service Yang
   Model";
                    }

                }
```

```
        }
    }

    grouping te-ref {
        description
            "The reference to TE.";
        choice te {
            description
                "The TE";
            case actn-vn {
                leaf actn-vn-ref {
                    type leafref {
                        path "/vn:actn/vn:vn/vn:vn-list/vn:vn-id";
                    }
                    description
                        "The reference to ACTN VN";
                }
            }
            case te-topo {
               leaf vn-topology-id{
                   type te-types:te-topology-id;
                   description
                       "An identifier to the TE Topology Model
                        where the abstract nodes and links of
                        the Topology can be found for Type 2
                        VNS";
               }
               leaf abstract-node {
                 type leafref {
                   path "/nw:networks/nw:network/nw:node/"
                   + "nw:node-id";
                 }
                 description
                   "a reference to the abstract node in TE
                   Topology";
               }
            }
            case te-tunnel {
                leaf-list te-tunnel-list {
                    type te:tunnel-ref;
```

```
                    description
                        "Reference to TE Tunnels";
                }

            }

        }

    }

    grouping te-endpoint-ref {
        description
            "The reference to TE endpoints.";
        choice te {
            description
                "The TE";
            case actn-vn {
                leaf actn-vn-ref {
                    type leafref {
                        path "/vn:actn/vn:ap/vn:access-point-list"
                        + "/vn:access-point-id";
                    }
                    description
                        "The reference to ACTN VN";
                }
            }
            case te {
               leaf ltp {
                   type te-types:te-tp-id;
                   description
                       "Reference LTP in the TE-topology";
               }
            }
        }

    }

    grouping service-mapping {
        description
            "Mapping between Services and TE";
        container service-mapping {
            description
                "Mapping between Services and TE";

            list mapping-list {
                key "map-id";
                description
                    "Mapping identified via a map-id";
                leaf map-id {
```

```
                        type uint32;
                        description
                            "a unique mapping identifier";
                    }
                    leaf map-type {
                        type identityref {
                      base map-type;
                    }
                        description
                            "Tunnel Bind or Tunnel Selection";
                    }
                    uses service-ref;

                    uses te-ref;
                }
            }
        }
        grouping site-mapping {
            description
                "Mapping between VPN access site and TE
                endpoints or AP";
            container site-mapping {
                description
                    "Mapping between VPN access site and TE
                    endpoints or AP";
                list mapping-list {
                    key "map-id";
                    description
                        "Mapping identified via a map-id";
                    leaf map-id {
                        type uint32;
                        description
                            "a unique mapping identifier";
                    }
                    uses site-ref;

                    uses te-endpoint-ref;
                }

            }
        }

        /*
```

```
           * Configuration data nodes
           */
          container te-service-mapping {
              description
                  "Mapping between Services and TE";
```



```
              uses service-mapping;

              uses site-mapping;
          }


      }
```

<CODE ENDS>

6. Security

The configuration, state, and action data defined in this document are designed to be accessed via a management protocol with a secure transport layer, such as NETCONF [RFC6241]. The NETCONF access control model [RFC6536] provides the means to restrict access for particular NETCONF users to a preconfigured subset of all available NETCONF protocol operations and content.

A number of configuration data nodes defined in this document are writable/deletable (i.e., "config true") These data nodes may be considered sensitive or vulnerable in some network environments.

7. IANA Considerations

This document registers the following namespace URIs in the IETF XML registry [RFC3688]:

```
---------------------------------------------------------------------
URI: urn:ietf:params:xml:ns:yang:ietf-te-service-mapping
Registrant Contact: The IESG.
XML: N/A, the requested URI is an XML namespace.
---------------------------------------------------------------------
```

This document registers the following YANG modules in the YANG Module.

Names registry [RFC7950]:

---

name: ietf-te-service-mapping

namespace: urn:ietf:params:xml:ns:yang:ietf-te-service-mapping
reference: RFC XXXX (TDB)

---

8. Acknowledgements

We thank Diego Caviglia and Igor Bryskin for useful discussions and motivation for this work.

9. References

9.1. Informative References

[RFC4110] R. Callon and M. Suzuki, "A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4110, July 2005.

[RFC6020] M. Bjorklund, Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC8309] Q. Wu, W. Liu and A. Farrel, "Service Models Explained", RFC 8309, January 2018.

[RFC8199] D. Bogdanovic, B. Claise, and C. Moberg, "YANG Module Classification", RFC 8199, July 2017.

[Netconf] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241.

[RFC8453] D. Cecarelli and Y. Lee, "Framework for Abstraction and Control of Traffic Engineered Networks", RFC 8453, August

2018.

[TE-Topology] X. Liu, et. al., "YANG Data Model for TE Topologies", draft-ietf-teas-yang-te-topo, work in progress.

[TE-Tunnel] T. Saad (Editor), "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te, work in progress.

[ACTN-VN-YANG] Y. Lee (Editor), "A Yang Data Model for ACTN VN Operation", draft-lee-teas-actn-vn-yang, work in progress.

[ACTN-Applicability] Y. Lee, et al, "Applicability of YANG models for Abstraction and Control of Traffic Engineered Networks, draft-ietf-teas-actn-yang, work in progress.

[RFC8299] Q. Wu, S. Litkowski, L.Tomotaki, and K. Ogaki, "YANG Data Model for L3VPN service delivery", RFC 8299, January 2018.

[L2SM-YANG] B. Wen, et al, "A YANG Data Model for L2VPN Service Delivery", draft-ietf-l2sm-l2vpn-service-model, work in progress.

[L1CSM-YANG] G. Fioccola, et al, "A Yang Data Model for L1 Connectivity Service Model (L1CSM)", draft-ietf-ccamp-l1csm-yang, work in progress.

10. Contributors

Adrian Farrel
adrian@olddog.co.uk

Authors' Addresses

Young Lee
Huawei Technologies
5340 Legacy Drive
Plano, TX 75023, USA
Phone: (469)277-5838

Email: leeyoung@huawei.com

Dhruv Dhody
Huawei Technologies

Email: dhruv.ietf@gmail.com

Daniele Ceccarelli
Ericsson
Torshamnsgatan,48
Stockholm, Sweden

Email: daniele.ceccarelli@ericsson.com

Jeff Tantsura
Huawei

EMail: jefftant@gmail.com

Giuseppe Fioccola
Telecom Italia
Email: giuseppe.fioccola@telecomitalia.it

Qin Wu
Huawei
Email: bill.wu@huawei.com