TEAS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 15 April 2026

D. Dhody
Huawei
B. Wu
Huawei Technologies

12 October 2025

IETF Network Slice Service Mapping YANG Model
draft-dhody-teas-ietf-network-slice-mapping-07

Abstract

This document provides a YANG data model to map IETF network slice service to Traffic Engineering (TE) models (e.g., the Virtual Network (VN) model or the TE Tunnel, etc). It also supports mapping to the VPN Network models and Network Resource Partition (NRP) models. These models are referred to as the IETF network slice service mapping model and are applicable generically for the seamless control and management of the IETF network slice service with underlying TE/ VPN support.

The models are principally used for monitoring and diagnostics of the management systems to show how the IETF network slice service requests are mapped onto underlying network resources and TE/VPN models.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 15 April 2026.

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 [RFC7950] is the language of choice for documenting data models, and YANG models have been produced to allow the configuration or modeling of a variety of network devices, protocol instances, and network services.

The YANG model discussed in this document augments the IETF Network Slice Service YANG model [RFC9543], which is used to operate IETF Network Slices during the IETF Network Slice instantiation. This provides a way to map IETF network slice service to Traffic Engineering (TE) models (e.g., the Virtual Network (VN) model or the TE Tunnel, etc). Alternatively, it also supports mapping to the VPN Network models and Network Resource Partition (NRP) models.

The model supports:

* A mapping of the IETF Network Slice with the Network Resource Partition (NRP). As per [RFC9543], NRP is a collection of resources (bufferage, queuing, scheduling, etc.) in the underlay network. The NRP YANG model is specified in [I-D.ietf-teas-nrp-yang]. The IETF Network Slice can be mapped to the NRP directly.

* A mapping of the IETF Network Slice with the VPN network models - LxNM. This mapping can be populated at the time of IETF network service realization. This mapping information is internal and used for monitoring and diagnostics purposes such as telemetry, auto-scaling, and closed-loop automation. Note that the LxNM may further map to other TE resources as specified in [I-D.ietf-teas-te-service-mapping-yang]. Optionally, a mapping to the NRP can also be populated.

* A mapping of the IETF Network Slice with the underlying TE resources directly. The TE resources could be in a form of VN, set of TE tunnels, TE abstract topology, etc. This mapping can be populated by the network at the time of realization of the IETF network slice service. It is also possible to configure the mapping provided one is aware of NRP/VN/tunnels. This mapping mode is used only when there is an awareness of VN or TE by the consumer of the model. Otherwise, this mapping information is internal and used for monitoring and diagnostics purposes such as telemetry, auto-scaling, and closed-loop automation.

* Possibility to request the creation of a new VN/Tunnel to be bound to IETF network slice.

* Indication to share the VN/Tunnel sharing (with or without modification) for the IETF network slice.

* Support for configuration of underlying TE properties (as opposed to existing VN or tunnels).

Note: The RFC Editor will replace XXXX with the number assigned to the RFC once this draft becomes an RFC.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1. Tree Diagrams

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in these diagrams is defined in [RFC8340].

2.2. Prefixes in Data Node Names

In this document, names of data nodes and other data model objects are often used without a prefix, as long as it is clear from the context in which the YANG module each name is defined. Otherwise, names are prefixed using the standard prefix associated with the corresponding YANG module, as shown in Table 1.

Prefix	YANG module	Reference
nw	ietf-network	[RFC8345]
tsmt	ietf-te-service-mapping-types	[I-D.ietf-teas-te-service-mapping-yang]
l3vpn-ntw	ietf-l3vpn-ntw	[RFC9182]
l2vpn-ntw	ietf-l2vpn-ntw	[RFC9291]
ietf-ns	ietf-network-slice	[I-D.ietf-teas-ietf-network-slice-nbi-yang]
nrp	ietf-nrp	[I-D.ietf-teas-nrp-yang]

Table 1

2.3. References in the Model

The following additional documents are referenced in the model defined in this document -

Document	Reference
Framework for IETF Network Slices	[RFC9543]

Table 2

3. Model Design

The YANG model specified in this document augments the IETF network slice service YANG model [I-D.ietf-teas-ietf-network-slice-nbi-yang].

Currently, the following mapping are supported:

* L3NM: The L3 network model (L3NM) describes a L3VPN Service in the Service Provider Network. It contains information on the Service Provider network and might include allocated resources. It can be used by network controllers to manage and control the L3VPN Service configuration in the Service Provider network. This model maps an IETF network slice to a L3VPN ID.

* L2NM: The L2 network model (L2NM) describes a L2VPN Service in the Service Provider Network. It contains information on the Service Provider network and might include allocated resources. It can be used by network controllers to manage and control the L2VPN Service configuration in the Service Provider network. This model maps an IETF network slice to a L2VPN ID.

* TE: The TE mapping is specified in [I-D.ietf-teas-te-service-mapping-yang]. The mapping can be done to the following TE resources:

  - Virtual Networks (VN) [RFC8453]

  - TE-Tunnels

  - TE-Topology

* NRP: [RFC9543] defines IETF network slice services that provide connectivity coupled with network resources commitment between a number of endpoints over a shared network infrastructure and, for scalability concerns, defines NRP to host one or a group of network slice services according to characteristics including SLOs and SLEs. Along with mapping to VPN, this model maps an IETF network slice to an NRP ID.

Attachment Circuits (ACs) are defined in [RFC9835] as the logical constructs that connect customer edges (CEs) to provider edges (PEs) and carry customer traffic into a RFC 9543 Network Slice Service. The YANG model in [I-D.ietf-teas-ietf-network-slice-nbi-yang] already includes a mapping to AC.

3.1. Open Questions

The following open questions need to be addressed in a future revision:

* Is there a need/use-case to map the IETF Network slice Connection Group and/or Connectivity Construct as well?

* Is there a need/use-case to map IETF Network slice Service Demarcation Points (SDPs)?

* Is there a need to indicate "map-type" (new, share) for NRP and VPNs?

4. Tree Structure

```
   module: ietf-network-slice-mapping

     augment /ietf-nss:network-slice-services/ietf-nss:slice-service:
       +--rw mapping!
          +--rw ns-mapping
             +--rw map-to?                                identityref
             +--rw (map)?
                +--:(nrp)
                |  +--rw nrp?
                |          -> /nw:networks/nrp:nrp-policies/nrp-policy/name
                +--:(l3vpn)
                |  +--rw l3vpn-id?                        leafref
                |  +--rw l3vpn-nrp?
                |          -> /nw:networks/nrp:nrp-policies/nrp-policy/name
                +--:(l2vpn)
                |  +--rw l2vpn-id?                        leafref
                |  +--rw l2vpn-nrp?
                |          -> /nw:networks/nrp:nrp-policies/nrp-policy/name
                +--:(te)
                   +--rw type?                           identityref
                   +--rw te-policy
                   |  +--rw path-affinities-values
                   |  |  +--rw path-affinities-value* [usage]
                   |  |        ...
                   |  +--rw path-affinity-names
                   |  |  +--rw path-affinity-name* [usage]
                   |  |        ...
                   |  +--rw protection-type?          identityref
                   |  +--rw availability-type?        identityref
                   +--rw (te)?
                   |  +--:(vn)
                   |  |  +--rw vn*
                   |  |          -> /vn:virtual-network/vn/id
                   |  +--:(te-topo)
                   |  |  +--rw te-topology-identifier
                   |  |  |     ...
                   |  |  +--rw abstract-node?
                   |  |          -> /nw:networks/network/node/node-id
                   |  +--:(te-tunnel)
                   |     +--rw te-tunnel*                te:tunnel-ref
                   |     +--rw sr-policy* [headend color-ref endpoint-ref]
                   |             {sr-policy}?
                   |           ...
                   +--rw template-ref?                   leafref
                           {template}?
```

5. YANG Model

```
<CODE BEGINS> file "ietf-network-slice-mapping@2025-10-13.yang"
module ietf-network-slice-mapping {
  yang-version 1.1;
  namespace
    "urn:ietf:params:xml:ns:yang:ietf-network-slice-mapping";
  prefix ietf-nsm;

  import ietf-network {
    prefix nw;
    reference
      "RFC 8345: A YANG Data Model for Network Topologies";
  }
  import ietf-network-slice-service {
    prefix ietf-nss;
    reference
      "I-D.ietf-teas-ietf-network-slice-nbi-yang: A YANG Data
       Model for the IETF Network Slice Service";
  }
  import ietf-te-service-mapping-types {
    prefix tsmt;
    reference
      "I-D.ietf-teas-te-service-mapping-yang: Traffic Engineering
       (TE) and Service Mapping YANG Data Model";
  }
  import ietf-l3vpn-ntw {
    prefix l3vpn-ntw;
    reference
      "RFC 9182: A YANG Network Data Model for Layer 3 VPNs";
  }
  import ietf-l2vpn-ntw {
    prefix l2vpn-ntw;
    reference
      "RFC 9291: A Layer 2 VPN Network YANG Model";
  }
  import ietf-nrp {
    prefix nrp;
    reference
      "I-D.ietf-teas-nrp-yang: A YANG Data Model for Network
       Resource Partitions (NRPs)";
  }

  organization
    "IETF Traffic Engineering Architecture and Signaling (TEAS)
     Working Group";
  contact
    "WG Web:  <https://datatracker.ietf.org/wg/teas/>
     WG List:  <mailto:teas@ietf.org>
     Editor: Dhruv Dhody <dhruv.ietf@gmail.com>
```

```
            Bo Wu <lana.wubo@huawei.com>";
    description
      "This module contains a YANG module to map the IETF Network
       Slice with Traffic Engineering (TE) or VPN Network models.

       Copyright (c) 2025 IETF Trust and the persons identified as
       authors of the code.  All rights reserved.

       Redistribution and use in source and binary forms, with or
       without modification, is permitted pursuant to, and subject to
       the license terms contained in, the Revised BSD License set
       forth in Section 4.c of the IETF Trust's Legal Provisions
       Relating to IETF Documents
       (https://trustee.ietf.org/license-info).

       This version of this YANG module is part of RFC XXXX; see the
       RFC itself for full legal notices.";

    revision 2025-10-13 {
      description
        "initial version.";
      reference
        "RFC XXXX: IETF Network Slice Service Mapping YANG Model";
    }

    identity map-to {
      description
        "Base identity from which specific map-to are derived.";
    }

    identity map-to-nrp {
      base map-to;
      description
        "Map to Network Resource Partition (NRP)";
    }

    identity map-to-vpn {
      base map-to;
      description
        "Map to VPN";
    }

    identity map-to-l3vpn {
      base map-to-vpn;
      description
        "Map to L3VPN";
    }
```

```
identity map-to-l2vpn {
  base map-to-vpn;
  description
    "Map to L2VPN";
}

identity map-to-l1vpn {
  base map-to-vpn;
  description
    "Map to L1VPN";
}

identity map-to-te {
  base map-to;
  description
    "Map to TE directly";
}

grouping ns-mapping {
  description
    "Mapping between IETF network slice and Network
     Resource Partition (NRP)/VPN/TE";
  container ns-mapping {
    description
      "The container for the mapping";
    leaf map-to {
      type identityref {
        base map-to;
      }
      description
        "Mapping to NRP/VPN/TE";
    }
    choice map {
      description
        "Mapping to NRP/VPN/TE";
      case nrp {
        leaf nrp {
          type leafref {
            path "/nw:networks/nrp:nrp-policies"
               + "/nrp:nrp-policy/nrp:name";
          }
          description
            "A reference to NRP name";
          reference
            "I-D.ietf-teas-nrp-yang: A YANG Data Model for
             Network Resource Partitions (NRPs)";
        }
      }
```

```
            case l3vpn {
              leaf l3vpn-id {
                type leafref {
                  path "/l3vpn-ntw:l3vpn-ntw"
                     + "/l3vpn-ntw:vpn-services"
                     + "/l3vpn-ntw:vpn-service"
                     + "/l3vpn-ntw:vpn-id";
                }
                description
                  "A reference to VPN ID";
              }
              leaf l3vpn-nrp {
                type leafref {
                  path "/nw:networks/nrp:nrp-policies"
                     + "/nrp:nrp-policy/nrp:name";
                }
                description
                  "An optional reference to NRP name";
                reference
                  "RFC9543: Framework
                   for IETF Network Slices";
              }
              description
                "Mapping to L3NM";
              reference
                "RFC9182: A YANG Network Data Model for
                 Layer 3 VPNs";
            }
            case l2vpn {
              leaf l2vpn-id {
                type leafref {
                  path "/l2vpn-ntw:l2vpn-ntw"
                     + "/l2vpn-ntw:vpn-services"
                     + "/l2vpn-ntw:vpn-service"
                     + "/l2vpn-ntw:vpn-id";
                }
                description
                  "A reference to VPN ID";
              }
              leaf l2vpn-nrp {
                type leafref {
                  path "/nw:networks/nrp:nrp-policies"
                     + "/nrp:nrp-policy/nrp:name";
                }
                description
                  "An optional reference to NRP";
                reference
                  "RFC9543: Framework
```

```
                  for IETF Network Slices";
            }
            description
              "Mapping to L2NM";
            reference
              "RFC 9291: A Layer 2 VPN Network YANG Model";
          }
          case te {
            uses tsmt:te-mapping;
            description
              "Mapping to TE directly";
            reference
              "I-D.ietf-teas-te-service-mapping-yang:
               Traffic Engineering (TE) and Service
               Mapping YANG Model";
          }
        }
      }
    }

    augment "/ietf-nss:network-slice-services/ietf-nss:slice-service" {
      description
        "IETF Network Slice augmented to include the mapping
         information to the network slice realization";
      container mapping {
        presence "Indicates Mapping information";
        description
          "Container to augment IETF network slice to
           include NRP / VPN / TE mappings";
        uses ns-mapping;
      }
    }
  }

  <CODE ENDS>
```

6. Security Considerations

The "ietf-network-slice-mapping" YANG module defines a data model that is designed to be accessed via YANG-based management protocols, such as NETCONF [RFC6241] and RESTCONF [RFC8040]. These YANG-based management protocols (1) have to use a secure transport layer (e.g., SSH [RFC4252], TLS [RFC8446], and QUIC [RFC9000]) and (2) have to use mutual authentication.

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.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., "config true", which is the default). All writable data nodes are likely to be sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) and delete operations to these data nodes without proper protection or authentication can have a negative effect on network operations. The following subtrees and data nodes have particular sensitivities/vulnerabilities:

* /ietf-nss:network-slice-services/ietf-nss:slice-service/mapping/ns-mapping/ - can configure Network Slice Service mapping.

There are no particularly sensitive readable data nodes.

There are no particularly sensitive RPC or action operations.

This YANG module uses groupings from other YANG modules that define nodes that may be considered sensitive or vulnerable in network environments. Refer to the Security Considerations of [I-D.ietf-teas-te-service-mapping-yang] for information as to which nodes may be considered sensitive or vulnerable in network environments.

7. IANA Considerations

IANA is requested to make the following allocation for the URIs in the "ns" subregistry within the "IETF XML Registry" [RFC3688]:

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

IANA is requested to make the following allocation for the YANG module in the "YANG Module Names" registry [RFC6020]:

```
---------------------------------------------------------------------
name:         ietf-network-slice-mapping
namespace:    urn:ietf:params:xml:ns:yang:ietf-network-slice-mapping
prefix:       ietf-nsm
reference:    RFC XXXX
---------------------------------------------------------------------
```

8. References

8.1. Normative References

[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/rfc/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/rfc/rfc3688>.

[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/rfc/rfc6020>.

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

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/rfc/rfc8340>.

[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/rfc/rfc8341>.

[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/rfc/rfc8345>.

[RFC9182] Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., Munoz, L., and A. Aguado, "A YANG Network Data Model for Layer 3 VPNs", RFC 9182, DOI 10.17487/RFC9182, February 2022, <https://www.rfc-editor.org/rfc/rfc9182>.

[RFC9291] Boucadair, M., Ed., Gonzalez de Dios, O., Ed., Barguil, S., and L. Munoz, "A YANG Network Data Model for Layer 2 VPNs", RFC 9291, DOI 10.17487/RFC9291, September 2022, <https://www.rfc-editor.org/rfc/rfc9291>.

[I-D.ietf-teas-ietf-network-slice-nbi-yang]
Wu, B., Dhody, D., Rokui, R., Saad, T., and J. Mullooly, "A YANG Data Model for the RFC 9543 Network Slice Service", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slice-nbi-yang-25, 9 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-nbi-yang-25>.

[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 Data Model", Work in Progress, Internet-Draft, draft-ietf-teas-te-service-mapping-yang-18, 12 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-te-service-mapping-yang-18>.

[I-D.ietf-teas-nrp-yang]
Wu, B., Dhody, D., Beeram, V. P., Saad, T., and S. Peng, "YANG Data Models for Network Resource Partitions (NRPs)", Work in Progress, Internet-Draft, draft-ietf-teas-nrp-yang-04, 21 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-nrp-yang-04>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

8.2. Informative References

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, <https://www.rfc-editor.org/rfc/rfc4252>.

[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/rfc/rfc6241>.

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

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[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/rfc/rfc8453>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[RFC9835] Boucadair, M., Ed., Roberts, R., Gonzalez de Dios, O., Barguil, S., and B. Wu, "A Network YANG Data Model for Attachment Circuits", RFC 9835, DOI 10.17487/RFC9835, September 2025, <https://www.rfc-editor.org/rfc/rfc9835>.

[RFC9543] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "A Framework for Network Slices in Networks Built from IETF Technologies", RFC 9543, DOI 10.17487/RFC9543, March 2024, <https://www.rfc-editor.org/rfc/rfc9543>.

[I-D.ietf-teas-ns-ip-mpls] Saad, T., Beeram, V. P., Dong, J., Halpern, J. M., and S. Peng, "Realizing Network Slices in IP/MPLS Networks", Work in Progress, Internet-Draft, draft-ietf-teas-ns-ip-mpls-05, 2 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ns-ip-mpls-05>.

Appendix A. Acknowledgments

Thanks to Jie Dong and Adrian Farrel for the initial discussion behind this document.

Appendix B. Examples

To be added in future revisions.

Authors' Addresses

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

Bo Wu
Huawei Technologies
101 Software Avenue, Yuhua District

Nanjing
210012
China
Email: lana.wubo@huawei.com