RFC 9408
A YANG Network Data Model for Service Attachment Points (SAPs)

Abstract

This document defines a YANG data model for representing an abstract view of the provider network topology that contains the points from which its services can be attached (e.g., basic connectivity, VPN, network slices). Also, the model can be used to retrieve the points where the services are actually being delivered to customers (including peer networks).

This document augments the 'ietf-network' data model defined in RFC 8345 by adding the concept of Service Attachment Points (SAPs). The SAPs are the network reference points to which network services, such as Layer 3 Virtual Private Network (L3VPN) or Layer 2 Virtual Private Network (L2VPN), can be attached. One or multiple services can be bound to the same SAP. Both User-to-Network Interface (UNI) and Network-to-Network Interface (NNI) are supported in the SAP data model.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9408.

Copyright Notice

Table of Contents

1. Introduction

Service providers offer a variety of network services to their customers. Such services include, but are not limited to, Virtual Private Networks (VPNs), Software-Defined Wide-Area Network (SD-WAN) overlay networks [BGP-SDWAN-USAGE], and network slices [IETF-NETWORK-SLICES]. In order to rationalize the overall service operations and allow for more automated service provisioning procedures, service providers need to maintain a view on where services can be

delivered to customers. For example, such a view can be used to feed an intelligence entity that is responsible for service order handling, service feasibility checks, tracking per-service coverage, etc. (e.g., Section 3.2 of [RFC8969]). To that aim, this document introduces the concept of Service Attachment Points (SAPs).

The SAPs represent the network reference points where network services can be delivered to customers. For example, this concept is used to decide where to attach and thus deliver the service in the Layer 3 VPN Service Model (L3SM) [RFC8299] and the Layer 2 VPN Service Model (L2SM) [RFC8466]. It can also be used to retrieve where such services are delivered to customers through the network configuration described in the Layer 3 VPN Network Model (L3NM) [RFC9182] and the Layer 2 VPN Network Model (L2NM) [RFC9291].

This document defines a YANG network model (Section 6) for representing, managing, and controlling the SAPs. The data model augments the 'ietf-network' module [RFC8345] by adding the concept of SAPs. Section 3 provides a sample usage of the model. This document explains the scope and purpose of a SAP network model and its relationship to other models (Section 4).

A network may support multiple services, potentially of different types. Whether a SAP topology is dedicated to services of a specific service type or an individual service, or is shared among many services of different types, is deployment specific. This document supports all of these deployment schemes.

This document does not make any assumptions about the services provided by a network to its users. VPN services (e.g., Layer 3 Virtual Private Network (L3VPN) or Layer 2 Virtual Private Network (L2VPN)) [RFC4026] are used for illustration purposes (Appendices A and B).

Given that User-to-Network Interface (UNI) and Network-to-Network Interface (NNI) are reference points that are widely used by operators to indicate the demarcation points when delivering services, both UNI and NNI SAPs are supported in this document. The reader may refer to [MEF6], [MEF17], [RFC6004], or [RFC6215] for examples of discussions regarding the use of UNI and NNI reference points. An example of NNI usage in a VPN context is provided in Appendix C.

The YANG data model in Section 6 conforms to the Network Management Datastore Architecture (NMDA) [RFC8342].

2. Terminology

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.

This document assumes that the reader is familiar with the contents of [RFC6241], [RFC7950], [RFC8345], and [RFC8309], as it uses terms from those RFCs.

The meanings of the symbols in tree diagrams are defined in [RFC8340].

This document uses the term "network model" as defined in Section 2.1 of [RFC8969].

This document uses the following terms:

Service provider: The organization responsible for operating the network that offers a service (e.g., a VPN) to customers.

Attachment Circuit (AC):   A channel that connects a Customer Edge (CE) to a Provider Edge (PE).

Customer Edge (CE):   Equipment that is dedicated to a particular customer and is directly connected to one or more PEs via ACs. A CE is usually located at the customer premises. A CE may be dedicated to a single service (e.g., an L3VPN), although it may support multiple VPNs if each one has separate ACs. A CE can be a router, a bridge, a switch, etc.

Provider Edge (PE):   Equipment owned and managed by the service provider that can support multiple services (e.g., VPNs) for different customers. A PE is directly connected to one or more CEs via ACs.

Service Attachment Points (SAPs):   An abstraction of the network reference points (e.g., the PE side of an AC, or the CE side of an AC for a provider-managed CE) where network services can be delivered and/or are delivered to customers. A SAP can be bound to one or multiple ACs.

3. Sample SAP Network Model Usage

A service provider network's management operations can be automated using a variety of means such as interfaces based on YANG modules [RFC8969] [RFC6241] [RFC8040]. From that standpoint, and considering the architecture depicted in Figure 1, a goal of this document is to provide a mechanism to show, via a YANG-based interface, an abstracted network view from the network controller to the service orchestration layer with a focus on where a service can be delivered to customers. The model is also used to retrieve the network reference points where a service is being delivered to customers. For services that require resources from peer networks, the model can also be used to expose NNIs.

```
                        +-----------------+
                        |    Customer     |
                        +--------+--------+
        Customer Service Models  |
           (e.g., L3SM, L2SM)    |
                        +--------+--------+
                        |     Service     |
                        |  Orchestration  |
                        +------+---+------+
            Network Models     |   | SAP Network Model
           (e.g., L3NM, L2NM)  |   |
                        +------+---+------+
                        |     Network     |
                        |   Controller    |
                        +--------+--------+
                                 |
        +------------------------+--------------------+
        |                     Network                 |
        +---------------------------------------------+
```
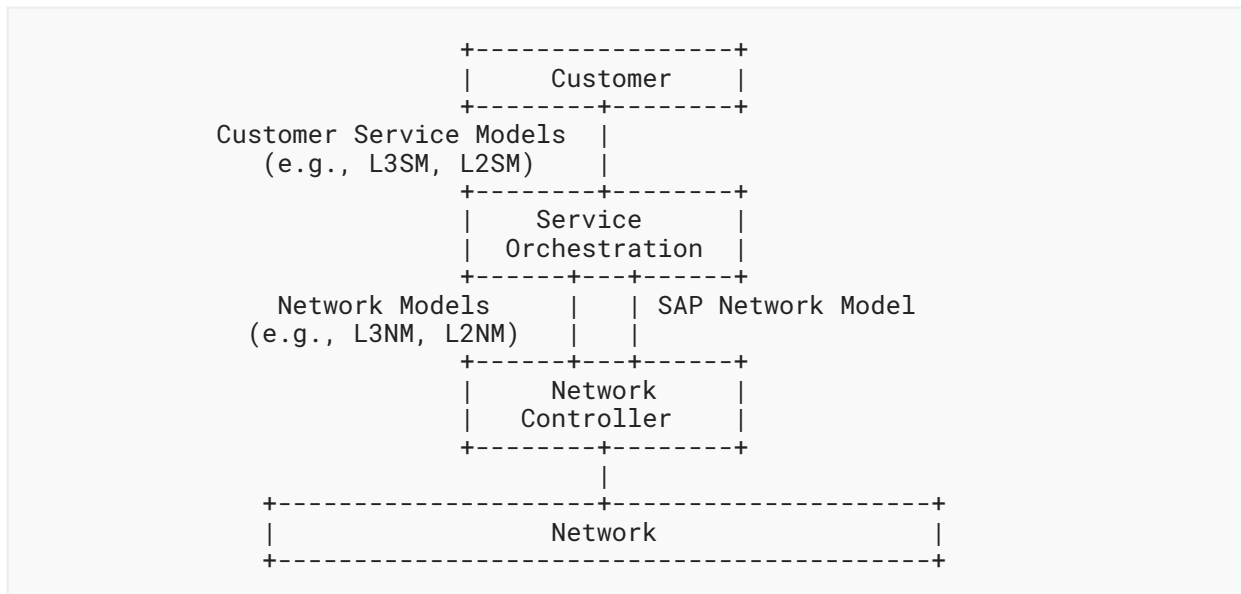
Figure 1: SAP Network Model Usage

The reader may refer to Section 5 of [RFC4026] for an overview of the building blocks that are usually invoked when characterizing a service provider network.

The service orchestration layer does not need to know about all the internals of the underlying network (e.g., P nodes (Section 5.3.1 of [RFC4026])). Figure 2 shows the abstract network view as seen by a service orchestrator. However, this view is not enough to provide to the service orchestration layer the information to create services in the network. The service topology needs to be able to expose the set of nodes and the attachment points associated with the nodes from which network services can be grafted (delivered).

```
         .----------.              .----------.
         |   PE1    |              |   PE2    |
         '----------'              '----------'
                     \          /
                      \------/
                       (      )
                     (          )
                       (      )
                      /------\
                     /          \
         .----------.              .----------.
         |   PE3    |              |   PE4    |
         '----------'              '----------'
```

Figure 2: Abstract Network Topology

Typically, and focusing on the UNIs, the service orchestration layer would see a set of PEs and a set of client-facing interfaces (physical or logical) to which CEs can be connected (or are actually connected). Such interfaces are also referred to as UNI-N (User-to-Network Interface, Network

side) [RFC6215]. The service orchestration layer can use these interfaces to set up the requested services or to commit the delivery of a service. Figure 3 depicts a sample SAP network topology that is maintained by the network controller and exposed to the service orchestration.

```
              .-+-. .-+-. .-+-.                     .-+-.           .-+-.
             .-|sap|-|sap|-|sap|-.                 .-|sap|-------|sap|-.
             | '---' '---' '---' |                 | '---'           '---' |
         .---.                   |                 |                       |
         |sap|       PE1         |                 |          PE2          |
         '---'                   |                 |                       |
             |                   |                 |                       |
             '_____'                 '_____'


              .-------------------.                 .-------------------.
              |                   |                 |                   |
              |                   |                 |                  .---.
              |        PE3        |                 |        PE4       |sap|
              |                   |                 |                  '---'
              | .---. .---. .---. |                 | .---. .---. .---. |
              '-|sap|-|sap|-|sap|-'                 '-|sap|-|sap|-|sap|-'
                '-+-' '-+-' '-+-'                     '-+-' '-+-' '-+-'
```
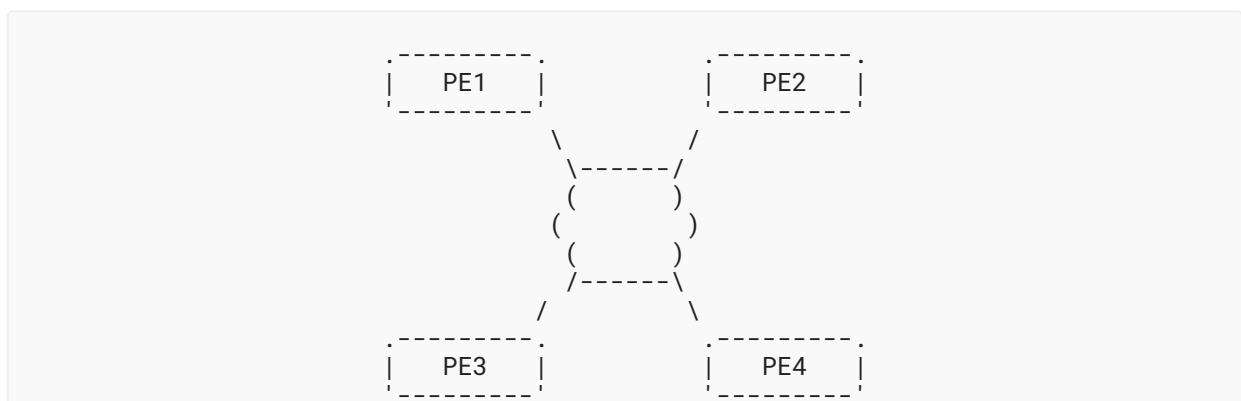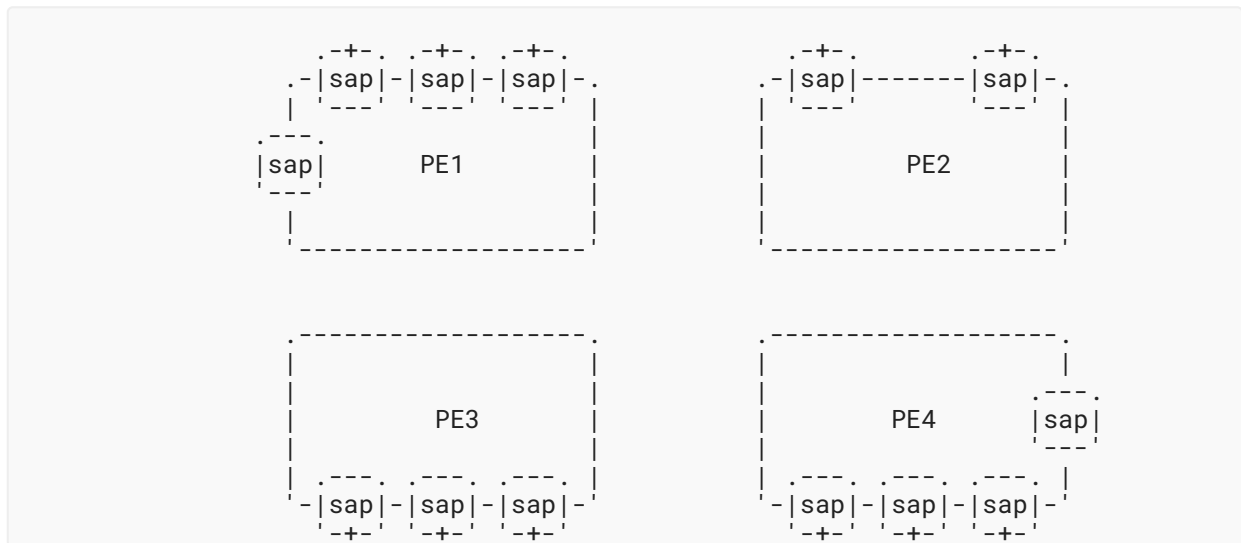
Figure 3: A SAP Network Topology

A single SAP network topology can be used for one or multiple service types (e.g., L3VPN, Ethernet VPN (EVPN)). The network controller can then expose the service types and associated interfaces via the SAPs.

As shown in Figure 4, the service orchestration layer will also have access to a set of customer service models (e.g., the L3SM or the L2SM) in the customer-facing interface and a set of network models (e.g., the L3NM and network topology data models) in the resource-facing interface. In this use case, it is assumed that the network controller is unaware of what happens beyond the PEs towards the CEs; it is only responsible for the management and control of the SAPs and the network between PEs. In order to correlate between delivery points expressed in service requests and SAPs, the SAP model may include a peer customer point identifier. That identifier can be a CE identifier, a site identifier, etc.
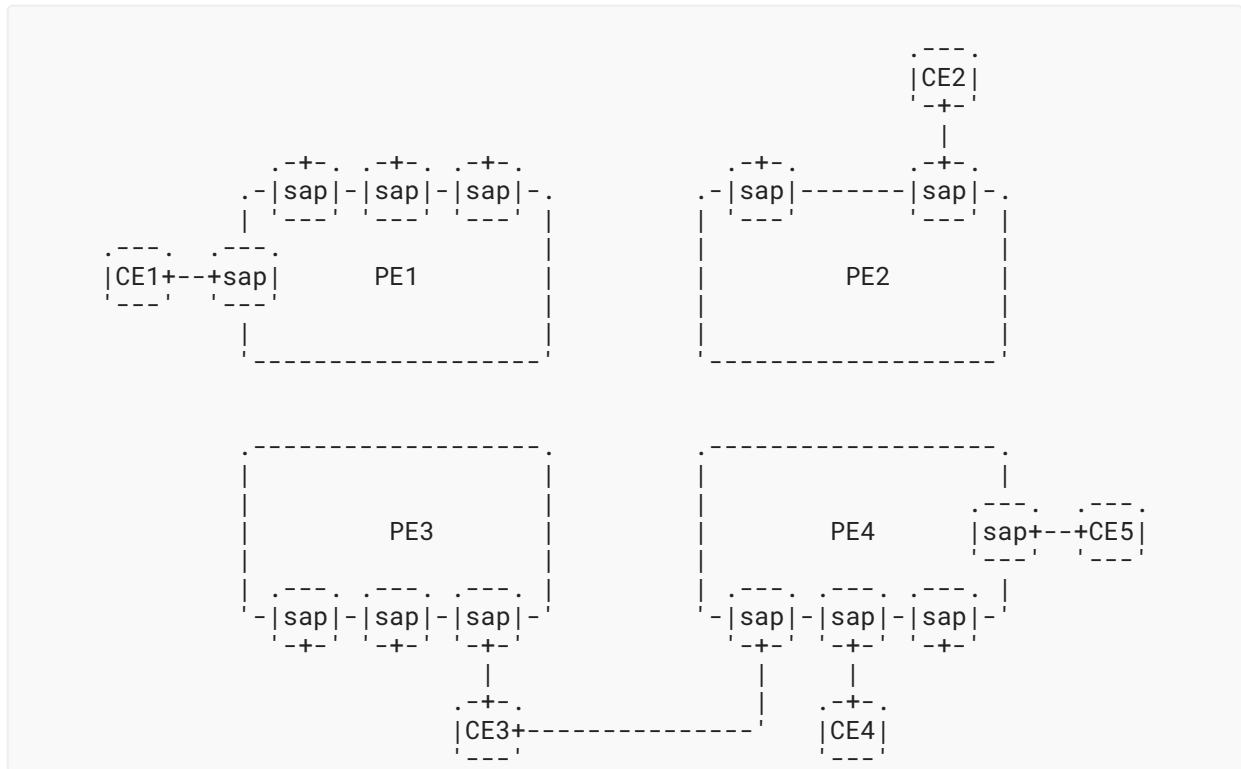
```
                                                            .---.
                                                            |CE2|
                                                            '-+-'
                                                              |
             .-+-. .-+-. .-+-.              .-+-.           .-+-.
            .-|sap|-|sap|-|sap|-.          .-|sap|-------|sap|-.
            | '---' '---' '---'  |         | '---'         '---' |
    .---. .---.                  |         |                     |
    |CE1+--+sap|      PE1        |         |         PE2         |
    '---' '---'                  |         |                     |
            |                    |         |                     |
            '--------------------'         '---------------------'


         .--------------------.          .--------------------.
         |                    |          |                    |
         |                    |          |                    |
         |        PE3         |          |        PE4      .---.  .---.
         |                    |          |                 |sap+--+CE5|
         |                    |          |                 '---'  '---'
         | .---. .---. .---.  |          | .---. .---. .---.  |
         '-|sap|-|sap|-|sap|-'           '-|sap|-|sap|-|sap|-'
           '-+-' '-+-' '-+-'               '-+-' '-+-' '-+-'
             |                                 |     |
           .-+-.                               |   .-+-.
           |CE3+--------------'                |   |CE4|
           '---'                               |   '---'
```

Figure 4: Network Topology with CEs and ACs

Refer to Appendix A for an example echoing the topology depicted in Figure 4.

4. Relationship to Other YANG Data Models

The SAP network model can be seen as inventory data associated with SAPs. The model maintains an inventory of customer-facing nodes contained in a network relying upon [RFC8345].

Figure 5 depicts the relationship of the SAP network model to other models. The SAP network model augments the network model defined in [RFC8345] and imports the network topology model defined in [RFC8345], while other technology-specific topology models (e.g., the model for Traffic Engineering (TE) topologies [RFC8795] or the model for Layer 3 topologies [RFC8346]) augment the network topology model defined in [RFC8345].
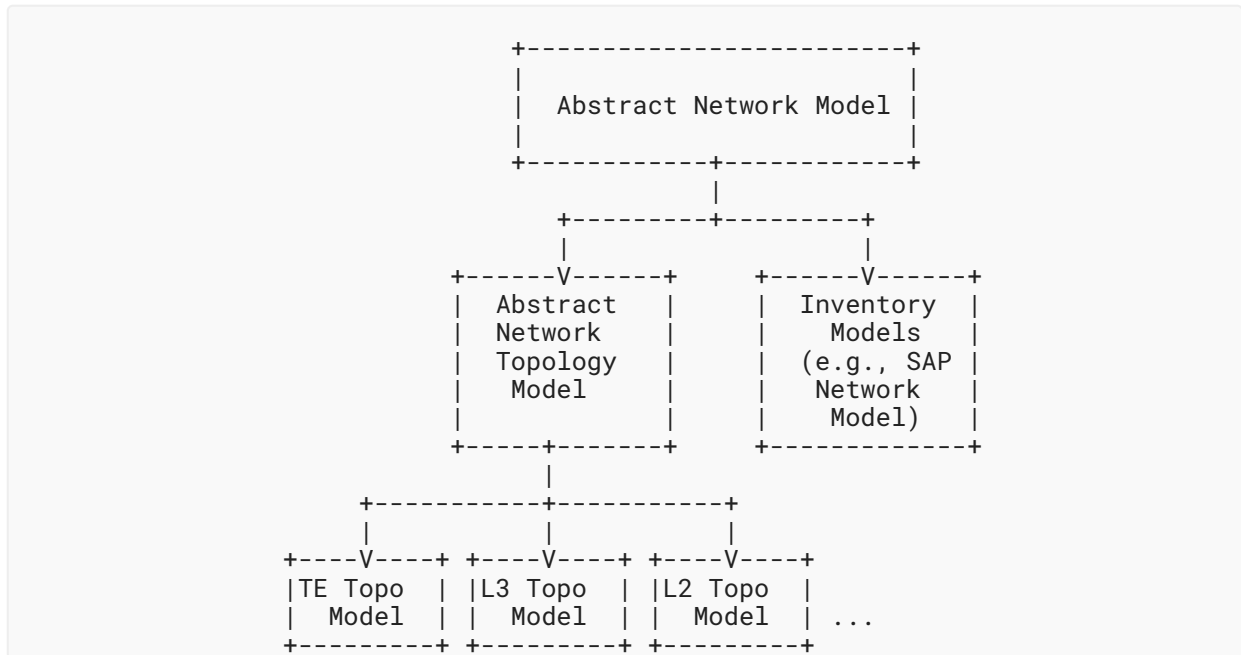
```
              +-------------------------+
              |                         |
              |   Abstract Network Model |
              |                         |
              +-----------+-------------+
                          |
              +---------+---------+
              |                   |
      +------V------+      +------V------+
      |  Abstract   |      | Inventory   |
      |  Network    |      |   Models    |
      |  Topology   |      | (e.g., SAP  |
      |   Model     |      |  Network    |
      |             |      |   Model)    |
      +-----+-------+      +-------------+
            |
   +----------+----------+
   |          |          |
+----V----+ +----V----+ +----V----+
|TE Topo  | |L3 Topo  | |L2 Topo  |
|  Model  | |  Model  | |  Model  | ...
+---------+ +---------+ +---------+
```

Figure 5: Relationship of SAP Network Model to Other Models

SAPs can be seen as customer-facing termination points (TPs) with specific service provisions. However, one difference between SAPs and TPs is that links are terminated by a single TP (Section 4.4.6 of [RFC8345]) while an AC can be terminated by multiple SAPs. Also, a SAP is neither a tunnel termination point (TTP) (Section 3.6 of [RFC8795]) nor a link.

In the context of Software-Defined Networking (SDN) [RFC7149] [RFC7426], the SAP YANG data model can be used to exchange information between control elements, so as to support VPN service provision and resource management as discussed in [RFC9182] and [RFC9291]. Through this data model, the service orchestration layer can learn the available endpoints (i.e., SAPs) of interconnection resources of the underlying network. The service orchestration layer can determine which interconnection endpoints to add to an L2VPN or L3VPN service. With the help of other data models (e.g., the L3SM [RFC8299] or the L2SM [RFC8466]), hierarchical control elements can also assess the feasibility of end-to-end IP connectivity or L2VPN connectivity and therefore can derive the sequence of domains and the points of interconnection to use.

Advanced interface-specific data nodes are not included in the SAP model. The interface identifiers listed in the SAP model can be used as filters to set or get such data using device models (e.g., [RFC7224]).

5. SAP Module Tree Structure

The SAP network model 'ietf-sap-ntw' builds on the 'ietf-network' module [RFC8345] by augmenting the nodes with SAPs.

The structure of the 'ietf-sap-ntw' module is shown in Figure 6.

```
module: ietf-sap-ntw
  augment /nw:networks/nw:network/nw:network-types:
    +--rw sap-network!
       +--rw service-type*   identityref
  augment /nw:networks/nw:network/nw:node:
    +--rw service* [service-type]
       +--rw service-type                  identityref
       +--rw sap* [sap-id]
          +--rw sap-id                    string
          +--rw description?              string
          +--rw parent-termination-point?  nt:tp-id
          +--rw attachment-interface?     string
          +--rw interface-type?           identityref
          +--rw encapsulation-type?       identityref
          +--rw role?                     identityref
          +--rw allows-child-saps?        boolean
          +--rw peer-sap-id*              string
          +--ro sap-status
          |  +--ro status?        identityref
          |  +--ro last-change?   yang:date-and-time
          +--rw service-status
             +--rw admin-status
             |  +--rw status?        identityref
             |  +--rw last-change?   yang:date-and-time
             +--ro oper-status
                +--ro status?        identityref
                +--ro last-change?   yang:date-and-time
```

Figure 6: SAP YANG Module Tree Structure

A SAP network topology can be used for one or multiple service types ('service-type'). Examples of supported service types are as follows:

- L3VPN [RFC4364]
- Virtual Private LAN Service (VPLS) [RFC4761] [RFC4762]
- Virtual Private Wire Service (VPWS) [RFC8214]
- BGP MPLS-based Ethernet VPN [RFC7432]
- VPWS in Ethernet VPN [RFC8214]
- Provider Backbone Bridging combined with Ethernet VPN (PBB-EVPN) [RFC7623]
- VXLAN-based EVPN [RFC8365] ("VXLAN" stands for "Virtual eXtensible Local Area Network")
- Virtual Network [RFC8453]
- Enhanced VPN (VPN+) [ENHANCED-VPN]
- Network slice service [IETF-NETWORK-SLICES]
- SD-WAN [BGP-SDWAN-USAGE]
- Basic IP connectivity

These service types build on the types that are already defined in [RFC9181] and additional types that are defined in this document. Other service types can be defined in future YANG modules (including future revisions of the YANG module defined in this document), if needed.

> Leveraging the service types defined in [RFC9181] is meant to ease the correlation
> between the SAP topology and the corresponding network models that are used to
> provision a specific service over a provider's network.

Filters based on the service type can be used to access per-service SAP topology. An example is depicted in Figure 10 in Appendix B.

A node in the topology can support one or multiple service types ('service-type') among those listed under the 'sap-network' container. A list of SAPs is then bound to each service type that is supported by a given node. Each SAP is characterized as follows:

'sap-id':   Includes an identifier that uniquely identifies a SAP within a node.

The same SAP may appear under distinct service types. In such a case, the same identifier is used for a shared SAP for each of these service types.

SAPs that are associated with the interfaces that are directly hosting services, interfaces that are ready to host per-service sub-interfaces (but are not yet activated), or services that are already instantiated on sub-interfaces are listed as SAPs. For illustration purposes, Figure 9 in Appendix B depicts how to indicate interfaces that are capable of hosting per-service sub-interfaces.

For example, 'sap-id' may be the VPN network access identifier defined in Section 7.6 of [RFC9182]. An example that illustrates the use of this attribute during service creation is provided in Appendix D.

'description':   Includes a textual description of the SAP.

'parent-termination-point':   Includes a reference to the parent termination point to which the SAP is bound. As per Section 4.2 of [RFC8345], a termination point terminates a link in a node. A termination point can be a physical port, an interface, etc.

The referenced parent termination point is expected to be a customer-facing termination point, not a core-facing termination point.

For example, this attribute is used to associate an interface with its sub-interfaces, as all these interfaces may be listed under the SAPs of a node. It is also used to link a SAP with the physical topology.

For example, this data node can be used to map the IETF Network Slice endpoints [IETF-NETWORK-SLICES] to the service/tunnel/path endpoints in the underlay network.

'attachment-interface':   Indicates a reference to the interface to which the SAP is bound. The same interface may host multiple services.

Whether the attachment identifier echoes the content of the attachment interface is deployment specific.

For example, this reference may be any of the identifiers ('l2-termination-point', 'local-bridge-reference', 'bearer-reference', or 'lag-interface-id') defined in Section 7.6.1 of [RFC9182] or 'l3-termination-point' as defined in Section 7.6.2 of [RFC9182]. The controller is responsible for ensuring that consistent references are used in the SAP and underlying device models or any other device inventory mechanism.

'interface-type':   Indicates whether a SAP is bound to a physical port, a loopback interface, a Link Aggregation Group (LAG) interface [IEEE802.1AX], an Integrated Routing and Bridging (IRB) interface (e.g., [RFC9135]), a local bridge reference, etc.

The mapping to the detailed interface types as per [RFC7224] is maintained by the controller. That mapping is used, for example, when the controller translates this SAP network model into device models (Section 4.4 of [RFC8969]).

'encapsulation-type':   Indicates the encapsulation type for the interface indicated in the 'attachment-interface' attribute. The types are taken from [RFC9181].

This data node can be used, for example, to decide whether an existing SAP can be (re)used to host a service or if a new sub-interface has to be instantiated.

'role':   Specifies the role of a SAP (e.g., a UNI or NNI).

A SAP inherits the role of its parent interface ('parent-termination-point').

'allows-child-saps':   When set to 'true', indicates that the attachment interface for this SAP is capable of hosting per-service sub-interfaces.

Whether a service can be directly attached to the parent SAP in addition to child SAPs depends on the service.

'peer-sap-id':   Includes references to the remote endpoints of an AC. This identifier may or may not be the same as the SAP identifier used in the peer's configuration. Note that the use of identical identifiers eases the correlation between a peer's service request and a local SAP.

Examples of such a reference are a site identifier (Section 6.3 of [RFC8299]), a Service Demarcation Point (SDP) identifier (Section 3.2 ("Core Terminology") of [IETF-NETWORK-SLICES]), and the IP address of a peer Autonomous System Border Router (ASBR).

'sap-status':   Indicates the operational status of a SAP. Values are taken from the values defined in [RFC9181].

When both a sub-interface and its parent interface are present but the parent interface is disabled, the status of the parent interface takes precedence over the status indicated for the sub-interface.

'service-status':   Indicates the administrative and operational status of the service for a given SAP. This information is particularly useful when many services are provisioned for the same SAP but only a subset of these services is activated. As such, the administrative 'service-status' **MUST NOT** be influenced by the value of the operational 'sap-status'.

The service 'oper-status' reflects the operational status of the service only as observed at a specific SAP, not the overall network-level status of the service connecting many SAPs. The network-level service status can be retrieved using specific network models, e.g., those listed in Section 7.3 of [RFC9182] or Section 7.3 of [RFC9291].

In order to assess the service delivery status for a given SAP, it is recommended to check both the administrative and operational service status ('service-status') in addition to the 'sap-status'. In doing so, a network controller (or operator) can detect anomalies. For example, if a service is administratively enabled for a SAP and the 'sap-status' of that SAP is reported as being down, the service 'oper-status' is also expected to be down. Retrieving a distinct service operational status under these conditions can be used as a trigger to detect an anomaly. Likewise, administrative status and operational status can be compared to detect service-specific SAP activation anomalies. For example, a service that is administratively declared as inactive for a SAP but reported as operationally active for that SAP is an indication that some service provision actions are needed to align the observed service status with the expected service status.

6. SAP YANG Module

This module imports types from [RFC6991], [RFC8345], and [RFC9181].

The 'sap-entry' and 'sap-list' are defined as groupings for the reuse of these nodes in service-specific YANG modules.

```
<CODE BEGINS> file "ietf-sap-ntw@2023-06-20.yang"

module ietf-sap-ntw {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-sap-ntw";
  prefix sap;

  import ietf-network-topology {
    prefix nt;
    reference
      "RFC 8345: A YANG Data Model for Network
                 Topologies, Section 6.2";
  }
  import ietf-network {
    prefix nw;
    reference
      "RFC 8345: A YANG Data Model for Network
                 Topologies, Section 6.1";
  }
  import ietf-vpn-common {
    prefix vpn-common;
    reference
      "RFC 9181: A Common YANG Data Model for Layer 2 and Layer 3
                 VPNs";
  }
  import ietf-yang-types {
    prefix yang;
```

```
          reference
            "RFC 6991: Common YANG Data Types, Section 3";
        }

        organization
          "IETF OPSA (Operations and Management Area) Working Group";
        contact
          "WG Web:   <https://datatracker.ietf.org/wg/opsawg/>
           WG List:  <mailto:opsawg@ietf.org>

           Editor:    Mohamed Boucadair
                      <mailto:mohamed.boucadair@orange.com>

           Author:    Oscar Gonzalez de Dios
                      <mailto:oscar.gonzalezdedios@telefonica.com>

           Author:    Samier Barguil
                      <mailto:samier.barguil_giraldo@nokia.com>

           Author:    Qin Wu
                      <mailto:bill.wu@huawei.com>

           Author:    Victor Lopez
                      <mailto:victor.lopez@nokia.com>";
        description
          "This YANG module defines a model for representing, managing,
           and controlling the Service Attachment Points (SAPs) in the
           network topology.

           Copyright (c) 2023 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 9408; see the
           RFC itself for full legal notices.";

        revision 2023-06-20 {
          description
            "Initial version.";
          reference
            "RFC 9408: A YANG Network Data Model for Service Attachment
                       Points (SAPs)";
        }

        identity virtual-network {
          base vpn-common:service-type;
          description
            "Virtual network.  Refers to a logical network instance
             that is built over a physical network.";
          reference
            "RFC 8453: Framework for Abstraction and Control of TE
                       Networks (ACTN)";
```

```
      }

      identity enhanced-vpn {
        base vpn-common:service-type;
        description
          "Enhanced VPN (VPN+).  VPN+ is an approach that is
           based on existing VPN and Traffic Engineering (TE)
           technologies but adds characteristics that specific
           services require over and above conventional VPNs.";
        reference
          "draft-ietf-teas-enhanced-vpn:
             A Framework for Enhanced Virtual Private Network
             (VPN+)";
      }

      identity network-slice {
        base vpn-common:service-type;
        description
          "IETF Network Slice.  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
           objectives.";
        reference
          "draft-ietf-teas-ietf-network-slices:
             A Framework for IETF Network Slices";
      }

      identity sdwan {
        base vpn-common:service-type;
        description
          "PE-based Software-Defined Wide-Area Network (SD-WAN).";
        reference
          "draft-ietf-bess-bgp-sdwan-usage:
             BGP Usage for SD-WAN Overlay Networks";
      }

      identity basic-connectivity {
        base vpn-common:service-type;
        description
          "Basic IP connectivity.  This is, for example, a plain
           form of connectivity offered to enterprises over a
           dedicated or shared MPLS infrastructure.";
      }

      identity interface-role {
        description
          "Base identity for the network role of an interface.";
      }

      identity uni {
        base interface-role;
        description
          "User-to-Network Interface (UNI).";
      }

      identity nni {
        base interface-role;
```

```
      description
        "Network-to-Network Interface (NNI).";
    }

    identity interface-type {
      description
        "Base identity for the interface type.";
    }

    identity phy {
      base interface-type;
      description
        "Physical port.";
    }

    identity loopback {
      base interface-type;
      description
        "Loopback interface.";
    }

    identity lag {
      base interface-type;
      description
        "Link Aggregation Group (LAG) interface.";
    }

    identity irb {
      base interface-type;
      description
        "Integrated Routing and Bridging (IRB) interface.  An IRB
         interface typically connects an IP Virtual Routing and
         Forwarding (IP-VRF) entity to a bridge domain.";
    }

    identity local-bridge {
      base interface-type;
      description
        "A local bridge reference to accommodate (for example)
         implementations that require internal bridging.
         When such a type is used, a reference to a local
         bridge domain is used to identify the interface.";
    }

    identity logical {
      base interface-type;
      description
        "Refers to a logical sub-interface that is typically
         used to bind a service.  This type is used only
         if none of the other more specific types (i.e.,
         'loopback', 'lag', 'irb', or 'local-bridge') can be used.";
    }

    grouping sap-entry {
      description
        "Service Attachment Point (SAP) entry information.";
      leaf sap-id {
        type string;
```

```
              description
                "Indicates an identifier that uniquely identifies
                 a SAP.";
            }
            leaf description {
              type string;
              description
                "A textual description of the SAP.";
            }
            leaf parent-termination-point {
              type nt:tp-id;
              description
                "Indicates the parent termination point to
                 which the SAP is attached.  A termination
                 point can be a physical port, an interface, etc.";
            }
            leaf attachment-interface {
              type string;
              description
                "Indicates the interface to which the SAP is bound.";
            }
            leaf interface-type {
              type identityref {
                base interface-type;
              }
              description
                "The type of the interface to which the SAP is bound.";
            }
            leaf encapsulation-type {
              type identityref {
                base vpn-common:encapsulation-type;
              }
              description
                "Encapsulation type of the interface to which the
                 SAP is bound.";
            }
            leaf role {
              type identityref {
                base interface-role;
              }
              description
                "Indicates the role of a SAP.";
            }
            leaf allows-child-saps {
              type boolean;
              description
                "Indicates whether the attachment interface of this
                 SAP is capable of hosting per-service sub-interfaces.";
            }
            leaf-list peer-sap-id {
              type string;
              description
                "Indicates an identifier of the peer's termination
                 identifier (e.g., a Customer Edge (CE)).  This
                 information can be used for correlation purposes,
                 such as identifying the SAP that is attached to
                 an endpoint that is provided in a service request.";
            }
```

```
      }

    grouping sap-list {
      description
        "SAP information.";
      list sap {
        key "sap-id";
        description
          "The SAPs are an abstraction of the points to which
           network services such as L3VPNs, L2VPNs, or network
           slices can be attached.";
        uses sap-entry;
        container sap-status {
          config false;
          description
            "Indicates the operational status of the SAP,
             independent of any service provisioned over it.";

          uses vpn-common:oper-status-timestamp;
        }
        container service-status {
          description
            "Indicates the service status.";
          container admin-status {
            description
              "Administrative service status.";
            leaf status {
              type identityref {
                base vpn-common:administrative-status;
              }
              description
                "Administrative status of the service provisioned
                 at the SAP.";
            }
            leaf last-change {
              type yang:date-and-time;
              description
                "Indicates the actual date and time of the service
                 status change.";
            }
          }
          container oper-status {
            config false;
            description
              "Operational status of the service provisioned
               at the SAP.";
            uses vpn-common:oper-status-timestamp;
          }
        }
      }
    }

    augment "/nw:networks/nw:network/nw:network-types" {
      description
        "Introduces a new network type for a SAP network.";
      container sap-network {
        presence "Indicates the SAP network type.";
        description
```

```
              "The presence of the container node indicates the
               SAP network type.";
          leaf-list service-type {
            type identityref {
              base vpn-common:service-type;
            }
            description
              "Indicates the set of supported service types.";
          }
        }
      }

    augment "/nw:networks/nw:network/nw:node" {
      when '../nw:network-types/sap:sap-network' {
        description
          "Augmentation parameters apply only for SAP
           networks.";
      }
      description
        "SAP parameters for the node level.";
      list service {
        key "service-type";
        description
          "A list of supported service types for the node.";
        leaf service-type {
          type identityref {
            base vpn-common:service-type;
          }
          description
            "Indicates a service type.";
        }
        uses sap-list;
      }
    }
  }

  <CODE ENDS>
```

7. IANA Considerations

This document registers the following namespace URI in the "ns" subregistry within the "IETF XML Registry" [RFC3688]:

URI: urn:ietf:params:xml:ns:yang:ietf-sap-ntw
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.

This document registers the following YANG module in the "YANG Module Names" subregistry [RFC6020] within the "YANG Parameters" registry:

Name: ietf-sap-ntw
Namespace: urn:ietf:params:xml:ns:yang:ietf-sap-ntw

Maintained by IANA?   N
Prefix: sap
Reference: RFC 9408

8. Security Considerations

The YANG module specified in this document defines a schema 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 [RFC8446].

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). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. These are the subtrees and data nodes and their sensitivity/vulnerability:

/nw:networks/nw:network/nw:node/sap:service/sap:sap
   This subtree specifies the configurations of the nodes in a SAP network model. Unexpected changes to this subtree (e.g., associating a SAP with another parent termination point) could lead to service disruption and/or network misbehavior. Such network misbehavior results mainly from a network configuration that is inconsistent with the intended behavior as defined by the operator (e.g., Section 4.2.1 of [RFC8969]).

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

/nw:networks/nw:network/nw:node/sap:service/sap:sap
   Unauthorized access to this subtree can disclose the operational state information of the nodes in a SAP network model (e.g., can disclose the identity of a customer 'peer-sap-id').

9. References

9.1. 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/info/rfc2119>.

[RFC3688]   Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/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/info/rfc6020>.

[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>.

[RFC6991]   Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[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>.

[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/info/rfc8174>.

[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>.

[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>.

[RFC8346]   Clemm, A., Medved, J., Varga, R., Liu, X., Ananthakrishnan, H., and N. Bahadur, "A YANG Data Model for Layer 3 Topologies", RFC 8346, DOI 10.17487/RFC8346, March 2018, <https://www.rfc-editor.org/info/rfc8346>.

[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/info/rfc8446>.

[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>.

[RFC9181]   Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., and Q. Wu, "A Common YANG Data Model for Layer 2 and Layer 3 VPNs", RFC 9181, DOI 10.17487/RFC9181, February 2022, <https://www.rfc-editor.org/info/rfc9181>.

9.2. Informative References

[BGP-SDWAN-USAGE]   Dunbar, L., Guichard, J., Sajassi, A., Drake, J., Najem, B., Banerjee, A., and
D. Carrel, "BGP Usage for SD-WAN Overlay Networks", Work in Progress,
Internet-Draft, draft-ietf-bess-bgp-sdwan-usage-09, 7 April 2023, <https://
datatracker.ietf.org/doc/html/draft-ietf-bess-bgp-sdwan-usage-09>.

[ENHANCED-VPN]   Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for
Enhanced Virtual Private Network (VPN+)", Work in Progress, Internet-Draft,
draft-ietf-teas-enhanced-vpn-12, 23 January 2023, <https://datatracker.ietf.org/
doc/html/draft-ietf-teas-enhanced-vpn-12>.

[IEEE802.1AX]   IEEE, "IEEE Standard for Local and Metropolitan Area Networks--Link
Aggregation", IEEE Std 802.1AX-2020, DOI 10.1109/IEEESTD.2020.9105034, 2020,
<https://doi.org/10.1109/IEEESTD.2020.9105034>.

[IETF-NETWORK-SLICES]   Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K.,
Contreras, L.M., and J. Tantsura, "A Framework for IETF Network Slices", Work
in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-19, 21 January
2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-19>.

[MEF17]   The Metro Ethernet Forum, "Technical Specification MEF 17, Service OAM
Requirements & Framework - Phase 1", April 2007, <https://www.mef.net/wp-
content/uploads/2015/04/MEF-17.pdf>.

[MEF6]   The Metro Ethernet Forum, "Technical Specification MEF 6, Ethernet Services
Definitions - Phase I", June 2004, <https://www.mef.net/Assets/
Technical_Specifications/PDF/MEF_6.pdf>.

[RFC4026]   Andersson, L. and T. Madsen, "Provider Provisioned Virtual Private Network
(VPN) Terminology", RFC 4026, DOI 10.17487/RFC4026, March 2005, <https://
www.rfc-editor.org/info/rfc4026>.

[RFC4364]   Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC
4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/
rfc4364>.

[RFC4761]   Kompella, K., Ed. and Y. Rekhter, Ed., "Virtual Private LAN Service (VPLS) Using
BGP for Auto-Discovery and Signaling", RFC 4761, DOI 10.17487/RFC4761,
January 2007, <https://www.rfc-editor.org/info/rfc4761>.

[RFC4762]   Lasserre, M., Ed. and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using
Label Distribution Protocol (LDP) Signaling", RFC 4762, DOI 10.17487/RFC4762,
January 2007, <https://www.rfc-editor.org/info/rfc4762>.

[RFC6004]   Berger, L. and D. Fedyk, "Generalized MPLS (GMPLS) Support for Metro Ethernet
Forum and G.8011 Ethernet Service Switching", RFC 6004, DOI 10.17487/
RFC6004, October 2010, <https://www.rfc-editor.org/info/rfc6004>.

[RFC6215] Bocci, M., Levrau, L., and D. Frost, "MPLS Transport Profile User-to-Network and Network-to-Network Interfaces", RFC 6215, DOI 10.17487/RFC6215, April 2011, <https://www.rfc-editor.org/info/rfc6215>.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <https://www.rfc-editor.org/info/rfc7149>.

[RFC7224] Bjorklund, M., "IANA Interface Type YANG Module", RFC 7224, DOI 10.17487/RFC7224, May 2014, <https://www.rfc-editor.org/info/rfc7224>.

[RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC7426, January 2015, <https://www.rfc-editor.org/info/rfc7426>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <https://www.rfc-editor.org/info/rfc7432>.

[RFC7623] Sajassi, A., Ed., Salam, S., Bitar, N., Isaac, A., and W. Henderickx, "Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)", RFC 7623, DOI 10.17487/RFC7623, September 2015, <https://www.rfc-editor.org/info/rfc7623>.

[RFC7951] Lhotka, L., "JSON Encoding of Data Modeled with YANG", RFC 7951, DOI 10.17487/RFC7951, August 2016, <https://www.rfc-editor.org/info/rfc7951>.

[RFC8214] Boutros, S., Sajassi, A., Salam, S., Drake, J., and J. Rabadan, "Virtual Private Wire Service Support in Ethernet VPN", RFC 8214, DOI 10.17487/RFC8214, August 2017, <https://www.rfc-editor.org/info/rfc8214>.

[RFC8299] Wu, Q., Ed., Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN Service Delivery", RFC 8299, DOI 10.17487/RFC8299, January 2018, <https://www.rfc-editor.org/info/rfc8299>.

[RFC8309] Wu, Q., Liu, W., and A. Farrel, "Service Models Explained", RFC 8309, DOI 10.17487/RFC8309, January 2018, <https://www.rfc-editor.org/info/rfc8309>.

[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/info/rfc8340>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://www.rfc-editor.org/info/rfc8342>.

[RFC8365] Sajassi, A., Ed., Drake, J., Ed., Bitar, N., Shekhar, R., Uttaro, J., and W. Henderickx, "A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)", RFC 8365, DOI 10.17487/RFC8365, March 2018, <https://www.rfc-editor.org/info/rfc8365>.

[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>.

[RFC9135] Sajassi, A., Salam, S., Thoria, S., Drake, J., and J. Rabadan, "Integrated Routing and Bridging in Ethernet VPN (EVPN)", RFC 9135, DOI 10.17487/RFC9135, October 2021, <https://www.rfc-editor.org/info/rfc9135>.

[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/info/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/info/rfc9291>.

Appendix A.   A Simplified SAP Network Example

An example of a SAP topology that is reported by a network controller is depicted in Figure 7. This example echoes the topology shown in Figure 4. Only a minimum information set is provided for each SAP. Particularly, 'parent-termination-point', 'attachment-interface', 'interface-type', 'encapsulation-type', and 'role' are not shown in the example. SAPs that are capable of hosting a service but are not yet activated are identified by 'sap-status/status' set to 'ietf-vpn-common:op-down' and 'service-status/admin-status/status' set to 'ietf-vpn-common:admin-down'. SAPs that are enabled to deliver a service are identified by 'service-status/admin-status/status' set to 'ietf-vpn-common:admin-up' and 'service-status/oper-status/status' set to 'ietf-vpn-common:op-up'. Note that none of the anomalies discussed in Section 5 are detected for these SAPs. The message body depicted in the figures below is encoded following the JSON encoding of YANG-modeled data as per [RFC7951].

```
{
  "ietf-network:networks": {
    "network": [
      {
        "network-types": {
          "ietf-sap-ntw:sap-network": {
            "service-type": [
              "ietf-vpn-common:l3vpn",
              "ietf-vpn-common:vpls"
            ]
          }
        },
        "network-id": "example:an-id",
        "node": [
          {
            "node-id": "example:pe1",
            "ietf-sap-ntw:service": [
              {
                "service-type": "ietf-vpn-common:l3vpn",
                "sap": [
                  {
                    "sap-id": "sap#11",
                    "peer-sap-id": ["ce-1"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
                      }
                    }
                  },
                  {
                    "sap-id": "sap#12",
                    "sap-status": {
                      "status": "ietf-vpn-common:op-down"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-down"
                      }
                    }
                  },
                  {
                    "sap-id": "sap#13",
                    "sap-status": {
                      "status": "ietf-vpn-common:op-down"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-down"
                      }
                    }
                  },
```

```
               {
                 "sap-id": "sap#14",
                 "sap-status": {
                   "status": "ietf-vpn-common:op-down"
                 },
                 "service-status": {
                   "admin-status": {
                     "status": "ietf-vpn-common:admin-down"
                   }
                 }
               }
             ]
           }
         ]
       },
       {
         "node-id": "example:pe2",
         "ietf-sap-ntw:service": [
           {
             "service-type": "ietf-vpn-common:l3vpn",
             "sap": [
               {
                 "sap-id": "sap#21",
                 "sap-status": {
                   "status": "ietf-vpn-common:op-down"
                 },
                 "service-status": {
                   "admin-status": {
                     "status": "ietf-vpn-common:admin-down"
                   }
                 }
               },
               {
                 "sap-id": "sap#22",
                 "peer-sap-id": ["ce-2"],
                 "sap-status": {
                   "status": "ietf-vpn-common:op-up"
                 },
                 "service-status": {
                   "admin-status": {
                     "status": "ietf-vpn-common:admin-up"
                   },
                   "oper-status": {
                     "status": "ietf-vpn-common:op-up"
                   }
                 }
               }
             ]
           }
         ]
       },
       {
         "node-id": "example:pe3",
         "ietf-sap-ntw:service": [
           {
             "service-type": "ietf-vpn-common:l3vpn",
             "sap": [
               {
```

```
                    "sap-id": "sap#31",
                    "sap-status": {
                      "status": "ietf-vpn-common:op-down"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-down"
                      }
                    }
                  },
                  {
                    "sap-id": "sap#32",
                    "sap-status": {
                      "status": "ietf-vpn-common:op-down"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-down"
                      }
                    }
                  },
                  {
                    "sap-id": "sap#33",
                    "peer-sap-id": ["ce-3"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
                      }
                    }
                  }
                ]
              }
            ]
          },
          {
            "node-id": "example:pe4",
            "ietf-sap-ntw:service": [
              {
                "service-type": "ietf-vpn-common:l3vpn",
                "sap": [
                  {
                    "sap-id": "sap#41",
                    "peer-sap-id": ["ce-3"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
```

```
                  }
                }
              },
              {
                "sap-id": "sap#42",
                "peer-sap-id": ["ce-4"],
                "sap-status": {
                  "status": "ietf-vpn-common:op-up"
                },
                "service-status": {
                  "admin-status": {
                    "status": "ietf-vpn-common:admin-up"
                  },
                  "oper-status": {
                    "status": "ietf-vpn-common:op-up"
                  }
                }
              },
              {
                "sap-id": "sap#43",
                "sap-status": {
                  "status": "ietf-vpn-common:op-down"
                },
                "service-status": {
                  "admin-status": {
                    "status": "ietf-vpn-common:admin-down"
                  }
                }
              },
              {
                "sap-id": "sap#44",
                "peer-sap-id": ["ce-5"],
                "sap-status": {
                  "status": "ietf-vpn-common:op-up"
                },
                "service-status": {
                  "admin-status": {
                    "status": "ietf-vpn-common:admin-up"
                  },
                  "oper-status": {
                    "status": "ietf-vpn-common:op-up"
                  }
                }
              }
            ]
          }
        ]
      }
    ]
  }
  ]
  }
}
```

Figure 7: A Simplified SAP Network Example

Appendix B.   A Simple Example of the SAP Network Model: Node Filter

In the example shown in Figure 8, PE1 (with a "node-id" set to "example:pe1", as shown in Figure 7) has two physical interfaces "GE0/6/1" and "GE0/6/4". Two sub-interfaces "GE0/6/4.1" and "GE0/6/4.2" are associated with the physical interface "GE0/6/4". Let us consider that four SAPs are exposed to the service orchestrator and mapped to these physical interfaces and sub-interfaces.
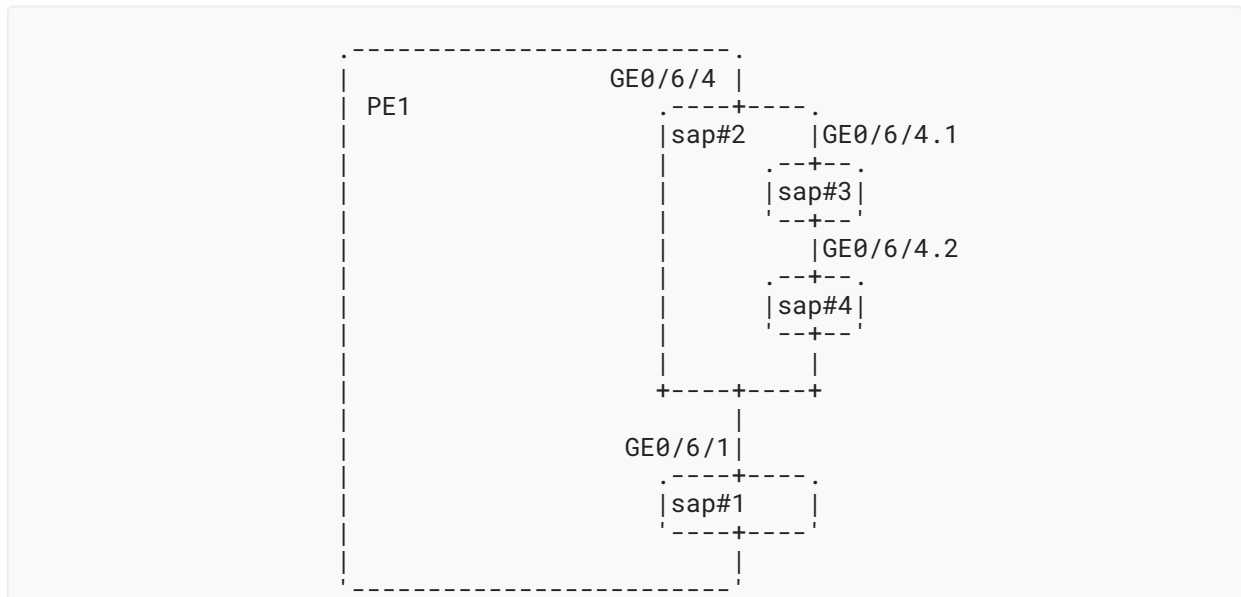
```
     .------------------------.
     |              GE0/6/4 |
     | PE1          .----+----.
     |              |sap#2    |GE0/6/4.1
     |              |       .--+--.
     |              |       |sap#3|
     |              |       '--+--'
     |              |          |GE0/6/4.2
     |              |        .--+--.
     |              |        |sap#4|
     |              |        '--+--'
     |              |          |
     |              +----+----+
     |                   |
     |              GE0/6/1|
     |              .----+----.
     |              |sap#1    |
     |              '----+----'
     |                   |
     '------------------------'
```

Figure 8: An Example of a PE and Its Physical/Logical Interfaces

Let us assume that no service is enabled yet for the SAP associated with the physical interface "GE0/6/1". Also, let us assume that, for the SAPs that are associated with the physical interface "GE0/6/4", VPLS and L3VPN services are activated on the two sub-interfaces "GE0/6/4.1" and "GE0/6/4.2", respectively. Both "sap#1" and "sap#2" are tagged as being capable of hosting per-service sub-interfaces ('allows-child-saps' is set to 'true').

For example, a service orchestrator can query what services are provided on which SAPs of PE1 from the network controller by sending a RESTCONF GET request. Figure 9 shows an example of the body of the RESTCONF response that is received from the network controller.

```
{
  "ietf-sap-ntw:service": [
    {
      "service-type": "ietf-vpn-common:l3vpn",
      "sap": [
        {
          "sap-id": "sap#1",
          "description": "Ready to host SAPs",
          "attachment-interface": "GE0/6/1",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
        {
          "sap-id": "sap#2",
          "description": "Ready to host SAPs",
          "attachment-interface": "GE0/6/4",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
        {
          "sap-id": "sap#3",
          "description": "A first SAP description",
          "parent-termination-point": "GE0/6/4",
          "attachment-interface": "GE0/6/4.1",
          "interface-type": "ietf-sap-ntw:logical",
          "encapsulation-type": "ietf-vpn-common:vlan-type",
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          },
          "service-status": {
            "admin-status": {
              "status": "ietf-vpn-common:admin-up"
            },
            "oper-status": {
              "status": "ietf-vpn-common:op-up"
            }
          }
        }
      ]
    },
    {
      "service-type": "ietf-vpn-common:vpls",
      "sap": [
        {
          "sap-id": "sap#1",
          "description": "Ready to host SAPs",
          "attachment-interface": "GE0/6/1",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
```

```
                "allows-child-saps": true,
                "sap-status": {
                  "status": "ietf-vpn-common:op-up"
                }
              },
              {
                "sap-id": "sap#2",
                "description": "Ready to host SAPs",
                "attachment-interface": "GE0/6/4",
                "interface-type": "ietf-sap-ntw:phy",
                "role": "ietf-sap-ntw:uni",
                "allows-child-saps": true,
                "sap-status": {
                  "status": "ietf-vpn-common:op-up"
                }
              },
              {
                "sap-id": "sap#4",
                "description": "Another description",
                "parent-termination-point": "GE0/6/4",
                "attachment-interface": "GE0/6/4.2",
                "interface-type": "ietf-sap-ntw:logical",
                "encapsulation-type": "ietf-vpn-common:vlan-type",
                "sap-status": {
                  "status": "ietf-vpn-common:op-up"
                },
                "service-status": {
                  "admin-status": {
                    "status": "ietf-vpn-common:admin-up"
                  },
                  "oper-status": {
                    "status": "ietf-vpn-common:op-up"
                  }
                }
              }
            ]
          }
        ]
      }
```

Figure 9: An Example of a Response Body to a Request with a Node Filter

Figure 10 shows an example of the response message body that is received from the network controller if the request includes a filter on the service type for a particular node:

```
{
  "ietf-sap-ntw:service": [
    {
      "service-type": "ietf-vpn-common:l3vpn",
      "sap": [
        {
          "sap-id": "sap#1",
          "description": "Ready to host SAPs",
          "attachment-interface": "GE0/6/1",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
        {
          "sap-id": "sap#2",
          "description": "Ready to host SAPs",
          "attachment-interface": "GE0/6/4",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
        {
          "sap-id": "sap#3",
          "description": "A first SAP description",
          "parent-termination-point": "GE0/6/4",
          "attachment-interface": "GE0/6/4.1",
          "interface-type": "ietf-sap-ntw:logical",
          "encapsulation-type": "ietf-vpn-common:vlan-type",
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          },
          "service-status": {
            "admin-status": {
              "status": "ietf-vpn-common:admin-up"
            },
            "oper-status": {
              "status": "ietf-vpn-common:op-up"
            }
          }
        }
      ]
    }
  ]
}
```

Figure 10: An Example of a Response Body to a Request with a Service Filter

Appendix C.   An Example of an NNI SAP: Inter-AS VPN Option A

Section 10 of [RFC4364] discusses several options to extend a VPN service beyond the scope of a single Autonomous System (AS). For illustration purposes, this section focuses on the so-called "Option A", but similar examples can be considered for other options.

In this option, an AS Border Router (ASBR) of an AS is directly connected to an ASBR of a neighboring AS. These two ASBRs are connected by multiple physical or logical interfaces. Also, at least one sub-interface is maintained by these ASBRs for each of the VPNs that require their routes to be passed from one AS to the other AS. Each ASBR behaves as a PE and treats the other as if it were a CE.

Figure 11 shows a simplified (excerpt) topology of two ASes A and B with a focus on the interconnection links between these two ASes.
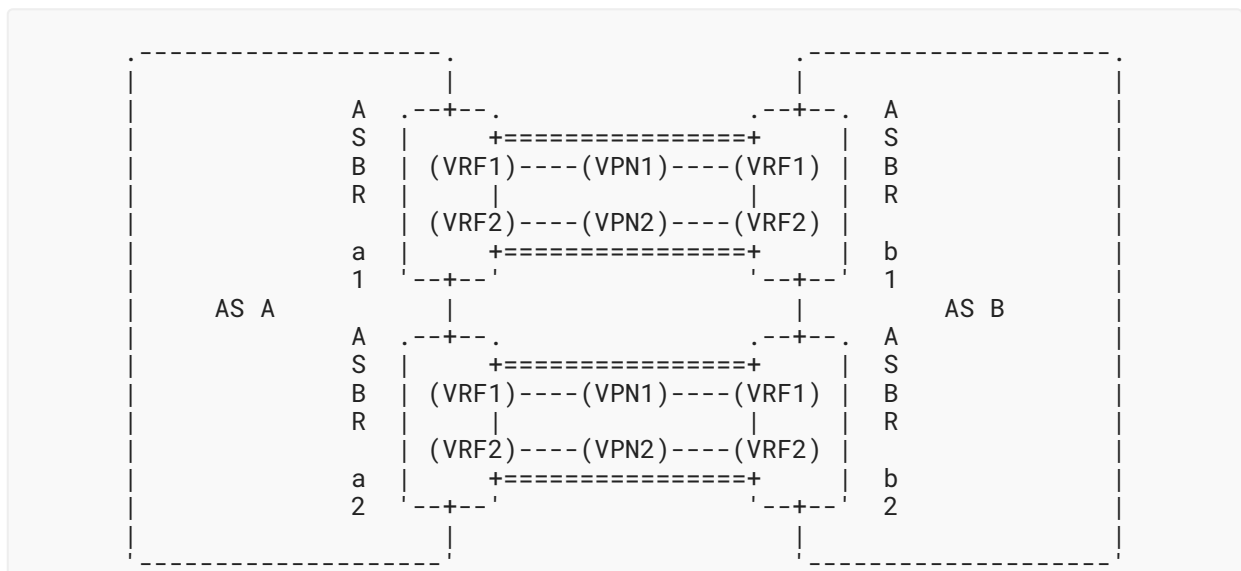
```
 .--------------------.                     .--------------------.
 |          |         |                     |         |          |
 |       A  .--+--.                       .--+--.  A            |
 |       S  |   +================+        |   S            |
 |       B  | (VRF1)----(VPN1)----(VRF1) |  B            |
 |       R  |   |                |   |  R            |
 |          | (VRF2)----(VPN2)----(VRF2) |            |
 |       a  |   +================+   |  b            |
 |       1  '--+--'                 '--+--'  1            |
 |     AS  A    |                         |    AS  B      |
 |       A  .--+--.                       .--+--.  A            |
 |       S  |   +================+        |   S            |
 |       B  | (VRF1)----(VPN1)----(VRF1) |  B            |
 |       R  |   |                |   |  R            |
 |          | (VRF2)----(VPN2)----(VRF2) |            |
 |       a  |   +================+   |  b            |
 |       2  '--+--'                 '--+--'  2            |
 |          |         |                     |         |          |
 '--------------------'                     '--------------------'
```

Figure 11: An Example of an Inter-AS VPN (Option A)

Figure 12 shows an example of a message body that is received from the network controller of AS A (with a focus on the NNIs shown in Figure 11).

```
{
  "ietf-network:networks": {
    "network": [
      {
        "network-types": {
          "ietf-sap-ntw:sap-network": {
            "service-type": [
              "ietf-vpn-common:l3vpn"
            ]
          }
        },
        "network-id": "example:an-id",
        "node": [
          {
            "node-id": "example:asbr-a1",
            "ietf-sap-ntw:service": [
              {
                "service-type": "ietf-vpn-common:l3vpn",
                "sap": [
                  {
                    "sap-id": "sap#11",
                    "description": "parent inter-as link#1",
                    "role": "ietf-sap-ntw:nni",
                    "allows-child-saps": true,
                    "peer-sap-id": ["asbr-b1"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    }
                  },
                  {
                    "sap-id": "sap#12",
                    "description": "parent inter-as link#2",
                    "role": "ietf-sap-ntw:nni",
                    "allows-child-saps": true,
                    "peer-sap-id": ["asbr-b1"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    }
                  },
                  {
                    "sap-id": "sap#13",
                    "description": "vpn1",
                    "role": "ietf-sap-ntw:nni",
                    "peer-sap-id": ["asbr-b1"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
                      }
                    }
                  }
                },
                {
```

```
                    "sap-id": "sap#14",
                    "description": "vpn2",
                    "role": "ietf-sap-ntw:nni",
                    "peer-sap-id": ["asbr-b1"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
                      }
                    }
                  }
                ]
              }
            ]
          },
          {
            "node-id": "example:asbr-a2",
            "ietf-sap-ntw:service": [
              {
                "service-type": "ietf-vpn-common:l3vpn",
                "sap": [
                  {
                    "sap-id": "sap#11",
                    "description": "parent inter-as link#1",
                    "role": "ietf-sap-ntw:nni",
                    "allows-child-saps": true,
                    "peer-sap-id": ["asbr-b2"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    }
                  },
                  {
                    "sap-id": "sap#12",
                    "description": "parent inter-as link#2",
                    "role": "ietf-sap-ntw:nni",
                    "allows-child-saps": true,
                    "peer-sap-id": ["asbr-b2"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    }
                  },
                  {
                    "sap-id": "sap#21",
                    "description": "vpn1",
                    "role": "ietf-sap-ntw:nni",
                    "peer-sap-id": ["asbr-b2"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
```

```
                    "oper-status": {
                      "status": "ietf-vpn-common:op-up"
                    }
                  }
                },
                {
                  "sap-id": "sap#22",
                  "description": "vpn2",
                  "role": "ietf-sap-ntw:nni",
                  "peer-sap-id": ["asbr-b2"],
                  "sap-status": {
                    "status": "ietf-vpn-common:op-up"
                  },
                  "service-status": {
                    "admin-status": {
                      "status": "ietf-vpn-common:admin-up"
                    },
                    "oper-status": {
                      "status": "ietf-vpn-common:op-up"
                    }
                  }
                }
              ]
            }
          ]
        }
      ]
    }
  ]
}
```

Figure 12: An Example of SAP Usage for an NNI

Appendix D.   Examples of Using the SAP Network Model in Service Creation

This section describes examples that illustrate the use of the SAP model for service creation purposes.

An example of a SAP topology is presented in Figure 7. This example includes four PEs with their SAPs, as well as the customer information.

Let us assume that an operator wants to create an L3VPN service between two PEs (PE3 and PE4) that are servicing two CEs (CE6 and CE7). To that aim, the operator would query the SAP topology and would obtain a response similar to what is depicted in Figure 7. That response indicates that the SAPs having "sap#31" and "sap#43" as attachment identifiers do not have any installed services. This is particularly inferred from (1) the administrative 'service-status' that is set to 'ietf-vpn-common:admin-down' for all the services that are supported by these two SAPs and (2) the absence of the anomalies discussed in Section 5. Note that none of the anomalies discussed in Section 5 are detected. Once the "free" SAPs are identified, the 'interface-type' and 'encapsulation-

type' are checked to see if the requested L3VPN service is compatible with the SAP characteristics. If they are compatible, the 'attachment-id' value can be used as the VPN network access identifier in an L3NM "create" query.

A similar process can be followed for creating the so-called "Inter-AS VPN Option A" services. Unlike the previous example, let us assume that an operator wants to create an L3VPN service between two PEs (PE3 and PE4) but these PEs are not in the same AS: PE3 belongs to AS A while PE4 belongs to AS B. The NNIs between these ASes are represented in Figure 11. The operator of AS A would query, via the controller of its AS, the SAP topology and would obtain not only the information that is depicted in Figure 7 but also the information shown in Figure 12 representing the NNIs. The operator would create the service in the AS A between PE3 and a free, compatible SAP in the ASBR A1. The same procedure is followed by the operator of AS B to create the service in the AS B between a free, compatible SAP in the ASBR B1 and PE4. The services can be provisioned in each of these ASes using the L3NM.

Let us now assume that, instead of the L3VPN service, the operator wants to set up an L2VPN service. If the 'interface-type' is a physical port, a new logical SAP can be created using the SAP model to cope with the service's needs (e.g., the 'encapsulation-type' attribute can be set to 'ietf-vpn-common:vlan-type'). Once the logical SAP is created, the 'attachment-id' of the new SAP is used to create an L2NM instance (Section 7.6 of [RFC9291]).

Acknowledgements

Thanks to Adrian Farrel, Daniel King, Dhruv Dhody, Benoit Claise, Bo Wu, Erez Segev, Raul Arco, Joe Clarke, Riyas Valiyapalathingal, Tom Petch, Olga Havel, and Richard Roberts for their comments.

Thanks to Martin Björklund for the YANG Doctors review, Menachem Dodge for the opsdir review, Mach Chen for the rtgdir review, Linda Dunbar for the genart review, and Ivaylo Petrov for the secdir review.

Special thanks to Adrian Farrel for the Shepherd review and Rob Wilton for the careful AD review.

Thanks to Lars Eggert, Roman Danyliw, and Zaheduzzaman Sarker for their comments during the IESG review.

Authors' Addresses

Mohamed Boucadair (EDITOR)
Orange
France
Email: mohamed.boucadair@orange.com

Oscar Gonzalez de Dios
Telefonica
Madrid
Spain
Email: oscar.gonzalezdedios@telefonica.com

Samier Barguil
Nokia
Madrid
Spain
Email: samier.barguil_giraldo@nokia.com

Qin Wu
Huawei
Yuhua District
101 Software Avenue
Nanjing
Jiangsu, 210012
China
Email: bill.wu@huawei.com

Victor Lopez
Nokia
Spain
Email: victor.lopez@nokia.com