Workgroup: OPSAWG
Internet-Draft: draft-dbwb-opsawg-sap-00
Published: 22 October 2021
Intended Status: Standards Track
Expires: 25 April 2022
Authors: O. Gonzalez de Dios S. Barguil Q. Wu
Telefonica Telefonica Huawei
M. Boucadair V. Lopez
Orange Nokia

A Network YANG Model for Service Attachment Points

Abstract

This document defines a YANG data model for representing an abstract view of the provider network topology containing the points from which its services can be attached (e.g., basic connectivity, VPN, network slices). The data model augments the 'ietf-network' data model by adding the concept of service attachment points (SAPs). The service attachment points are the points to which network services (such as L3VPN or L2VPN) can be attached. The customer endpoint of an attachment circuits are not covered in the SAP network topology.

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 25 April 2022.

Table of Contents

1. Introduction

The service attachment point (SAP) is an important architectural concept in many implementations and deployments of services such as VPNs, SDWAN, or managed VoIP services. It has already been used to decide where to attach and, thus, deliver the service in the L3SM [RFC8299] and the L2SM [RFC8466].

This document defines a YANG network model for representing, managing, and controlling the service attachment points (SAPs). The data model augments the 'ietf-network' module [RFC8345] by adding the concept of service attachment points. The service attachment points are abstraction of the points where network services such as L3VPNs or L2VPNs can be attached.

This document does not make any assumption about the service provided by the network to the users. VPN services are used for illustration purposes. This concept can also be used to decide network slice SAPs [I-D.ietf-teas-ietf-network-slices].

In the context of Software-Defined Networking (SDN) [RFC7149] [RFC7426], the defined YANG data model in this document can be used to exchange information between control elements, so as to support VPN service provision and resource management discussed in [I-D.ietf-opsawg-l3sm-l3nm][I-D.ietf-opsawg-l2nm]. Through this data model, the service orchestration layer can learn the available endpoints (i.e., SAPs) of interconnection resource of the underlying network.

The service orchestration layer can determine which endpoint of interconnection to add to L2VPN or L3VPN service. With the help of other data models (e.g., L3SM [RFC8299] or L2SM [RFC8466]), hierarchical control elements could determine the feasibility of an end-to-end IP connectivity or L2VPN connectivity and therefore derive the sequence of domains and the points of interconnection to use.

This document explains the scope and purpose of a SAP network model and its relation with the service models and describes how it can be used by a network operator. The document also shows how the topology and service models fit together.

The YANG data model in this document 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], and [RFC8309]. The document uses terms from those documents.

Tree diagrams used in this document follow the notation defined in [RFC8340].

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

This document uses the following terms:

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

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

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

attachment circuits. A PE is usually located at an SP point of presence (PoP).

Attachment point (AP): Describes a service's end point characteristics and its reference to a Termination Point (TP) of the PE; used as service access point for service.

3. SAP Network Model Usage

Management operations of a service provider network can be automated using a variety of means such as interfaces based on YANG modules [RFC8969]. From that standpoint, and considering the architecture depicted in Figure 1, the 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.

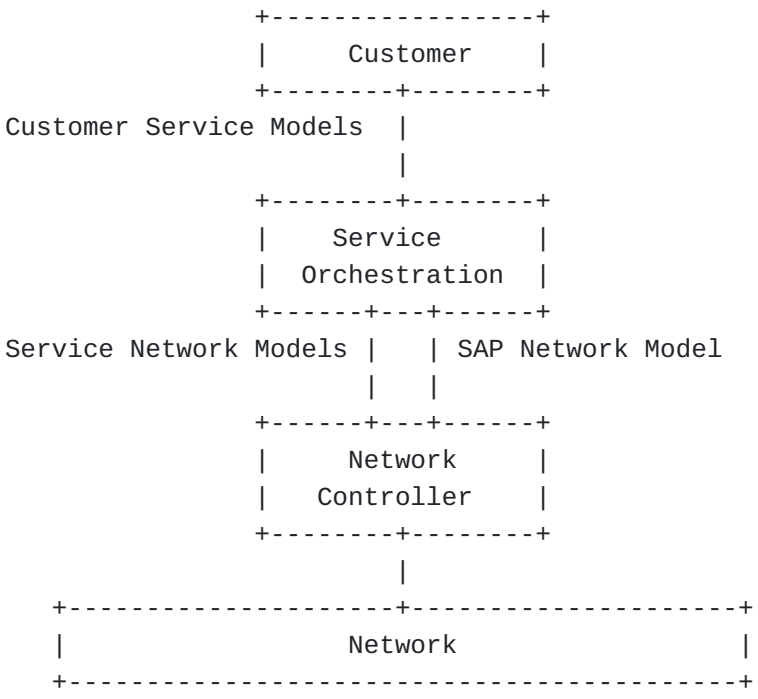

Figure 1: SAP Network Model Usage

Let us consider the example of a typical service provider network (Figure 2), with PE and P nodes.

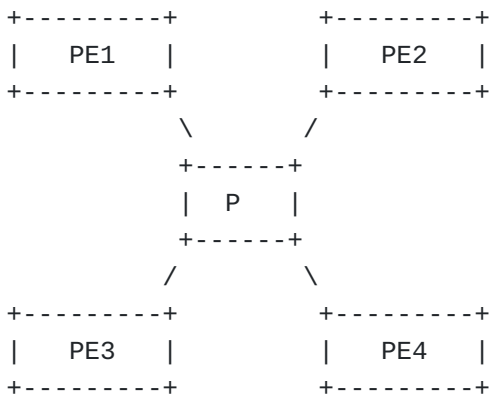

Figure 2: Sample Network Topology

The Service Orchestration layer does not need to know about the internals of the underlying network (e.g., P nodes). Figure 3 shows the abstract network view as seen by the 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 need is 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).

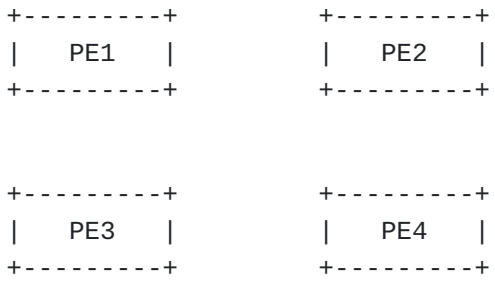

Figure 3: Abstract Network Topology

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). The Service Orchestration layer can use them to setup the requested services or to commit the delivery of a service. Figure 4 depicts the SAP network topology that is maintained by the network controller and exposed to the Service Orchestration.

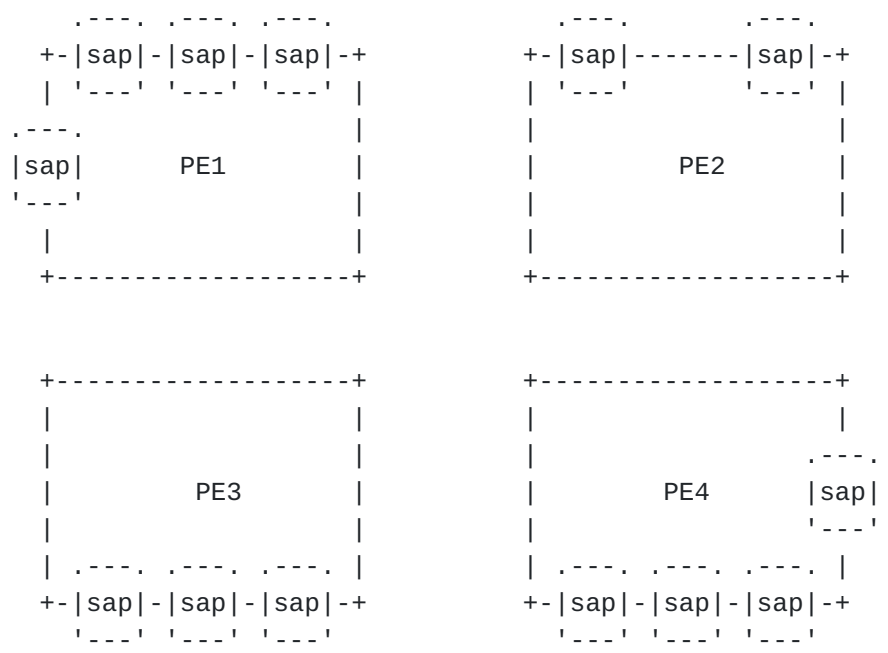

Figure 4: SAP Network Topology

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

As shown in Figure 5, the Service Orchestration layer will have also access to a set of Customer Service Model, e.g., an L3SM or L2SM data model in the customer-facing interface and a set of network models, e.g., 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 network between PEs.

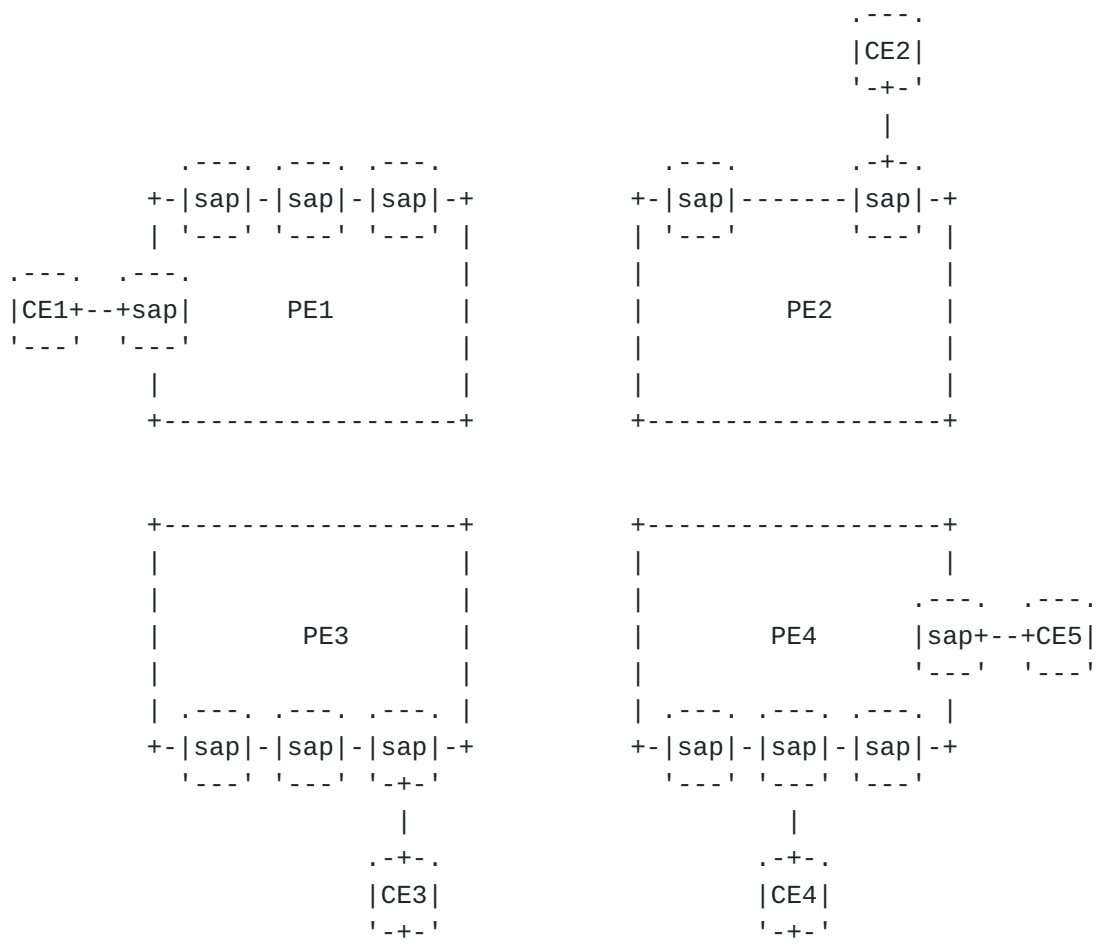

Figure 5: Network Topology with CEs and ACs

4. SAP Module Tree Structure

The SAP network model builds on the network data model defined in the 'ietf-network' module [RFC8345], augmenting the nodes with service attachment points, which anchor the links and are contained in nodes. The 'service-attachment-point' attribute defined in the SAP network model is not a tunnel termination point (TTP) nor a link, but an abstraction of the termination point defined in [RFC8345].

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 sap-type*   identityref
  augment /nw:networks/nw:network/nw:node:
    +--rw service-attachment-point* [attachment-id]
       +--rw attachment-id          nt:tp-id
       +--ro interface-type?        identityref
       +--rw admin-status?          boolean
       +--rw oper-status?           boolean
       +--rw encapsulation-type?    identityref
       +--rw sap-type*              identityref
       +--rw service-description?   string
```

Figure 6: YANG Module Structure

A SAP network topology can be used for one single service type or multiple types ("sap-type"). When a SAP topology is used for many service types, the underlying nodes must support at least one of these service types. Examples of supported service types are listed below:

- *L3VPN,
- *Virtual Private LAN Service (VPLS) using BGP [RFC4761],
- *VPLS using Label Distribution Protocol (LDP) [RFC4762],
- *Virtual Private Wire Service (VPWS) [RFC8214],
- *BGP MPLS-Based Ethernet VPN [RFC7432],
- *Ethernet VPN (EVPN) [RFC8365],
- *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN) [RFC7623],
- *Virtual Networks [RFC8453],
- *Enhanced VPN (VPN+) [I-D.ietf-teas-enhanced-vpn], and
- *Network slice [I-D.ietf-teas-ietf-network-slices].

A service attachment point is identified by an interface name ("attachment-id"), an interface type ("type"), a status ("admin-status", and "oper-status"), an encapsulation type ("encapsulation-type"), one or a list of service types ("sap-type") such as L3VPN or network slice, a description of the service(s) ("service-description").

5. Relation with other Models

The SAP network model can be seen as an inventory data associated with service attachment points. The model maintains an inventory of nodes contained in a network based on [RFC8345].

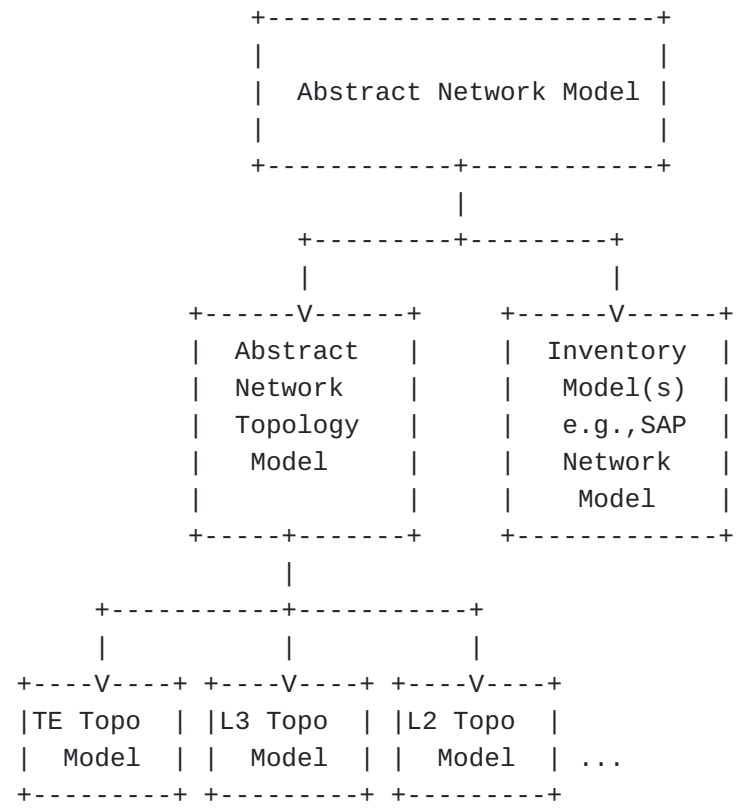

Figure 7: Relation of SAP Network Model to Other Models

Figure 7 depicts the relationship of the SAP network model to other models. The SAP network model augments from the Network model [RFC8345] and imports Network Topology model, while other technology-specific topology models (e.g., TE Topologies model [RFC8795] or L3 Topology model [RFC8346]) augment from the Network Topology.

6. SAP YANG Module

This module imports types from [RFC8343], [RFC8345], and [I-D.ietf-opsawg-vpn-common].

```
<CODE BEGINS> file "ietf-sap-ntw@2021-10-16.yang"

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

  import ietf-interfaces {
    prefix if;
    reference
      "RFC 8343: A YANG Data Model for Interface Management";
  }
  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 UUUU: A Layer 2/3 VPN Common YANG Model";
  }

  organization
    "IETF OPSA (Operations and Management Area) Working Group ";
  contact
    "Editor:   Oscar Gonzalez de Dios
               <mailto:oscar.gonzalezdedios@telefonica.com>
     Editor:   Samier Barguil
               <mailto:samier.barguilgiraldo.ext@telefonica.com>
     Editor:   Qin Wu
               <mailto:bill.wu@huawei.com>
     Editor:   Mohamed Boucadair
               <mailto:mohamed.boucadair@orange.com>";
  description
    "This YANG module defines a model for representing, managing,
     and controlling the Service Attachment Points (SAPs) in the
     network topology.

     Copyright (c) 2021 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 Simplified 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
   (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
   for full legal notices.";

revision 2021-10-16 {
  description
    "Initial version";
  reference
    "RFC XXXX: A Network YANG Model for Service Attachment
               Point (SAP)";
}

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

identity l3vpn {
  base service-type;
  description
    "L3VPN service.";
  reference
    "RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)";
}

identity enhanced-vpn {
  base 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 traditional VPNs.";
  reference
    "I-D.ietf-teas-enhanced-vpn:
       A Framework for Enhanced Virtual Private Network
       (VPN+) Services";
}

identity network-slice {
  base 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
    "I-D.ietf-teas-ietf-network-slices:
       Framework for IETF Network Slices";
}

identity vpls {
  base service-type;
  description
    "VPLS service.";
  reference
    "RFC 4761: Virtual Private LAN Service (VPLS) Using BGP for
               Auto-Discovery and Signaling
     RFC 4762: Virtual Private LAN Service (VPLS) Using Label
               Distribution Protocol (LDP) Signaling";
}

identity vpws {
  base service-type;
  description
    "Virtual Private Wire Service (VPWS) service.";
  reference
    "RFC 4664: Framework for Layer 2 Virtual Private Networks
               (L2VPNs), Section 3.1.1";
}

identity vpws-evpn {
  base service-type;
  description
    "EVPN used to support VPWS service.";
  reference
    "RFC 8214: Virtual Private Wire Service Support in Ethernet VPN";
}

identity pbb-evpn {
  base service-type;
  description
    "Provider Backbone Bridging (PBB) EVPNs service.";
  reference
    "RFC 7623: Provider Backbone Bridging Combined with Ethernet VPN
               (PBB-EVPN)";
}

identity mpls-evpn {
  base service-type;
  description
```

```
    "MPLS-based EVPN service.";
  reference
    "RFC 7432: BGP MPLS-Based Ethernet VPN";
}

identity vxlan-evpn {
  base service-type;
  description
    "VXLAN-based EVPN service.";
  reference
    "RFC 8365: A Network Virtualization Overlay Solution Using
               Ethernet VPN (EVPN)";
}

identity virtual-network {
  base service-type;
  description
    "Virtual network.";
  reference
    "RFC 8453: Framework for Abstraction and Control of TE
               Networks (ACTN)";
}

/*
 Other network service types may be added.
 */

grouping sap-information {
  description
    "Service Attachment Point (SAP) information.";
  list service-attachment-point {
    key "attachment-id";
    description
      "The service attachment points are abstraction of
       the points where network services such as L3VPNs,
       L2VPNs, or network slices can be attached.";
    leaf attachment-id {
      type nt:tp-id;
      description
        "Indicates the name of the interface.";
    }
    leaf interface-type {
      type identityref {
        base if:interface-type;
      }
      config false;
      description
        "The type of the interface.";
    }
```

```
    leaf admin-status {
      type boolean;
      description
        "Indicates the administrative status of the SAP.";
    }
    leaf oper-status {
      type boolean;
      description
        "Indicates the operational status.";
    }
    leaf encapsulation-type {
      type identityref {
        base vpn-common:encapsulation-type;
      }
      description
        "Encapsulation type.";
    }
    leaf-list sap-type {
      type identityref {
        base service-type;
      }
      description
        "SAP type.";
    }
    leaf service-description {
      type string;
      description
        "A textual description of the service(s).";
    }
  }
}

augment "/nw:networks/nw:network/nw:network-types" {
  description
    "Introduces a new network type for SAP network.";
  container sap-network {
    presence "Indicates SAP Network Type.";
    description
      "The presence of the container node indicates the
       SAP network type.";
    leaf-list sap-type {
      type identityref {
        base service-type;
      }
      description
        "Indicates a service type.";
    }
  }
}
```

```
  augment "/nw:networks/nw:network/nw:node" {
    description
      "Parameters for the service attachment point level.";
    uses sap-information;
  }
}

<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 registry [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 XXXX
```

8. Security Considerations

The YANG module specified in this document defines 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-attachment-point/
sap:attachment-id

This subtree specifies the configurations of the nodes in a SAP network model. Unexpected changes to this subtree could lead to service disruption and/or network misbehavior.

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-attachment-point

Unauthorized access to this subtree can disclose the operational state information of the nodes in a SAP network model.

9. Acknowledgements

Thanks to Adrian Farrell and Daniel King for the suggestions on the names used in a previous version.

10. References

10.1. Normative References

[I-D.ietf-opsawg-vpn-common] Barguil, S., Dios, O. G. D., Boucadair, M., and Q. Wu, "A Layer 2/3 VPN Common YANG Model", Work in Progress, Internet-Draft, draft-ietf-opsawg-vpn-common-12, 29 September 2021, <https://www.ietf.org/archive/id/draft-ietf-opsawg-vpn-common-12.txt>.

[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>.

[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>.

10.2. Informative References

[I-D.ietf-opsawg-l2nm]

Barguil, S., Dios, O. G. D., Boucadair, M., and L. A. Munoz, "A Layer 2 VPN Network YANG Model", Work in Progress, Internet-Draft, draft-ietf-opsawg-l2nm-09, 20 October 2021, <https://www.ietf.org/archive/id/draft-ietf-opsawg-l2nm-09.txt>.

[I-D.ietf-opsawg-l3sm-l3nm] Barguil, S., Dios, O. G. D., Boucadair, M., Munoz, L. A., and A. Aguado, "A Layer 3 VPN Network YANG Model", Work in Progress, Internet-Draft, draft-ietf-opsawg-l3sm-l3nm-18, 8 October 2021, <https://www.ietf.org/archive/id/draft-ietf-opsawg-l3sm-l3nm-18.txt>.

[I-D.ietf-teas-enhanced-vpn] Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Network (VPN+) Services", Work in Progress, Internet-Draft, draft-ietf-teas-enhanced-vpn-08, 12 July 2021, <https://www.ietf.org/archive/id/draft-ietf-teas-enhanced-vpn-08.txt>.

[I-D.ietf-teas-ietf-network-slices]
Farrel, A., Gray, E., Drake, J., Rokui, R., Homma, S., Makhijani, K., Contreras, L. M., and J. Tantsura, "Framework for IETF Network Slices", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-04, 23 August 2021, <https://www.ietf.org/archive/id/draft-ietf-teas-ietf-network-slices-04.txt>.

[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>.

[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>.

[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>.

[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>.

[RFC8343] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 8343, DOI 10.17487/RFC8343, March 2018, <https://www.rfc-editor.org/info/rfc8343>.

[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>.

Authors' Addresses

Oscar Gonzalez de Dios
Telefonica
Madrid
Spain

Email: oscar.gonzalezdedios@telefonica.com

Samier Barguil
Telefonica
Madrid
Spain

Email: samier.barguilgiraldo.ext@telefonica.com

Qin Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China

Email: bill.wu@huawei.com

Mohamed Boucadair
Orange
France

Email: mohamed.boucadair@orange.com

Victor Lopez
Nokia
Spain

Email: victor.lopez@nokia.com