OPSAWG
Internet-Draft
Intended status: Standards Track
Expires: October 4, 2020

O. Gonzalez de Dios, Ed.
S. Barguil
Telefonica
Q. Wu
Huawei
M. Boucadair
Orange

April 2, 2020

A YANG Model for User-Network Interface (UNI) Topologies
draft-ogondio-opsawg-uni-topology-01

Abstract

This document defines a YANG data model for representing an abstract view of the Service Provider network topology containing the points from which its services can be attached (e.g., basic connectivity, VPN, SDWAN). The data model augments the 'ietf-network' data model by adding the concept of service-attachment-points. The service-attachment-points are an abstraction of the points to which network services (such as L3 VPN or L2 VPN) can be attached.

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 October 4, 2020.

Table of Contents

1. Introduction 2
1.1. Terminology 3
1.2. Requirements Language 4
2. UNI Topology Model Usage 4
3. YANG Module Structure Details 5
4. YANG module 6
5. IANA Considerations 9
6. Security Considerations 9
7. Implementation Status 10
8. Acknowledgements 10
9. References 10
9.1. Normative References 10
9.2. Informative References 11
Authors' Addresses 12

1. Introduction

The User-Network Interface (UNI) is an important architectural concept in many implementations and deployments of services such as VPNs or managed VoIP services.

This document defines a YANG data model for representing, managing and controlling the User Network Interface (UNI) topology. 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 L3 VPNs or L2 VPNs can be attached.

This document does not make any assumption about the service provided by the network to the users. VPN service is used for illustration purposes.

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]. Through this data model, the service orchestration layer can learn the capability and available endpoint(s) 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 model [RFC8299] and L3NM model) and mechanism, hierarchical control elements could determine the feasibility of an end-to-end path and to derive the sequence of domains and the points of interconnection to use.

This document explains the scope and purpose of a uni topology 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].

1.1. Terminology

This document assumes that the reader is familiar with the contents of [RFC6241], [RFC7950] and [RFC8309]. The document uses terminologies from those documents. Tree diagrams used in this document follow the notation defined in [RFC8340].

This document uses the following terms:

Service Provider (SP): The organization (usually a commercial undertaking) 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 PE devices via attachment circuits. A CE is usually located at the customer premises, and is usually dedicated to a single service (e.g VPN), although it may support multiple VPNs if each one has separate attachment circuits. A CE device 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, and is directly connected to one or more CE devices via attachment circuits. A PE is usually located at an SP point of presence (PoP).

Attachment point(AP): Describe a service's end point characteristics and its reference to a Termination Point (TP) of the Provider Edge (PE) Node; used as service access point for VPN service, for example.

1.2. Requirements Language

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

2. UNI Topology Model Usage

Management operations of a service provider network can be automated using a variety of means such as interfaces based on YANG modules. Considering the architecture depicted in Figure 1, the goal is to be able to show via a YANG-based interface an abstracted network view from the network controller to the service orchestration layer.

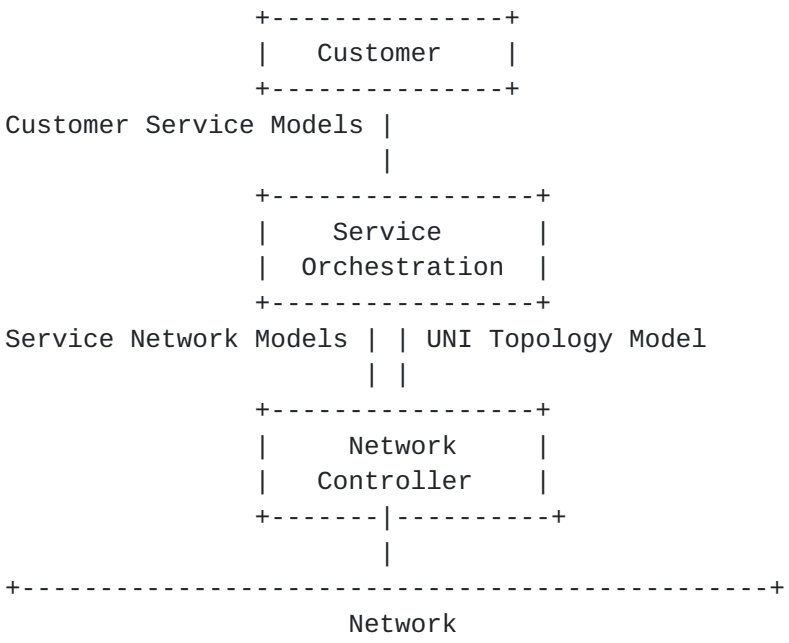

Figure 1

The service orchestration layer does not need to know about the internals of the network. Hence, the abstraction's need is to be able to get the set of nodes, and the attachment points associated with the nodes from which network services can be grafted (delivered). Let us consider the example of a typical Service Provider network (Figure 2), with PE and P nodes. The Service orchestration layer would see a set of PEs, and a set of client-facing ports to which CEs can be connected (or are actually connected). Service orchestration layer will have also access to a set of Customer Service Model, e.g., a 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 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.

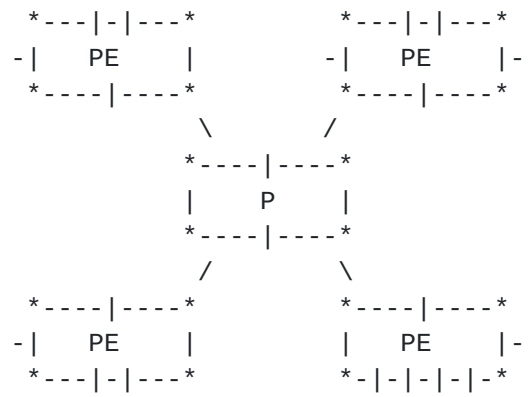

Figure 2

How the abstracted view of the network controller can look like is depicted in Figure 3.

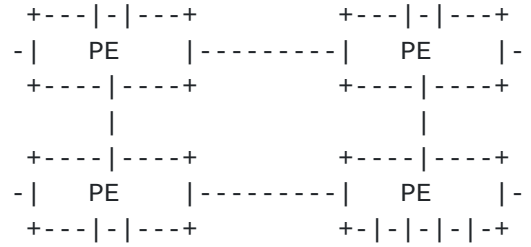

Figure 3

3. YANG Module Structure Details

The abstract (base) network data model is defined in the 'ietf-network' module of [RFC8345].

The UNI-topology 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 structure of the 'ietf-uni-topology' module is shown in Figure 4.

```
module: ietf-uni-topology
  augment /nw:networks/nw:network/nw:node:
    +--rw service-attachment-point* [attachment-id]
       +--rw attachment-id         nt:tp-id
       +--rw type?                 identityref
       +--rw admin-status?         boolean
       +--rw oper-status?          boolean
       +--rw encapsulation-type?   string
```

Figure 4

4. YANG module

This module imports types from [RFC8343] and [RFC8345].

```
<CODE BEGINS>  file "ietf-uni-topology@2020-04-02.yang"
module ietf-uni-topology {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-uni-topology";
  prefix uni;

  import ietf-interfaces {
    prefix if;
    reference
      "RFC 8343: A YANG Data Model for Interface Management";
  }
  import ietf-network-topology {
    prefix nt;
    reference
      "Section 6.2 of RFC 8345: A YANG Data Model for Network
       Topologies";
  }
  import ietf-network {
    prefix nw;
    reference
      "Section 6.1 of RFC 8345: A YANG Data Model for Network
          Topologies";
  }

  organization
    "IETF OPSA (Operations and Management Area) Working Group ";
  contact
   "   Editor:    Oscar Gonzalez de Dios
              <mailto:oscar.gonzalezdedios@telefonica.com>
       Editor:   Samier Barguil
              <mailto:alejandro.aguado_martin@nokia.com>
       Editor:    Qin Wu
              <mailto:victor.lopezalvarez@telefonica.com>
```

```
          Editor:   Mohamed Boucadair
                    <mailto:daniel.voyer@bell.ca>
       ";
     description
       "This YANG module defines a model for representing, managing
        and controlling the User Network Interface (UNI) topology.
        Copyright (c) 2020 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 2020-04-02 {
       description
         "Initial version";
       reference
         "RFC XXXX: A YANG Model for User-Network Interface (UNI)
                    Topologies";
     }

     grouping uni-information-group {
       description
         "User-Network Interface Information";
       list service-attachment-point {
         key "attachment-id";
         description
           "The service attachment points are abstraction of
            the points where network services such as L3 VPNs
            or L2 VPNs can be attached.";
         leaf attachment-id {
           type nt:tp-id;
           description
             "Name of the interface";
         }
         leaf type {
           type identityref {
             base if:interface-type;
           }
           config false;
           description
```

```
            "The type of the interface.";
          reference
            "RFC 8343: A YANG Data Model for Interface Management";
        }
        leaf admin-status {
          type boolean;
          description
            "Administrative Status UP/DOWN";
        }
        leaf oper-status {
          type boolean;
          description
            "Operational Status UP/DOWN";
        }
        leaf encapsulation-type {
          type string;
          description
            "Encapsulation type.  By default, the
             encapsulation type is set to 'untagged'.";
        }
      }
    }

    augment "/nw:networks/nw:network/nw:network-types" {
      description
        "Introduces new network type for UNI Unicast topology";
      container uni-topology {
        presence "indicates UNI Unicast topology";
        description
          "The presence of the container node indicates UNI
           topology";
      }
    }

    augment "/nw:networks/nw:network/nw:node" {
      description
        "Parameters for the service edge point level.";
      uses uni-information-group;
    }
  }
  <CODE ENDS>
```

Figure 5

5. 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-uni-topology
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-uni-topology
namespace:    urn:ietf:params:xml:ns:yang:ietf-uni-topology
maintained by IANA: N
prefix:       uni
reference:    RFC XXXX
---------------------------------------------------------------
```

6. 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 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/uni:service-attachment-point/ uni:attachment-id

This subtree specifies the configurations of the nodes in a UNI network topology. 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:

o /nw:networks/nw:network/nw:node/uni:service-attachment-point

Unauthorized access to this subtree can disclose the operational state information of the nodes in a UNI topology.

7. Implementation Status

This section will be used to track the status of the implementations of the model. It is aimed at being removed if the document becomes RFC.

8. Acknowledgements

Thanks to Adrian Farrell and Daniel King for the suggestions on the names.

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>.

[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>.

[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>.

9.2. Informative References

[I-D.ietf-opsawg-l3sm-l3nm] Barguil, S., Dios, O., Boucadair, M., Munoz, L., and A. Aguado, "A Layer 3 VPN Network YANG Model", draft-ietf-opsawg-l3sm-l3nm-02 (work in progress), March 2020.

[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>.

[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>.

Authors' Addresses

Oscar Gonzalez de Dios (editor)
Telefonica
Madrid
ES

Email: oscar.gonzalezdedios@telefonica.com

Samier Barguil
Telefonica
Madrid
ES

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
Caen
France

Email: mohamed.boucadair@orange.com