Internet Engineering Task Force (IETF)
Request for Comments: 9181
Category: Standards Track
ISSN: 2070-1721

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

February 2022

A Common YANG Data Model for Layer 2 and Layer 3 VPNs

Abstract

This document defines a common YANG module that is meant to be reused by various VPN-related modules such as Layer 3 VPN and Layer 2 VPN network models.

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/rfc9181.

Table of Contents

Authors' Addresses

1. Introduction

The IETF has specified YANG modules for VPN services, e.g., the Layer 3 VPN Service Model (L3SM) [RFC8299] or the Layer 2 VPN Service Model (L2SM) [RFC8466]. Other relevant YANG data models are the Layer 3 VPN Network Model (L3NM) [RFC9182] and the Layer 2 VPN Network Model (L2NM) [L2NM-YANG]. There are common data nodes and structures that are present in all of these models or at least a subset of them.

This document defines a common YANG module that is meant to be reused by various VPN-related modules such as the L3NM [RFC9182] and the L2NM [L2NM-YANG]: "ietf-vpn-common" (Section 4).

The "ietf-vpn-common" module includes a set of identities, types, and groupings that are meant to be reused by other VPN-related YANG modules independently of their layer (e.g., Layer 2, Layer 3) and the type of the module (e.g., network model, service model), including possible future revisions of existing models (e.g., the L3SM [RFC8299] or the L2SM [RFC8466]).

2. Terminology

The terminology for describing YANG modules is defined in [RFC7950].

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

The reader may refer to [RFC4026] and [RFC4176] for VPN-related terms.

This document inherits many terms from [RFC8299] and [RFC8466] (e.g., Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communications (URLLC), Massive Machine Type Communications (mMTC)).

3. Description of the VPN Common YANG Module

The "ietf-vpn-common" module defines a set of common VPN-related features, including the following:

Encapsulation features, such as the following:

* dot1Q [IEEE802.1Q],
* QinQ [IEEE802.1ad],
* link aggregation [IEEE802.1AX], and
* Virtual eXtensible Local Area Networks (VXLANs) [RFC7348].

Multicast [RFC6513].

Routing features, such as the following:

* BGP [RFC4271],
* OSPF [RFC4577] [RFC6565],
* IS-IS [ISO10589],
* RIP [RFC2080] [RFC2453],
* Bidirectional Forwarding Detection (BFD) [RFC5880] [RFC7880], and
* Virtual Router Redundancy Protocol (VRRP) [RFC5798].

Also, the module defines a set of identities, including the following:

'service-type': Used to identify the VPN service type. Examples of supported service types are as follows:

* L3VPN,

* Virtual Private LAN Service (VPLS) using BGP [RFC4761],

* VPLS using the Label Distribution Protocol (LDP) [RFC4762],

* Virtual Private Wire Service (VPWS) [RFC8214],

* BGP MPLS-Based Ethernet VPN [RFC7432],

* Ethernet VPN (EVPN) [RFC8365], and

* Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN) [RFC7623].

'vpn-signaling-type': Used to identify the signaling mode used for a given service type. Examples of supported VPN signaling types are as follows:

* L2VPNs using BGP [RFC6624],

* LDP [RFC5036], and

* Layer Two Tunneling Protocol (L2TP) [RFC3931].

The module covers both IPv4 [RFC0791] and IPv6 [RFC8200] identities. It also includes multicast-related identities such as Internet Group Management Protocol version 1 (IGMPv1) [RFC1112], IGMPv2 [RFC2236], IGMPv3 [RFC3376], Multicast Listener Discovery version 1 (MLDv1) [RFC2710], MLDv2 [RFC3810], and Protocol Independent Multicast (PIM) [RFC7761].

The reader should refer to Section 4 for the full list of supported identities (identities related to address families, VPN topologies, network access types, operational and administrative status, site or node role, VPN service constraints, routing protocols, route import and export policies, bandwidth, Quality of Service (QoS), etc.).

The "ietf-vpn-common" module also contains a set of reusable VPN-related groupings. Figure 1 provides the tree diagram that depicts the common groupings for the "ietf-vpn-common" module.

```
module: ietf-vpn-common
  grouping vpn-description:
    +-- vpn-id?            vpn-id
    +-- vpn-name?          string
    +-- vpn-description?   string
    +-- customer-name?     string
  grouping vpn-profile-cfg:
    +-- valid-provider-identifiers
       +-- external-connectivity-identifier* [id]
       |       {external-connectivity}?
       |  +-- id   string
       +-- encryption-profile-identifier* [id]
       |  +-- id   string
       +-- qos-profile-identifier* [id]
       |  +-- id   string
       +-- bfd-profile-identifier* [id]
       |  +-- id   string
       +-- forwarding-profile-identifier* [id]
```

```
      |  +-- id   string
      +-- routing-profile-identifier* [id]
         +-- id   string
  grouping oper-status-timestamp:
    +--ro status?         identityref
    +--ro last-change?   yang:date-and-time
  grouping service-status:
    +-- status
       +-- admin-status
       |  +-- status?         identityref
       |  +-- last-change?    yang:date-and-time
       +--ro oper-status
          +--ro status?         identityref
          +--ro last-change?    yang:date-and-time
  grouping underlay-transport:
    +-- (type)?
       +--:(abstract)
       |  +-- transport-instance-id?   string
       |  +-- instance-type?           identityref
       +--:(protocol)
          +-- protocol*                identityref
  grouping vpn-route-targets:
    +-- vpn-target* [id]
    |  +-- id                   uint8
    |  +-- route-targets* [route-target]
    |  |  +-- route-target      rt-types:route-target
    |  +-- route-target-type    rt-types:route-target-type
    +-- vpn-policies
       +-- import-policy?   string
       +-- export-policy?   string
  grouping route-distinguisher:
    ...
  grouping vpn-components-group:
    +-- groups
       +-- group* [group-id]
          +-- group-id    string
  grouping placement-constraints:
    +-- constraint* [constraint-type]
       +-- constraint-type?   identityref
       +-- target
          +-- (target-flavor)?
             +--:(id)
             |  +-- group* [group-id]
             |     +-- group-id    string
             +--:(all-accesses)
             |  +-- all-other-accesses?   empty
             +--:(all-groups)
                +-- all-other-groups?     empty
  grouping ports:
    ...
  grouping qos-classification-policy:
    ...
```

Figure 1: VPN Common Tree

The descriptions of the common groupings are provided below:

'vpn-description':
   A YANG grouping that provides common administrative VPN
   information such as an identifier, a name, a textual description,
   and a customer name.

'vpn-profile-cfg':
   A YANG grouping that defines a set of valid profiles (encryption,
   routing, forwarding, etc.) that can be bound to a Layer 2/3 VPN.
   This document does not make any assumptions about the structure of

such profiles but allows "gluing" a VPN service with other parameters that can be required locally to provide value-added features to requesting customers.

For example, a service provider may provide external connectivity to a VPN customer (e.g., to a private or public cloud, Internet). Such a service may involve tweaking both filtering and NAT rules (e.g., binding a Virtual Routing and Forwarding (VRF) interface with a NAT instance as discussed in Section 2.10 of [RFC8512]). These value-added features may be bound to all, or a subset of, network accesses. Some of these value-added features may be implemented in nodes other than Provider Edges (PEs) (e.g., a P node or even a dedicated node that hosts the NAT function).

Elaborating on the structure of these profiles is beyond the scope of this document.

'oper-status-timestamp':
A YANG grouping that defines the operational status updates of a VPN service or component.

'service-status':
A YANG grouping that defines the administrative and operational status of a component. The grouping can be applied to the whole service or an endpoint.

'underlay-transport':
A YANG grouping that defines the type of the underlay transport for a VPN service or how that underlay is set.

The underlay transport can be expressed as an abstract transport instance (e.g., an identifier of a VPN+ instance [Enhanced-VPN-Framework], a virtual network identifier [ACTN-VN-YANG] [RFC8453], or a network slice name [Network-Slices-Framework]) or as an ordered list of the actual protocols to be enabled in the network.

The module supports a rich set of protocol identifiers that can be used, for example, to refer to an underlay transport. Examples of supported protocols are as follows:

* IP in IP [RFC2003] [RFC2473],

* Generic Routing Encapsulation (GRE) [RFC1701] [RFC1702] [RFC7676],

* MPLS in UDP [RFC7510],

* Generic Network Virtualization Encapsulation (Geneve) [RFC8926],

* Segment Routing (SR) [RFC8660] [RFC8663] [RFC8754],

* Resource ReSerVation Protocol (RSVP) with traffic engineering extensions [RFC3209], and

* BGP with labeled prefixes [RFC8277].

'vpn-route-targets':
A YANG grouping that defines Route Target (RT) import/export rules used in a BGP-enabled VPN. This grouping can be used for both L3VPNs [RFC4364] and L2VPNs [RFC4664]. Note that this is modeled as a list to ease the reuse of this grouping in modules where an RT identifier is needed (e.g., associating an operator with RTs).

'route-distinguisher':

A YANG grouping that defines Route Distinguishers (RDs).

As depicted in Figure 2, the module supports the following RD assignment modes: direct assignment, full automatic assignment, automatic assignment from a given pool, and no assignment.

Also, the module accommodates deployments where only the Assigned Number subfield of RDs (Section 4.2 of [RFC4364]) is assigned from a pool while the Administrator subfield is set to, for example, the Router ID that is assigned to a VPN node. The module supports three modes for managing the Assigned Number subfield: explicit assignment, automatic assignment from a given pool, and full automatic assignment.

```
  grouping route-distinguisher:
    +-- (rd-choice)?
       +--:(directly-assigned)
       |  +-- rd?               rt-types:route-distinguisher
       +--:(directly-assigned-suffix)
       |  +-- rd-suffix?        uint16
       +--:(auto-assigned)
       |  +-- rd-auto
       |     +-- (auto-mode)?
       |     |  +--:(from-pool)
       |     |  |  +-- rd-pool-name?   string
       |     |  +--:(full-auto)
       |     |     +-- auto?           empty
       |     +--ro auto-assigned-rd?
       |     |       rt-types:route-distinguisher
       +--:(auto-assigned-suffix)
       |  +-- rd-auto-suffix
       |     +-- (auto-mode)?
       |     |  +--:(from-pool)
       |     |  |  +-- rd-pool-name?        string
       |     |  +--:(full-auto)
       |     |     +-- auto?                empty
       |     +--ro auto-assigned-rd-suffix?   uint16
       +--:(no-rd)
          +-- no-rd?            empty
```

Figure 2: Route Distinguisher Grouping Subtree

'vpn-components-group':
A YANG grouping that is used to group VPN nodes, VPN network accesses, or sites. For example, diversity or redundancy constraints can be applied on a per-group basis.

'placement-constraints':
A YANG grouping that is used to define the placement constraints of a VPN node, VPN network access, or site.

'ports':
A YANG grouping that defines ranges of source and destination port numbers and operators. The subtree of this grouping is depicted in Figure 3.

```
  grouping ports:
    +-- (source-port)?
    |  +--:(source-port-range-or-operator)
    |     +-- source-port-range-or-operator
    |        +-- (port-range-or-operator)?
    |           +--:(range)
    |           |  +-- lower-port    inet:port-number
    |           |  +-- upper-port    inet:port-number
    |           +--:(operator)
    |              +-- operator?     operator
```

```
|              +-- port          inet:port-number
+-- (destination-port)?
   +--:(destination-port-range-or-operator)
      +-- destination-port-range-or-operator
         +-- (port-range-or-operator)?
            +--:(range)
            |  +-- lower-port    inet:port-number
            |  +-- upper-port    inet:port-number
            +--:(operator)
               +-- operator?     operator
               +-- port          inet:port-number
```

Figure 3: Port Numbers Grouping Subtree

'qos-classification-policy':
A YANG grouping that defines a set of QoS classification policies based on various Layer 3/4 and application match criteria. The subtree of this grouping is depicted in Figure 4.

The QoS match criteria reuse groupings that are defined in the packet fields module "ietf-packet-fields" (Section 4.2 of [RFC8519]).

Any Layer 4 protocol can be indicated in the 'protocol' data node under 'l3', but only TCP- and UDP-specific match criteria are elaborated on in this version, as these protocols are widely used in the context of VPN services. Future revisions can be considered to add other Layer-4-specific parameters (e.g., the Stream Control Transmission Protocol [RFC4960]), if needed.

Some transport protocols use existing protocols (e.g., TCP or UDP) as the substrate. The match criteria for such protocols may rely upon the 'protocol' under 'l3', TCP/UDP match criteria as shown in Figure 4, part of the TCP/UDP payload, or a combination thereof. This version of the module does not support such advanced match criteria. Future revisions of the module may consider adding match criteria based on the transport protocol payload (e.g., by means of a bitmask match).

```
  grouping qos-classification-policy:
    +-- rule* [id]
       +-- id                          string
       +-- (match-type)?
       |  +--:(match-flow)
       |  |  +-- (l3)?
       |  |  |  +--:(ipv4)
       |  |  |  |  +-- ipv4
       |  |  |  |     +-- dscp?                          inet:dscp
       |  |  |  |     +-- ecn?                           uint8
       |  |  |  |     +-- length?                        uint16
       |  |  |  |     +-- ttl?                           uint8
       |  |  |  |     +-- protocol?                      uint8
       |  |  |  |     +-- ihl?                           uint8
       |  |  |  |     +-- flags?                         bits
       |  |  |  |     +-- offset?                        uint16
       |  |  |  |     +-- identification?                uint16
       |  |  |  |     +-- (destination-network)?
       |  |  |  |     |  +--:(destination-ipv4-network)
       |  |  |  |     |     +-- destination-ipv4-network?
       |  |  |  |     |           inet:ipv4-prefix
       |  |  |  |     +-- (source-network)?
       |  |  |  |        +--:(source-ipv4-network)
       |  |  |  |           +-- source-ipv4-network?
       |  |  |  |                 inet:ipv4-prefix
       |  |  |  +--:(ipv6)
       |  |  |     +-- ipv6
```

```
|  |  |        +-- dscp?                          inet:dscp
|  |  |        +-- ecn?                           uint8
|  |  |        +-- length?                        uint16
|  |  |        +-- ttl?                           uint8
|  |  |        +-- protocol?                      uint8
|  |  |        +-- (destination-network)?
|  |  |        |  +--:(destination-ipv6-network)
|  |  |        |     +-- destination-ipv6-network?
|  |  |        |               inet:ipv6-prefix
|  |  |        +-- (source-network)?
|  |  |        |  +--:(source-ipv6-network)
|  |  |        |     +-- source-ipv6-network?
|  |  |        |               inet:ipv6-prefix
|  |  |        +-- flow-label?
|  |  |                  inet:ipv6-flow-label
|  |  +-- (l4)?
|  |     +--:(tcp)
|  |     |  +-- tcp
|  |     |     +-- sequence-number?              uint32
|  |     |     +-- acknowledgement-number?       uint32
|  |     |     +-- data-offset?                  uint8
|  |     |     +-- reserved?                     uint8
|  |     |     +-- flags?                        bits
|  |     |     +-- window-size?                  uint16
|  |     |     +-- urgent-pointer?               uint16
|  |     |     +-- options?                      binary
|  |     |     +-- (source-port)?
|  |     |     |  +--:(source-port-range-or-operator)
|  |     |     |     +-- source-port-range-or-operator
|  |     |     |        +-- (port-range-or-operator)?
|  |     |     |           +--:(range)
|  |     |     |           |  +-- lower-port
|  |     |     |           |  |       inet:port-number
|  |     |     |           |  +-- upper-port
|  |     |     |           |          inet:port-number
|  |     |     |           +--:(operator)
|  |     |     |              +-- operator?    operator
|  |     |     |              +-- port
|  |     |     |                      inet:port-number
|  |     |     +-- (destination-port)?
|  |     |        +--:(destination-port-range-or-operator)
|  |     |           +-- destination-port-range-or-operator
|  |     |              +-- (port-range-or-operator)?
|  |     |                 +--:(range)
|  |     |                 |  +-- lower-port
|  |     |                 |  |       inet:port-number
|  |     |                 |  +-- upper-port
|  |     |                 |          inet:port-number
|  |     |                 +--:(operator)
|  |     |                    +-- operator?    operator
|  |     |                    +-- port
|  |     |                            inet:port-number
|  |     +--:(udp)
|  |        +-- udp
|  |           +-- length?                       uint16
|  |           +-- (source-port)?
|  |           |  +--:(source-port-range-or-operator)
|  |           |     +-- source-port-range-or-operator
|  |           |        +-- (port-range-or-operator)?
|  |           |           +--:(range)
|  |           |           |  +-- lower-port
|  |           |           |  |       inet:port-number
|  |           |           |  +-- upper-port
|  |           |           |          inet:port-number
|  |           |           +--:(operator)
|  |           |              +-- operator?    operator
```

```
|  |           |              +-- port
|  |           |                     inet:port-number
|  |           +-- (destination-port)?
|  |              +--:(destination-port-range-or-operator)
|  |                 +-- destination-port-range-or-operator
|  |                    +-- (port-range-or-operator)?
|  |                       +--:(range)
|  |                       |  +-- lower-port
|  |                       |  |       inet:port-number
|  |                       |  +-- upper-port
|  |                       |          inet:port-number
|  |                       +--:(operator)
|  |                          +-- operator?     operator
|  |                          +-- port
|  |                                  inet:port-number
|  +--:(match-application)
|     +-- match-application?   identityref
+-- target-class-id?           string
```

Figure 4: QoS Classification Subtree

4. Layer 2/3 VPN Common Module

This module uses types defined in [RFC6991], [RFC8294], and [RFC8519]. It also uses the extension defined in [RFC8341].

```
<CODE BEGINS> file "ietf-vpn-common@2022-02-11.yang"
module ietf-vpn-common {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-vpn-common";
  prefix vpn-common;

  import ietf-netconf-acm {
    prefix nacm;
    reference
      "RFC 8341: Network Configuration Access Control Model";
  }
  import ietf-routing-types {
    prefix rt-types;
    reference
      "RFC 8294: Common YANG Data Types for the Routing Area";
  }
  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types, Section 3";
  }
  import ietf-packet-fields {
    prefix packet-fields;
    reference
      "RFC 8519: YANG Data Model for Network Access
                 Control Lists (ACLs)";
  }

  organization
    "IETF OPSAWG (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:   Samier Barguil
               <mailto:samier.barguilgiraldo.ext@telefonica.com>
     Editor:   Oscar Gonzalez de Dios
               <mailto:oscar.gonzalezdedios@telefonica.com>
```

```
   Author:   Qin Wu
             <mailto:bill.wu@huawei.com>";
description
  "This YANG module defines a common module that is meant
   to be reused by various VPN-related modules (e.g., the
   Layer 3 VPN Service Model (L3SM), the Layer 2 VPN Service
   Model (L2SM), the Layer 3 VPN Network Model (L3NM), and
   the Layer 2 VPN Network Model (L2NM)).

   Copyright (c) 2022 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 9181; see the
   RFC itself for full legal notices.";

revision 2022-02-11 {
  description
    "Initial revision.";
  reference
    "RFC 9181: A Common YANG Data Model for Layer 2 and Layer 3
               VPNs";
}

/******** Collection of VPN-related features ********/
/*
 * Features related to encapsulation schemes
 */

feature dot1q {
  description
    "Indicates support for dot1Q encapsulation.";
  reference
    "IEEE Std 802.1Q: IEEE Standard for Local and Metropolitan
                      Area Networks--Bridges and Bridged
                      Networks";
}

feature qinq {
  description
    "Indicates support for QinQ encapsulation.";
  reference
    "IEEE Std 802.1ad: IEEE Standard for Local and Metropolitan
                       Area Networks---Virtual Bridged Local
                       Area Networks---Amendment 4: Provider
                       Bridges";
}

feature vxlan {
  description
    "Indicates support for Virtual eXtensible Local Area
     Network (VXLAN) encapsulation.";
  reference
    "RFC 7348: Virtual eXtensible Local Area Network (VXLAN):
               A Framework for Overlaying Virtualized Layer 2
               Networks over Layer 3 Networks";
}

feature qinany {
  description
```

```
    "Indicates support for QinAny encapsulation.
     The outer VLAN tag is set to a specific value, but
     the inner VLAN tag is set to any.";
}

feature lag-interface {
  description
    "Indicates support for Link Aggregation Groups (LAGs)
     between VPN network accesses.";
  reference
    "IEEE Std 802.1AX: IEEE Standard for Local and Metropolitan
                       Area Networks--Link Aggregation";
}

/*
 * Features related to multicast
 */

feature multicast {
  description
    "Indicates support for multicast capabilities in a VPN.";
  reference
    "RFC 6513: Multicast in MPLS/BGP IP VPNs";
}

feature igmp {
  description
    "Indicates support for the Internet Group Management
     Protocol (IGMP).";
  reference
    "RFC 1112: Host Extensions for IP Multicasting
     RFC 2236: Internet Group Management Protocol, Version 2
     RFC 3376: Internet Group Management Protocol, Version 3";
}

feature mld {
  description
    "Indicates support for Multicast Listener Discovery (MLD).";
  reference
    "RFC 2710: Multicast Listener Discovery (MLD) for IPv6
     RFC 3810: Multicast Listener Discovery Version 2 (MLDv2)
               for IPv6";
}

feature pim {
  description
    "Indicates support for Protocol Independent Multicast
     (PIM).";
  reference
    "RFC 7761: Protocol Independent Multicast - Sparse Mode
               (PIM-SM): Protocol Specification (Revised)";
}

/*
 * Features related to address family types
 */

feature ipv4 {
  description
    "Indicates IPv4 support in a VPN.  That is, IPv4 traffic
     can be carried in the VPN, IPv4 addresses/prefixes can
     be assigned to a VPN network access, IPv4 routes can be
     installed for the Customer Edge to Provider Edge (CE-PE)
     link, etc.";
  reference
    "RFC 791: Internet Protocol";
```

```
}

feature ipv6 {
  description
    "Indicates IPv6 support in a VPN.  That is, IPv6 traffic
     can be carried in the VPN, IPv6 addresses/prefixes can
     be assigned to a VPN network access, IPv6 routes can be
     installed for the CE-PE link, etc.";
  reference
    "RFC 8200: Internet Protocol, Version 6 (IPv6)
               Specification";
}

/*
 * Features related to routing protocols
 */

feature rtg-ospf {
  description
    "Indicates support for OSPF as the Provider Edge to
     Customer Edge (PE-CE) routing protocol.";
  reference
    "RFC 4577: OSPF as the Provider/Customer Edge Protocol
               for BGP/MPLS IP Virtual Private Networks (VPNs)
     RFC 6565: OSPFv3 as a Provider Edge to Customer Edge
               (PE-CE) Routing Protocol";
}

feature rtg-ospf-sham-link {
  description
    "Indicates support for OSPF sham links.";
  reference
    "RFC 4577: OSPF as the Provider/Customer Edge Protocol
               for BGP/MPLS IP Virtual Private Networks (VPNs),
               Section 4.2.7
     RFC 6565: OSPFv3 as a Provider Edge to Customer Edge
               (PE-CE) Routing Protocol, Section 5";
}

feature rtg-bgp {
  description
    "Indicates support for BGP as the PE-CE routing protocol.";
  reference
    "RFC 4271: A Border Gateway Protocol 4 (BGP-4)";
}

feature rtg-rip {
  description
    "Indicates support for RIP as the PE-CE routing protocol.";
  reference
    "RFC 2453: RIP Version 2
     RFC 2080: RIPng for IPv6";
}

feature rtg-isis {
  description
    "Indicates support for IS-IS as the PE-CE routing
     protocol.";
  reference
    "ISO10589: Information technology - Telecommunications and
               information exchange between systems -
               Intermediate System to Intermediate System
               intra-domain routeing information exchange
               protocol for use in conjunction with the protocol
               for providing the connectionless-mode network
               service (ISO 8473)";
```

```
}

feature rtg-vrrp {
  description
    "Indicates support for the Virtual Router Redundancy
     Protocol (VRRP) in the CE-PE link.";
  reference
    "RFC 5798: Virtual Router Redundancy Protocol (VRRP)
               Version 3 for IPv4 and IPv6";
}

feature bfd {
  description
    "Indicates support for Bidirectional Forwarding Detection
     (BFD) between the CE and the PE.";
  reference
    "RFC 5880: Bidirectional Forwarding Detection (BFD)";
}

/*
 * Features related to VPN service constraints
 */

feature bearer-reference {
  description
    "A bearer refers to properties of the CE-PE attachment that
     are below Layer 3.
     This feature indicates support for the bearer reference
     access constraint, i.e., the reuse of a network connection
     that was already ordered to the service provider apart from
     the IP VPN site.";
}

feature placement-diversity {
  description
    "Indicates support for placement diversity constraints in
     the customer premises.  An example of these constraints
     may be to avoid connecting a site network access to the
     same PE as a target site network access.";
}

/*
 * Features related to bandwidth and Quality of Service (QoS)
 */

feature qos {
  description
    "Indicates support for Classes of Service (CoSes) in
     the VPN.";
}

feature inbound-bw {
  description
    "Indicates support for the inbound bandwidth in a VPN,
     i.e., support for specifying the download bandwidth from
     the service provider network to the VPN site.  Note that
     the L3SM uses 'input' to identify the same feature.
     That terminology should be deprecated in favor of
     the terminology defined in this module.";
}

feature outbound-bw {
  description
    "Indicates support for the outbound bandwidth in a VPN,
     i.e., support for specifying the upload bandwidth from
     the VPN site to the service provider network.  Note that
```

```
     the L3SM uses 'output' to identify the same feature.
     That terminology should be deprecated in favor of the
     terminology defined in this module.";
}

/*
 * Features related to security and resilience
 */

feature encryption {
  description
    "Indicates support for encryption in the VPN.";
}

feature fast-reroute {
  description
    "Indicates support for Fast Reroute (FRR) capabilities for
     a VPN site.";
}

/*
 * Features related to advanced VPN options
 */

feature external-connectivity {
  description
    "Indicates support for the VPN to provide external
     connectivity (e.g., Internet, private or public cloud).";
  reference
    "RFC 4364: BGP/MPLS IP Virtual Private Networks
               (VPNs), Section 11";
}

feature extranet-vpn {
  description
    "Indicates support for extranet VPNs, i.e., the capability
     of a VPN to access a list of other VPNs.";
  reference
    "RFC 4364: BGP/MPLS IP Virtual Private Networks
               (VPNs), Section 1.1";
}

feature carriers-carrier {
  description
    "Indicates support for Carriers' Carriers in VPNs.";
  reference
    "RFC 4364: BGP/MPLS IP Virtual Private Networks
               (VPNs), Section 9";
}

/*
 * Identities related to address families
 */

identity address-family {
  description
    "Defines a type for the address family.";
}

identity ipv4 {
  base address-family;
  description
    "Identity for an IPv4 address family.";
}

identity ipv6 {
```

```
  base address-family;
  description
    "Identity for an IPv6 address family.";
}

identity dual-stack {
  base address-family;
  description
    "Identity for IPv4 and IPv6 address families.";
}

/*
 * Identities related to VPN topology
 */

identity vpn-topology {
  description
    "Base identity of the VPN topology.";
}

identity any-to-any {
  base vpn-topology;
  description
    "Identity for any-to-any VPN topology.  All VPN sites
     can communicate with each other without any restrictions.";
}

identity hub-spoke {
  base vpn-topology;
  description
    "Identity for Hub-and-Spoke VPN topology.  All Spokes can
     communicate with Hubs only and not with each other.  Hubs
     can communicate with each other.";
}

identity hub-spoke-disjoint {
  base vpn-topology;
  description
    "Identity for Hub-and-Spoke VPN topology where Hubs cannot
     communicate with each other.";
}

identity custom {
  base vpn-topology;
  description
    "Identity for custom VPN topologies where the role of the
     nodes is not strictly Hub or Spoke.  The VPN topology is
     controlled by the import/export policies.  The custom
     topology reflects more complex VPN nodes, such as a
     VPN node that acts as a Hub for certain nodes and a Spoke
     for others.";
}

/*
 * Identities related to network access types
 */

identity site-network-access-type {
  description
    "Base identity for site network access types.";
}

identity point-to-point {
  base site-network-access-type;
  description
    "Point-to-point access type.";
```

```
}

identity multipoint {
  base site-network-access-type;
  description
    "Multipoint access type.";
}

identity irb {
  base site-network-access-type;
  description
    "Integrated Routing and Bridging (IRB).
     Identity for pseudowire connections.";
}

identity loopback {
  base site-network-access-type;
  description
    "Loopback access type.";
}

/*
 * Identities related to operational and administrative status
 */

identity operational-status {
  description
    "Base identity for operational status.";
}

identity op-up {
  base operational-status;
  description
    "Operational status is Up/Enabled.";
}

identity op-down {
  base operational-status;
  description
    "Operational status is Down/Disabled.";
}

identity op-unknown {
  base operational-status;
  description
    "Operational status is Unknown.";
}

identity administrative-status {
  description
    "Base identity for administrative status.";
}

identity admin-up {
  base administrative-status;
  description
    "Administrative status is Up/Enabled.";
}

identity admin-down {
  base administrative-status;
  description
    "Administrative status is Down/Disabled.";
}

identity admin-testing {
```

```
  base administrative-status;
  description
    "Administrative status is Up for testing purposes.";
}

identity admin-pre-deployment {
  base administrative-status;
  description
    "Administrative status reflects a pre-deployment phase,
     i.e., prior to the actual deployment of a service.";
}

/*
 * Identities related to site or node roles
 */

identity role {
  description
    "Base identity of a site or node role.";
}

identity any-to-any-role {
  base role;
  description
    "Any-to-any role.";
}

identity spoke-role {
  base role;
  description
    "A node or a site is acting as a Spoke.";
}

identity hub-role {
  base role;
  description
    "A node or a site is acting as a Hub.";
}

identity custom-role {
  base role;
  description
    "VPN node with a custom or complex role in the VPN.  For
     some sources/destinations, it can behave as a Hub, but for
     others, it can act as a Spoke, depending on the configured
     policy.";
}

/*
 * Identities related to VPN service constraints
 */

identity placement-diversity {
  description
    "Base identity for access placement constraints.";
}

identity bearer-diverse {
  base placement-diversity;
  description
    "Bearer diversity.

     The bearers should not use common elements.";
}

identity pe-diverse {
```

```
  base placement-diversity;
  description
    "PE diversity.";
}

identity pop-diverse {
  base placement-diversity;
  description
    "Point of Presence (POP) diversity.";
}

identity linecard-diverse {
  base placement-diversity;
  description
    "Linecard diversity.";
}

identity same-pe {
  base placement-diversity;
  description
    "Having sites connected on the same PE.";
}

identity same-bearer {
  base placement-diversity;
  description
    "Having sites connected using the same bearer.";
}

/*
 * Identities related to service types
 */

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

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

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

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

identity pbb-evpn {
  base service-type;
  description
    "Provider Backbone Bridging (PBB) EVPN 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)";
}

/*
 * Identities related to VPN signaling types
 */

identity vpn-signaling-type {
  description
    "Base identity for VPN signaling types.";
}

identity bgp-signaling {
  base vpn-signaling-type;
  description
    "Layer 2 VPNs using BGP signaling.";
  reference
    "RFC 6624: Layer 2 Virtual Private Networks Using BGP for
               Auto-Discovery and Signaling
     RFC 7432: BGP MPLS-Based Ethernet VPN";
}

identity ldp-signaling {
  base vpn-signaling-type;
  description
    "Targeted Label Distribution Protocol (LDP) signaling.";
  reference
    "RFC 5036: LDP Specification";
}

identity l2tp-signaling {
  base vpn-signaling-type;
  description
    "Layer Two Tunneling Protocol (L2TP) signaling.";
```

```
  reference
    "RFC 3931: Layer Two Tunneling Protocol - Version 3 (L2TPv3)";
}

/*
 * Identities related to routing protocols
 */

identity routing-protocol-type {
  description
    "Base identity for routing protocol types.";
}

identity static-routing {
  base routing-protocol-type;
  description
    "Static routing protocol.";
}

identity bgp-routing {
  if-feature "rtg-bgp";
  base routing-protocol-type;
  description
    "BGP routing protocol.";
  reference
    "RFC 4271: A Border Gateway Protocol 4 (BGP-4)";
}

identity ospf-routing {
  if-feature "rtg-ospf";
  base routing-protocol-type;
  description
    "OSPF routing protocol.";
  reference
    "RFC 4577: OSPF as the Provider/Customer Edge Protocol
                for BGP/MPLS IP Virtual Private Networks (VPNs)
     RFC 6565: OSPFv3 as a Provider Edge to Customer Edge
                (PE-CE) Routing Protocol";
}

identity rip-routing {
  if-feature "rtg-rip";
  base routing-protocol-type;
  description
    "RIP routing protocol.";
  reference
    "RFC 2453: RIP Version 2
     RFC 2080: RIPng for IPv6";
}

identity isis-routing {
  if-feature "rtg-isis";
  base routing-protocol-type;
  description
    "IS-IS routing protocol.";
  reference
    "ISO10589: Information technology - Telecommunications and
                information exchange between systems -
                Intermediate System to Intermediate System
                intra-domain routeing information exchange
                protocol for use in conjunction with the protocol
                for providing the connectionless-mode network
                service (ISO 8473)";
}

identity vrrp-routing {
```

```
  if-feature "rtg-vrrp";
  base routing-protocol-type;
  description
    "VRRP protocol.

     This is to be used when LANs are directly connected to
     PEs.";
  reference
    "RFC 5798: Virtual Router Redundancy Protocol (VRRP)
               Version 3 for IPv4 and IPv6";
}

identity direct-routing {
  base routing-protocol-type;
  description
    "Direct routing.

     This is to be used when LANs are directly connected to PEs
     and must be advertised in the VPN.";
}

identity any-routing {
  base routing-protocol-type;
  description
    "Any routing protocol.

     For example, this can be used to set policies that apply
     to any routing protocol in place.";
}

identity isis-level {
  if-feature "rtg-isis";
  description
    "Base identity for the IS-IS level.";
  reference
    "ISO10589: Information technology - Telecommunications and
               information exchange between systems -
               Intermediate System to Intermediate System
               intra-domain routeing information exchange
               protocol for use in conjunction with the protocol
               for providing the connectionless-mode network
               service (ISO 8473)";
}

identity level-1 {
  base isis-level;
  description
    "IS-IS Level 1.";
}

identity level-2 {
  base isis-level;
  description
    "IS-IS Level 2.";
}

identity level-1-2 {
  base isis-level;
  description
    "IS-IS Levels 1 and 2.";
}

identity bfd-session-type {
  if-feature "bfd";
  description
    "Base identity for the BFD session type.";
```

```
}

identity classic-bfd {
  base bfd-session-type;
  description
    "Classic BFD.";
  reference
    "RFC 5880: Bidirectional Forwarding Detection (BFD)";
}

identity s-bfd {
  base bfd-session-type;
  description
    "Seamless BFD.";
  reference
    "RFC 7880: Seamless Bidirectional Forwarding Detection
               (S-BFD)";
}

/*
 * Identities related to route import and export policies
 */

identity ie-type {
  description
    "Base identity for import/export routing profiles.
     These profiles can be reused between VPN nodes.";
}

identity import {
  base ie-type;
  description
    "Import routing profile.";
  reference
    "RFC 4364: BGP/MPLS IP Virtual Private Networks
               (VPNs), Section 4.3.1";
}

identity export {
  base ie-type;
  description
    "Export routing profile.";
  reference
    "RFC 4364: BGP/MPLS IP Virtual Private Networks
               (VPNs), Section 4.3.1";
}

identity import-export {
  base ie-type;
  description
    "Import/export routing profile.";
}

/*
 * Identities related to bandwidth and QoS
 */

identity bw-direction {
  description
    "Base identity for the bandwidth direction.";
}

identity inbound-bw {
  if-feature "inbound-bw";
  base bw-direction;
  description
```

```
    "Inbound bandwidth.";
}

identity outbound-bw {
  if-feature "outbound-bw";
  base bw-direction;
  description
    "Outbound bandwidth.";
}

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

identity bw-per-cos {
  if-feature "qos";
  base bw-type;
  description
    "The bandwidth is per CoS.";
}

identity bw-per-port {
  base bw-type;
  description
    "The bandwidth is per a given site network access.";
}

identity bw-per-site {
  base bw-type;
  description
    "The bandwidth is per site.  It is applicable to all the
     site network accesses within a site.";
}

identity bw-per-service {
  base bw-type;
  description
    "The bandwidth is per VPN service.";
}

identity qos-profile-direction {
  if-feature "qos";
  description
    "Base identity for the QoS profile direction.";
}

identity site-to-wan {
  base qos-profile-direction;
  description
    "From the customer site to the provider's network.
     This is typically the CE-to-PE direction.";
}

identity wan-to-site {
  base qos-profile-direction;
  description
    "From the provider's network to the customer site.
     This is typically the PE-to-CE direction.";
}

identity both {
  base qos-profile-direction;
  description
    "Both the WAN-to-site direction and the site-to-WAN
     direction.";
```

```
}

/*
 * Identities related to underlay transport instances
 */

identity transport-instance-type {
  description
    "Base identity for underlay transport instance types.";
}

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

identity enhanced-vpn {
  base transport-instance-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 classical VPNs.";
  reference
    "draft-ietf-teas-enhanced-vpn-09:
       A Framework for Enhanced Virtual Private Network
       (VPN+) Services";
}

identity ietf-network-slice {
  base transport-instance-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-05:
       Framework for IETF Network Slices";
}

/*
 * Identities related to protocol types.  These types are
 * typically used to identify the underlay transport.
 */

identity protocol-type {
  description
    "Base identity for protocol types.";
}

identity ip-in-ip {
  base protocol-type;
  description
    "Transport is based on IP in IP.";
  reference
    "RFC 2003: IP Encapsulation within IP
     RFC 2473: Generic Packet Tunneling in IPv6 Specification";
}

identity ip-in-ipv4 {
```

```
  base ip-in-ip;
  description
    "Transport is based on IP over IPv4.";
  reference
    "RFC 2003: IP Encapsulation within IP";
}

identity ip-in-ipv6 {
  base ip-in-ip;
  description
    "Transport is based on IP over IPv6.";
  reference
    "RFC 2473: Generic Packet Tunneling in IPv6 Specification";
}

identity gre {
  base protocol-type;
  description
    "Transport is based on Generic Routing Encapsulation
     (GRE).";
  reference
    "RFC 1701: Generic Routing Encapsulation (GRE)
     RFC 1702: Generic Routing Encapsulation over IPv4 networks
     RFC 7676: IPv6 Support for Generic Routing Encapsulation
               (GRE)";
}

identity gre-v4 {
  base gre;
  description
    "Transport is based on GRE over IPv4.";
  reference
    "RFC 1702: Generic Routing Encapsulation over IPv4
               networks";
}

identity gre-v6 {
  base gre;
  description
    "Transport is based on GRE over IPv6.";
  reference
    "RFC 7676: IPv6 Support for Generic Routing Encapsulation
               (GRE)";
}

identity vxlan-trans {
  base protocol-type;
  description
    "Transport is based on VXLANs.";
  reference
    "RFC 7348: Virtual eXtensible Local Area Network (VXLAN):
               A Framework for Overlaying Virtualized Layer 2
               Networks over Layer 3 Networks";
}

identity geneve {
  base protocol-type;
  description
    "Transport is based on Generic Network Virtualization
     Encapsulation (Geneve).";
  reference
    "RFC 8926: Geneve: Generic Network Virtualization
               Encapsulation";
}

identity ldp {
```

```
  base protocol-type;
  description
    "Transport is based on LDP.";
  reference
    "RFC 5036: LDP Specification";
}

identity mpls-in-udp {
  base protocol-type;
  description
    "Transport is based on MPLS in UDP.";
  reference
    "RFC 7510: Encapsulating MPLS in UDP";
}

identity sr {
  base protocol-type;
  description
    "Transport is based on Segment Routing (SR).";
  reference
    "RFC 8660: Segment Routing with the MPLS Data Plane
     RFC 8663: MPLS Segment Routing over IP
     RFC 8754: IPv6 Segment Routing Header (SRH)";
}

identity sr-mpls {
  base sr;
  description
    "Transport is based on SR with the MPLS data plane.";
  reference
    "RFC 8660: Segment Routing with the MPLS Data Plane";
}

identity srv6 {
  base sr;
  description
    "Transport is based on SR over IPv6.";
  reference
    "RFC 8754: IPv6 Segment Routing Header (SRH)";
}

identity sr-mpls-over-ip {
  base sr;
  description
    "Transport is based on SR over MPLS over IP.";
  reference
    "RFC 8663: MPLS Segment Routing over IP";
}

identity rsvp-te {
  base protocol-type;
  description
    "Transport setup relies upon RSVP-TE.";
  reference
    "RFC 3209: RSVP-TE: Extensions to RSVP for LSP Tunnels";
}

identity bgp-lu {
  base protocol-type;
  description
    "Transport setup relies upon BGP-based labeled prefixes.";
  reference
    "RFC 8277: Using BGP to Bind MPLS Labels to Address Prefixes";
}

identity unknown {
```

```
  base protocol-type;
  description
    "Unknown protocol type.";
}

/*
 * Identities related to encapsulation types
 */

identity encapsulation-type {
  description
    "Base identity for encapsulation types.";
}

identity priority-tagged {
  base encapsulation-type;
  description
    "Priority-tagged interface.";
}

identity dot1q {
  if-feature "dot1q";
  base encapsulation-type;
  description
    "dot1Q encapsulation.";
}

identity qinq {
  if-feature "qinq";
  base encapsulation-type;
  description
    "QinQ encapsulation.";
}

identity qinany {
  if-feature "qinany";
  base encapsulation-type;
  description
    "QinAny encapsulation.";
}

identity vxlan {
  if-feature "vxlan";
  base encapsulation-type;
  description
    "VXLAN encapsulation.";
}

identity ethernet-type {
  base encapsulation-type;
  description
    "Ethernet encapsulation type.";
}

identity vlan-type {
  base encapsulation-type;
  description
    "VLAN encapsulation type.";
}

identity untagged-int {
  base encapsulation-type;
  description
    "Untagged interface type.";
}
```

```
identity tagged-int {
  base encapsulation-type;
  description
    "Tagged interface type.";
}

identity lag-int {
  if-feature "lag-interface";
  base encapsulation-type;
  description
    "LAG interface type.";
}

/*
 * Identities related to VLAN tags
 */

identity tag-type {
  description
    "Base identity for VLAN tag types.";
}

identity c-vlan {
  base tag-type;
  description
    "Indicates a Customer VLAN (C-VLAN) tag, normally using
     the 0x8100 Ethertype.";
}

identity s-vlan {
  base tag-type;
  description
    "Indicates a Service VLAN (S-VLAN) tag.";
}

identity s-c-vlan {
  base tag-type;
  description
    "Uses both an S-VLAN tag and a C-VLAN tag.";
}

/*
 * Identities related to VXLANs
 */

identity vxlan-peer-mode {
  if-feature "vxlan";
  description
    "Base identity for VXLAN peer modes.";
}

identity static-mode {
  base vxlan-peer-mode;
  description
    "VXLAN access in the static mode.";
}

identity bgp-mode {
  base vxlan-peer-mode;
  description
    "VXLAN access by BGP EVPN learning.";
}

/*
 * Identities related to multicast
 */
```

```
identity multicast-gp-address-mapping {
  if-feature "multicast";
  description
    "Base identity for multicast group mapping types.";
}

identity static-mapping {
  base multicast-gp-address-mapping;
  description
    "Static mapping, i.e., an interface is attached to the
     multicast group as a static member.";
}

identity dynamic-mapping {
  base multicast-gp-address-mapping;
  description
    "Dynamic mapping, i.e., an interface is added to the
     multicast group as a result of snooping.";
}

identity multicast-tree-type {
  if-feature "multicast";
  description
    "Base identity for multicast tree types.";
}

identity ssm-tree-type {
  base multicast-tree-type;
  description
    "Source-Specific Multicast (SSM) tree type.";
}

identity asm-tree-type {
  base multicast-tree-type;
  description
    "Any-Source Multicast (ASM) tree type.";
}

identity bidir-tree-type {
  base multicast-tree-type;
  description
    "Bidirectional tree type.";
}

identity multicast-rp-discovery-type {
  if-feature "multicast";
  description
    "Base identity for Rendezvous Point (RP) discovery types.";
}

identity auto-rp {
  base multicast-rp-discovery-type;
  description
    "Auto-RP discovery type.";
}

identity static-rp {
  base multicast-rp-discovery-type;
  description
    "Static type.";
}

identity bsr-rp {
  base multicast-rp-discovery-type;
  description
```

```
    "Bootstrap Router (BSR) discovery type.";
}

identity group-management-protocol {
  if-feature "multicast";
  description
    "Base identity for multicast group management protocols.";
}

identity igmp-proto {
  base group-management-protocol;
  description
    "IGMP.";
  reference
    "RFC 1112: Host Extensions for IP Multicasting
     RFC 2236: Internet Group Management Protocol, Version 2
     RFC 3376: Internet Group Management Protocol, Version 3";
}

identity mld-proto {
  base group-management-protocol;
  description
    "MLD.";
  reference
    "RFC 2710: Multicast Listener Discovery (MLD) for IPv6
     RFC 3810: Multicast Listener Discovery Version 2 (MLDv2)
               for IPv6";
}

identity pim-proto {
  if-feature "pim";
  base routing-protocol-type;
  description
    "PIM.";
  reference
    "RFC 7761: Protocol Independent Multicast - Sparse Mode
               (PIM-SM): Protocol Specification (Revised)";
}

identity igmp-version {
  if-feature "igmp";
  description
    "Base identity for indicating the IGMP version.";
}

identity igmpv1 {
  base igmp-version;
  description
    "IGMPv1.";
  reference
    "RFC 1112: Host Extensions for IP Multicasting";
}

identity igmpv2 {
  base igmp-version;
  description
    "IGMPv2.";
  reference
    "RFC 2236: Internet Group Management Protocol, Version 2";
}

identity igmpv3 {
  base igmp-version;
  description
    "IGMPv3.";
  reference
```

```
    "RFC 3376: Internet Group Management Protocol, Version 3";
}

identity mld-version {
  if-feature "mld";
  description
    "Base identity for indicating the MLD version.";
}

identity mldv1 {
  base mld-version;
  description
    "MLDv1.";
  reference
    "RFC 2710: Multicast Listener Discovery (MLD) for IPv6";
}

identity mldv2 {
  base mld-version;
  description
    "MLDv2.";
  reference
    "RFC 3810: Multicast Listener Discovery Version 2 (MLDv2)
               for IPv6";
}

/*
 * Identities related to traffic types
 */

identity tf-type {
  description
    "Base identity for traffic types.";
}

identity multicast-traffic {
  base tf-type;
  description
    "Multicast traffic.";
}

identity broadcast-traffic {
  base tf-type;
  description
    "Broadcast traffic.";
}

identity unknown-unicast-traffic {
  base tf-type;
  description
    "Unknown unicast traffic.";
}

/*
 * Identities related to customer applications
 */

identity customer-application {
  description
    "Base identity for customer applications.";
}

identity web {
  base customer-application;
  description
    "Web applications (e.g., HTTP, HTTPS).";
```

```
}

identity mail {
  base customer-application;
  description
    "Mail application.";
}

identity file-transfer {
  base customer-application;
  description
    "File transfer application (e.g., FTP, Secure FTP (SFTP)).";
}

identity database {
  base customer-application;
  description
    "Database application.";
}

identity social {
  base customer-application;
  description
    "Social-network application.";
}

identity games {
  base customer-application;
  description
    "Gaming application.";
}

identity p2p {
  base customer-application;
  description
    "Peer-to-peer application.";
}

identity network-management {
  base customer-application;
  description
    "Management application (e.g., Telnet, syslog, SNMP).";
}

identity voice {
  base customer-application;
  description
    "Voice application.";
}

identity video {
  base customer-application;
  description
    "Video-conference application.";
}

identity embb {
  base customer-application;
  description
    "Enhanced Mobile Broadband (eMBB) application.
     Note that eMBB applications demand network performance
     with a wide variety of such characteristics as data rate,
     latency, loss rate, reliability, and many other
     parameters.";
}
```

```
identity urllc {
  base customer-application;
  description
    "Ultra-Reliable and Low Latency Communications (URLLC)
     application.  Note that URLLC applications demand
     network performance with a wide variety of such
     characteristics as latency, reliability, and many other
     parameters.";
}

identity mmtc {
  base customer-application;
  description
    "Massive Machine Type Communications (mMTC) application.
     Note that mMTC applications demand network performance
     with a wide variety of such characteristics as data rate,
     latency, loss rate, reliability, and many other
     parameters.";
}

/*
 * Identities related to service bundling
 */

identity bundling-type {
  description
    "The base identity for the bundling type.  It supports a
     subset or all Customer Edge VLAN IDs (CE-VLAN IDs)
     associated with an L2VPN service.";
}

identity multi-svc-bundling {
  base bundling-type;
  description
    "Multi-service bundling, i.e., multiple CE-VLAN IDs
     can be associated with an L2VPN service at a site.";
}

identity one2one-bundling {
  base bundling-type;
  description
    "One-to-one service bundling, i.e., each L2VPN can
     be associated with only one CE-VLAN ID at a site.";
}

identity all2one-bundling {
  base bundling-type;
  description
    "All-to-one bundling, i.e., all CE-VLAN IDs are mapped
     to one L2VPN service.";
}


/*
 * Identities related to Ethernet services
 */

identity control-mode {
  description
    "Base identity for the type of control mode used with the
     Layer 2 Control Protocol (L2CP).";
}

identity peer {
  base control-mode;
  description
```

```
    "'peer' mode, i.e., participate in the protocol towards
     the CE.  Peering is common for the Link Aggregation Control
     Protocol (LACP) and the Ethernet Local Management Interface
     (E-LMI) and, occasionally, for the Link Layer Discovery
     Protocol (LLDP).  For VPLSs and VPWSs, the subscriber can
     also request that the peer service provider enable
     spanning tree.";
}

identity tunnel {
  base control-mode;
  description
    "'tunnel' mode, i.e., pass to the egress or destination
     site.  For Ethernet Private Lines (EPLs), the expectation
     is that L2CP frames are tunneled.";
}

identity discard {
  base control-mode;
  description
    "'Discard' mode, i.e., discard the frame.";
}

identity neg-mode {
  description
    "Base identity for the type of negotiation mode.";
}

identity full-duplex {
  base neg-mode;
  description
    "Full-duplex negotiation mode.";
}

identity auto-neg {
  base neg-mode;
  description
    "Auto-negotiation mode.";
}

/******** VPN-related type ********/

typedef vpn-id {
  type string;
  description
    "Defines an identifier that is used with a VPN module.
     For example, this can be a service identifier, a node
     identifier, etc.";
}

/******* VPN-related reusable groupings *******/

grouping vpn-description {
  description
    "Provides common VPN information.";
  leaf vpn-id {
    type vpn-common:vpn-id;
    description
      "A VPN identifier that uniquely identifies a VPN.
       This identifier has a local meaning, e.g., within
       a service provider network.";
  }
  leaf vpn-name {
    type string;
    description
      "Used to associate a name with the service
```

```
        in order to facilitate the identification of
        the service.";
    }
    leaf vpn-description {
      type string;
      description
        "Textual description of a VPN.";
    }
    leaf customer-name {
      type string;
      description
        "Name of the customer that actually uses the VPN.";
    }
  }

  grouping vpn-profile-cfg {
    description
      "Grouping for VPN profile configuration.";
    container valid-provider-identifiers {
      description
        "Container for valid provider profile identifiers.";
      list external-connectivity-identifier {
        if-feature "external-connectivity";
        key "id";
        description
          "List of profile identifiers that uniquely identify
           profiles governing how external connectivity is
           provided to a VPN.  A profile indicates the type of
           external connectivity (Internet, cloud, etc.), the
           sites/nodes that are associated with a connectivity
           profile, etc.  A profile can also indicate filtering
           rules and/or address translation rules.  Such features
           may involve PE, P, or dedicated nodes as a function
           of the deployment.";
        leaf id {
          type string;
          description
            "Identification of an external connectivity profile.
             The profile only has significance within the service
             provider's administrative domain.";
        }
      }
      list encryption-profile-identifier {
        key "id";
        description
          "List of encryption profile identifiers.";
        leaf id {
          type string;
          description
            "Identification of the encryption profile to be used.
             The profile only has significance within the service
             provider's administrative domain.";
        }
      }
      list qos-profile-identifier {
        key "id";
        description
          "List of QoS profile identifiers.";
        leaf id {
          type string;
          description
            "Identification of the QoS profile to be used.  The
             profile only has significance within the service
             provider's administrative domain.";
        }
      }
```

```
    list bfd-profile-identifier {
      key "id";
      description
        "List of BFD profile identifiers.";
      leaf id {
        type string;
        description
          "Identification of the BFD profile to be used.  The
           profile only has significance within the service
           provider's administrative domain.";
      }
    }
    list forwarding-profile-identifier {
      key "id";
      description
        "List of forwarding profile identifiers.";
      leaf id {
        type string;
        description
          "Identification of the forwarding profile to be used.
           The profile only has significance within the service
           provider's administrative domain.";
      }
    }
    list routing-profile-identifier {
      key "id";
      description
        "List of routing profile identifiers.";
      leaf id {
        type string;
        description
          "Identification of the routing profile to be used by
           the routing protocols within sites, VPN network
           accesses, or VPN nodes for referring to VRF's
           import/export policies.

           The profile only has significance within the service
           provider's administrative domain.";
      }
    }
    nacm:default-deny-write;
  }
}

grouping oper-status-timestamp {
  description
    "This grouping defines some operational parameters for the
     service.";
  leaf status {
    type identityref {
      base operational-status;
    }
    config false;
    description
      "Operational status.";
  }
  leaf last-change {
    type yang:date-and-time;
    config false;
    description
      "Indicates the actual date and time of the service status
       change.";
  }
}

grouping service-status {
```

```
  description
    "Service status grouping.";
  container status {
    description
      "Service status.";
    container admin-status {
      description
        "Administrative service status.";
      leaf status {
        type identityref {
          base administrative-status;
        }
        description
          "Administrative service status.";
      }
      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 service status.";
      uses oper-status-timestamp;
    }
  }
}

grouping underlay-transport {
  description
    "This grouping defines the type of underlay transport for
     the VPN service or how that underlay is set.  It can
     include an identifier for an abstract transport instance to
     which the VPN is grafted or indicate a technical
     implementation that is expressed as an ordered list of
     protocols.";
  choice type {
    description
      "A choice based on the type of underlay transport
       constraints.";
    case abstract {
      description
        "Indicates that the transport constraint is an abstract
         concept.";
      leaf transport-instance-id {
        type string;
        description
          "An optional identifier of the abstract transport
           instance.";
      }
      leaf instance-type {
        type identityref {
          base transport-instance-type;
        }
        description
          "Indicates a transport instance type.  For example,
           it can be a VPN+, an IETF network slice, a virtual
           network, etc.";
      }
    }
    case protocol {
      description
        "Indicates a list of protocols.";
```

```
      leaf-list protocol {
        type identityref {
          base protocol-type;
        }
        ordered-by user;
        description
          "A client-ordered list of transport protocols.";
      }
    }
  }
}

grouping vpn-route-targets {
  description
    "A grouping that specifies Route Target (RT) import/export
     rules used in a BGP-enabled VPN.";
  reference
    "RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)
     RFC 4664: Framework for Layer 2 Virtual Private Networks
                (L2VPNs)";
  list vpn-target {
    key "id";
    description
      "RTs.  AND/OR operations may be defined based on the
       assigned RTs.";
    leaf id {
      type uint8;
      description
        "Identifies each VPN target.";
    }
    list route-targets {
      key "route-target";
      description
        "List of RTs.";
      leaf route-target {
        type rt-types:route-target;
        description
          "Conveys an RT value.";
      }
    }
    leaf route-target-type {
      type rt-types:route-target-type;
      mandatory true;
      description
        "Import/export type of the RT.";
    }
  }
  container vpn-policies {
    description
      "VPN service policies.  'vpn-policies' contains references
       to the import and export policies to be associated with
       the VPN service.";
    leaf import-policy {
      type string;
      description
        "Identifies the import policy.";
    }
    leaf export-policy {
      type string;
      description
        "Identifies the export policy.";
    }
  }
}

grouping route-distinguisher {
```

```
description
  "Grouping for Route Distinguishers (RDs).";
choice rd-choice {
  description
    "RD choice between several options for providing the RD
     value.";
  case directly-assigned {
    description
      "Explicitly assigns an RD value.";
    leaf rd {
      type rt-types:route-distinguisher;
      description
        "Indicates an RD value that is explicitly assigned.";
    }
  }
  case directly-assigned-suffix {
    description
      "The value of the Assigned Number subfield of the RD.
       The Administrator subfield of the RD will be
       based on other configuration information such as the
       Router ID or Autonomous System Number (ASN).";
    leaf rd-suffix {
      type uint16;
      description
        "Indicates the value of the Assigned Number
         subfield that is explicitly assigned.";
    }
  }
  case auto-assigned {
    description
      "The RD is auto-assigned.";
    container rd-auto {
      description
        "The RD is auto-assigned.";
      choice auto-mode {
        description
          "Indicates the auto-assignment mode.  The RD can be
           automatically assigned with or without
           indicating a pool from which the RD should be
           taken.

           For both cases, the server will auto-assign an RD
           value 'auto-assigned-rd' and use that value
           operationally.";
        case from-pool {
          leaf rd-pool-name {
            type string;
            description
              "The auto-assignment will be made from the pool
               identified by 'rd-pool-name'.";
          }
        }
        case full-auto {
          leaf auto {
            type empty;
            description
              "Indicates that an RD is fully auto-assigned.";
          }
        }
      }
      leaf auto-assigned-rd {
        type rt-types:route-distinguisher;
        config false;
        description
          "The value of the auto-assigned RD.";
      }
```

```
      }
    }
    case auto-assigned-suffix {
      description
        "The value of the Assigned Number subfield will be
         auto-assigned.  The Administrator subfield will be
         based on other configuration information such as the
         Router ID or ASN.";
      container rd-auto-suffix {
        description
          "The Assigned Number subfield is auto-assigned.";
        choice auto-mode {
          description
            "Indicates the auto-assignment mode of the
             Assigned Number subfield.  This number can be
             automatically assigned with or without indicating a
             pool from which the value should be taken.

             For both cases, the server will auto-assign
             'auto-assigned-rd-suffix' and use that value to
             build the RD that will be used operationally.";
          case from-pool {
            leaf rd-pool-name {
              type string;
              description
                "The assignment will be made from the pool
                 identified by 'rd-pool-name'.";
            }
          }
          case full-auto {
            leaf auto {
              type empty;
              description
                "Indicates that the Assigned Number subfield is
                 fully auto-assigned.";
            }
          }
        }
        leaf auto-assigned-rd-suffix {
          type uint16;
          config false;
          description
            "Includes the value of the Assigned Number subfield
             that is auto-assigned.";
        }
      }
    }
    case no-rd {
      description
        "Uses the 'empty' type to indicate that the RD has no
         value and is not to be auto-assigned.";
      leaf no-rd {
        type empty;
        description
          "No RD is assigned.";
      }
    }
  }
}

grouping vpn-components-group {
  description
    "Grouping definition to assign group IDs to associate
     VPN nodes, sites, or network accesses.";
  container groups {
    description
```

```
      "Lists the groups to which a VPN node, a site, or a
       network access belongs.";
    list group {
      key "group-id";
      description
        "List of group IDs.";
      leaf group-id {
        type string;
        description
          "The group ID to which a VPN node, a site, or a
           network access belongs.";
      }
    }
  }
}

grouping placement-constraints {
  description
    "Constraints related to placement of a network access.";
  list constraint {
    key "constraint-type";
    description
      "List of constraints.";
    leaf constraint-type {
      type identityref {
        base placement-diversity;
      }
      description
        "Diversity constraint type.";
    }
    container target {
      description
        "The constraint will apply against this list of
         groups.";
      choice target-flavor {
        description
          "Choice for the group definition.";
        case id {
          list group {
            key "group-id";
            description
              "List of groups.";
            leaf group-id {
              type string;
              description
                "The constraint will apply against this
                 particular group ID.";
            }
          }
        }
        case all-accesses {
          leaf all-other-accesses {
            type empty;
            description
              "The constraint will apply against all other
               network accesses of a site.";
          }
        }
        case all-groups {
          leaf all-other-groups {
            type empty;
            description
              "The constraint will apply against all other
               groups managed by the customer.";
          }
        }
```

```
      }
    }
  }
}

grouping ports {
  description
    "Choice of specifying source or destination port numbers.";
  choice source-port {
    description
      "Choice of specifying the source port or referring to a
       group of source port numbers.";
    container source-port-range-or-operator {
      description
        "Source port definition.";
      uses packet-fields:port-range-or-operator;
    }
  }
  choice destination-port {
    description
      "Choice of specifying a destination port or referring to a
       group of destination port numbers.";
    container destination-port-range-or-operator {
      description
        "Destination port definition.";
      uses packet-fields:port-range-or-operator;
    }
  }
}

grouping qos-classification-policy {
  description
    "Configuration of the traffic classification policy.";
  list rule {
    key "id";
    ordered-by user;
    description
      "List of marking rules.";
    leaf id {
      type string;
      description
        "An identifier of the QoS classification policy rule.";
    }
    choice match-type {
      default "match-flow";
      description
        "Choice for classification.";
      case match-flow {
        choice l3 {
          description
            "Either IPv4 or IPv6.";
          container ipv4 {
            description
              "Rule set that matches the IPv4 header.";
            uses packet-fields:acl-ip-header-fields;
            uses packet-fields:acl-ipv4-header-fields;
          }
          container ipv6 {
            description
              "Rule set that matches the IPv6 header.";
            uses packet-fields:acl-ip-header-fields;
            uses packet-fields:acl-ipv6-header-fields;
          }
        }
        choice l4 {
          description
```

```
                "Includes Layer-4-specific information.
                 This version focuses on TCP and UDP.";
              container tcp {
                description
                  "Rule set that matches the TCP header.";
                uses packet-fields:acl-tcp-header-fields;
                uses ports;
              }
              container udp {
                description
                  "Rule set that matches the UDP header.";
                uses packet-fields:acl-udp-header-fields;
                uses ports;
              }
            }
          }
          case match-application {
            leaf match-application {
              type identityref {
                base customer-application;
              }
              description
                "Defines the application to match.";
            }
          }
        }
        leaf target-class-id {
          type string;
          description
            "Identification of the class of service.  This
             identifier is internal to the administration.";
        }
      }
    }
  }
  <CODE ENDS>
```

5. 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.

The "ietf-vpn-common" module defines a set of identities, types, and groupings. These nodes are intended to be reused by other YANG modules. The module by itself does not expose any data nodes that are writable, data nodes that contain read-only state, or RPCs. As such, there are no additional security issues related to the "ietf-vpn-common" module that need to be considered.

Modules that use the groupings that are defined in this document should identify the corresponding security considerations. For example, reusing some of these groupings will expose privacy-related information (e.g., 'customer-name'). Disclosing such information may be considered a violation of the customer-provider trust relationship.

6. IANA Considerations

IANA has registered the following URI in the "ns" subregistry within the "IETF XML Registry" [RFC3688]:

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

IANA has registered the following YANG module in the "YANG Module Names" subregistry [RFC6020] within the "YANG Parameters" registry.

Name: ietf-vpn-common
Namespace: urn:ietf:params:xml:ns:yang:ietf-vpn-common
Maintained by IANA? N
Prefix: vpn-common
Reference: RFC 9181

7. References

7.1. Normative References

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

[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>.

[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>.

[RFC8294] Liu, X., Qu, Y., Lindem, A., Hopps, C., and L. Berger, "Common YANG Data Types for the Routing Area", RFC 8294, DOI 10.17487/RFC8294, December 2017, <https://www.rfc-editor.org/info/rfc8294>.

[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>.

[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>.

[RFC8519] Jethanandani, M., Agarwal, S., Huang, L., and D. Blair, "YANG Data Model for Network Access Control Lists (ACLs)", RFC 8519, DOI 10.17487/RFC8519, March 2019, <https://www.rfc-editor.org/info/rfc8519>.

7.2. Informative References

[ACTN-VN-YANG]
Lee, Y., Ed., Dhody, D., Ed., Ceccarelli, D., Bryskin, I., and B. Yoon, "A YANG Data Model for VN Operation", Work in Progress, Internet-Draft, draft-ietf-teas-actn-vn-yang-13, 23 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-actn-vn-yang-13>.

[Enhanced-VPN-Framework]
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-09, 25 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-enhanced-vpn-09>.

[IEEE802.1ad]
IEEE, "IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks---Amendment 4: Provider Bridges", <https://standards.ieee.org/standard/802_1ad-2005.html>.

[IEEE802.1AX]
IEEE, "IEEE Standard for Local and Metropolitan Area Networks--Link Aggregation", <https://standards.ieee.org/standard/802_1AX-2020.html>.

[IEEE802.1Q]
IEEE, "IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks", <https://standards.ieee.org/standard/802_1Q-2018.html>.

[ISO10589] ISO, "Information technology - Telecommunications and information exchange between systems - Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)", International Standard 10589:2002, Second Edition, November 2002, <https://www.iso.org/standard/30932.html>.

[L2NM-YANG]
Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., and L. Munoz, "A Layer 2 VPN Network YANG Model", Work in Progress, Internet-Draft, draft-ietf-opsawg-l2nm-12, 22 November 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-l2nm-12>.

[Network-Slices-Framework]
Farrel, A., Ed., Gray, E., Drake, J., Rokui, R., Homma, S., Makhijani, K., Contreras, LM., and J. Tantsura, "Framework for IETF Network Slices", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-05, 25 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-05>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, DOI 10.17487/RFC1112, August 1989, <https://www.rfc-editor.org/info/rfc1112>.

[RFC1701] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, DOI 10.17487/RFC1701, October 1994, <https://www.rfc-editor.org/info/rfc1701>.

[RFC1702] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation over IPv4 networks", RFC 1702, DOI 10.17487/RFC1702, October 1994, <https://www.rfc-editor.org/info/rfc1702>.

[RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, DOI 10.17487/RFC2003, October 1996, <https://www.rfc-editor.org/info/rfc2003>.

[RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, DOI 10.17487/RFC2080, January 1997, <https://www.rfc-editor.org/info/rfc2080>.

[RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, DOI 10.17487/RFC2236, November 1997, <https://www.rfc-editor.org/info/rfc2236>.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, DOI 10.17487/RFC2453, November 1998, <https://www.rfc-editor.org/info/rfc2453>.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, DOI 10.17487/RFC2473, December 1998, <https://www.rfc-editor.org/info/rfc2473>.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999, <https://www.rfc-editor.org/info/rfc2710>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, DOI 10.17487/RFC3376, October 2002, <https://www.rfc-editor.org/info/rfc3376>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed., "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, DOI 10.17487/RFC3931, March 2005, <https://www.rfc-editor.org/info/rfc3931>.

[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>.

[RFC4176] El Mghazli, Y., Ed., Nadeau, T., Boucadair, M., Chan, K., and A. Gonguet, "Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management", RFC 4176, DOI 10.17487/RFC4176, October 2005, <https://www.rfc-editor.org/info/rfc4176>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC4577] Rosen, E., Psenak, P., and P. Pillay-Esnault, "OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4577, DOI 10.17487/RFC4577, June 2006, <https://www.rfc-editor.org/info/rfc4577>.

[RFC4664] Andersson, L., Ed. and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, DOI 10.17487/RFC4664, September 2006, <https://www.rfc-editor.org/info/rfc4664>.

[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>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <https://www.rfc-editor.org/info/rfc4960>.

[RFC5036] Andersson, L., Ed., Minei, I., Ed., and B. Thomas, Ed., "LDP Specification", RFC 5036, DOI 10.17487/RFC5036, October 2007, <https://www.rfc-editor.org/info/rfc5036>.

[RFC5798] Nadas, S., Ed., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 5798, DOI 10.17487/RFC5798, March 2010, <https://www.rfc-editor.org/info/rfc5798>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC6513] Rosen, E., Ed. and R. Aggarwal, Ed., "Multicast in MPLS/ BGP IP VPNs", RFC 6513, DOI 10.17487/RFC6513, February 2012, <https://www.rfc-editor.org/info/rfc6513>.

[RFC6565] Pillay-Esnault, P., Moyer, P., Doyle, J., Ertekin, E., and M. Lundberg, "OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol", RFC 6565, DOI 10.17487/RFC6565, June 2012, <https://www.rfc-editor.org/info/rfc6565>.

[RFC6624] Kompella, K., Kothari, B., and R. Cherukuri, "Layer 2 Virtual Private Networks Using BGP for Auto-Discovery and Signaling", RFC 6624, DOI 10.17487/RFC6624, May 2012, <https://www.rfc-editor.org/info/rfc6624>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual

eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/info/rfc7348>.

[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>.

[RFC7510] Xu, X., Sheth, N., Yong, L., Callon, R., and D. Black, "Encapsulating MPLS in UDP", RFC 7510, DOI 10.17487/RFC7510, April 2015, <https://www.rfc-editor.org/info/rfc7510>.

[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>.

[RFC7676] Pignataro, C., Bonica, R., and S. Krishnan, "IPv6 Support for Generic Routing Encapsulation (GRE)", RFC 7676, DOI 10.17487/RFC7676, October 2015, <https://www.rfc-editor.org/info/rfc7676>.

[RFC7761] Fenner, B., Handley, M., Holbrook, H., Kouvelas, I., Parekh, R., Zhang, Z., and L. Zheng, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", STD 83, RFC 7761, DOI 10.17487/RFC7761, March 2016, <https://www.rfc-editor.org/info/rfc7761>.

[RFC7880] Pignataro, C., Ward, D., Akiya, N., Bhatia, M., and S. Pallagatti, "Seamless Bidirectional Forwarding Detection (S-BFD)", RFC 7880, DOI 10.17487/RFC7880, July 2016, <https://www.rfc-editor.org/info/rfc7880>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[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>.

[RFC8277] Rosen, E., "Using BGP to Bind MPLS Labels to Address Prefixes", RFC 8277, DOI 10.17487/RFC8277, October 2017, <https://www.rfc-editor.org/info/rfc8277>.

[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>.

[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>.

[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>.

[RFC8512] Boucadair, M., Ed., Sivakumar, S., Jacquenet, C., Vinapamula, S., and Q. Wu, "A YANG Module for Network Address Translation (NAT) and Network Prefix Translation (NPT)", RFC 8512, DOI 10.17487/RFC8512, January 2019, <https://www.rfc-editor.org/info/rfc8512>.

[RFC8660] Bashandy, A., Ed., Filsfils, C., Ed., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing with the MPLS Data Plane", RFC 8660, DOI 10.17487/RFC8660, December 2019, <https://www.rfc-editor.org/info/rfc8660>.

[RFC8663] Xu, X., Bryant, S., Farrel, A., Hassan, S., Henderickx, W., and Z. Li, "MPLS Segment Routing over IP", RFC 8663, DOI 10.17487/RFC8663, December 2019, <https://www.rfc-editor.org/info/rfc8663>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

[RFC8926] Gross, J., Ed., Ganga, I., Ed., and T. Sridhar, Ed., "Geneve: Generic Network Virtualization Encapsulation", RFC 8926, DOI 10.17487/RFC8926, November 2020, <https://www.rfc-editor.org/info/rfc8926>.

[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>.

Appendix A. Example of Common Data Nodes in Early L2NM/L3NM Designs

In order to avoid duplication of data nodes and to ease passing data among layers (i.e., from the service layer to the network layer and vice versa), early versions of the L3NM reused many of the data nodes that are defined in the L3SM. Nevertheless, that approach was abandoned because that design was interpreted as if the deployment of the L3NM depends on the L3SM, while this is not required. For example, a service provider may decide to use the L3NM to build its L3VPN services without exposing the L3SM to customers.

Likewise, early versions of the L2NM reused many of the data nodes that are defined in both the L2SM and the L3NM. An example of L3NM groupings reused in the L2NM is shown in Figure 5. Such reuse of data nodes was interpreted as if the deployment of the L2NM requires support for the L3NM, which is not required.

```
module ietf-l2vpn-ntw {
 ...
  import ietf-l3vpn-ntw {
    prefix l3vpn-ntw;
    reference
      "RFC 9182: A YANG Network Data Model for Layer 3 VPNs";
  }
  ...
```

```
    container l2vpn-ntw {
      ...
      container vpn-services {
        list vpn-service {
          ...
          uses l3vpn-ntw:service-status;
          uses l3vpn-ntw:svc-transport-encapsulation;
          ...
        }
      }
      ...
    }
  }
```

Figure 5: Excerpt from the L2NM YANG Module

Acknowledgements

During the discussions of this work, helpful comments and reviews were received from (listed alphabetically) Alejandro Aguado, Raul Arco, Miguel Cros Cecilia, Joe Clarke, Dhruv Dhody, Adrian Farrel, Roque Gagliano, Christian Jacquenet, Kireeti Kompella, Julian Lucek, Tom Petch, Erez Segev, and Paul Sherratt. Many thanks to them.

This work is partially supported by the European Commission under Horizon 2020 Secured autonomic traffic management for a Tera of SDN flows (Teraflow) project (grant agreement number 101015857).

Many thanks to Radek Krejci for the YANG Doctors review, Wesley Eddy for the tsvart review, Ron Bonica and Victoria Pritchard for the RtgDir review, Joel Halpern for the genart review, Tim Wicinski for the opsdir review, and Suresh Krishnan for the intdir review.

Special thanks to Robert Wilton for the AD review.

Thanks to Roman Danyliw, Lars Eggert, Warren Kumari, Erik Kline, Zaheduzzaman Sarker, Benjamin Kaduk, and ric Vyncke for the IESG review.

Contributors

Italo Busi
Huawei Technologies

Email: Italo.Busi@huawei.com

Luis Angel Munoz
Vodafone

Email: luis-angel.munoz@vodafone.com

Victor Lopez
Nokia
Madrid
Spain

Email: victor.lopez@nokia.com

Authors’ Addresses

Samier Barguil
Telefonica
Madrid

Spain

Email: samier.barguilgiraldo.ext@telefonica.com

Oscar Gonzalez de Dios (editor)
Telefonica
Madrid
Spain

Email: oscar.gonzalezdedios@telefonica.com

Mohamed Boucadair (editor)
Orange
France

Email: mohamed.boucadair@orange.com

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

Email: bill.wu@huawei.com