Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 26 August 2026

K. Lambrechts
NetEdge

22 February 2026

An Extensible Architecture for Service Modeling
draft-lambrechts-onsen-svc-yang-00

Abstract

This document describes problems with the currently published IETF service modules and defines a modular service modeling structure that extracts technology-agnostic constructs into a base ietf-svc module, separates Ethernet-specific treatment into ietf-eth-svc, and layers VPN-oriented intent in ietf-vpn-svc, with bis versions of the L2SM and L3SM augmenting the shared foundation.

Status of This Memo

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

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

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

This Internet-Draft will expire on 26 August 2026.

Table of Contents

1. Introduction

The Layer 2 VPN Service Model (L2SM) [RFC8466] and Layer 3 VPN Service Model (L3SM) [RFC8299] YANG models provide a standardized approach to modeling L2VPN and L3VPN services. However, these models do not interact with each other, and are not designed to be extensible so that additional services can be added.

This document describes a new, extensible architecture for services modules and defines a YANG module that can be used as the base for any customer service. The goals of this work are to reduce duplication between existing L2SM and L3SM work, enable new service types to reuse common abstractions, and let operators expose a consistent customer-facing interface while retaining flexibility for technology-specific extensions.

2. Limitations of the Current Service Models

The following sections describe problems with the approach taken by the current L2SM and L3SM modules.

2.1. High Levels of Duplication between the Service Models

The L2SM and L3SM individually cover all the inputs to deliver either L2VPN or L3VPN services, including an abstracted view of the customer's site locations. This means that an operator that offers both types of services must manage two separate models with a large amount of duplicated information.

When additional service models are defined for new service types, the current approach requires further duplication, making the problem worse.

2.2. Limited Interoperability between Service Models

It is impossible to express certain relationships between the L2VPN and L3VPN services being ordered, such as diversity or bandwidth constraints. This is especially important in deployment scenarios where common infrastructure hardware is used for providing both L2VPN and L3VPN services.

2.3. Missing Support for Network Technology Layering

The current L2SM and L3SM models do not have a way to express the relationships between the different technology layers that are used to provision the overall service. For example, an operator may want to specify that an L3VPN service should be delivered over a specific underlying L2VPN service, or that an SD-WAN service should be delivered over a specific Internet access service. The lack of support for network layering makes it difficult to model and manage complex service offerings that involve multiple layers of abstraction and different technologies.

2.4. Complexity in Creating a Single View of Services

Currently, the L2SM and L3SM do not contain operational state. If these modules are extended with state nodes, e.g., so it is possible to retrieve information about the current health of a customer’s services, the separation of L2SM, L3SM, and other service models makes correlating the service impact of underlying failures affecting more than one service type more difficult.

3. Proposed Solution

This document revisits the existing L2SM and L3SM models, introducing a new structure with a common base model. This removes the duplication between service models, and enables much simpler interworking between different service types. It also forms an extensible basis for the definition of new service models in the future.

The core of the module structure is defined in ietf-svc. This provides a technology-agnostic service skeleton covering sites, site-network-accesses, diversity constraints, and bearer references. Additionally, Ethernet-centric constructs such as bandwidth profiles and QoS classification are moved into a dedicated ietf-eth-svc module so that Ethernet-based services can share the same primitives without cluttering the core service skeleton.

The ietf-vpn-svc module builds on this core and defines VPN-oriented attributes such as service type, topology, cloud, and extranet reachability, carriers' carrier, and policy filters.

Finally, the technology specific parameters for L2VPN and L3VPN services are augmented into the shared service framework. The L3VPN module retains the routing, multicast, address-allocation, NAT, and BFD constructs from [RFC8299]. The L2VPN module retains the Ethernet- and OAM-specific behaviors from [RFC8466] (e.g., bundling, CE-VLAN preservation, L2CP handling, CFM, and Y.1731) while leveraging the shared service skeleton, the Ethernet treatment constructs in ietf-eth-svc, and the VPN service identities from ietf-vpn-svc.

The augment relationships across the modules are shown in Figure 1.

```
module: ietf-svc                      (Base service skeleton)
  +-- augment: ietf-eth-svc           (Ethernet attributes, e.g QoS)
    +-- augment: ietf-vpn-svc         (VPN service common attributes)
      +-- augment: ietf-l2vpn-svc     (L2VPN-specific attributes)
      +-- augment: ietf-l3vpn-svc     (L3VPN-specific attributes)
```

Figure 1: Service module augmentation relationships

By aligning the L2SM and L3SM models on a common foundation, this work reduces duplication, improves consistency of service exposure to customers and OSS/BSS systems, and simplifies the introduction of future service types that can reuse the same base abstractions. Examples of new services that could be modeled on top of the same base include (business) internet access, cloud interconnect, or even optical wavelength services.

4. Relationships to Other Work

The Layer 2 VPN Network Model (L2NM) [RFC9291] and Layer 3 VPN Network Model (L3NM) [RFC9182] may benefit from being re-built on top of a similarly abstracted foundation, but they are outside the scope of this document.

Adoption of the Common YANG Data Model for Layer 2 and Layer 3 VPNs [RFC9181] at the service model level may be beneficial and should be considered as part of this work.

5. IANA Considerations

This memo includes no request to IANA.

6. Security Considerations

The security posture of this document follows the guidance in the L3SM [RFC8299]. The NETCONF Access Control Model (NACM) [RFC8341] should be used to restrict protocol operations and data nodes to authorized principals.

New augments added to the base service skeleton must describe any additional security-sensitive leaves and specify suitable NACM rules. When encryption or authentication material is conveyed (e.g., keys or credentials), operators must ensure secure transport and operational processes (rotation, revocation, audit) consistent with their policy.

7. References

7.1. Normative References

[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>.

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

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

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

[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>.

[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>.

Author’s Address

Kris Lambrechts
NetEdge
Email: kris@netedge.plus
URI: https://www.netedge.plus