Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 27, 2020

Z. Li
Huawei Technologies

July 26, 2019

# Cross-Area Work in the IETF
# draft-li-cross-area-ietf-work-00

## Abstract

This document investigates the benefits of cross-area work in the IETF. It is examines existing cross-area work and identifies other possibilities for work that spans more than one area. The intention is to help community members who focus their work within a specific area to understand related work in other areas and to motivate efficient cooperation across different areas in the IETF.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

## 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 January 27, 2020.

## Copyright Notice

Table of Contents



## 1. Introduction

With the development of new network technologies such as cloud computing, 5G, IoT, etc., very many applications are carried over the network. Each has different needs for network bandwidth, latency, jitter, and packet loss, etc.

Work in the IETF is divided into Areas. The demands of the new technologies motivates innovation and new architectures in multiple network layers, and resulting cross-area work is increasing in the IETF. Existing protocol practice shows that people who focus on one specific area are sometimes not aware of related work in different areas. Some cross-area work is not recognized until late in the lifecycle so that useful experiences cannot be shared early in the development. Fixing problems that are identified late can become time consuming.

This document investigates the benefits of cross-area work in the IETF. It is examines existing cross-area work and identifies other possibilities for work that spans more than one area. The intention

is to help community members who focus their work within a specific area to understand related work in other areas and to motivate efficient cooperation across different areas in the IETF.

## 2. Terminology

SRv6: Segment Routing over IPv6

MPLS: Multi-Protocol Label Switch

## 3. SRv6

Segment Routing is an important networking technology developed in the IETF. SRv6 is the Segment Routing deployed on the IPv6 data plane[RFC8200] and SRv6 network programming [I-D.ietf-spring-srv6-network-programming] is introduced to support multiple services which have requirements on the SRv6 network. The related areas and Working Groups for SRv6 are shown in Figure 1: the work can be categorized into Basics, Encapsulations, Protocols, YANG, Use cases, and Others.

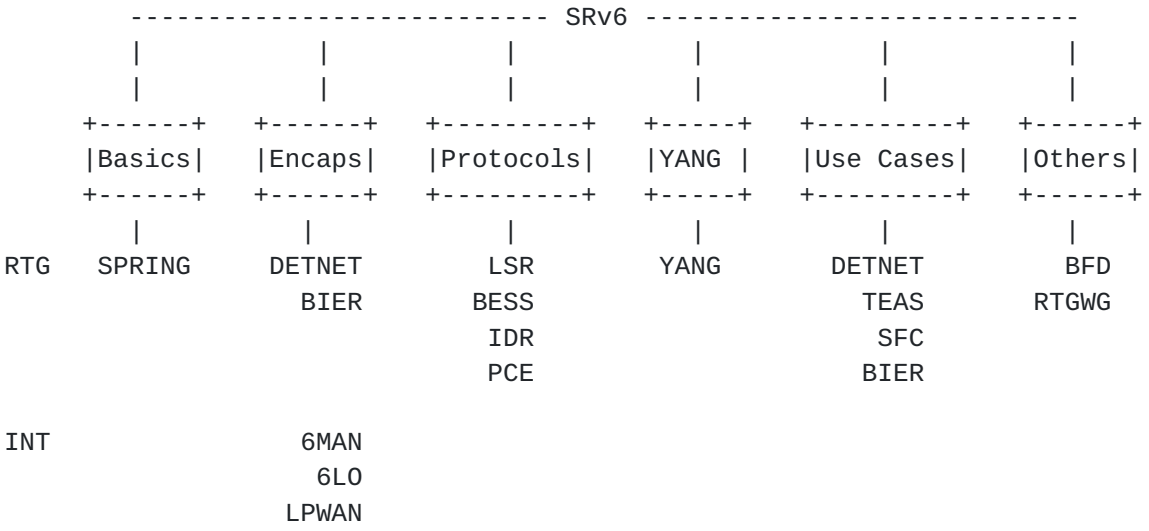


Figure 1: Related Areas/WGs for SRv6

The major IETF areas for SRv6 work are the RTG area and the INT area. There is work in multiple working groups in the RTG area, and the major work in the INT area includes the new IPv6 encapsulation and the possible compression work on the IPv6 header.

## 4. YANG Models

Data models written in the YANG modelling language [RFC6020] can be used for service and network management to provide a programmatic approach for representing (virtual) services or networks and for deriving configuration information that will be forwarded to network and service components that are used to build and deliver the service.

YANG module developers have taken both top-down and bottom-up approaches to develop modules [RFC8199] and to establish a mapping between network technology and customer requirements on the top or abstracting common construct from various network technologies on the bottom. There are many data models including configuration and service models that have been specified or are being specified by the IETF. They cover many of the networking protocols and techniques.

Figure 2 is from [I-D.wu-model-driven-management-virtualization] provides and provides an overview of various macro-functional blocks at different levels that articulate the various YANG data modules. In this figure, example models developed in the IETF are layered as Network Service Models, Network Resource Models, and Network Element Models. The Network Element Models are further layered into Composition Models and Function Models.

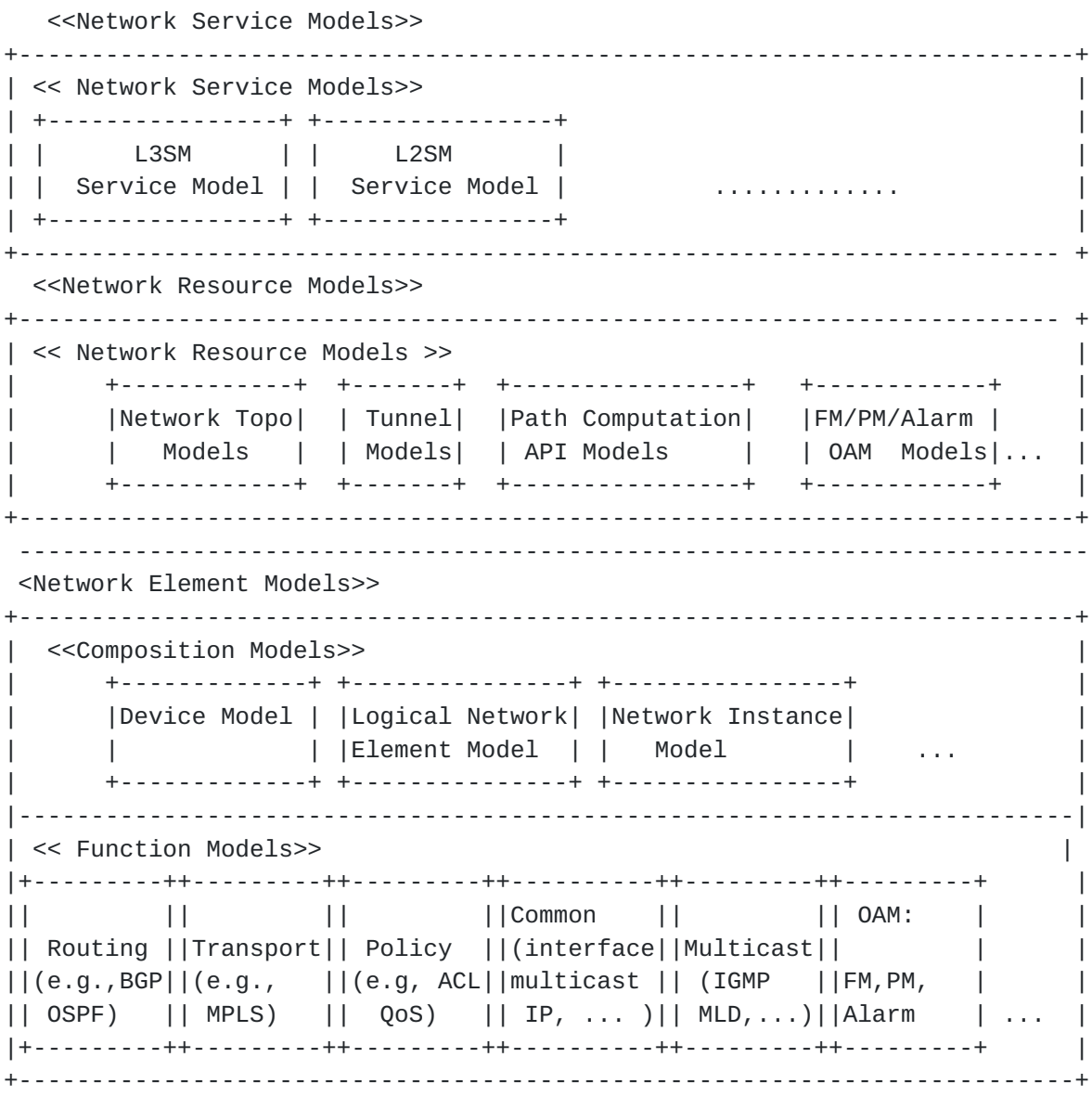


Figure 2: An overview of Layered YANG Modules

A Network Service Model [RFC8309] is a kind of high level data model. It describes a service and the parameters of the service in a portable way that can be used uniformly and independent of the equipment and operating environment. In the OPS area, the Layer Three Virtual Private Network Service Model (L3SM) [RFC8299] and the Layer Two Virtual Private Network Service Model (L2SM) [RFC8466] define L3VPN and L2VPN services that can be ordered by a customer from a network operator. In the RTG area, the Virtual Network (VN) model[I-D.ietf-teas-actn-vn-yang] provides a YANG data model generally applicable to any mode of VN operation.

The category of Network Resource Models includes topology modules and tunnel modules worked on in the RTG area, as well as the resource management tool models worked in both the RTG and OPS areas.

A Network Element model is used to describe how a service can be implemented by activating and tweaking a set of functions (enabled in one or multiple devices, or hosted in cloud infrastructures) that are involved in the delivery of the service. This includes various models for individual protocols specified in the RTG, OPS, TSV, and INT areas.

## 5. Network Intelligence/Telemetry

It is conceivable that an intent-driven autonomic network [RFC7575] is the logical next step for network evolution following Software Defined Network (SDN). This approach aims to reduce (or even eliminate) human labor, make the most efficient usage of network resources, and provide better services more aligned with customer requirements. Although it takes time to reach the ultimate goal, the journey has started nevertheless.

Network Intelligence and Telemetry are the cornerstone for the intent-driven autonomic network.

### 5.1. Network Telemetry

Network telemetry has emerged as a mainstream technical term to refer to the newer data collection and consumption techniques, distinguishing itself from the conventional techniques for network OAM. Network Telemetry acquires network data remotely for network monitoring and operation. It addresses the current network operation issues and enables smooth evolution toward intent-driven autonomous networks.

The Network Telemetry Framework [I-D.ietf-opsawg-ntf] provides a layered categorization for the telemetry technologies developed in the IETF across areas including OPS, TSV (IPPM working group), RTG (MPLS and NVO3 working groups), and INT (6MAN working group). The categorization is shown in Figure 3.

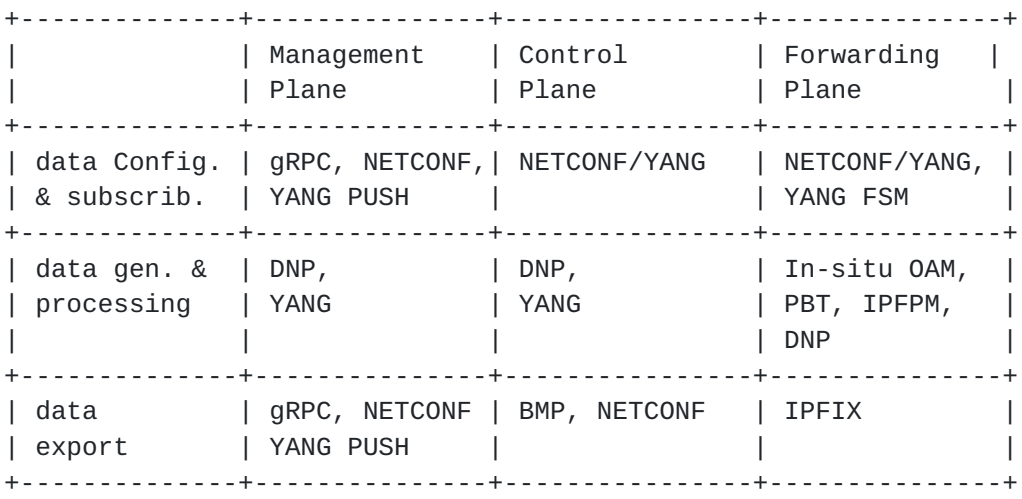


Figure 3: Layer Category of Network Telemetry Framework

The categories shown in Figure 3 are as follows:

- Management Plane Telemetry: This refers to work on the push extensions for NETCONF [I-D.ietf-netconf-yang-push]. This work is on-going in the NETCONF working group in the OPS area.

- Control Plane Telemetry: BGP is a very important protocol in the control plane. The GROW working group in the OPS area is developing the BGP Monitoring Protocol (BMP) [RFC7854] to monitor BGP sessions and to provide a convenient interface for obtaining route views.

- Data Plane Telemetry: In-situ Flow Information Telemetry (IFIT) [I-D.song-opsawg-ifit-framework] is a new proposal that enumerates several key components and describes how they could be assembled to achieve a complete solution for on-path user traffic telemetry in carrier networks. It includes two major modes that are described in further documents: Postcard mode in [I-D.song-ippm-postcard-based-telemetry] and Passport mode in [I-D.ietf-ippm-ioam-data].
[I-D.zhou-ippm-enhanced-alternate-marking] proposes a lightweight way to achieve most measurement requirements. In general, the basic mechanism is discussed in the IPPM working group in the TSV area, and specific encapsulations are discussed in the working groups dedicated to the associated protocols including the 6MAN working group in the INT area for IPv6 and SRv6, and the MPLS and NVO3 working groups in the RTG area for MPLS and VXLAN.

### 5.2. Network Intelligence

Thanks to advances in computing and storage technologies, today's big data analytics gives network operators an unprecedented opportunity to gain network insights and move toward network autonomy. Some operators have started to explore the application of Artificial Intelligence (AI) to make sense of network data. Software tools can use the network data to detect and react to network faults, anomalies, and policy violations, as well as to predict future events. In turn, the network policy can be updated for planning, intrusion prevention, optimization, and self-healing.

This topic is relatively new and requires a central place for discussion. The IRTF's Network Management Research Group (NMRG) recently discussed Network Intent [I-D.li-nmrg-intent-classification] while [I-D.kim-nmrg-rl] presents intelligent network management scenarios based on reinforcement-learning approaches.

## 6. 5G Transport

As work on the requirements, architecture, and protocols to support 5G progress, cross-area work is gaining momentum to address major requirements for transport systems to underlie 5G. This includes work on network slicing, deterministic latency/low latency, etc.

1. Network Slicing

Transport network slicing involves work in the IETF RTG area and the INT area. In the TEAS working group in the RTG area, [I-D.ietf-teas-enhanced-vpn] specifies a framework for using existing, modified, and potentially new networking technologies as components to provide Enhanced Virtual Private Network (VPN+) services to satisfy the network slicing requirement. SR is an important transport technologies for network slicing and the SPRING working group is also involved.

The DMM WG in the INT area focuses on the mobility work involved in supporting end-to-end network slicing. When considering RAN slicing and Mobile Core slicing, other SDOs (such as 3GPP and the BBF) are also ntvolved, interacting with each other and with the IETF via liasions.

2. Deterministic latency/Low latency

The main relevant WG is Detnet which belongs to the RTG area. The technologies developed in the TSV area and the ART area can also provide the latency service.

## 7. Cross-layer Work

Layering is an important network design principle. Cross-layer work often gives rise to cross-area work.

As ideas around network services are progressing cross-layer work is as an important research are such as path-aware networking in the IRTF's Path Aware Networking Research Group (PANRG), and application-aware IPv6 networking proposed by [I-D.li-6man-app-aware-ipv6-network].

### 7.1. Path-Aware Networking

Work on the path-aware network is being done in the PANRG. The Internet architecture assumes a division between the end-to-end functionality of the transport layer and the properties of the path between endpoints. Increased diversity in access networks, and ubiquitous mobile connectivity, have made this architecture's assumptions about paths less tenable. Multipath protocols taking advantage of this mobile connectivity begin to show us a way forward: if endpoints cannot control the path, at least they can determine the properties of the path by choosing among paths available to them. The PANRG aims to support research in bringing path awareness to transport and application layer protocols, and to bring research in this space to the attention of the Internet engineering and protocol design community.

The group's scope overlaps with existing IETF and IRTF efforts (and also with some past efforts). Of the existing overlaps, the group collaborates with working groups and research groups chartered to work on multipath transport protocols (MPTCP, QUIC, TSVWG), congestion control in multiply-connected environments (ICCRG), and alternate routing architectures (e.g., PCE and LISP). The charter is also related to the questions discussed in a number of past BoF sessions, e.g. SPUD, PLUS, and BANANA.

### 7.2. Application-aware IPv6 Networking

[I-D.li-6man-app-aware-ipv6-network] proposes possible work on application-aware IPv6 networking (APN6). As the Internet continues to develop, the decoupling of applications from network transport causes the operation actions on service provider networks to be pipelined which becomes the bottleneck of network service deployment. Moreover, a multitude of applications with varying needs for network bandwidth, latency, jitter, and packet loss are being carried over the IP network. However it is hard for the network to learn the applications' service requirements which make it difficult for an operator to provide truly fine-grain traffic operations for the

applications and to guarantee their SLA requirements. APN6 aims to make use of an IPv6 extensions header to convey the application related information including its requirements along with the packet to tell the network how to adjust the network resources to facilitate the deployment of services.

The scope of the work overlaps with existing IETF and IRTF efforts including, but not limited to, multiple working groups in RTG area, the 6MAN working group in the INT area, and the IRTF's ICNRG and PANRG.

## 8. IANA Considerations

This document makes no request of IANA.

## 9. Security Considerations

Security is a fundamental part of all work done at the IETF. At the least this requires security considerations to be part of every RFC published, and attention should also be given to privacy requirements. This work is usually supported by reviews from security experts on the Security Directorate and is a good example of cross-area work. Furthermore, when major new technologies are being developed within the IETF it is possible to ask for security advisors to be appointed for working groups. And from time to time, new work needs to be spun up in the SEC area to support demands from new protocols.

## 10. References

### 10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

### 10.2. Informative References

[I-D.ietf-ippm-ioam-data] Brockners, F., Bhandari, S., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mizrahi, T., Mozes, D., Lapukhov, P., Chang, R., daniel.bernier@bell.ca, d., and J. Lemon, "Data Fields for In-situ OAM", draft-ietf-ippm-ioam-data-06 (work in progress), July 2019.

[I-D.ietf-netconf-yang-push]
Clemm, A. and E. Voit, "Subscription to YANG Datastores", draft-ietf-netconf-yang-push-25 (work in progress), May 2019.

[I-D.ietf-opsawg-ntf]
Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", draft-ietf-opsawg-ntf-01 (work in progress), June 2019.

[I-D.ietf-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J., daniel.voyer@bell.ca, d., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-01 (work in progress), July 2019.

[I-D.ietf-teas-actn-vn-yang]
Lee, Y., Dhody, D., Ceccarelli, D., Bryskin, I., and B. Yoon, "A Yang Data Model for VN Operation", draft-ietf-teas-actn-vn-yang-06 (work in progress), July 2019.

[I-D.ietf-teas-enhanced-vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Networks (VPN+) Service", draft-ietf-teas-enhanced-vpn-02 (work in progress), July 2019.

[I-D.kim-nmrg-rl]
Kim, M., Han, Y., and Y. Hong, "Intelligent Reinforcement-learning-based Network Management", draft-kim-nmrg-rl-05 (work in progress), July 2019.

[I-D.li-6man-app-aware-ipv6-network]
Li, Z., Peng, S., Xie, C., and L. Cong, "Application-aware IPv6 Networking", draft-li-6man-app-aware-ipv6-network-00 (work in progress), July 2019.

[I-D.li-nmrg-intent-classification]
Li, C., Cheng, Y., Strassner, J., Havel, O., LIU, W., Martinez-Julia, P., Nobre, J., and D. Lopez, "Intent Classification", draft-li-nmrg-intent-classification-01 (work in progress), July 2019.

[I-D.song-ippm-postcard-based-telemetry]
Song, H., Zhou, T., Li, Z., Shin, J., and K. Lee, "Postcard-based On-Path Flow Data Telemetry", draft-song-ippm-postcard-based-telemetry-04 (work in progress), June 2019.

[I-D.song-opsawg-ifit-framework]
Song, H., Li, Z., Zhou, T., Qin, F., Shin, J., and J. Jin, "In-situ Flow Information Telemetry Framework", draft-song-opsawg-ifit-framework-03 (work in progress), July 2019.

[I-D.wu-model-driven-management-virtualization]
Wu, Q., Boucadair, M., Jacquenet, C., Contreras, L., Lopez, D., Xie, C., Cheng, W., and Y. Lee, "A Framework for Automating Service and Network Management with YANG", draft-wu-model-driven-management-virtualization-05 (work in progress), July 2019.

[I-D.zhou-ippm-enhanced-alternate-marking]
Zhou, T., Fioccola, G., Li, Z., Lee, S., Cociglio, M., and Z. Li, "Enhanced Alternate Marking Method", draft-zhou-ippm-enhanced-alternate-marking-03 (work in progress), July 2019.

[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>.

[RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", RFC 7575, DOI 10.17487/RFC7575, June 2015, <https://www.rfc-editor.org/info/rfc7575>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/info/rfc7854>.

[RFC8199] Bogdanovic, D., Claise, B., and C. Moberg, "YANG Module Classification", RFC 8199, DOI 10.17487/RFC8199, July 2017, <https://www.rfc-editor.org/info/rfc8199>.

[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>.

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

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

[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

Zhenbin Li
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: lizhenbin@huawei.com