Networking Working Group
Internet-Draft
Intended status: Informational
Expires: January 4, 2020

Q. Wu
Huawei
M. Boucadair
C. Jacquenet
Orange
L. Miguel Contreras Murillo
Telifonica
D. Lopez
Telefonica I+D
C. Xie
China Telecom
W. Cheng
China Mobile
Y. Lee
Futurewei

July 3, 2019

A Framework for Automating Service and Network Management with YANG
draft-wu-model-driven-management-virtualization-05

Abstract

Data models for service and network management provides a programmatic approach for representing (virtual) services or networks and deriving configuration information that will be forwarded to network and service components that are used to build and deliver the service. Data Models can be used during various phases of the service and network management life cycle, such as service instantiation, service provisioning, optimization, monitoring, and diagnostic. Also, data models are are instrumental in the automation of network management. They also provide closed-loop control for the sake of adaptive and deterministic service creation, delivery, and maintenance.

This document provides a framework that describes and discusses an architecture for service and network management automation that takes advantage of YANG modeling technologies. This framework is drawn from a network provider perspective irrespective of the origin of a data module andcan accommodate even modules that are developed outside the IETF.

The document aims to exemplify an approach that specifies the journey from technology-agnostic services to technology-specific actions.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 3
  1.1. Terminology 5
2. Layered YANG Modules: An Overview 6
  2.1. Network Service and Resource Models 6
    2.1.1. Network Service Models: Definition and Samples . . . 7
    2.1.2. Network Resource Models: Definitions and Samples . . 7
  2.2. Network Element Models: Definitions and Samples 10
    2.2.1. Model Composition 11
    2.2.2. Protocol/Function Configuration Models: Definitions and Samples 12
3. Architectural Concepts 15
  3.1. Data Models: Layering and Representation 15
  3.2. Automation of service delivery procedures 15
  3.3. Service Fullfillment Automation 16

3.4. Module Decomposition and Composition 16
4. Architecture Overview 17
4.1. End-to-End Service Delivery and Service Assurance Procedure 18
4.1.1. Resource Collection and Abstraction (a) 18
4.1.2. Service Exposure & Abstraction (b) 18
4.1.3. IP Service Mapping (c) 19
4.1.4. IP Service Composition (d) 19
4.1.5. IP Service Provision (e) 20
4.1.6. Performance Measurement and Alarm Telemetry (g) . . . 20
4.1.7. IP Service to TE Mapping (f) 20
4.1.8. Path Management (h) 21
4.1.9. TE Resource Exposure (i) 21
5. Sample Service Coordination via YANG Moodules 22
5.1. L3VPN Service Delivery via Coordinated YANG Modules . . . 22
5.2. 5G Transport Service Delivery via Coordinated YANG Modules 22
6. Modules Usage in Automated Virtualized Network Environment: Sample Examples 24
6.1. Network-initiated Resource Creation 24
6.2. Customer-initiated Dynamic Resource Creation 25
7. Security Considerations 27
8. IANA Considerations 27
9. Contributors 28
10. Acknowledgements 28
11. Informative References 28
Authors' Addresses 36

1. Introduction

The service management system usually comprises service activation/provision and service operation. Current service delivery procedures, from the processing of customer's requirements and order to service delivery and operation, typically assume the manipulation of data sequentially into multiple OSS/BSS applications that may be managed by different departments within the service provider's organization (e.g., billing factory, design factory, network operation center, etc.). In addition, many of these applications have been developed in-house over the years and operating in a silo mode. The lack of standard data input/output (i.e., data model) also raises many challenges in system integration and often results in manual configuration tasks. Secondly, many current service fulfillment might not support real time streaming telemetry capability in high frequency and in high throughput on the current state of networking and therefore have slow response to the network changes. Software Defined Networking (SDN) becomes crucial to address these challenges.

Software-Defined Networking techniques [RFC7149] are meant to automate the overall service delivery procedures and typically rely upon (standard) data models that are used to not only reflect service providers'savoir-faire but also to dynamically instantiate and enforce a set of (service-inferred) policies that best accommodate what has been (contractually) defined (and possibly negotiated) with the customer. [RFC7149] provides a first tentative to rationalize that service provider's view on the SDN space by identifying concrete technical domains that need to be considered and for which solutions can be provided:

- Techniques for the dynamic discovery of topology, devices, and capabilities, along with relevant information and data models that are meant to precisely document such topology, devices, and their capabilities.

- Techniques for exposing network services [RFC8309] and their characteristics.

- Techniques used by service-requirement-derived dynamic resource allocation and policy enforcement schemes, so that networks can be programmed accordingly.

- Dynamic feedback mechanisms that are meant to assess how efficiently a given policy (or a set thereof) is enforced from a service fulfillment and assurance perspective.

Models are key for each of these technical items. Service and network management automation is an important step to improve the agility of network operations and infrastructures.

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. At the time of writing this document (2019), 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. However, how these models work together to configure a device, manage a set of devices involved in a service, or even provide a service is something that is not currently documented either within the IETF or other SDOs (e.g., MEF).

This document provides a framework that describes and discusses an architecture for service and network management automation that takes advantage of YANG modeling technologies and investigates how different layer YANG data models interact with each other (e.g., service mapping, model composing) in the context of service delivery

and fulfillment. This framework is drawn from a network provider perspective irrespective of the origin of a data module andcan accommodate even modules that are developed outside the IETF.

The document also identifies a list of modules and use cases to exemplify the proposed approach, but it does not claim to be exhaustive.

It is not the intent of this document to provide an inventory of tools and mechanisms used in specific network and service management domains; such inventory can be found in documents such as [RFC7276].

1.1. Terminology

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

The following terms are defined in [RFC8309][RFC8199] and are not redefined here:

- Network Operator
- Customer
- Service
- Data Model
- Service Model
- Customer Service Model
- Service Delivery Model
- Network Service Module
- Network Element Module

The following terms are defined in this document as follows:

Network Resource Module: The Network Resource Module is used by a network operator to allocate the resource(e.g., tunnel resource, topology resource) for the service or schedule the resource to meet the service requirements define in the Service Model.

2. Layered YANG Modules: An Overview

Figure 1 provides an overview of various macro-functional blocks at different levels that articulate the various YANG data modules. In this figure, we use IETF defined YANG data model as an example Models.

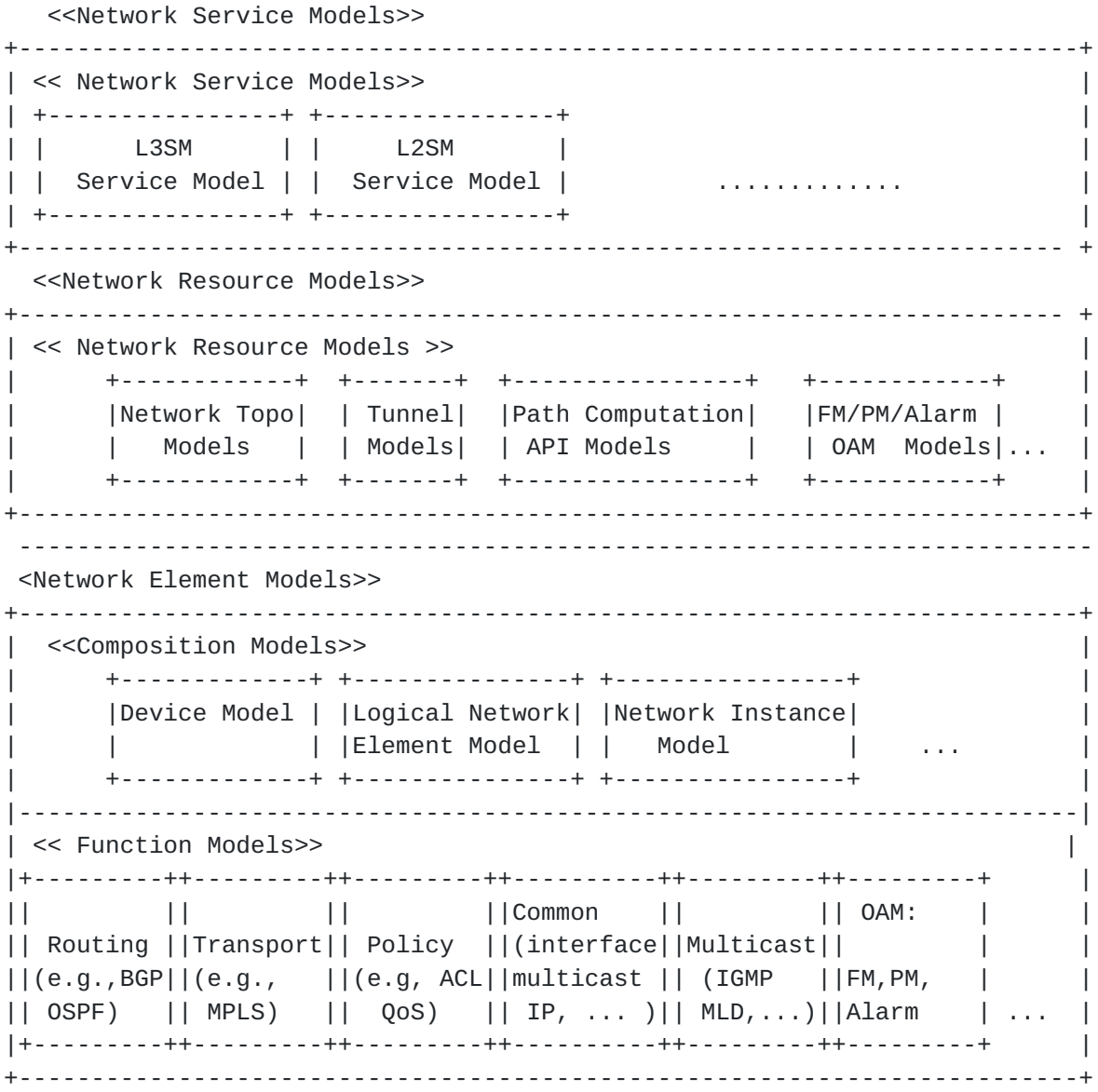


Figure 1: An overview of Layered YANG Modules

2.1. Network Service and Resource Models

2.1.1. Network Service Models: Definition and Samples

As described in [RFC8309], the service is "some form of connectivity between customer sites and the Internet and/or between customer sites across the network operator's network and across the Internet". More concretely, an IP connectivity service can be defined as the IP transfer capability characterized by a (Source Nets, Destination Nets, Guarantees, Scope) tuple where "Source Nets" is a group of unicast IP addresses, "Destination Nets" is a group of IP unicast and/or multicast addresses, and "Guarantees" reflects the guarantees (expressed in terms of Quality Of Service (QoS), performance, and availability, for example) to properly forward traffic to the said "Destination" [RFC7297].

For example:

- L3SM model [RFC8299] defines the L3VPN service ordered by a customer from a network operator.

- L2SM model [RFC8466] defines the L2VPN service ordered by a customer from a network operator.

- VN model [I-D.ietf-teas-actn-vn-yang]provides a YANG data model generally applicable to any mode of Virtual Network (VN) operation.

2.1.2. Network Resource Models: Definitions and Samples

Figure 2 depicts a set of Network resource YANG modules such as topology models or tunnel models:

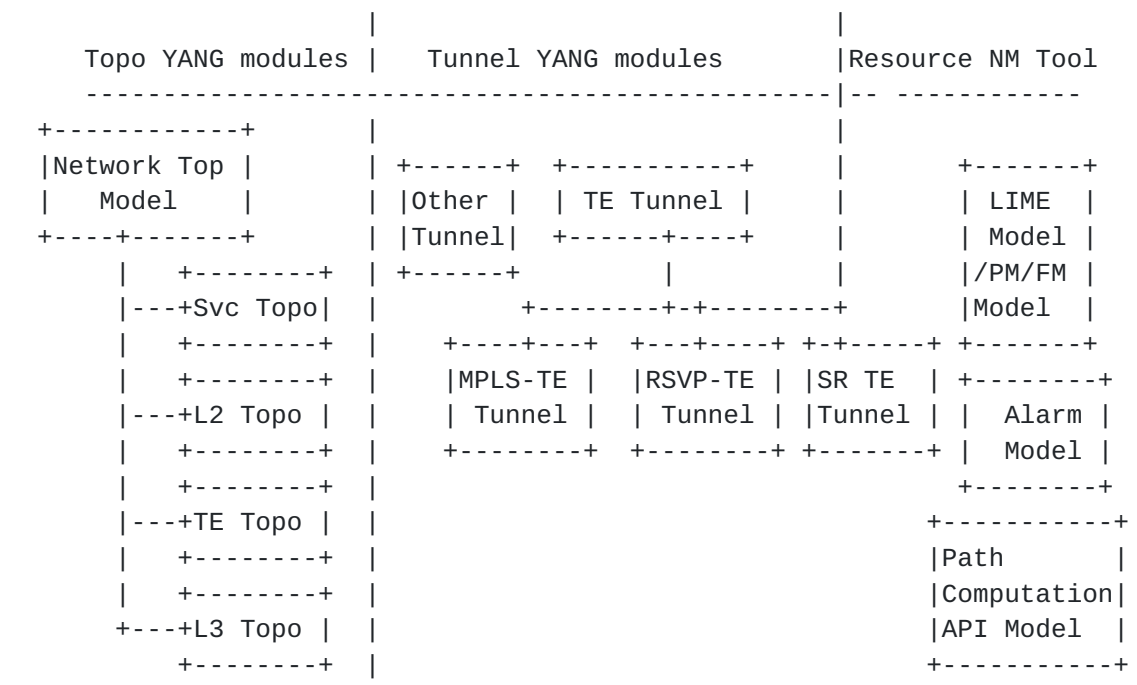


Figure 2: Sample Resource Facing Network Models

Topology YANG module Examples:

- Network Topology Models: [RFC8345] defines a base model for network topology and inventories. Network topology data include link resource, node resource, and terminate-point resources.

- TE Topology Models: [I.D-ietf-teas-yang-te-topo] defines a data model for representing and manipulating TE topologies.

  This module is extended from network topology model defined in [RFC8345] with TE topologies specifics. This model contains technology-agnostic TE Topology building blocks that can be augmented and used by other technology-specific TE Topology models.

- L3 Topology Models

  [RFC8346] defines a data model for representing and manipulating L3 Topologies. This model is extended from the network topology model defined in [RFC8345] with L3 topologies specifics.

- L2 Topology Models

  [I.D-ietf-i2rs-yang-l2-topology] defines a data model for representing and manipulating L2 Topologies. This model is

extended from the network topology model defined in [RFC8345] with L2 topologies specifics.

Tunnel YANG module Examples:

- Tunnel identities [I-D.ietf-softwire-iftunnel] to ease manipulating extensions to specific tunnels.

- TE Tunnel Model

  [I.D-ietf-teas-yang-te] defines a YANG module for the configuration and management of TE interfaces, tunnels and LSPs.

- SR TE Tunnel Model

  [I.D-ietf-teas-yang-te] augments the TE generic and MPLS-TE model(s) and defines a YANG module for Segment Routing (SR) TE specific data.

- MPLS TE Model

  [I.D-ietf-teas-yang-te] augments the TE generic and MPLS-TE model(s) and defines a YANG module for MPLS TE configurations, state, RPC and notifications.

- RSVP-TE MPLS Model

  [I.D-ietf-teas-yang-rsvp-te] augments the RSVP-TE generic module with parameters to configure and manage signaling of MPLS RSVP-TE LSPs.

Resource NM Tool Models:

- Path Computation API Model

  [I.D-ietf-teas-path-computation] YANG module for a stateless RPC which complements the stateful solution defined in [I.D-ietf-teas-yang-te].

- OAM Models (including Fault Management (FM) and Performance Monitoring)

  [RFC8532] defines a base YANG module for the management of OAM protocols that use Connectionless Communications. [RFC8533] defines a retrieval method YANG module for connectionless OAM protocols. [RFC8531] defines a base YANG module for connection oriented OAM protocols. These three models are intended to

provide consistent reporting, configuration and representation for connection-less OAM and Connection oriented OAM separately.

Alarm monitoring is a fundamental part of monitoring the network. Raw alarms from devices do not always tell the status of the network services or necessarily point to the root cause. [I.D-ietf-ccamp-alarm-module]defines a YANG module for alarm management.

- Generic Policy Model

The Simplified Use of Policy Abstractions (SUPA) policy-based management framework [RFC8328] defines base YANG modules [I-D.ietf-supa-generic-policy-data-model]to encode policy. These models point to device-, technology-, and service-specific YANG modules developed elsewhere. Policy rules within an operator's environment can be used to express high-level, possibly network-wide, policies to a network management function (within a controller, an orchestrator, or a network element). The network management function can then control the configuration and/or monitoring of network elements and services. This document describes the SUPA basic framework, its elements, and interfaces.

2.2. Network Element Models: Definitions and Samples

Network Element models (Figure 3) are 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 service delivery. The following figure uses IETF defined models as an example.

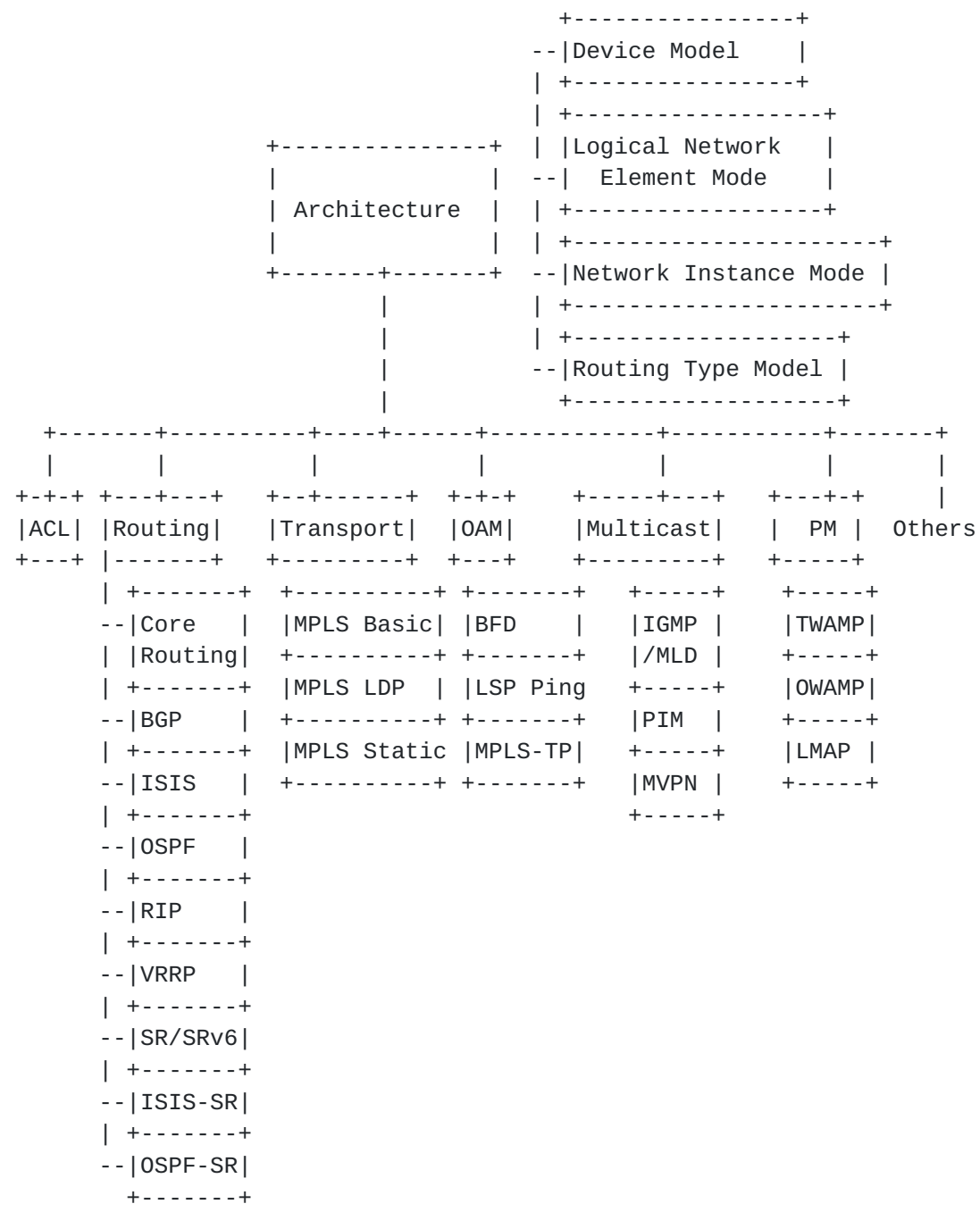


Figure 3: Network Element Modules Overview

2.2.1. Model Composition

- Device Model

  [I.D-ietf-rtgwg-device-model] presents an approach for organizing YANG modules in a comprehensive logical structure that may be used to configure and operate network devices. The structure is itself

represented as an example YANG module, with all of the related component models logically organized in a way that is operationally intuitive, but this model is not expected to be implemented.

- Logical Network Element Model

  [RFC8530] defines a logical network element module which can be used to manage the logical resource partitioning that may be present on a network device. Examples of common industry terms for logical resource partitioning are Logical Systems or Logical Routers.

- Network Instance Model

  [RFC8529] defines a network instance module. This module can be used to manage the virtual resource partitioning that may be present on a network device. Examples of common industry terms for virtual resource partitioning are Virtual Routing and Forwarding (VRF) instances and Virtual Switch Instances (VSIs).

2.2.1.1. Schema Mount

Modularity and extensibility were among the leading design principles of the YANG data modeling language. As a result, the same YANG module can be combined with various sets of other modules and thus form a data model that is tailored to meet the requirements of a specific use case. [RFC8528] defines a mechanism, denoted schema mount, that allows for mounting one data model consisting of any number of YANG modules at a specified location of another (parent) schema.

That capability does not cover design time.

2.2.2. Protocol/Function Configuration Models: Definitions and Samples

BGP: [I-D.ietf-idr-bgp-yang-model] defines a YANG module for configuring and managing BGP, including protocol, policy, and operational aspects based on data center, carrier and content provider operational requirements.

MPLS: [I-D.ietf-mpls-base-yang] defines a base model for MPLS which serves as a base framework for configuring and managing an MPLS switching subsystem. It is expected that other MPLS technology YANG modules (e.g. MPLS LSP Static, LDP or RSVP-TE models) will augment the MPLS base YANG module.

QoS: [I-D.asechoud-netmod-diffserv-model] describes a YANG module of Differentiated Services for configuration and operations.

ACL: Access Control List (ACL) is one of the basic elements used to configure device forwarding behavior. It is used in many networking technologies such as Policy Based Routing, Firewalls, etc. [RFC8519] describes a data model of Access Control List (ACL) basic building blocks.

NAT: For the sake of network automation and the need for programming Network Address Translation (NAT) function in particular, a data model for configuring and managing the NAT is essential. [RFC8512] defines a YANG module for the NAT function covering a variety of NAT flavors such as Network Address Translation from IPv4 to IPv4 (NAT44), Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers (NAT64), customer-side translator (CLAT), Stateless IP/ICMP Translation (SIIT), Explicit Address Mappings (EAM) for SIIT, IPv6-to-IPv6 Network Prefix Translation (NPTv6), and Destination NAT. [RFC8513] specifies a YANG module for the DS-Lite AFTR.

Stateless Address Sharing: [I-D.ietf-softwire-yang] specifies a YANG module for A+P address sharing, including Lightweight 4over6, Mapping of Address and Port with Encapsulation (MAP-E), and Mapping of Address and Port using Translation (MAP-T) softwire mechanisms.

Multicast: [I-D.ietf-pim-yang] defines a YANG module that can be used to configure and manage Protocol Independent Multicast (PIM) devices. [I-D.ietf-pim-igmp-mld-yang] defines a YANG module that can be used to configure and manage Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) devices. [I-D.ietf-pim-igmp-mld-snooping-yang] defines a YANG module that can be used to configure and manage Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping devices.

EVPN: [I-D.ietf-bess-evpn-yang] defines a YANG module for Ethernet VPN services. The model is agnostic of the underlay. It apply to MPLS as well as to VxLAN encapsulation. The model is also agnostic of the services including E-LAN, E-LINE and E-TREE services. This document mainly focuses on EVPN and Ethernet-Segment instance framework.

L3VPN: [I-D.ietf-bess-l3vpn-yang] defines a YANG module that can be used to configure and manage BGP L3VPNs [RFC4364]. It contains VRF specific parameters as well as BGP specific parameters applicable for L3VPNs.

L2VPN: [I-D.ietf-bess-l2vpn-yang] defines a YANG module for MPLS based Layer 2 VPN services (L2VPN) [RFC4664] and includes switching between the local attachment circuits. The L2VPN model covers point-to-point VPWS and Multipoint VPLS services. These services use signaling of Pseudowires across MPLS networks using LDP [RFC8077][RFC4762] or BGP [RFC4761].

Routing Policy: [I-D.ietf-rtgwg-policy-model] defines a YANG module for configuring and managing routing policies in a vendor-neutral way and based on actual operational practice. The model provides a generic policy framework which can be augmented with protocol-specific policy configuration.

BFD: [I-D.ietf-bfd-yang]defines a YANG module that can be used to configure and manage Bidirectional Forwarding Detection (BFD) [RFC5880]. BFD is a network protocol which is used for liveness detection of arbitrary paths between systems.

SR/SRv6: [I-D.ietf-spring-sr-yang] a YANG module for segment routing configuration and operation. [I-D.raza-spring-srv6-yang] defines a YANG module for Segment Routing IPv6 (SRv6) base. The model serves as a base framework for configuring and managing an SRv6 subsystem and expected to be augmented by other SRv6 technology models accordingly.

Core Routing: [RFC8349] defines the core routing data model, which is intended as a basis for future data model development covering more-sophisticated routing systems. It is expected that other Routing technology YANG modules (e.g., VRRP, RIP, ISIS, OSPF models) will augment the Core Routing base YANG module.

PM:

[I.D-ietf-ippm-twamp-yang] defines a data model for client and server implementations of the Two-Way Active Measurement Protocol (TWAMP).

[I.D-ietf-ippm-stamp-yang] defines the data model for implementations of Session-Sender and Session-Reflector for Simple Two-way Active Measurement Protocol (STAMP) mode using YANG.

[RFC8194] defines a data model for Large-Scale Measurement Platforms (LMAPs).

3. Architectural Concepts

3.1. Data Models: Layering and Representation

As described in [RFC8199], layering of modules allows for better reusability of lower-layer modules by higher-level modules while limiting duplication of features across layers.

The data modules developed by IETF can be classified into service level, network level and device level modules. Different service level modules may rely on the same set of network level or device level modules. Service level modules usually follow top down approach and are mostly customer-facing modules providing a common model construct for higher level network services, which can be further mapped to network technology-specific modules at lower layer.

Network level modules mostly follow a bottom-up approach and are mainly network resource-facing modules and describe various aspects of a network infrastructure, including devices and their subsystems, and relevant protocols operating at the link and network layers across multiple devices (e.g., Network topology and TE Tunnel modules).

Device level modules usually follow a bottom-up approach and are mostly technology-specific modules used to realize a service.

3.2. Automation of service delivery procedures

To dynamically provide service offerings, Service level modules can be used by an operator. One or more monolithic Service modules can be used in the context of a composite service activation request (e.g., delivery of a caching infrastructure over a VPN). Such modules are used to feed a decision-making intelligence to adequately accommodate customer's needs.

Also, such modules may be used jointly with services that require dynamic invocation. An example is provided by the service modules defined by the DOTS WG to dynamically trigger requests to handle DDoS attacks [I-D.ietf-dots-signal-channel][I-D.ietf-dots-data-channel].

Network level modules can be derived from service level modules and used to provision, monitor, instantiate the service and provide lifecycle management of network resources, e.g., expose network resources to customers or operators to provide service fulfillment and assurance and allow customers or operators to dynamically adjust

the network resources based on service requirements as described in service level modules and the current network performance information described in the Northbound telemetry modules.

3.3. Service Fullfillment Automation

To operate the service, Device level modules derived from Service level modules or Network level modules can be used to provision each involved network function/device with the proper configuration information, and operate the network based on service requirements as described in the Service level module(s).

In addition, the operational state including configuration that is in effect together with statistics should be exposed to upper layers to provide better network visibility (and assess to what extent the derived low level modules are consistent with the upper level inputs). Note that it is important to relate telemetry data with configuration data to used closed loops at the different stages of service delivery, from resource allocation to service operation, in particular.

3.4. Module Decomposition and Composition

To support top-down service delivery, the service parameters captured in service level module(s) need to be decomposed into a set of configuration parameters that may be specific to one or more technologies; these technology-specific parameters will be grouped together per technique to define technology-specific device level modules or network level modules.

In addition, these technology-specific device level models can be further assembled together to provision each involved network function/device or each involved administrative domain to improve provision efficiency.

For example, IETF rtgwg and netmod working groups have already been tasked to define a model composition mechanism (i.e., Schema Mount mechanism) and relevant grouping base models such as network instance model, logical network element model . The model composition mechanism can be used to assembler different model together while grouping based models can be used to setup and administrate both virtualized system and physical systems .

IETF also developed a YANG catalog tool to manage metadata around IETF- defined modules; it allows both YANG developers and operators to discover appropriate YANG modules that may be used to automate services operations. This YANG tool catalog tools can be used to

select appropriate models for grouping purposes or even to identify gaps.

4. Architecture Overview

The architectural considerations described in the previous section lead to the architecture described in this section and illustrated in Figure 4.

The interfaces and interactions shown in the figure and labeled (a) through (j) are further described in Section 4.1.

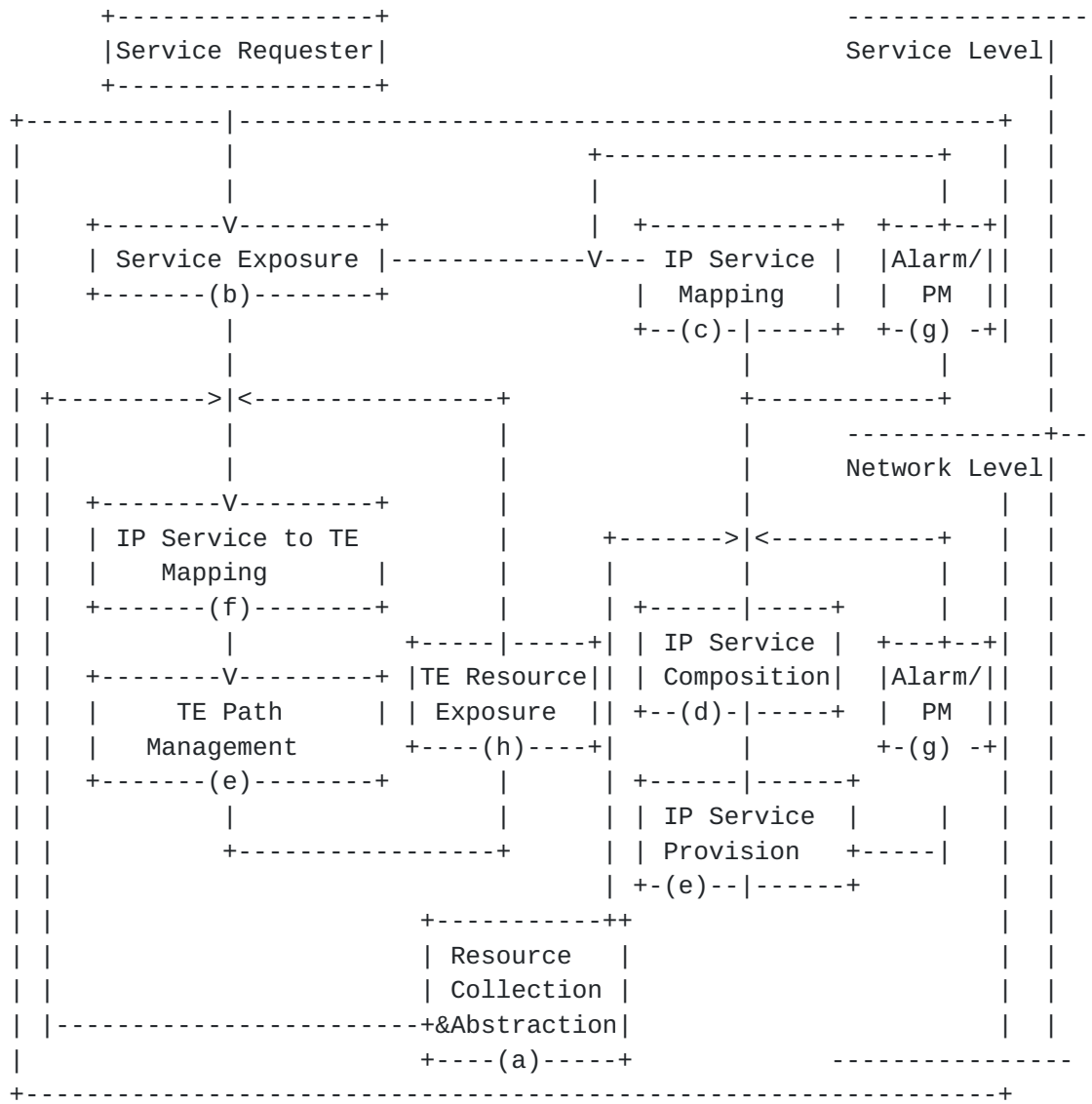


Figure 4: Service and Network Management Automation with YANG

4.1. End-to-End Service Delivery and Service Assurance Procedure

4.1.1. Resource Collection and Abstraction (a)

Network Resources such as links, nodes, or terminate-point resources can be collected from the network and aggregated or abstracted to the management system. Periodic fetching of data is not an adequate solution for applications requiring frequent or prompt updates of network resources. Applying polling-based solutions to retrieve network resource information impacts networks, devices, and applications' loads. These limitations can be addressed by including generic object subscription mechanisms within network elements.

These resources can be modelled using network topology models, L3 topology model, L2 topology model, TE topology model, L3 TE topology model, SR TE topology models at different layers.

In some cases, there may be multiple overlay topologies built on top of the same underlay topology, and the underlay topology can also be built from one or more lower layer underlay topologies. The network resources and management objects in these multi-layer topologies are not recommended to be exposed to customers, but rather exposed to the management system for IP service mapping and Path Management.

4.1.2. Service Exposure & Abstraction (b)

Service exposure & abstraction is used to capture services offered to customers.

Service abstraction can be used by a customer to request a service (ordering and order handling). One typical example is that a customer can use a L3SM service model to request L3VPN service by providing the abstract technical characterization of the intended service.

Service catalogs can be created to expose the various services and the information needed to invoke/order a given service.

YANG modules can be grouped into various service bundles; each service bundle corresponds to a set of YANG modules that have been released or published. Then, a mapping can be established between service abstraction at higher layer and service bundle or a set of YANG modules at lower layer.

4.1.3. IP Service Mapping (c)

Service abstraction starts with high-level abstractions exposing the business capabilities or capturing customer requirements. Then, it needs to map them to resource abstraction and specific network technologies.

Therefore, the interaction between service abstraction in the overlay and network resource abstraction in the underlay is required. For example, in the L3SM service model, a VPN service topology is described as e.g., hub and spoke and any-to-any, single-homed, dual-homed, multi-homed relation between PEs and CEs, but we don't know how this service topology can be mapped into the underlying network topology Section 4.1.8

In addition, there is a need to decide on a mapping between service abstraction and the underlying specific network technologies. Take L3SM service model as an example, to deliver a L3VPN service, we need to map L3SM service view defined in Service model into detailed configuration view defined by specific configuration models for network elements, configuartion information includes:

- VRF definition, including VPN Policy expression
- Physical Interface
- IP layer (IPv4, IPv6).
- QoS features such as classification, profiles, etc.
- Routing protocols: support of configuration of all protocols listed in the document, as well as routing policies associated with those protocols.
- Multicast Support
- NAT or address sharing
- Security functions

4.1.4. IP Service Composition (d)

These configuration models are further grouped together into service bundles, as described in Figure 3using, e.g., device models, logical network element models or network instance models defined in [I.D-ietf-rtgwg-device-model] [RFC8530] [RFC8529] and provide the association between an interface and its associated LNE and NI and populate them into appropriate devices(e.g., PE and CE).

4.1.5. IP Service Provision (e)

IP Service Provision is used to provide IP network devices with a set of configuration information, e.g., network element models such as BGP, ACL, QoS, Interface model, Network instance models to configure PE and CE devices within the site, etc. A BGP policy model is used to establish VPN membership between sites and VPN Service Topology. Experience shows that "pushing" configuration information to each device one after the other is not efficient.

To automate the configuration of service elements, we first assemble all the related network elements models into logical network element model as defined in [RFC8530] and then establish an association with an interface and a set of network element configurations.

In addition, not all the parameters of the service level model or network level model(e.g., mapped from service level model) needs to be specified, in many cases, some default values, or even some values depending of some contextual information (e.g., the particular service / network element / location / etc) should be taken to automate the configuration process.

Seconldy, IP Service Provision can be used to setup tunnels between sites and setup tunnels between PEs and CEs based upon tunnel-related configuration information that can be derived from service abstraction. However, when tunnel-related configuration parameters cannot be generated from service abstraction, other service Mapping procedure is required,e.g.,IP Service to TE mapping procdure described in Section 4.1.7.

4.1.6. Performance Measurement and Alarm Telemetry (g)

Once the tunnel or VPN is setup, PM and Alarm information per tunnel or per link based on network topology can be collected and report to the management system. This information can be further aggregated and abstracted from layered network topology to monitor and manage network Performance on the topology at different layer or the overlay topology between VPN sites. These network performance information or VPN performance information (e.g., latency or bandwidth utilization between two VPN sites) can be put into NBI telemetry model or NBI performance monitoring model at either service level or network level to further optimize the network or provide troubleshooting support.

4.1.7. IP Service to TE Mapping (f)

Take L3VPN service model as an example, the management system will use L3SM service model to determine where to connect each site-network-access of a particular site to the provider network (e.g.,

PE, aggregation switch). The L3SM Service model includes parameters that can help design the VPN, according to customer's requirements, for example.

Nodes used to connect a site may be captured in relevant clauses of a service exposure model (e.g., Customer Nodes Map [RFC7297]).

When Site location is determined, PE and CE device location will be selected. Then we can replace parameters and constraints that can influence the meshing of the site-network-access with specified PE and CE device information associated with site-network-access and generate resource facing VN Overlay Resource model. One example of resource facing VN Overlay Resource model is TEAS VN Service Model [I-D.ietf-teas-actn-vn-yang].

This VN model can be used to calculate node and link resource to meet service requirements based on Network Topology models collected at step (a).

4.1.8. Path Management (h)

Path Management includes Path computation and Path setup. For example, we can derive an instantiated L3SM service model into a resource facing VN Model, with selected PE and CE in each site, we can calculate point- to-point or multipoint end-to-end paths between sites based on the VPN Overlay Resource Model.

After identifying node and link resources required to meet service requirements, the mapping between overlay topology and underlay topology can be established, e.g., establish an association between VPN service topology defined in customer-facing model and underlying network topology defined in the TE topology model (e.g., one overlay node is supported by multiple underlay nodes, one overlay link is supported by multiple underlay nodes) and generate end-to-end VPN topology.

4.1.9. TE Resource Exposure (i)

When tunnel-related configuration parameters cannot be derived from service abstraction, IP Service-to-TE Mapping procedure can be used to generate TE Resource Exposure view, this TE resource Exposure view can be modeled as a resource-facing VPN model which is translated and instantiated from a L3SM model and manage TE resources based on path management information and PM and alarm telemetry information.

Operators may use this dedicated TE resource Exposure view to dynamically capture the overall network status and topology to:

- Perform all the requested recovery operations upon detecting network failures affecting the network service.

- Adjust resource distribution and update to end to end Service topology models

- Provide resource scheduling to better guarantee services for customers and to improve the efficiency of network resource usage.

5. Sample Service Coordination via YANG Moodules

5.1. L3VPN Service Delivery via Coordinated YANG Modules

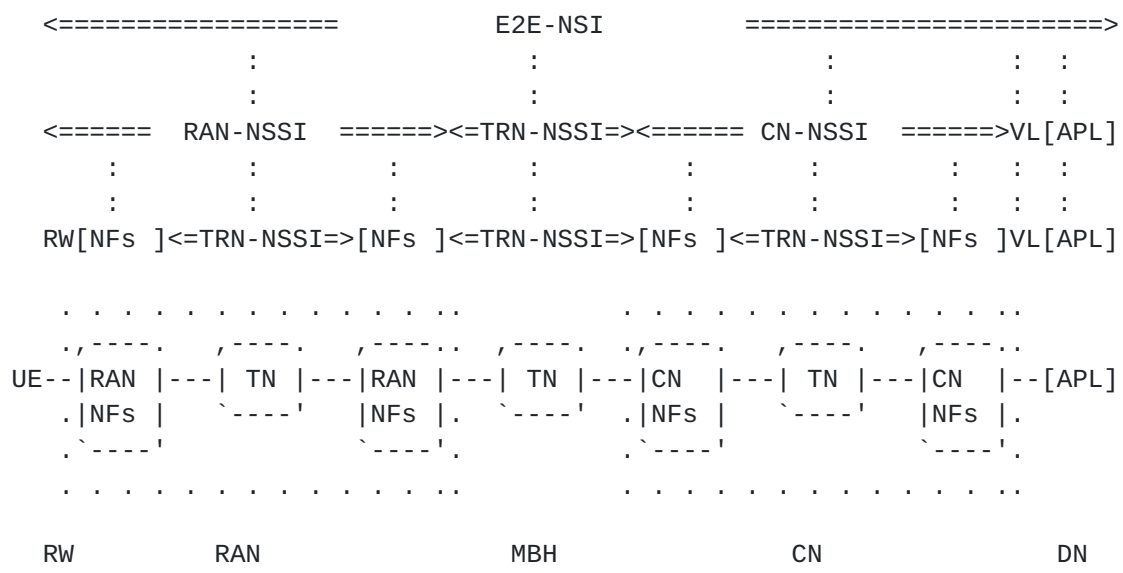
Take L3VPN service as an example, IETF has already developed L3VPN service model [RFC8299] which can be used to describe L3VPN service. To enforce L3VPN service and program the network, a set of network element models are needed, e.g., BGP model, Network Instance model, ACL model, Multicast Model, QoS model, or NAT model.

These network element models can be grouped into different release bundles or feature bundles using Schema Mount technology to meet different tailored requirements and deliver the L3VPN service.

To support the creation of logical network elements on a network device and deliver a virtualized network, Logical Network Element (LNE) models can be used to manage its own set of modules such as ACL, QoS, or Network Instance modules.

5.2. 5G Transport Service Delivery via Coordinated YANG Modules

The overview of network slice structure as defined in the 3GPP 5GS is shown in Figure 5. The terms are described in specific 3GPP documents (e.g., [TS.23.501-3GPP] and [TS.28.530-3GPP]).



*Legends
UE: User Equipment
RAN: Radio Access Network
CN: Core Network
DN: Data Network
TN: Transport Network
MBH: Mobile Backhaul
RW: Radio Wave
NF: Network Function
APL: Application Server
NSI: Network Slice Instance
NSSI: Network Slice Subnet Instance

Figure 5: Overview of Structure of NS in 3GPP 5GS

To support 5G service (e.g., 5G MBB service), L3VPN service model [RFC8299] and TEAS VN model [I-D. ietf-teas-actn-vn-yang] can be both provided to describe 5G MBB Transport Service or connectivity service. L3VPN service model is used to describe end-to-end connectivity service while TEAS VN model is used to describe TE connectivity service between VPN sites or between RAN NFs and Core network NFs.

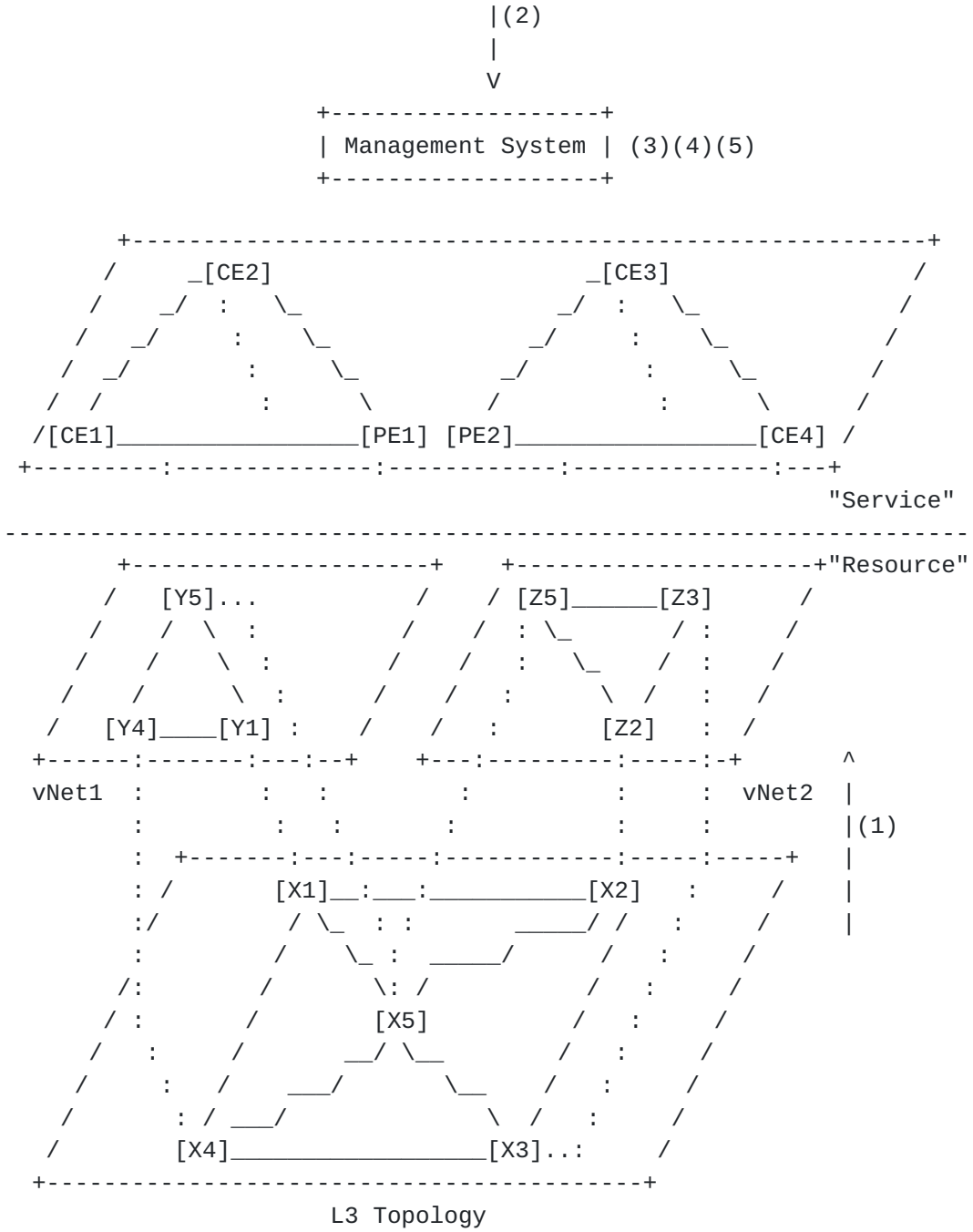
VN in TEAS VN model and support point-to-point or multipoint-to-multipoint connectivity service and can be seen as one example of network slice.

TE Service mapping model can be used to map L3VPN service requests onto underlying network resource and TE models to get TE network setup.

For IP VPN service provision, L3VPN service model is used to derive a set of configuration parameterswhich will be bound to different network element models and group them together to form feature or service bundles to deliver the VPN service.

6. Modules Usage in Automated Virtualized Network Environment: Sample Examples

6.1. Network-initiated Resource Creation



The following steps are performed to deliver the service within the network management automation architecture proposed in this document:

1. Pre-provision multiple virtualized networks on top of the same basic network infrastructure based on pre-configured service requirements and establish resource pool for each virtualized network and expose to the customer with several service templates through web portal.

2. Selects and uses one which best accommodates its requirement among the service templates.

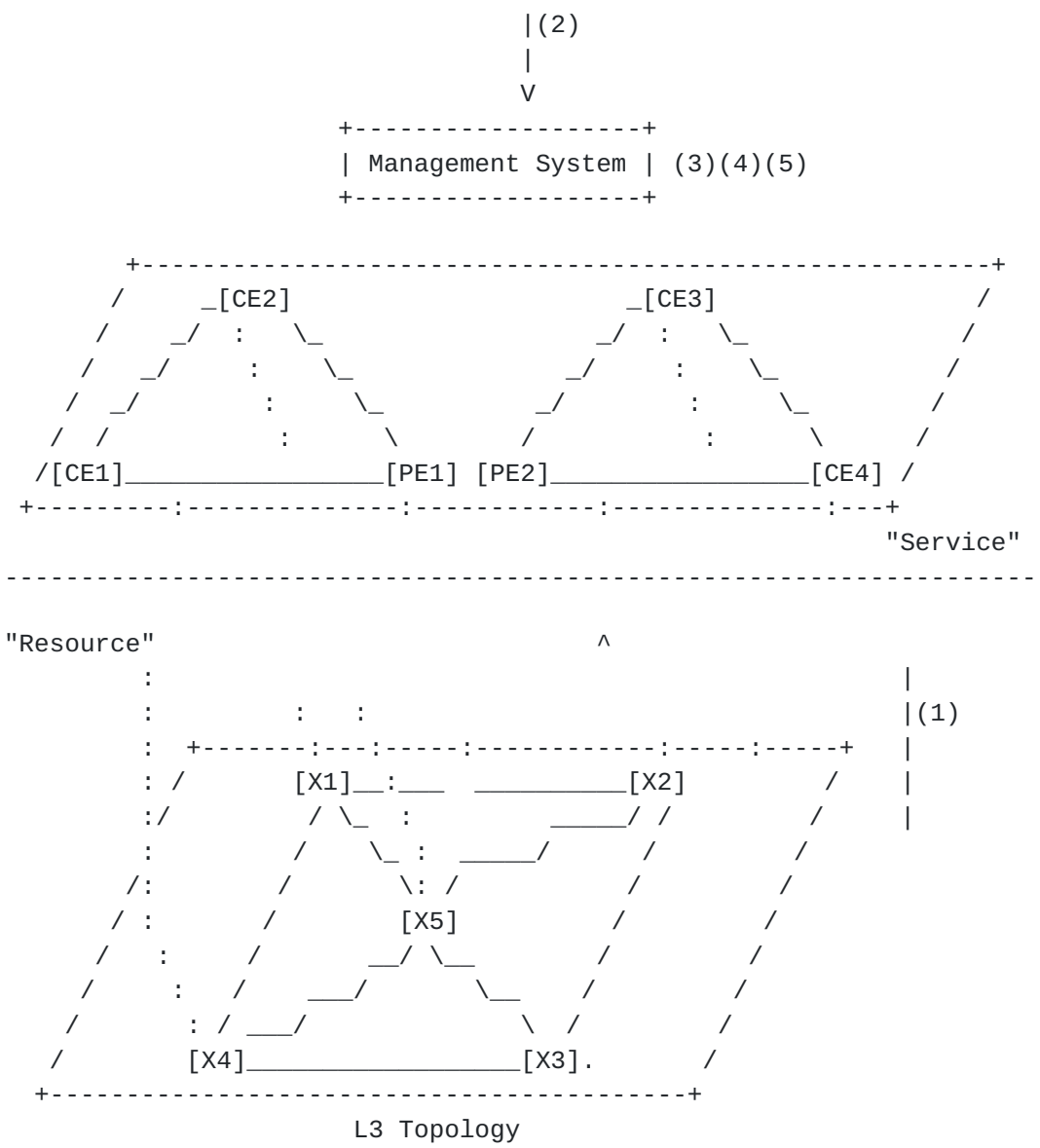
3. Calculate the node resource, link resource corresponding to connectivity between sites and create resource facing VN Network based on selected service template, and

4. Setup tunnels between sites and map them into the selected virtualized network topology and establish resource facing VN topology based on TEAS VN model [I-D.ietf-teas-actn-vn-yang] and TE tunnel based on TE Tunnel model.

   The resource-facing VN model and corresponding TE Tunnel model can be further used to notify all the parameter changes and event related to VN topology or Tunnel. This information can be further used to adjust network resource distributed in the network.

The network initiated resource creation is similar to ready-made Network Slice creation pattern discussed in Section 5.1 of [I-D.homma-slice-provision-models].

6.2. Customer-initiated Dynamic Resource Creation



L3 Topology

The following steps are performed to deliver the service within the network management automation architecture proposed in this document:

1. Establish resource pool for the basic common network infrastructure.

2. Request to create two sites based on L3SM Service model with each having one network access connectivity:

   Site A: Network-Access A, Bandwidth=20M, for class "foo", guaranteed-bw-percent = 10, One-Way-Delay=70 msec

   Site B: Network-Access B, Bandwidth=30M, for class "foo1", guaranteed-bw-percent = 15, One-Way-Delay=60 msec

3. Create a new service topology based on Service Type and service requirements (e.g., Service Type, Site location, Number of Slices, QoS requirements corresponding to network connectivity within a L3VPN) defined in L3SM service model.

4. Translate L3SM service model into resource facing TEAS VN Model [I-D.ietf-teas-actn-vn-yang] and a set of Network element models to enable the protocols on the network device and get the network setup, and the generated resource facing TEAS VN model can be further used to calculate the node resource, link resource corresponding to connectivity between sites.

5. Setup tunnels between sites and map them with the network infrastructure and establish resource facing VN topology based on TEAS VN model and TE tunnel based on TE Tunnel model. The resource facing TEAS VN model and corresponding TE Tunnel model can be used to notify all the parameter changes and event related to VN topology or Tunnel. These information can be further used to adjust network resource distributed within the network.

The customer-initiated resource creation is similar to customer made Network Slice creation pattern discussed in Section 5.2 of [I-D.homma-slice-provision-models].

7. Security Considerations

Security considerations specific to each of the technologies and protocols listed in the document are discussed in the specification documents of each of these techniques.

(Potential) security considerations specific to this document are listed below:

- Create forwarding loops by mis-configuring the underlying network.
- Leak sensitive information: special care should be considered when translating between the various layers introduced in the document.
- ...tbc

8. IANA Considerations

There are no IANA requests or assignments included in this document.

9. Contributors

Shunsuke Homma
Japan

Email: s.homma0718+ietf@gmail.com

10. Acknowledgements

Thanks to Joe Clark and Greg Mirsky for the review.

11. Informative References

[I-D.arkko-arch-virtualization]
Arkko, J., Tantsura, J., Halpern, J., and B. Varga, "Considerations on Network Virtualization and Slicing", draft-arkko-arch-virtualization-01 (work in progress), March 2018.

[I-D.asechoud-netmod-diffserv-model]
Choudhary, A., Shah, S., Jethanandani, M., Liu, B., and N. Strahle, "YANG Model for Diffserv", draft-asechoud-netmod-diffserv-model-03 (work in progress), June 2015.

[I-D.clacla-netmod-model-catalog]
Clarke, J. and B. Claise, "YANG module for yangcatalog.org", draft-clacla-netmod-model-catalog-03 (work in progress), April 2018.

[I-D.homma-slice-provision-models]
Homma, S., Nishihara, H., Miyasaka, T., Galis, A., OV, V., Lopez, D., Contreras, L., Ordonez-Lucena, J., Martinez-Julia, P., Qiang, L., Rokui, R., Ciavaglia, L., and X. Foy, "Network Slice Provision Models", draft-homma-slice-provision-models-00 (work in progress), February 2019.

[I-D.ietf-bess-evpn-yang]
Brissette, P., Shah, H., Hussain, I., Tiruveedhula, K., and J. Rabadan, "Yang Data Model for EVPN", draft-ietf-bess-evpn-yang-07 (work in progress), March 2019.

[I-D.ietf-bess-l2vpn-yang]
Shah, H., Brissette, P., Chen, I., Hussain, I., Wen, B., and K. Tiruveedhula, "YANG Data Model for MPLS-based L2VPN", draft-ietf-bess-l2vpn-yang-10 (work in progress), July 2019.

[I-D.ietf-bess-l3vpn-yang]
Jain, D., Patel, K., Brissette, P., Li, Z., Zhuang, S., Liu, X., Haas, J., Esale, S., and B. Wen, "Yang Data Model for BGP/MPLS L3 VPNs", draft-ietf-bess-l3vpn-yang-04 (work in progress), October 2018.

[I-D.ietf-bfd-yang]
Rahman, R., Zheng, L., Jethanandani, M., Networks, J., and G. Mirsky, "YANG Data Model for Bidirectional Forwarding Detection (BFD)", draft-ietf-bfd-yang-17 (work in progress), August 2018.

[I-D.ietf-ccamp-alarm-module]
Vallin, S. and M. Bjorklund, "YANG Alarm Module", draft-ietf-ccamp-alarm-module-09 (work in progress), April 2019.

[I-D.ietf-ccamp-flexigrid-media-channel-yang]
Madrid, U., Perdices, D., Lopezalvarez, V., Dios, O., King, D., Lee, Y., and G. Galimberti, "YANG data model for Flexi-Grid media-channels", draft-ietf-ccamp-flexigrid-media-channel-yang-02 (work in progress), March 2019.

[I-D.ietf-ccamp-flexigrid-yang]
Madrid, U., Perdices, D., Lopezalvarez, V., Dios, O., King, D., Lee, Y., and G. Galimberti, "YANG data model for Flexi-Grid Optical Networks", draft-ietf-ccamp-flexigrid-yang-03 (work in progress), March 2019.

[I-D.ietf-ccamp-l1csm-yang]
Fioccola, G., Lee, K., Lee, Y., Dhody, D., and D. Ceccarelli, "A YANG Data Model for L1 Connectivity Service Model (L1CSM)", draft-ietf-ccamp-l1csm-yang-09 (work in progress), March 2019.

[I-D.ietf-ccamp-mw-yang]
Ahlberg, J., Ye, M., Li, X., Spreafico, D., and M. Vaupotic, "A YANG Data Model for Microwave Radio Link", draft-ietf-ccamp-mw-yang-13 (work in progress), November 2018.

[I-D.ietf-ccamp-otn-topo-yang]
Zheng, H., Guo, A., Busi, I., Sharma, A., Liu, X., Belotti, S., Xu, Y., Wang, L., and O. Dios, "A YANG Data Model for Optical Transport Network Topology", draft-ietf-ccamp-otn-topo-yang-06 (work in progress), February 2019.

[I-D.ietf-ccamp-otn-tunnel-model]
Zheng, H., Guo, A., Busi, I., Sharma, A., Rao, R., Belotti, S., Lopezalvarez, V., Li, Y., and Y. Xu, "OTN Tunnel YANG Model", draft-ietf-ccamp-otn-tunnel-model-06 (work in progress), February 2019.

[I-D.ietf-ccamp-wson-tunnel-model]
Lee, Y., Dhody, D., Guo, A., Lopezalvarez, V., King, D., Yoon, B., and R. Vilata, "A Yang Data Model for WSON Tunnel", draft-ietf-ccamp-wson-tunnel-model-03 (work in progress), March 2019.

[I-D.ietf-dots-data-channel]
Boucadair, M. and R. K, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", draft-ietf-dots-data-channel-29 (work in progress), May 2019.

[I-D.ietf-dots-signal-channel]
K, R., Boucadair, M., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", draft-ietf-dots-signal-channel-34 (work in progress), May 2019.

[I-D.ietf-idr-bgp-model]
Jethanandani, M., Patel, K., and S. Hares, "BGP YANG Model for Service Provider Networks", draft-ietf-idr-bgp-model-06 (work in progress), June 2019.

[I-D.ietf-ippm-stamp-yang]
Mirsky, G., Xiao, M., and W. Luo, "Simple Two-way Active Measurement Protocol (STAMP) Data Model", draft-ietf-ippm-stamp-yang-03 (work in progress), March 2019.

[I-D.ietf-ippm-twamp-yang]
Civil, R., Morton, A., Rahman, R., Jethanandani, M., and K. Pentikousis, "Two-Way Active Measurement Protocol (TWAMP) Data Model", draft-ietf-ippm-twamp-yang-13 (work in progress), July 2018.

[I-D.ietf-mpls-base-yang]
Saad, T., Raza, K., Gandhi, R., Liu, X., and V. Beeram, "A YANG Data Model for MPLS Base", draft-ietf-mpls-base-yang-10 (work in progress), February 2019.

[I-D.ietf-pim-igmp-mld-snooping-yang]
Zhao, H., Liu, X., Liu, Y., Sivakumar, M., and A. Peter, "A Yang Data Model for IGMP and MLD Snooping", draft-ietf-pim-igmp-mld-snooping-yang-08 (work in progress), June 2019.

[I-D.ietf-pim-igmp-mld-yang]
Liu, X., Guo, F., Sivakumar, M., McAllister, P., and A. Peter, "A YANG Data Model for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD)", draft-ietf-pim-igmp-mld-yang-15 (work in progress), June 2019.

[I-D.ietf-pim-yang]
Liu, X., McAllister, P., Peter, A., Sivakumar, M., Liu, Y., and f. hu, "A YANG Data Model for Protocol Independent Multicast (PIM)", draft-ietf-pim-yang-17 (work in progress), May 2018.

[I-D.ietf-rtgwg-device-model]
Lindem, A., Berger, L., Bogdanovic, D., and C. Hopps, "Network Device YANG Logical Organization", draft-ietf-rtgwg-device-model-02 (work in progress), March 2017.

[I-D.ietf-rtgwg-policy-model]
Qu, Y., Tantsura, J., Lindem, A., and X. Liu, "A YANG Data Model for Routing Policy Management", draft-ietf-rtgwg-policy-model-06 (work in progress), March 2019.

[I-D.ietf-softwire-iftunnel]
Boucadair, M., Farrer, I., and R. Asati, "Tunnel Interface Types YANG Module", draft-ietf-softwire-iftunnel-07 (work in progress), June 2019.

[I-D.ietf-softwire-yang]
Farrer, I. and M. Boucadair, "YANG Modules for IPv4-in-IPv6 Address plus Port (A+P) Softwires", draft-ietf-softwire-yang-16 (work in progress), January 2019.

[I-D.ietf-spring-sr-yang]
Litkowski, S., Qu, Y., Lindem, A., Sarkar, P., and J. Tantsura, "YANG Data Model for Segment Routing", draft-ietf-spring-sr-yang-12 (work in progress), February 2019.

[I-D.ietf-supa-generic-policy-data-model]
Halpern, J. and J. Strassner, "Generic Policy Data Model for Simplified Use of Policy Abstractions (SUPA)", draft-ietf-supa-generic-policy-data-model-04 (work in progress), June 2017.

[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-05 (work in progress), June 2019.

[I-D.ietf-teas-sf-aware-topo-model]
Bryskin, I., Liu, X., Lee, Y., Guichard, J., Contreras, L., Ceccarelli, D., and J. Tantsura, "SF Aware TE Topology YANG Model", draft-ietf-teas-sf-aware-topo-model-03 (work in progress), March 2019.

[I-D.ietf-teas-te-service-mapping-yang]
Lee, Y., Dhody, D., Ceccarelli, D., Tantsura, J., Fioccola, G., and Q. Wu, "Traffic Engineering and Service Mapping Yang Model", draft-ietf-teas-te-service-mapping-yang-01 (work in progress), March 2019.

[I-D.ietf-teas-yang-l3-te-topo]
Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Dios, "YANG Data Model for Layer 3 TE Topologies", draft-ietf-teas-yang-l3-te-topo-04 (work in progress), March 2019.

[I-D.ietf-teas-yang-path-computation]
Busi, I., Belotti, S., Lopezalvarez, V., Dios, O., Sharma, A., Shi, Y., Vilata, R., Sethuraman, K., Scharf, M., and D. Ceccarelli, "Yang model for requesting Path Computation", draft-ietf-teas-yang-path-computation-05 (work in progress), March 2019.

[I-D.ietf-teas-yang-rsvp-te]
Beeram, V., Saad, T., Gandhi, R., Liu, X., Bryskin, I., and H. Shah, "A YANG Data Model for RSVP-TE Protocol", draft-ietf-teas-yang-rsvp-te-06 (work in progress), April 2019.

[I-D.ietf-teas-yang-sr-te-topo]
Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and S. Litkowski, "YANG Data Model for SR and SR TE Topologies", draft-ietf-teas-yang-sr-te-topo-04 (work in progress), March 2019.

[I-D.ietf-teas-yang-te]
Saad, T., Gandhi, R., Liu, X., Beeram, V., and I. Bryskin, "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te-21 (work in progress), April 2019.

[I-D.ietf-teas-yang-te-topo]
Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Dios, "YANG Data Model for Traffic Engineering (TE) Topologies", draft-ietf-teas-yang-te-topo-22 (work in progress), June 2019.

[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>.

[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>.

[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>.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <https://www.rfc-editor.org/info/rfc7149>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <https://www.rfc-editor.org/info/rfc7276>.

[RFC7297] Boucadair, M., Jacquenet, C., and N. Wang, "IP Connectivity Provisioning Profile (CPP)", RFC 7297, DOI 10.17487/RFC7297, July 2014, <https://www.rfc-editor.org/info/rfc7297>.

[RFC8077] Martini, L., Ed. and G. Heron, Ed., "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", STD 84, RFC 8077, DOI 10.17487/RFC8077, February 2017, <https://www.rfc-editor.org/info/rfc8077>.

[RFC8194] Schoenwaelder, J. and V. Bajpai, "A YANG Data Model for LMAP Measurement Agents", RFC 8194, DOI 10.17487/RFC8194, August 2017, <https://www.rfc-editor.org/info/rfc8194>.

[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>.

[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>.

[RFC8328] Liu, W., Xie, C., Strassner, J., Karagiannis, G., Klyus, M., Bi, J., Cheng, Y., and D. Zhang, "Policy-Based Management Framework for the Simplified Use of Policy Abstractions (SUPA)", RFC 8328, DOI 10.17487/RFC8328, March 2018, <https://www.rfc-editor.org/info/rfc8328>.

[RFC8345] Clemm, A., Medved, J., Varga, R., Bahadur, N., Ananthakrishnan, H., and X. Liu, "A YANG Data Model for Network Topologies", RFC 8345, DOI 10.17487/RFC8345, March 2018, <https://www.rfc-editor.org/info/rfc8345>.

[RFC8346] Clemm, A., Medved, J., Varga, R., Liu, X., Ananthakrishnan, H., and N. Bahadur, "A YANG Data Model for Layer 3 Topologies", RFC 8346, DOI 10.17487/RFC8346, March 2018, <https://www.rfc-editor.org/info/rfc8346>.

[RFC8349] Lhotka, L., Lindem, A., and Y. Qu, "A YANG Data Model for Routing Management (NMDA Version)", RFC 8349, DOI 10.17487/RFC8349, March 2018, <https://www.rfc-editor.org/info/rfc8349>.

[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>.

[RFC8513] Boucadair, M., Jacquenet, C., and S. Sivakumar, "A YANG Data Model for Dual-Stack Lite (DS-Lite)", RFC 8513, DOI 10.17487/RFC8513, January 2019, <https://www.rfc-editor.org/info/rfc8513>.

[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>.

[RFC8528] Bjorklund, M. and L. Lhotka, "YANG Schema Mount", RFC 8528, DOI 10.17487/RFC8528, March 2019, <https://www.rfc-editor.org/info/rfc8528>.

[RFC8529] Berger, L., Hopps, C., Lindem, A., Bogdanovic, D., and X. Liu, "YANG Data Model for Network Instances", RFC 8529, DOI 10.17487/RFC8529, March 2019, <https://www.rfc-editor.org/info/rfc8529>.

[RFC8530] Berger, L., Hopps, C., Lindem, A., Bogdanovic, D., and X. Liu, "YANG Model for Logical Network Elements", RFC 8530, DOI 10.17487/RFC8530, March 2019, <https://www.rfc-editor.org/info/rfc8530>.

[RFC8531] Kumar, D., Wu, Q., and Z. Wang, "Generic YANG Data Model for Connection-Oriented Operations, Administration, and Maintenance (OAM) Protocols", RFC 8531, DOI 10.17487/RFC8531, April 2019, <https://www.rfc-editor.org/info/rfc8531>.

[RFC8532] Kumar, D., Wang, Z., Wu, Q., Ed., Rahman, R., and S. Raghavan, "Generic YANG Data Model for the Management of Operations, Administration, and Maintenance (OAM) Protocols That Use Connectionless Communications", RFC 8532, DOI 10.17487/RFC8532, April 2019, <https://www.rfc-editor.org/info/rfc8532>.

[RFC8533] Kumar, D., Wang, M., Wu, Q., Ed., Rahman, R., and S. Raghavan, "A YANG Data Model for Retrieval Methods for the Management of Operations, Administration, and Maintenance (OAM) Protocols That Use Connectionless Communications", RFC 8533, DOI 10.17487/RFC8533, April 2019, <https://www.rfc-editor.org/info/rfc8533>.

Authors' Addresses

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

Email: bill.wu@huawei.com

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Christian
Orange
Rennes 35000
France

Email: christian.jacquenet@orange.com

Luis Miguel Contreras Murillo
Telifonica

Email: luismiguel.contrerasmurillo@telefonica.com

Diego R. Lopez
Telefonica I+D
Spain

Email: diego.r.lopez@telefonica.com

Chongfeng Xie
China Telecom
Beijing
China

Email: xiechf.bri@chinatelecom.cn

Weiqiang Cheng
China Mobile

Email: chengweiqiang@chinamobile.com

Young Lee
Futurewei

Email: younglee.tx@gmail.com