Framework for Automating Service and Network Management with YANG
draft-wu-model-driven-management-virtualization-02

Abstract

Model driven service and network management provides a programmatic and standards-based way of representing virtual services or networks and configuration to the network device that are used to construct the service. It can be used at various phases of service and network management life cycle such as service instantiation, service provision, optimization, monitoring, and diagnostic. Also, it can be designed to automate network management and provide closed-loop control for the sake of agile service creation, delivery and maintenance.

This document provides a framework that describes and discusses an architecture for service and network management automation with YANG Modeling technologies. An applicability of YANG data model to automation of virtualized network service is also investigated.

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 September 9, 2019.
Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ........................................... 3
2. Architectural Concepts ................................ 4
   2.1. Data Models: Layering and Representation ........ 4
   2.2. Service Activation and Provision Automation ...... 5
   2.3. Service Enforcement Configuration Model Composition .... 5
   2.4. A Catalog for YANG Modules ....................... 5
3. IETF YANG Modules: An Overview ..................... 6
   3.1. Network Service and Resource Models .............. 6
      3.1.1. Network Service Models: Definition and Samples ... 7
      3.1.2. Network Resource Models ....................... 7
   3.2. Network Element Models .......................... 11
      3.2.1. Model Composition ............................. 12
      3.2.2. Protocol/Function Configuration Models .......... 13
4. YANG model Catalog for L3VPN Service .................. 15
5. YANG model Catalog for 5G Transport Service ........... 16
6. Architecture Overview ............................... 17
   6.1. End-to-End Service Delivery and Service Assurance Procedure ......................... 18
      6.1.1. Resource Collection and Abstraction (a) ........ 18
      6.1.2. Service Exposure & Abstraction (b) ............. 19
      6.1.3. IP Service Mapping (c) ......................... 19
      6.1.4. IP Service Composition (d) .................... 20
      6.1.5. IP Service Provision (e) ....................... 20
      6.1.6. Performance Measurement and Alarm Telemetry (f) ... 21
      6.1.7. IP Service to TE Mapping (g) .................. 21
      6.1.8. Path Management (h) ........................... 22
      6.1.9. TE Resource Exposure (i) ...................... 22
7. Model usage in automated virtualized network environment:
   Sample Examples .................................... 22
   7.1. Network initiated resource creation .................. 22
   7.2. Customer initiated Dynamic Resource Creation ....... 24
1. Introduction

The manage system usually comprise service activation/provision system and service enforcement system. Traditional service delivery work flow, from customer order to practical service provision, the work flow process typically involves inputting data sequentially into multiple OSS/BSS applications managed by different departments; Many of these applications are custom built over the years and operating in silo mode; Lacking of standard data input/output also causes lots of challenge in system integration and results in manual data entry; Customer MACD (Move, Add, Change, Delete) will incur the same repetitive process in many cases. Secondly traditional service fulfill system lack a programmatic and standards-based way of writing configurations to any network device and has slow response to the network changes and doesn’t provide real time monitoring capability in high frequency and in high throughput on the current state of the system. Therefore model driven network management becomes crucial to address these challenges.

For years, the IETF has been driving the industry transition from an overloaded Software Defined Networking (SDN) buzzword to focus on specific areas such as modeling-driven network management. [RFC7149] provides a first tentative to rationalize that space by identifying concrete technical domains that need to be considered:

- Techniques for the dynamic discovery of network 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. Automation is a key step to improve the agility of network operations and infrastructure.

In the later development, as described in [RFC8199], YANG module developers have taken both top-down and bottom-up approaches to develop modules and establish mapping between network technology and customer requirements on the top or abstracting common construct from various network technologies. At the time of writing this document (2018), we see the large number of data models including configuration models and service models developed or under development in IETF covering much of networking protocols and techniques. In addition, how these models work together to fully configure a device, or manage a set of devices involved in a service aren’t developed yet in IETF.

This document takes both bottom up approach and top down approach to provide a framework that discusses the architecture for network management automation, with a focus on network virtualization environment.

This document also describes specific YANG modules needed to realize connectivity services and investigates how top down built model (e.g., customer-facing data models) interact with bottom up built model (network resource-facing data models) in the context of service delivery and assurance.

2. Architectural Concepts

2.1. 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 IETF has developed large number of 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 models providing a common model construct for higher level network services, which can be further mapped to network technology-specific models at lower layer.

Network level modules mostly follow bottom up approach and are mainly network resource-facing model 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 bottom up approach and are mostly technology-specific modules used to realize a service.

### 2.2. Service Activation and Provision Automation

To provide more agile service offering, Service level module can be used by the operator to communicate with the customer and have rapid response to customer needs. Network level module can be translated from service level module and used to provision, monitor, instantiate the service and provide lifecycle management of network resource, e.g., expose network resource to the customer or operators.

### 2.3. Service Enforcement Configuration Model Composition

To provide network management automation, lower level technology-specific models need to be assembled together to provision each involved network function/device and operate the network based on service requirements described in the service level model.

IETF RTGWG working group has already been tasked to define service elements configuration model composition mechanism and develop several composition model such as network instance model, logical network element model and device model.

These models can be used to setup and administrate both virtualized system and physical system.

### 2.4. A Catalog for YANG Modules

The idea of a catalog is similar to service catalogs in traditional IT environments. Service catalogs serve as a software-based registries of available services with information needed to discover and invoke available services.

The IETF has already tasked to develop a YANG catalog which can be used to manage not only IETF defined modules, but also non-IETF defined ones [I-D.clacla-netmod-model-catalog].

The YANG catalog allows to align IETF work with other SDOs work and prevent duplicated building blocks being developed. It also encourages reusability of common building blocks.

The YANG catalog allows both YANG developers and operators to discover the more mature YANG modules that may be used to automate services operations.
### Network Service and Resource Models

Service and Network Resource modules define what the "service"/"resource" is. These modules can be classified into two categories:

- Network Service Models
- Network Resource Models
3.1.1. Network Service Models: Definition and Samples

As described in [RFC8309], the service is some form of connectivity between customer sites and the Internet or between customer sites across the network operator's network and across the Internet. Such connectivity service is described without resource allocation or with half service resource correlation.

For example,

- L3SM model [RFC8299] defines the L3VPN service ordered by a the customer from a network operator.
- L2SM model [RFC8466] defines the L2VPN service ordered by a the customer from a network operator.
- L1CSM model [I-D.ietf-ccamp-l1csm-yang] defines a YANG data model for Layer 1 Connectivity Service Model (L1CSM).
- TEAS VN model [I-D.ietf-teas-actn-vn-yang] defines YANG data model for the Abstraction and Control of Traffic Engineered (TE) networks (ACTN) Virtual Network Service (VNS) operation. Unlike L3SM model, ACTN model can also be used as operator facing model, e.g., establish interconnection between L3VPN sites across multiple ASs.
- TE service mapping model [I-D.lee-teas-te-service-mapping-yang] a YANG data model to map service model (e.g., L3SM) and Traffic Engineering model (e.g., TE Tunnel or the Abstraction and Control of Traffic Engineered Networks Virtual Network model). This model is applicable to the operation’s need for a seamless control and management of their VPN services with TE tunnel support and principally used to allow monitoring and diagnostics of the management systems to show how the service requests are mapped onto underlying network resource and TE models.
- Composed VPN model [I-D.evenwu-opsawg-yang-composed-vpn] defines a YANG data model that can be used by a network operator to configure a VPN service in multiple administrative domain environment consisting of L2VPN or L3VPN or a mixture of the two. This model provides an abstracted view of VPN service configuration components at different layer.

3.1.2. Network Resource Models

Figure 1 shows a set of Network resource YANG modules such as topology models, tunnel models:
Topo YANG Models | Tunnel YANG Models | Resource NM Tool
----------------------------------|-- --
|+------------+|       |    |
| | Network Top | | Other | | TE Tunnel | | LIME |
| | Model | | | | | |
| +--------+ |       | +------| +-----------+ |       | |

---+Svc Topo| +--------+ | +----------|+--------+ |+-----------|
| |       | |       | | Model | | |
| +--------+ |       | | MPLS-TE | RSVP-TE | SR TE | +----------+
| +--------+ | Tunnel | Tunnel | Tunnel | | Alarm |

---+L2 Topo | +--------+ | +--------+ | +--------+ | ++----------+

---+TE Topo | +--------+ | +--------+ | ++----------+

---+L3 Topo | +--------+ | +--------+ | ++----------+

Figure 1: Sample Resource Facing Network Models

Topology YANG Models:

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


  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.
Internet-Draft and Network Management Automation with Y  March 2019

- **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.

- **L3 TE Topology Models**

  When traffic engineering is enabled on a layer 3 network topology, there will be a corresponding TE topology. [I.D-ietf-teas-yang-l3-te-topo] defines data models for layer 3 traffic engineering topologies. Two data models are defined, one is layer 3 TE topology model, the other is packet switching TE topology model. Layer 3 TE topology model is extended from Layer 3 topology model. Packet switching TE topology model is extended from TE topology model.

- **SR TE Topology Models**

  [I-D.ietf-teas-yang-sr-te-topo] defines a YANG module for Segment Routing (SR) topology and Segment Routing (SR) traffic engineering (TE) topology. Two models are defined, one is SR topology model, the other is SR TE topology model, SR topology model is extended from L3 Topology model. SR TE topology model is extended from both SR Topology model and L3 TE topology model.

- **SF Aware TE Topology YANG Model**

  [I-D.ietf-teas-sf-aware-topo-model] defines a YANG data model for TE network topologies that are network service and function aware.

- **Optical Transport Topology Models:**

  OTN Transport Topology Model: [I-D.ietf-ccamp-otn-topo-yang] defines a YANG data model to describe the topologies of an Optical Transport Network (OTN).

  WSON Transport Topology Model: [I-D.ietf-ccamp-wson-yang] defines a YANG data model for the routing and wavelength assignment (RWA) Traffic Engineering (TE) topology in wavelength switched optical networks (WSONs).

  Flex-Grid Transport Topology Model: [I-D.ietf-ccamp-flexigrid-yang] defines a YANG model for flexi-grid objects in the dynamic optical network, including the nodes, transponders and links.
between them, as well as how such links interconnect nodes and
transponders.

Tunnel YANG Models:

- 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.

- Optical Transport Tunnel Models:
  
  * Flexigrid Media Channel Tunnel Models: [I-D.ccamp-flexigrid-
    media-channel-yang] defines a YANG model for the flexi-grid
    media-channel. This YANG module defines the whole path from a
    source transponder or node to the destination through a number
    of intermediate nodes in the flexi-grid network.
  
  * WSON Tunnel Model: [I-D.ccamp-wson-tunnel-model] defines a YANG
    data model for WSON tunnel model.
  
  * OTN Tunnel Model: [I-D. ietf-ccamp-otn-tunnel-model]defines a
    YANG data model for OTN tunnel Model.

Resource NM Tool Models:

- Path Computation API Model
Internet-Draft Service and Network Management Automation with Y March 2019

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

- **OAM Models**

  [I.D-ietf-lime-yang-connectionless-oam] defines a base YANG module for the management of OAM protocols that use Connectionless Communications. [I.D-ietf-lime-yang-connectionless-oam-methods] defines a retrieval method YANG module for connectionless OAM protocols. [I.D-ietf-lime-yang-connection-oriented-oam-model] defines a base YANG module for connection oriented OAM protocols. These three models can be used to provide consistent reporting, configuration and representation.

- **Alarm Models**

  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 data models to encode policy. These models point to device-, technology-, and service-specific YANG data models 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.

3.2. Network Element Models

Network Element models are used to describe how a service can be implemented by activating and tweaking a set of functions (enabled in one or multiple devices) that are involved in the service delivery.
3.2.1. Model Composition

- Device Model

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

### 3.2.1.1. 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.

### 3.2.2. Protocol/Function Configuration Models

- **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 models (e.g. MPLS LSP Static, LDP or RSVP-TE models) will augment the MPLS base YANG model.
QoS: [I-D.asechoud-netmod-diffserv-model] describes a YANG model 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. [I.D-ietf-netmod-acl-model] 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. [I.D-ietf-opsawg-nat-yang] defines a YANG module for the NAT function.

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 data model 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 data model for Ethernet VPN services. The model is agnostic of the underlay. It applies 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 model 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 data model 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 data model 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 data model 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 data model for segment routing configuration and operation. [I-D.raza-spring-srv6-yang] defines a YANG data model 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 models (e.g. VRRP, RIP, ISIS, OSPF models) will augment the Core Routing base YANG model.

PM Models:


[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).

4. YANG model Catalog for L3VPN Service

The model catalog provides enough information for users to determine which YANG modules or module bundles are available to describe a specific service or technology. 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,
NAT model, these network element models can be grouped into different
release bundles or feature bundle using Schema Mount technology to
meet different tailored requirements and realize L3VPN service. To
support the creation of logical network elements on a network device
and enable automation of virtualized network, Logical Network
Element(LNE) model can be used to manages its own set of modules such
as ACL, QoS, Network Instance modules.

5. YANG model Catalog for 5G Transport Service

The overview of structure of Network slice in the 3GPP 5GS is shown
in Figure 4. The terms are described in the 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

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 and 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 will be translated into a set of network element configuration parameters, these configuration parameters will go to different network element models and group them together to form feature bundle or service bundle to get L3VPN network setup.

6. Architecture Overview

The architectural considerations and conclusions described in the previous section lead to the architecture described in this section and illustrated in Figure 3.

The interfaces and interactions shown in the figure and labeled (a) through (j) are further described in Section 5.1.
### 6.1 End-to-End Service Delivery and Service Assurance Procedure

#### 6.1.1 Resource Collection and Abstraction (a)

Network Resource 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 resource. Applying polling-based solutions to retrieve network resource also imposes a load on networks, devices, and applications. These limitations can be addressed by including generic object subscription mechanisms within network elements.

These resources can be modelled using network topology model, 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 have multiple overlay topologies built on top of the same underlay topology, and the underlay topology can be also built from one or more lower layer underlay topology.

In some cases, there may have multiple overlay topologies built on top of the same underlay topology, and the underlay topology can be also built from one or more lower layer underlay topology. The network resources and management objects in these multi-layer topologies are not recommended to be exposed to customers who (will) order the service from the management system, instead it will be exposed to the management system for IP service mapping and TE path Management.

The abstract view is likely to be technology-agnostic.

6.1.2. 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 L3SM service model to request L3VPN service by providing the abstract technical characterization of the intended service. Such L3VPN service describes various aspects of network infrastructure, including devices and their subsystems, and relevant protocols operating at the link and network layers across multiple device. The L3SM service model can be used to interact with the network infrastructure, e.g., configure sites, decide QoS parameters to be applied to end to end connectivity between VPN sites, select PEs, CEs, etc.

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 is corresponding 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.

6.1.3. IP Service Mapping (c)

Service abstraction starts with high-level abstractions exposing the business capabilities or capturing customer requirements. Then, it needs to maps 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, we describe VPN service topology including sites relationship, 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 underlying network topology. For detailed interaction, please refer to Section 6.1.8

In addition, there is a need to decide on a mapping between service abstraction and underlying specific network technologies. Take L3SM service model as an example, to realize 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, these configuration models include:

- 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

6.1.4. IP Service Composition (d)

These detailed configuration models are further assembled together into service bundle described in Figure 2 using, e.g., device model, logical network element model or network instance model 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).

6.1.5. IP Service Provision (e)

IP Service Provision is used to provision network infrastructure using various configuration models, e.g., use network element models such as BGP, ACL, QoS, Interface model, Network instance models to configure PE and CE device within the site. BGP Policy model is used to establish VPN membership between sites and VPN Service Topology.
Traditionally, "push" service element configuration model one by one to the network device and provide association between an interface and each service element configuration model is not efficient.

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

In addition, IP Service Provision can be used to setup tunnels between sites and setup tunnels between PE and CE within the site when tunnels related configuration parameters can be generated from service abstraction. However when tunnels related configuration parameters can not be generated from service abstraction, IP Service to TE Mapping procedure is required.

6.1.6. Performance Measurement and Alarm Telemetry (f)

Once the tunnel is setup, PM and Warning information per tunnel or per link based on network topology can be collected and report to the management system. This information can be used to optimize the network or provide troubleshooting support.

6.1.7. IP Service to TE Mapping (g)

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). L3SM Service model proposes parameters and constraints that can influence the meshing of the site-network-access.

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 Overlay Resource model can be used to calculate node and link resource to Meet service requirements based on Network Topology models collected at step (a).
6.1.8. Path Management (h)

Path Management includes Path computation and Path setup. For example, we can translate L3SM service model into resource facing VN Model, with selected PE and CE in each site, we can calculate point to point or multipoint end to end path between sites based on VN 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 VN topology.

6.1.9. TE Resource Exposure (i)

When tunnels related configuration parameters can not be generated 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 resource facing VN model which is translated and instantiated from L3SM model and manage TE resource 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.

7. Model usage in automated virtualized network environment: Sample Examples

7.1. Network initiated resource creation
The following steps are performed to deliver the service within the network management automation architecture proposed in this document:

- 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.
Selects and uses one which fulfills most its requirement among the service templates.

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

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. These 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].

7.2. Customer initiated Dynamic Resource Creation
The following steps are performed to deliver the service within the network management automation architecture proposed in this document:

- Establish resources pool for the basic common network infrastructure.
- 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
Create a new service topology based on Service Type and service requirements (e.g., Slice Service Type, Slice location, Number of Slices, QoS requirements corresponding to network connectivity within a Slice) defined in L3SM service model.

Translate L3SM service model into resource facing TEAS VN Model [I-D.ietf-teas-actn-vn-yang], and calculate the node resource, link resource corresponding to connectivity between sites or connectivity between PE and CE within Site in the service topology based on generated resource facing TEAS VN model.

Setup tunnels between sites and tunnel between PE and CE within Site and map them into basic 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].

8. 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

9. IANA Considerations

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

Shunsuke Homma
NTT
Japan

Email: shunsuke.homma.fp@hco.ntt.co.jp

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.evenwu-opsawg-yang-composed-vpn]
Even, R., Bo, W., Wu, Q., and Y. Cheng, "YANG Data Model
for Composed VPN Service Delivery",
draft-evenwu-opsawg-yang-composed-vpn-03 (work in progress),
March 2019.

[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-06 (work in progress),
October 2018.

[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-09 (work in progress),
October 2018.
Internet-DraService and Network Management Automation with Y March 2019

[I-D.ietf-bess-l3vpn-yang]
Jain, D., Patel, K., Brissette, P., Li, Z., Zhuang, S.,

[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-ccamp-alarm-module]

[I-D.ietf-ccamp-flexigrid-media-channel-yang]
Madrid, U., Perdices, D., Lopezalvarez, V., Dios, O.,

[I-D.ietf-ccamp-flexigrid-yang]
Madrid, U., Perdices, D., Lopezalvarez, V., Dios, O.,

[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.

[I-D.ietf-ccamp-otn-topo-yang]
Zheng, H., Guo, A., Busi, I., Sharma, A., Liu, X.,


[I-D.ietf-spring-sr-yang]

[I-D.ietf-teas-actn-vn-yang]

[I-D.ietf-teas-sf-aware-topo-model]

[I-D.ietf-teas-te-service-mapping-yang]

[I-D.ietf-teas-yang-l3-te-topo]

[I-D.ietf-teas-yang-path-computation]

[I-D.ietf-teas-yang-rsvp-te]

[I-D.ietf-teas-yang-sr-te-topo]


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

Young Lee  
Huawei  
Email: leeyoung@huawei.com