A YANG Data Model for L2VPN Service Delivery

draft-wen-l2sm-l2vpn-service-model-03

Bin Wen (Comcast)
Giuseppe Fioccola (Telecom Italia)
ChongFeng Xie (China Telecom)
Luay Jalil (Verizon)
Traditional Service Delivery Workflow Limitations

- From customer order entry to actual service provisioning, the workflow process of traditional service delivery model 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 process in many cases.

- Modernizing all these existing OSS/BSS systems requires tremendous effort in both manpower and capital spending.
Motivation Behind a Standard Service Model

- Service delivery automation has demonstrated high potential of cost reduction and quick implementation to meet the surging customer demands.

- As the industry is entering a new era of SDN, many providers are facing the challenge of how to protect and leverage existing investment in BSS/OSS tool while transforming into automated service delivery model.

- Network automation offers many benefits in terms of improved scalability and reliability by replacing the high-touch manual provisioning model with a real-time, automated approach. However, there’s still gap to be filled in order to present service information currently maintained in the traditional OSS/BSS model to the new management system such as network orchestrator.
Reference Architecture for the Use of the L2SM

Customer Service Requester

L2VPN Service Model

Service Orchestration

Service Delivery Model

Network Orchestration

Network

Config Manager

Device Model

Application BSS/OSS
The IETF YANG Data Model for L2VPN Service

- The Layer 2 Service Model provides an abstracted interface to request, configure and manage the components of a L2VPN service.
- This model is intended to be used by a subscriber to communicate with the provider on certain service attributes and inter-connect arrangements.
- The L2SM data can be used as input for an orchestration layer that is responsible for configuring the network elements to enable the service.
- The network orchestrator can also pass L2SM data back to existing OSS/BSS applications.
Network Orchestrator vs Service Orchestrator

• The concept behind Network Service Orchestration is to decouple the customer services from actual network components, while automatically provisioning network elements to the service specifications.

• In the past couple of years, the industry has seen lots of development in Network Orchestrator to control the network resources; However, very little attention has been paid to how to present the service attribute to the Network Orchestrator.

• In order to overcome the bottleneck of traditional OSS/BSS practice and reduce revenue cycle, a new SDN component, Service Orchestrator, can be placed as far north as the interface between the service provider and the enterprise customers or partner providers.

• The Service Orchestrator consumes requests for services expressed in a standard form using YANG, applies operator policies, and generates instructions to the Network Orchestrator.
Layer 2 VPN Service Types

- **E-Line services:** Point-to-Point Layer 2 connections.
  - **EPL (Ethernet Private Line):** EPL service provides delivering of all customer service frames between UNI-to-UNI interfaces using All-to-One Bundling. All unicast/broadcast/multicast packets are delivered unconditionally over the EVC. No service multiplexing is allowed on an EPL UNI interface.
  - **EVPL (Ethernet Virtual Private Line):** On the other hand, EVPL service supports multiplexing more than one Point-to-Point, or even other virtual private services, on the same UNI interface. Ingress service frames are conditionally transmitted through one of the EVCs based upon pre-agreed C-tag to EVC mapping. EVPL supports multiple C-tags to one EVC bundling.

- **E-LAN services:** Multipoint-to-Multipoint Layer 2 connections.
  - **EVP-LAN (Ethernet Virtual Private LAN Service):** EVP-LAN allows connecting to multiple EVCs from one or more of the UNI interfaces. Services frame disposition is based on C-tag to EVC mapping. EVP-LAN supports multiple C-tags to one EVC bundling.
L2SM Applicable Case 1: Single Provider EVC

- A P-t-P or MP-t-MP Ethernet Virtual Circuit with two or more UNI interconnect interfaces in a single provider’s network

Baseline Scenario: Single Operator (EVC Owner) Single Metro Network
L2SM Applicable Case 2: Multi-Provider EVC

- A P-t-P or MP-t-MP Ethernet Virtual Circuit with off-net UNI interfaces across more than one provider’s network; E-NNI connections between providers
L2SM Applicable Case 3: E-Access OVC

- A P-t-P Operator Virtual Circuit between customer UNI interface and E-NNI inter-connect
Overview of the L2SM YANG Model

• The L2SM is centered around a subscriber and structured to support multiple circuits of various service types for the same subscriber.

• The L2SM YANG module is divided into the following three main containers:
  – customer-info
  – vpn-services
  – site
The “customer-info” container

• The “customer-info” container has essential information to reference the subscriber for query purpose: customer-account-number, customer-name, customer-operation-center (customer-noc-street-address, customer-noc-phone-number)
The “vpn-services” container

• The “vpn-services” container is intended for service-wide attributes
• Each service is identified by a “svc-id”, which is unique in the entire network of the service provider; Based on the service-type, the “svc-id” is derived from either evc-id or ovc-id
• Multiple “vpn-svc” sub-containers can be placed under “vpn-services”
• Currently, the L2SM module supports the following signaling options: MP-BGP VPLS/VPWS, MP-BGP EVPN and T-LDP PWE
• There are also optional parameters for advanced features such as load-balancing and service protection
The “site” container

• All external facing interfaces associated with an Ethernet service are listed under “sites”, including both UNI and E-NNI types; Any other internal interface is out-of-scope from L2SM perspective

• The “site” container is intended for the provider to store information of detailed implementation arrangement with either the end customer or peer operators at each inter-connect location

• For each UNI or E-NNI site, there are sub-containers to maintain physical link attributes, service frame and Layer 2 control protocol frame disposition, Ethernet Service OAM attributes, and service bandwidth profile and priority level agreement

• In general, a site should inherit service attributes from the “vpn-services” container; nevertheless, certain site-specific options are allowed, signaling or load-balancing option for example
Design Team Discussion:
Alignment with L3SM

• Add some discussion of relationship to L3SM
  – Initially this would be to say that the models are entirely independent.
  – Later work might share model structure especially around customer and site identification,
  – but for now the models simply share look and feel for these aspects.
Design Team Discussion: adding SLA targets

• SLA target: delay, jitter, frame loss, service availability, etc.

• Consider adding under service
  – Add a whole container for "MEF SLA target"
    Model on MEF work

• This issue was brought up on the list, author hasn’t decided how to address this issue.
Design Team Discussion

• Need example to explain
  – how these service parameters are used
  – How to map service parameter to input parameter of protocol configuration.
  – Solicit WG input on this
Design Team Discussion

**protection-type**” and “**number of retries**

- Protection type refers to the action the device will take when the limit is reached. So, currently, we either “shutdown” the service or trigger an alarm or trap.

- Number of retries refer to the restoration of service after an action (i.e. shutdown) has been taken.

- *protection-type” and “number of retries"* will be documented under “*mac-loop-prevention*
YANG Compilation error fixed

- Thank AD Benoit to make a sanitary check on the draft
- The YANG Compilation error has been fixed in v-(01)

MEF reference 23.1 update

- MEF 23.1 has been superseded by MEF 23.2.
- It was published in August this year after the reference was inserted.

Action: Fixed in the next update.
Next Step

• Prepare reply Liaison in response to MEF liaison and establish a collaboration with MEF
• Address Open issues raised and prepare a new revision
• Solicit broadly review from community