YANG Data Model for Composed VPN Service Delivery

draft-evenwu-opsawg-yang-composed-vpn-03

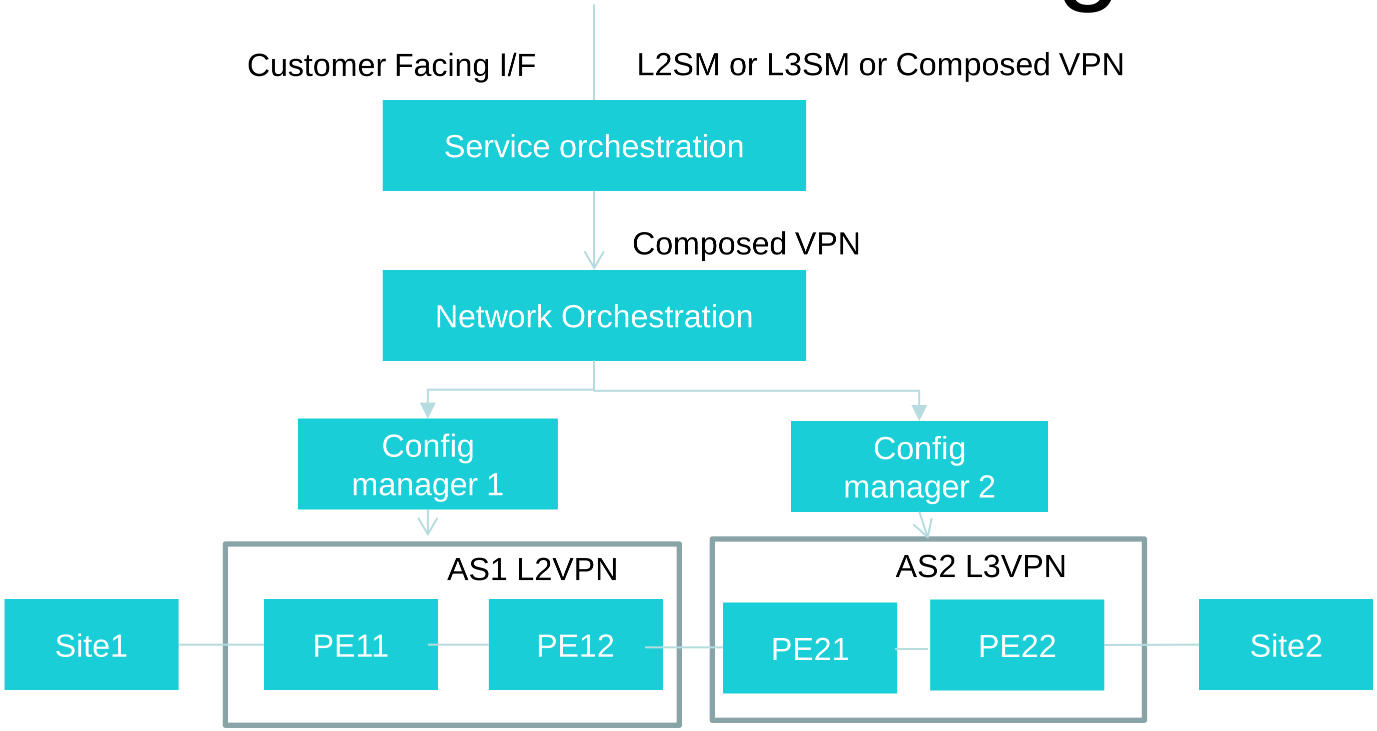
Qin Wu
Roni Even
Bo Wu
Ying Cheng

IETF104 Prague

Document status

- This document defines a YANG data model that can be used by a network operator to configure a VPN service that spans multiple administrative domains. The model is not a configuration model to be used directly on network elements
- The data model is used in a Service Provider.
- The 01 version was presented in IETF103, 02 version was updated to reflect the comments from IETF 102 and 03 version addresses comments from Adrian Farrell.
- The major changes are:
  - Better text about the document motivation and use cases
  - Change the data model to align with L3SM and L2SM

Service Model Usage



- Two Typical ways to deploy the composed VPN model.
  - Independent model: The network orchestration uses the composed VPN model and translate it to segmented VPN for each Administrative Domain.
  - Use Customer facing model (e.g. L3SM) as input to service orchestration layer that will translate to the composed VPN model.

Major changes

- Emphases that it is used at a single service provider whose network is divided to multiple administrative domains (may be used by multiple SPs based on peering agreements). The requirement is for a single service orchestration.
- A Composed VPN can be classified into three categories based on the domain specific VPN types the interworking option may vary depending on the inter-domain technology, such as IP or MPLS forwarding

Composed VPN	Domain 1	Domain 2	Domain N	Interworking option
L3VPN	L2VPN	L2VPN	L3VPN	OPTION A
L3VPN	L3VPN	L3VPN	L3VPN	OPTION A/B/C
L2VPN	L2VPN	L2VN	L2VPN	OPTION A/B/C

Major changes

- Update the data model to be inline with the L3SM and L2SM and add the security and QoS support based on the interworking option.

Next Step

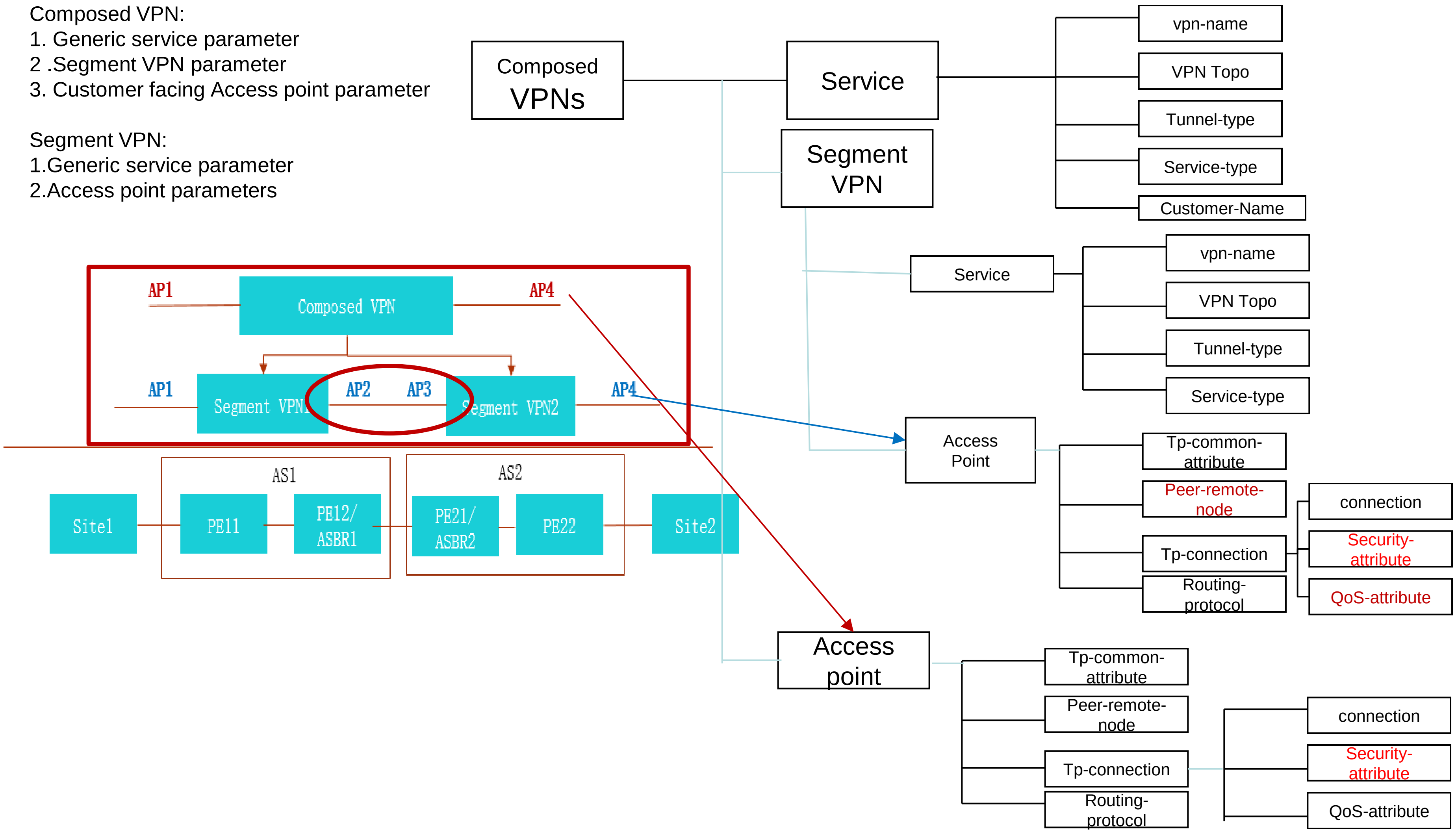
- Create milestone for composed VPN
- Adopt the draft as the initial document.

Backup Slides

Composed VPN Model Definition

Composed VPN:
1. Generic service parameter
2 .Segment VPN parameter
3. Customer facing Access point parameter

Segment VPN:
1.Generic service parameter
2.Access point parameters



Secure inter domain connection – Section 5.2.2.1

- This model is applied to a single SP. Although there are different domain separation, implicit trust exists between the ASs because they have the same operational control, for example from orchestrator's perspective. May be used between SPs that has a federation between the domains.
- The model specifies different security parameters depending on the various Inter-AS options:
  - Option A uses interfaces or sub-interfaces between autonomous system border routers (ASBRs) to keep the VPNs separate, so there is strict separation between VPNs.
  - Option B can be secured with configuration on the control plane and the data plane. On the control plane, the session can be secured by use of peer authentication of BGP. In addition, prefix filters can be deployed to control which routes can be received from the other AS. On the data plane, labeled packets are exchanged and checked to verify that this label on the data plane has really been assigned on the control plane. An MPLS label security could be enabled under the connection node.
  - Option C can be secured on the control plane, but the data plane does not provide any mechanism to check and block the packets to be sent into the other AS. On the control plane, model C has two interfaces between autonomous systems: The ASBRs exchange IPv4 routes with labels via eBGP. The other interface is the RRs exchange VPN-IPv4 routes with labels via multihop MP-eBGP. The prefixes exchanged can be controlled through route maps, equally the route targets. On the data plane, the traffic exchanged between the ASBRs contains two labels. One is VPN label set by the ingress PE to identify the VPN. The other is PE label specifies the LSP to the egress PE. The Authentication and routing policy parameter could be set under the BGP peering configuration.