YANG Data Model for SD-WAN VPN service model delivery
draft-sun-opsawg-sdwan-service-model-01

Qiong Sun
China Telecom

Bo Wu (presenter)
Qin Wu
Huawei Technologies
Status Update from IETF 102

• This draft defines a SD-WAN VPN service model
  – Deliver SD-WAN VPN services by provisioning the CE devices on behalf of the customer.
  – Provide secure connectivity over multiple WAN access and management simplification.

• Presented in IETF 102 Montreal and proposed by China telecom based on their deployment experience, got a few feedback from opsawg community
  – Agreed it was a good starting point and had synergy with ONUG.

• A dedicate slot in rtgwg session in IETF 102 for SD-WAN
  – ONUG Open SDWAN Exchange API progress was updated (Steve Wood), and service model requirements was proposed

• Changes since previous version
  – Reference Update
  – Model re-structure and security and QoS policy reclassification
  – Change segment network into subVPN
Motivation

• Functionality of **CE-based VPN** described in RFC 4110 (Provider provisioned VPN Framework) provides foundation for SD-WAN technology
  – CE based VPN term (RFC4026)
  – CE based Model(RFC4110)

• SD-WAN has more functionality than CE-based VPN:
  – **SR for SD-WAN**: draft-dukes-spring-sr-for-sdwan
    • CE of SD-WAN could be attached to Internet or MPLS network
    • CE can make **L3-L7 flow classification** and **steer the flow of different SLA to different path**.
  – **Secure L3VPN**: draft-rosen-bess-secure-l3vpn specifies a C-PE term, that CE can offer fine granularity virtual network separation, with BGP as control plane to advertise virtual network routing.
  – **controller based IPSEC VPN** : Compared to conventional peer to peer model, controller based IPSEC VPN approaches are in study
    • draft-ietf-i2nsf-sdn-ipsec-flow-protection-02, Netconf central management
    • draft-carrel-ipsecme-controller-ike, BGP or Netconf both could be candidate controller
Proposal

• Based on CE-based VPN
  – Document common requirements and functionalities applicable to various SD-WAN use case defined in various IETF drafts.
  – With Additional functionality of **CE-based VPN** described in RFC 4110 (Provider provisioned VPN Framework)
    • Hybrid WAN connection
    • Different SLA path steering
    • Multi-tenant separation inside a VPN
  – Allow common and unified management and configuration with various different underlying technology in control plane and forwarding plane
SD-WAN VPN Service overview

- **A SD-WAN VPN includes**
  - **Two or more sites**
    - Each site has one or more CE devices
      - Each device could connect to MPLS or Internet (SR-for-SD-WAN)
  - **One ore more SubVPN**
    - Each SubVPN has its own topology and policy (secure-L3VPN)
    - L3-L7 flow classification (SR-for-SDWAN)
    - Multi SLA path steering classification (SR-for-SDWAN)
Difference with ONUG service model

- ONUG service model (ONUG OSE API Interworking progress) is used for service interworking between SD-WAN vendor domains inside a enterprise network:
  - OSE Gateway Service API for **reachability**: Gateway Service creation, interface configuration, segmentation instance creation, cross-connect
  - OSE **Path Management** Service API: Flow classification, SLA definition, Preferred path selection
- The SD-WAN service model is used to define **connectivity service** and support multiple domain service orchestration (similar to L3SM) in a service provider network, which could provide abstraction of path management service and reachability service.
  - SD-WAN VPN management: site configuration, subVPN configuration and application aware **path selection policy**
ONAP SD-WAN VPN service automation@ IETF 103 hackathon

- Verify SD-WAN service YANG to create a SD-WAN VPN service

- Participating components
  - Service Configuration API
  - ONAP SDN-C
  - SD-WAN controller
  - Physical CE, virtual CE

SD-WAN service model based API

ONAP SDN-C(orchestrator)

SD-WAN controller (Domain Controller)

SiteA

SiteB

SD-WAN service model based API

Device Model

Mgmt network

Underlay network

Data link

SD-WAN VPN connection

Postman API

Rest API

OPSAWG IETF 103 Bangkok Nov 03 - 09, 2018
Next steps

• The authors appreciate thoughts, feedback, and text on the content of the documents.
Backup slides
Model Design

• An abstraction of Service requirements to set up the service, no specific detail regarding protocol and element detailed configuration

• SD-WAN VPN model takes same path as L2SM and adopt a similar model structure as L3SM, but add two major components:
  – Site: extended with **multiple transport network links**
  – **subVPN network**: Customer could have multiple virtual network which are not allowed to communicate with each other
  – **Policies**: Policy could be applied per subVPN in application or flow granularity

Site attributes:
  • CE device
  • Transport network link
    ▪ Network type (DSL, MPLS, LTE)
    ▪ IP addressing
    ▪ Protocol

Virtual tenant network between multiple sites

• Path selection policy
• QOS policy
• Security policy

subVPN network

subVPN topology

Site list

LAN network list

Site role in topology

Hub, Spoke, any to any
Path selection policy

- Customers define their own applications and flow classification
  - Voice, video, game, critical data
- Application or flow SLA
  - Monitor the delay, jitter or packet of application or flow
- Path selection: based on the status, steer the traffic to appropriate transport network link