ONAP
OPEN NETWORK AUTOMATION PLATFORM

ONAP CCVPN

Blueprint Overview

ONAP CCVPN Blueprint Improves Agility and Provides Cross-Domain Connectivity

OVERVIEW:

- Build high-bandwidth, flat OTN (Optical Transport Networks) on demand
- Offer international end to end services to enterprises
- Work across carriers with MEF Interlude aligned API
- Close loop VPN adjustment

CURRENT CHALLENGES:

- Service scheduling and resource maintenance are manual processes
- Demand for private line bandwidth is driving the expansion to OTN
- No bridge or platform available to connect different service providers

SOLUTION:

- ONAP to orchestrate SOTN only, SD-WAN only, Combined service of SOTN and SD-WAN
- External API to play the role of cross operators communication
- SDN-C to act as OTN super controller
- ONAP to support the design of composite service
- ONAP to deploy edge and edge applications

Overview

Network-as-a-service is in demand, compelling Communication Service Providers (CSPs) to build high-bandwidth, flat, super high-speed OTNs (Optical Transport Networks), to meet the growing demands of the digital economy and our information-based society. CSPs also want to provide additional value to customers through high-speed, flexible and intelligent services. For example, CSPs see demand for dynamic and flexible VPN service in SMB customers.

Furthermore, CSPs want to offer international end to end network services to their enterprise customers. The ability to collaborate and interwork across carrier networks is of paramount importance in such scenarios.

The CCVPN (Cross Domain and Cross Layer VPN) blueprint is a cross carrier solution combining SOTN (Software-defined Optical Transport Network) and SD-WAN (Software-defined Wide Area Network) network-as-a-service orchestrated and managed by ONAP, to realize unified management and scheduling of resources and services, and to deploy value added services automatically. This blueprint shows how to connect vCPE/uCPE devices across CSPs using SD-WAN and across multiple network domains within a CSP. The service also crosses networking layers by connecting L3 devices across E-Line type L2 network connections. In the case of two operators, two instances of ONAP are deployed at two different geographic sites.

The focus of CCVPN is from an end to end perspective and includes the following scenarios:

- SOTN only, to manage and orchestrate network services
- SD-WAN, to realize cross-layer VPN services
- End to end cross carrier private line, to interconnect multiple CSP networks

Additionally, ONAP addresses the following additional scenarios:

- Multi-sites service creation, which allows the customer to choose as many sites as they want.
- Service Change Management, to allow the customer to dynamically add more branch sites or value-added services on demand
- Allow third party analytics applications to optimize the running service instances

Problem Statement

Current SOTN network services have disadvantages, such as:

- Manual processes: Manual involvement is required in service scheduling and resource maintenance which is time-consuming, expensive and difficult to scale.
- Lack of dynamic network configuration: With the high demand for large bandwidth in private lines, expansion to OTN is required. The existing solutions do not provide automated dynamic reconfiguration of networks.
- Multi-Provider connectivity: Currently, there is no bridge or platform to connect different service providers, which drastically limits the utility of network-as-a-service.

New Requirements

There is an immediate demand for the following requirements that is not addressed by current solutions.

- Self-service
  - Self-service for client-side virtual premise equipment (vCPE) and cloud-side virtual gateway (VG)
  - On-demand VPN service to SMB and enterprise customers

- Dynamic configuration and real-time monitoring
  - Real-time resource monitoring and update
  - Multi-constrained end to end route computation
  - Addition of new sites
  - Addition of value-added services like AI Apps.
- Cross-operator functionality
  - VPN service deployment by overlay mode, without changes to CSP network
  - Federation across two operator ONAP instances for service instantiation enabled through east-west-API that is aligned with the MEF Interlude API
  - OTN equipment operation and scheduling for different vendor products
- Multi-domain network end to end service provisioning and survivability
- Intelligent Bandwidth on demand
  - AI applications at the edge could tell apart an alarm, then report it to ONAP and trigger close loop bandwidth adjustment.

Solution

The Open Network Automation Platform (ONAP) project orchestrates CCVPN using software defined networking (SDN) and network functions virtualization (NFV) to address the problems with existing solutions and also to support additional requirements.

ONAP is an open source project that provides a common platform for telecommunications, cable and cloud operators and their solution providers to rapidly design, implement and manage differentiated services. ONAP provides orchestration, automation and end to end lifecycle management of network services. It includes all the Management and Orchestration (MANO) layer functionality specified by the ETSI NFV architecture; additionally, it provides a network service design framework and FCAPS (fault, configuration, accounting, performance, security) functionality.

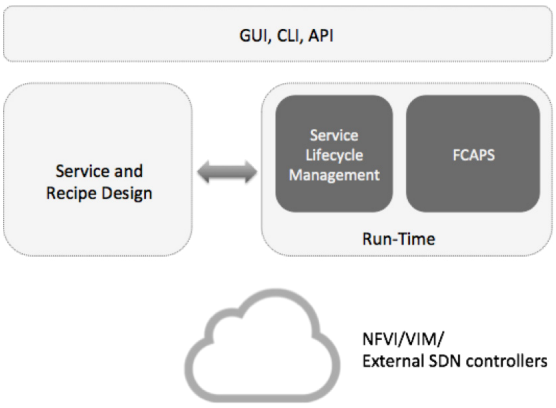

Figure 1: ONAP Functionality

ONAP includes a CCVPN blueprint demonstration for two purposes:

- Show how ONAP can used by CSPs to implement CCVPN
- Provide an additional use case to the ONAP developer community to help them prioritize features and platform optimizations

The ONAP CCVPN blueprint incorporates commercial virtualized network functions (VNFs) to create and manage the underlying vCPE (virtual Customer Premises Equipment) services, that was developed in an open community through collaboration between commercial VNF, VIM and SDN device vendors. More specifically, in this blueprint, ONAP interworks with vendor-specific VNF managers (VNFMs), element management systems (EMSs), Virtual Infrastructure Manager (VIMs) and SDN controllers across two CSP networks. The use of commercial software could offer CSPs a path to production.

The functionality of CCVPN consists of the following:

1. PE and physical network (which can provide MEF EPL service as abstract resource) onboarding in ONAP, along with corresponding VNFMs and EMSs
2. Cross-domain orchestration across multiple physical networks that includes route calculation based on abstract topology; support for end-to-end E-Line services across domains over OTN Network-to-Network (NNI) handover
3. Cross-operator end to end service provisioning
4. Closed-loop reroute for cross-domain service, in case of route failures in any of the domains
5. Closed-loop bandwidth adjustments
6. Value added service provisioning, AI apps, SFC (Service Function Chaining), etc.

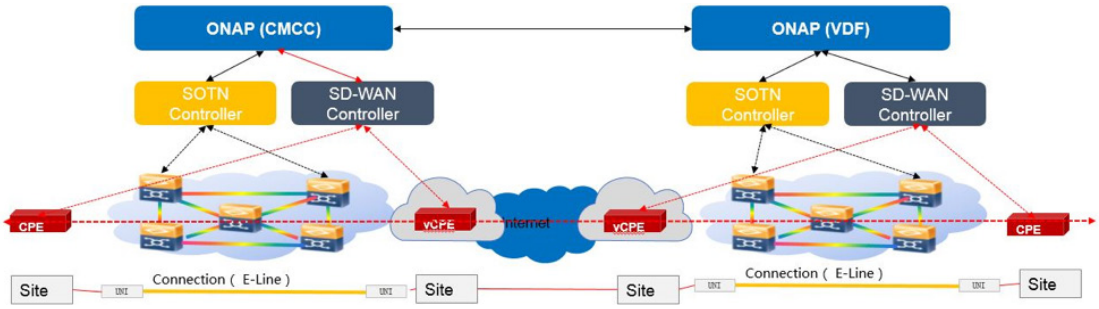

Figure 2: ONAP CCVPN Blueprint

Implementation Details

The CCVPN blueprint involves the following tasks:

- L1(OTN) and L2(ETH) topology discovery from multiple domain controllers
- Service and resource on-boarding and design
- Service deployment and configuration with ONAP<-->ONAP communication
- Self-service adaptation (closed loop showing bandwidth on demand)
- Add additional sites or services within sites (customers could choose the number of sites on demands when creating a service. Customers also could add or delete a site dynamically when a service is running)
- Add value added service like AI apps. (The intelligent security system developed by CMCC was tested in this case, AI apps like face recognition and speech recognition can detect the anomaly, the intelligent security system will then report to ONAP the alarm event.)
- Model-driven route optimization for OTN paths between domains
- Service termination
- Disaster recovery

During onboarding and design phase, one end to end service is created using SDC. This service is composed of these two kinds of resources:

- VPN resource
- Site resource
- SOTN underlay

If this service is SD-WAN only, it only includes VPN resource and Site resource; if this is SOTN only, it only includes Site resource and SOTN underlay. If this is a cross layer service, then it will include all three resources.

One CCVPN scenario may contain only SD-WAN service, only SOTN service or combined service of SD-WAN and SOTN. These numerous options provide the required flexibility to end users. This task also includes DCAE template, Policy, SO workflow (BPMN), and SDN-C Directed Graph (DG) design.

Once the design phase is complete, the various artifacts are automatically distributed to the right runtime component of ONAP, and the user does not have to take any special steps. ONAP uses a sophisticated set of algorithms, independent of the CCVPN blueprint, to distribute the right artifact to the right runtime software component.

After the artifacts have been distributed to the right component, runtime processes take over. Runtime deployment is triggered via the ONAP Portal application called the Use Case UI (UUI). The service orchestrator (SO) and its virtual function controller (VF-C) and SDN controller (SDN-C), jointly complete initial deployment and subsequent lifecycle management. The end to end CCVPN service is broken down into the four respective services described above. Each of these services is orchestrated first;

API calls are also made to the partner ONAP for orchestrating these services in the partner's network. Subsequently, the end to end CCVPN service is orchestrated. Many of the 30 projects in ONAP and 3rd party software components interact with the CCVPN blueprint (a full discussion is outside the scope of this document). In fact, VF-C and SDN-C depend on third-party SOTN and SD-WAN controllers for deployment and lifecycle management of specific VNFs and DCI (DC interconnection) network connections as well as third-party EMSs for VNF configuration and monitoring.

In summary, the end-to-end implementation is carried out in the following phases:

- **Phase 1:** CCVPN Service design
- **Phase 2:** CCVPN service creation within one ONAP
- **Phase 3:** Cross-Carrier Service Creation

Once the service deployment is complete, the Data Collection Analytics and Events (DCAE) software configures data collectors for monitoring. In the CCVPN blueprint, the network is monitored through the SOTN controller and SD-WAN controller. Events are sent by DCAE to the alarm correlation engine — Holmes. Holmes collapses two failure alarms for the same event into one and generates an event that then triggers a policy to execute a reroute or bandwidth adjustment event. The self-healing action calls SO to take the appropriate action.

CCVPN enables the CSP to support two types of service functions to its customers:

- Basic VPN service between sites, where the number of sites and the bandwidth among them could be adjusted dynamically.
- Value-added services like AI apps, which could be part of the initial service procurement before its creation or added on demand to a running service instance.

Several ONAP projects such as SDC, SO, UUI, External API, Policy and Holmes are enhanced to support this blueprint.

Summary

ONAP is used to design, deploy, monitor and manage the lifecycle of a complex end to end CCVPN service. The key point demonstrated by CCVPN is the peering of ONAP across CSPs. The CCVPN blueprint uses production-ready VNFs, SDN controllers and VIM/NFVI software from commercial vendors.

Early test results, conducted by two ONAP Platinum members (Vodafone and China Mobile) in their labs, are promising: service deployment times are slashed from months to hours or minutes. Similarly, basic service assurance can be addressed in real time instead of minutes or hours. Hardware and network efficiency goes up, since services can be scaled up and down as needed. Finally, the operations and management burden is reduced through automation, helping CSPs move from a break-fix mentality to a plan-build process.

ONAP helps fulfill the promise of automation for end-to-end network-as-a-service through the CCVPN blueprint. Using ONAP to manage the complete lifecycle of the CCVPN blueprint brings increased agility and cross-domain connectivity for CSPs.

Resources

CCVPN blueprint wiki page