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

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 network-as-a-service
- Unified management and scheduling of resources and services
- ONAP SDN-C performs the role of OTN super controller

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, the 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 SOTN (Super high-speed Optical Transport 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

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 are not addressed by current solutions.

- Self-service
  - Self-service for client-side vCPE and cloud-side 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

- 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

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.

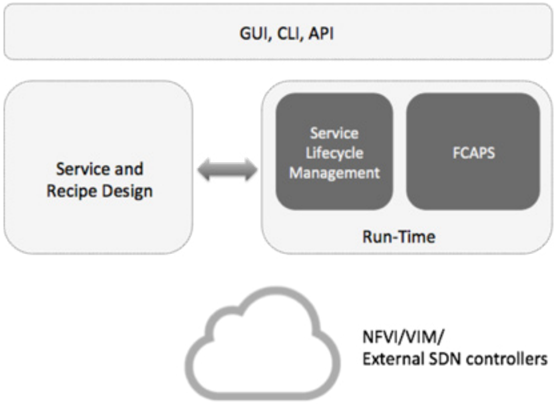

Figure 1: ONAP Functionality

ONAP Casablanca release 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 offers CSPs a path to production.

The functionality of CCVPN consists of the following:

1. CPE 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
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

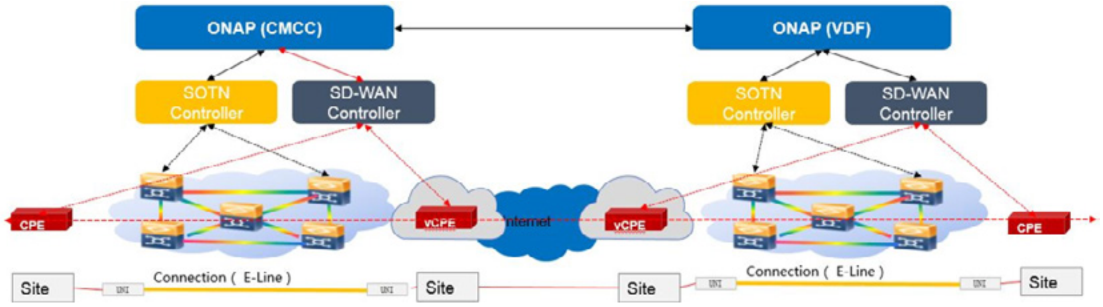

Figure 2: ONAP CCVPN Blueprint

Implementation Details

The CCVPN blueprint involves the following tasks:

- Service and resource on-boarding and design
- Service deployment and configuration with ONAP<-->ONAP communication
- Self-service adaptation (closed loop showing bandwidth on demand, subsequent release)
- Auto-scaling based on fault and performance (subsequent release)
- Fault detection and auto-healing (subsequent release)
- Data correlation and analytics (subsequent release)
- Service termination

During the onboarding and design phase, four services are created using SDC:

- SOTN VPN Infrastructure Service
- SD-WAN VPN Infrastructure Service
- Site DC Service
- Site Enterprise Service

One CCVPN scenario may contain one SOTN VPN Infrastructure Service, one or more each of SD-WAN VPN Infrastructure Services, DC Services and Site Enterprise Services. Likewise, each SD-WAN VPN Infrastructure Service can attach to more than one site. 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) or through a customer self-service portal. 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 are orchestrated; 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:** SOTN Orchestration
  - Single Domain
  - Multiple Domains
- **Phase 2:** Cross-Carrier Service Creation
- **Phase 3:** SD-WAN 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, both the VIM and VNFs are monitored. Events are sent by DCAE to the alarm correlation engine—Holmes. If Holmes detects two concurrent failure alarms as described above, it generates an event that then triggers a policy to execute the self-healing action. The self-healing action calls VF-C (which in turn calls external VNFMs) to restart the VNF instances as appropriate.

Several ONAP projects such as UUI, External API, Policy and Holmes had to be 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 results (from the tests conducted by China Mobile and Vodafone across their networks) are promising: service deployment times are slashed from months to hours or minutes. Similarly, service assurance can be addressed in real time instead of minutes or hours. Hardware 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