CABLE ACCESS NETWORK VIRTUALIZATION

HEADEND RE-ARCHITECTED AS A DATA CENTER

A Technical Paper prepared for SCTE/ISBE by

Ruobin Zheng
Cloud Networking Chief Researcher
Huawei Technologies Co.,Ltd.
Huawei Headquarter, Bantian, Longgang District, Shenzhen, China
(86) 075528978020
zhengruobin@huawei.com

Wenle Yang
Senior Engineer
Huawei Technologies Co.,Ltd.
Huawei Headquarter, Bantian, Longgang District, Shenzhen, China
(86) 075528977366
yangwenle@huawei.com

Table of Contents

List of Figures

List of Tables

Introduction

A significant rise in the number of diversified services and applications has promoted the rapid development of the broadband industry. With the continuous rollout of new services, such as 8K video and virtual reality (VR), the access bandwidth starts to move from megabit to gigabit. Multiple system operator (MSO) networks face lots of challenges as they try to match the diverse set of service requirements and service characteristics.

1. Management Complexity for Multi-service and Multi-access

MSO networks are migrating to support full services that cover residents, enterprises, mobile backhaul, and wholesale services. With the rise of new services (e.g. 4k, 8k, VR) and the trend of Internet of Things (IoT) and Fifth-generation (5G), service requirements may further include extreme broadband, ultra-low latency, massive connections and ultra-high reliability, which impose strong demands on the access network.

Besides, the new technologies further introduce massive remote nodes. While the cable access network architecture migrates to the distributed mode, the number of standalone remote nodes will scale up greatly. This growth in standalone remote nodes and the need to separately manage them will lead to a longer Time to Market (TTM) and complex Operations and Maintenance (O&M).

2. Scalability and Energy Efficiency in Remote Nodes

In the IoT and 5G deployment scenario, many access elements are widely distributed in outdoor facilities. One of the performance targets is ultra-low energy consumption. These new low-power remote nodes need to be as simple as possible especially as it relates to Operations, Administration and Maintenance (OAM) and a long service life.

Considering the complexity of the IoT network and the heterogeneous network, the remote nodes will need to handle various protocols. With all of these functions, the remote nodes will become very complex, making it hard to meet the requirements mentioned above.

3. Big Gap between Slow Network Evolution and Rapid Service Innovation Requirements

Regarding the traditional way for new service provisioning, a variety of access devices need to be separately configured and may even require hardware changes. In addition, network topology, vendor switch model, and software version all must be taken into account. Especially when many access elements are widely distributed in outdoor facilities, it is not easy to touch all of them. That means the current “rigid” network is extremely hard to evolve to the next generation and will lead to a fairly long time to market for new services.

4. Sharing Difficulty of Access Network

The current methods for sharing the access network (e.g. bitstream), where service packages are only differentiated by bandwidth and few configurable options, limits the ability to provide more advanced features which in turn limits richer service differentiation.

Traditionally, retailers and service providers have only had a limited capability to monitor, control and manage access resources. As access technologies advance, resources that can be accessed by a third party become increasingly more programmable and feature rich, which brings advantages but also introduces an increased risk that network harm could occur if controls are not exercised properly. It can also be time-consuming for retailers and service providers to do service provisioning. The infrastructure provider usually has to deal with a large range of varying requirements from retailers and service providers, which makes it difficult to do network planning or perform technology changes in a timely manner.

To meet the rapid growth of traffic and connections, access to the Headend requires fiber, and the network needs to be more flat. With respect to the challenges and changes in the access network, this paper explores cable access network virtualization with Software Defined Networks (SDN) and Network Functions Virtualization (NFV) technologies, which aim to provide a more flexible and future-proof access network. The network will be transformed into a data center-based architecture, and network functions and services will run in the cloud. Considering some strong demands such as the low latency requirements for 4K / 8K / VR video and the Internet of things (IoT), the data center is expected to move from the clouds down to the Headend where it is closer to the end devices.

With the concept of re-architecting the Headend as a data center, a Programmable Virtual Converged Cable Access Platform (VCCAP) is introduced as a cloud-oriented access network solution. The following content will give a detailed description of this solution, which includes a high-level virtualization architecture and its important components, with the benefits embodied.

High-level Architecture of Cable Access Network Virtualization

By introducing SDN and NFV, the proposed programmable virtual CCAP is based on the high-level architecture of cable access network virtualization. This is depicted in Figure 1. IoT, 5G, Fiber to the Distribution Point (FTTDp) and distributed CCAP are displayed as the example access modes.

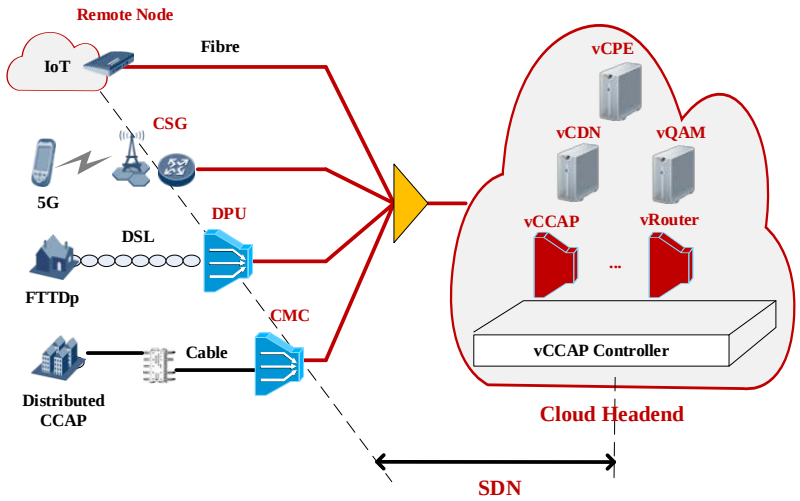

Figure 1 - High-level Architecture of Access Network Virtualization

The main concept is that of a centralized controller for a virtual access network. Based on the separation of control plane and forwarding plane, the control plane of the remote node is relocated and centralized in a virtual CCAP (vCCAP) controller. The vCCAP controller can also act as a vCCAP Hypervisor implementing access-network abstraction and slicing to make multi-tenant and multi-service operation in one physical network. The vCCAP controller can be located in a Headend/Hub which can be deployed as a cloud platform or in other words be re-architected as a data center.

The vCCAP application running on top of the vCCAP controller will be discussed in details in the following section. Customer premises equipment (CPE), Content Delivery Network (CDN), Router, and Quadrature Amplitude Modulation (QAM) can also be virtualized in the data center at the Headend. The vCCAP controller talks to the remote nodes through a southbound interface, and also provides an open northbound interface, e.g. open Network Application Programming Interface (API).

With the control and data planes decoupled, the remote nodes are able to be decoupled from services and applications and become dummy but programmable devices which include a programmable forwarding plane. Thus, long-tail service TTM can be accelerated and the need to upgrade all remote nodes can be eliminated.

Thanks to this centralization of intelligence, remote nodes can become plug & play, and will automatically register to, and be controlled by, the vCCAP controller in the Headend. This virtualized access network architecture can greatly reduce Operating Expenses (OPEX) and facilitate new service innovation.

Virtual CCAP

5. Concept of vCCAP and virtual line

A vCCAP is a logical entity that represents a physical node or a part thereof. Each vCCAP has a group of virtual lines, which represent a group of physical lines connected to the corresponding physical CCAP. Similar to the physical line identification (ID) which identifies the physical line, the virtual lines are identified through a virtual line ID.

Figure 2 shows an example of a vCCAP, which represents one physical remote node (e.g. Cable Media Converter (CMC)). The vCCAP interfaces represent the user-side interfaces of the physical node. The activation of the vCCAP includes:

- When a remote node is up, a vCCAP will be automatically generated in the vCCAP Controller.

- vCCAP will automatically get a management IP address for itself.

- vCCAP initiates self-configuration and self-service provisioning to support remote node plug & play.

- Future new functions or protocol enhancements can be implemented in vCCAP without the need to upgrade the physical remote nodes.

- vCCAP can support protocol conversion between Layer 3 (L3) (e.g. Simple Network Management Protocol (SNMP) / NETCONF / File Transfer Protocol (FTP)/ Common Open

Policy Service Protocol (COPS) / OpenFlow) and Layer 2 (L2) (e.g. ONU management and control interface (OMCI) / Ethernet Operations, Administration, and Maintenance (OAM)).

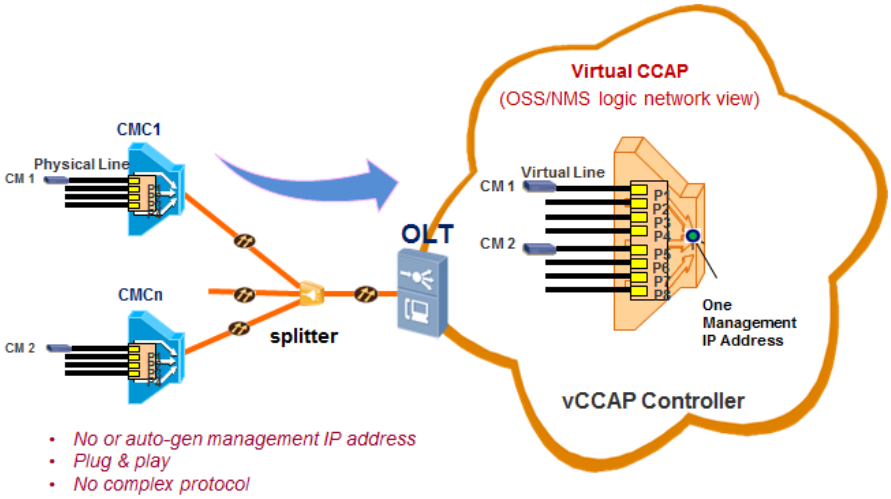

Figure 2 - Overview of vCCAP

The management systems only sees the vCCAP. The vCCAP hides the actual details of the underlying access network infrastructure. A vCCAP allows the physical remote node to be simplified through three aspects:

- The absence of a management IP address or an auto-generated management IP address;

- Plug and play;

- No complex L3 and above protocols, e.g. SNMP/NETCONF/FTP/COPS/Openflow, is possible.

6. Two types of vCCAP

Physical nodes in the cable access network can be combined or segregated to form different vCCAPs. Two types of vCCAP are identified based on different granularity of slicing and abstraction, e.g. per node or per port. In both cases there exists a mapping between physical line IDs and virtual line IDs which are maintained by the vCCAP controller.

Figure 3 describes Type 1 vCCAP where the vCCAP represents one or more than one physical nodes. For example, Remote Node 1 is mapped to vCCAP 1, while Remote Node 2 and Remote Node 3 are mapped to vCCAP 2.

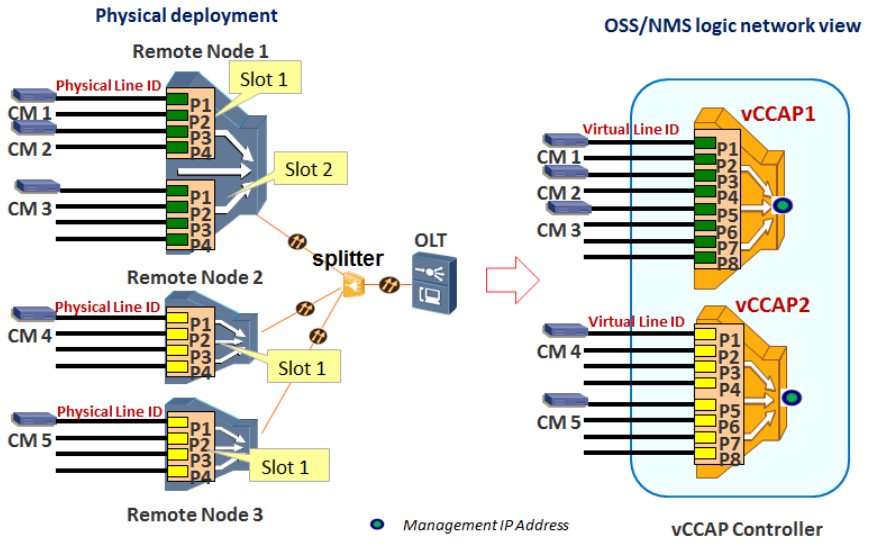

Figure 3 - Type 1 vCCAP

Table 1 shows the mapping between physical line ID and virtual line ID for Type 1 vCCAP described in Figure 3.

Table 1 - Line ID Mapping Table for Type 1 vCCAP

Physical Line ID	Virtual Line ID
Remote node1/slot1/port1	vCCAP1/port1
Remote node1/slot1/port2	vCCAP1/port2
……	……
Remote node1/slot2/port1	vCCAP1/port5
……	……
Remote node1/slot2/port4	vCCAP1/port8
Remote node3/slot1/port1	vCCAP2/port1
Remote node3/slot1/port2	vCCAP2/port2
……	……
Remote node2/slot1/port1	vCCAP2/port5
……	……
Remote node2/slot1/port4	vCCAP2/port8

Figure 4 describes Type 2 vCCAP where the vCCAP represents more than one physical interface on more than one physical node. The interfaces of one remote node are assigned to different vCCAPs, and some interfaces may not be mapped into any of the vCCAPs.

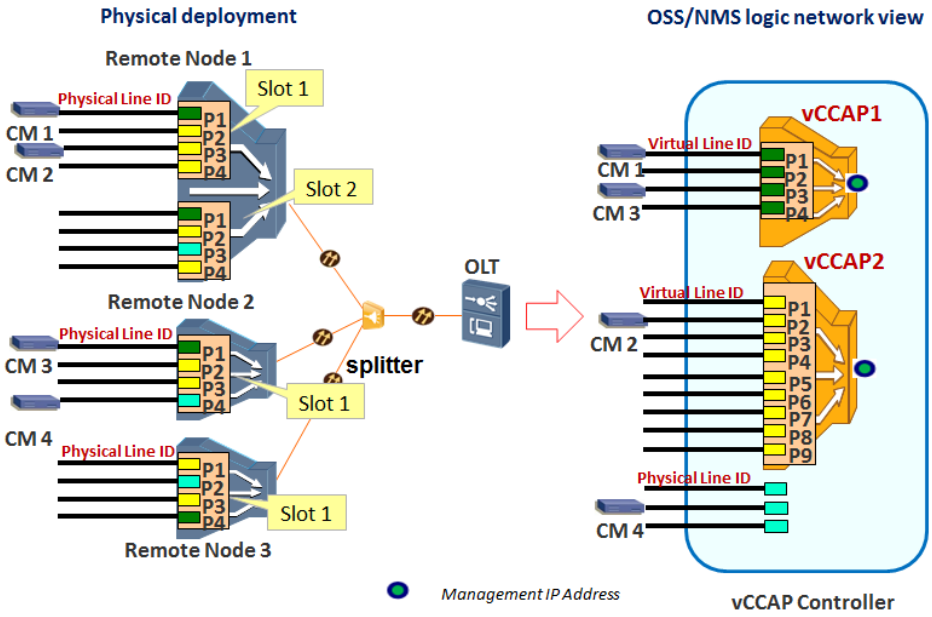

Figure 4 - Type 2 vCCAP

Table 2 shows the mapping between physical line ID and virtual line ID for Type 2 vCCAP described in Figure 4.

Table 2 - Line ID Mapping Table for Type 2 vCCAP

Line ID Mapping Table

Physical Line ID	Virtual Line ID
Remote node1/slot1/port1	vCCAP1/ port1
Remote node1/slot2/port1	vCCAP1/port2
Remote node2/slot1/port1	vCCAP1/port3
Remote node3/slot1/port4	vCCAP1/port4
Remote node1/slot1/port2	vCCAP2/port1
Remote node1/slot1/port3	vCCAP2/port2
Remote node1/slot1/port4	vCCAP2/port3
Remote node1/slot2/port2	vCCAP2/port4
Remote node1/slot2/port4	vCCAP2/port5
Remote node2/slot1/port2	vCCAP2/port6
Remote node2/slot1/port3	vCCAP2/port7
Remote node3/slot1/port1	vCCAP2/port8
Remote node3/slot1/port3	vCCAP2/port9

Unmapped Physical Ports

Physical Line ID
Remote node1/slot2/port3
Remote node2/slot1/port4
Remote node3/slot1/port2

By slicing and abstracting the physical cable access-network into multiple vCCAPs, the infrastructure provider can support network-sharing for other operators (e.g. retailor) or implement multiple services in one physical access network. The vCCAP and its virtual lines can be controlled and managed by a service provider or a retailer without the need to be aware of changes to physical nodes or physical lines in the

infrastructure network. Security in the infrastructure network can be enhanced, and an easier and more efficient way for the service provider or the retailer to manage their user ports is possible.

Type 1 vCCAP has natural isolation of both forwarding plane and control plane between physical nodes. Only a software upgrade is required during the migration to multi-operator or multi-service sharing in one physical device. It can be deployed in both brown field and green field deployments.

For Type 2 vCCAP, both forwarding resource and control resource of each port have to be isolated in a device. A hardware upgrade may be needed in order to migrate to multi-operator sharing in one physical device. Type 2 vCCAP may only be deployed in a green field deployment.

Access Network Function as a Service

As illustrated in Figure 5, each vCCAP can have a subset of network functions to support different service requirements. These functions can be allocated by vCCAP controller based on the full function set of the infrastructure network. The network function set in each vCCAP can be defined by the infrastructure provider based on the service requirements and the capability of the infrastructure network.

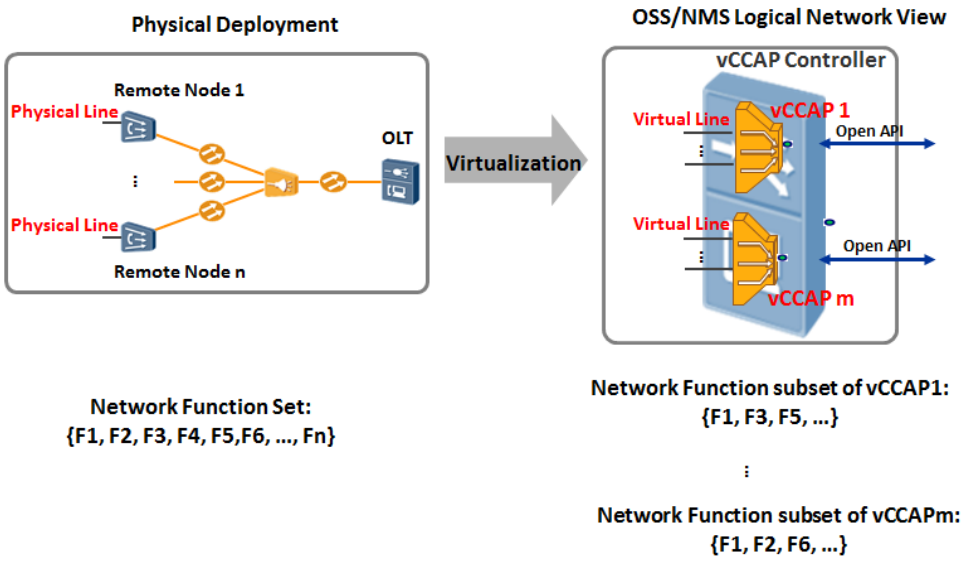

Figure 5 - Access Network Function Virtualization and Allocation

The virtualized access network functions include network functions of the access nodes. They can be functions in the control plane or the data plane. Example functions could be Quality of Service (QoS) policies, filtering, multicast group control, authentication, authorization and accounting, and dynamic address provisioning. The granularity of the network function is flexible so that several functions can be combined into a bigger one and made available as a service.

The access network function as a service can be further illustrated by the following example, where we make the assumption that the infrastructure network has the capability to support the service requirements.

The example assumes that there are requirements for the deployment of mobile backhaul services and residential services, and the infrastructure provider plans to allocate two vCCAPs based on the same physical access network to perform the service deployment. Based on the requirement of mobile backhaul service, the network function subset assigned to one vCCAP can include the clock synchronization function, the Multi-Protocol Label Switching (MPLS) forwarding function, and the IP/MPLS signaling function. Similarly, based on the requirement of residential services, the network function subset assigned to the other vCCAP can include the Authentication, Authorization and Accounting (AAA) authenticator/proxy function, the Dynamic Host Configuration Protocol (DHCP) relay/proxy function, the Internet Group Management Protocol (IGMP) proxy/snooping function and the flow classification and QoS mapping function. Then the two types of services can be provisioned through the two vCCAPs separately yet based on the same infrastructure.

Thus, the network virtualization has the potential to turn traditional access network sharing into Network as a Service (NaaS), which enables:

- Faster time to market and the rollout of new services
- Multi-instance virtualization of access networks

A flexible sharing mode is enabled for the multi-tenant scenario, where the infrastructure operator owns, maintains and virtualizes physical access network resources, while the service operators or third parties can operate, control and manage their assigned vCCAPs and provide differentiated services. This network virtualization is also appropriate for a network operator that wants to slice its access network in order to offer a multi-service solution in one physical network for customers (e.g., for residential, enterprise or mobile backhaul markets) and wants to be able to use a vertical organization structure for aspects related to customers, services and resources.

Programmable vCCAP Reference Architecture

Based on the access network virtualization, Figure 6 shows a detailed reference architecture of the programmable vCCAP. With a vCCAP controller, the programmable vCCAP disaggregates CCAP devices, virtualizes CPE and CCAP control and management functions into the cloud, and distributes Data-Over-Cable Service Interface Specifications (DOCSIS) processing to the remote node.

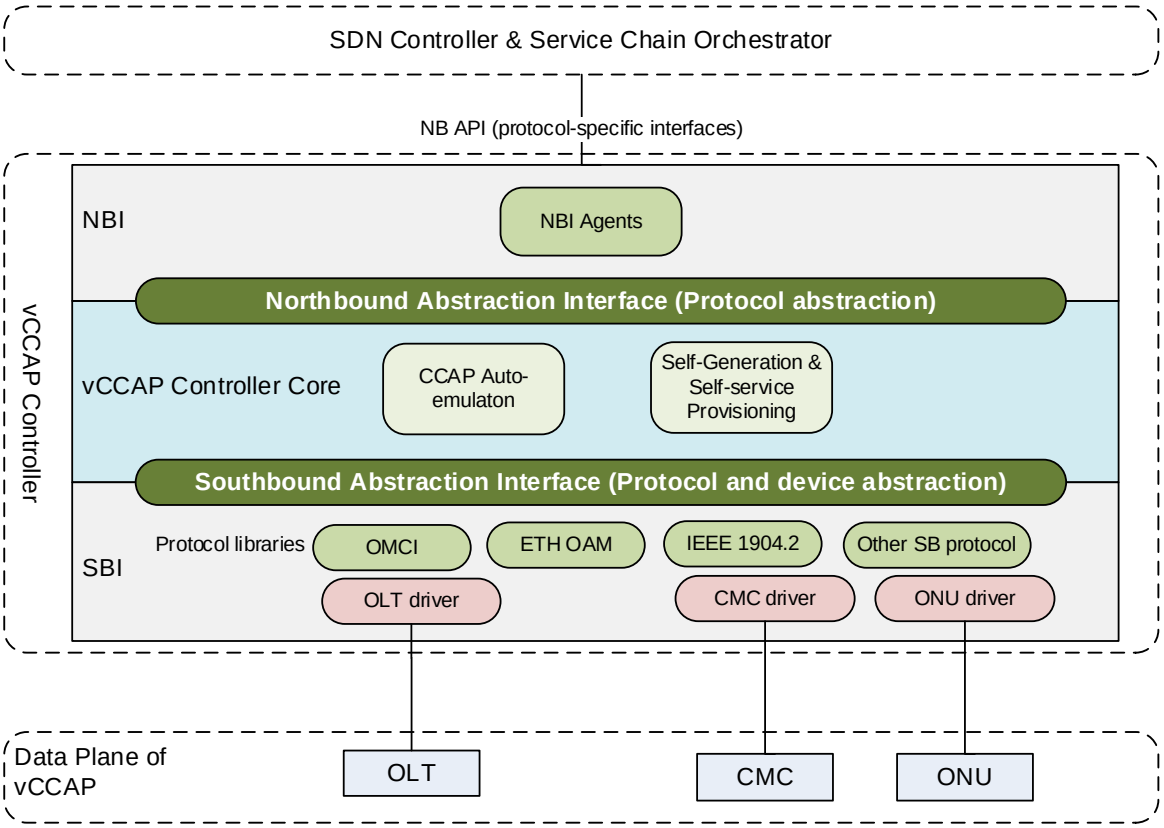

Figure 6 – Programmable vCCAP Reference Architecture

A three-layer architecture is proposed, which consists of an infrastructure layer, a control layer (including vCCAP controller, SDN controller and Service Chain Orchestrator), and an application layer. The vCCAP Controller, which is software running in the cloud, controls and manages the physical devices (e.g. CMC and optical line terminal (OLT)) in the infrastructure layer through the southbound interface (SBI), and the northbound communicates with the SDN controller and Service Chain Orchestrator. The SDN Controller allows applications to tailor network behaviors to suit their needs, and the Service Chain Orchestrator can program services instead of re-architecting the infrastructure layer and the management system for every new service.

Two functions of CCAP Auto-Emulation and vCCAP Self-Generation & Self-Service Provisioning are introduced in the core of vCCAP controller.

The CCAP Auto-Emulation function abstracts and represents the underlying distributed access network elements (e.g. OLT, CMC or Optical Network Unit (ONU)) as one integrated monolithic CCAP, and performs the conversion between this abstract view at the northbound interface (NBI) and the management, configuration, reporting and alarming functions for each of the physical devices at the SBI, which hides the device level details. Different access technologies can be enabled without modifying the existing MSO configuration and management system.

For details, the control and management system configures the forwarding entries for the data plane of the vCCAP without needing to be aware of the access devices' details or the specific access technologies.

Based on some decomposition policies, the CCAP Auto-Emulation function translates the forwarding entries' commands into the forwarding entries of the corresponding access devices (which can be OLTs) and its remote nodes (e.g. CMCs or ONUs), and maps the ingress/egress ports of the vCCAP to the ingress/egress ports on the physical devices.

The vCCAP controller's SBI contains device driver plugins that support communication with the access devices in the network. Device driver plugins, which may be device-specific or generic device drivers, may use southbound protocol libraries provided as common resources, or they can embed their own protocols as needed. Thus, a protocol conversion between layer 3 and layer 2 can be realized by the vCCAP controller, with the purpose of keeping remote nodes as simple as possible (e.g. only layer 2 devices) and leaving the complexity to the vCCAP. By receiving messages with layer 3 protocols such as NETCONF, SNMP, and OpenFlow, the vCCAP controller can use layer 2 protocols in the southbound direction with respect to specific access scenarios such as OMCI for Passive Optical Network (PON), or Institute of Electrical and Electronics Engineers (IEEE) 1904.2 for IoT, 5G, Ethernet 802.3, WiFi etcetera.

With the other module of vCCAP Self-Generation and Self-Service Provisioning in the vCCAP Controller Core, a physical access network can be sliced and programmed into multiple vCCAPs by using machine learning technology. Multi-service or new services can be automatically provisioned through different vCCAPs with different subsets of network or service functions separately under the same physical access network. Thus, it has the ability to turn the traditional business model into NaaS, lower the OPEX and accelerate service innovation and delivery.

Intelligent vCCAP Self-Generator

To create a vCCAP, the main challenges observed are as follows:

- The Operators are usually not aware of what and how many network resources, e.g. the network functions and the service functions are exactly required by the vCCAP, and how to map the virtual resources to the physical resources of the infrastructure. Especially for the service providers who need to lease the virtual resources from the infrastructure provider, it is a waste if their vCCAPs are assigned with spare resources for worst case.

- Facing competition from the OTT providers, the Operators have to speed up the service Time-to-market. Manual upgrade of a vCCAP when service requirements change will lead to a long service deployment time and high OPEX.

With the above considerations, an operation mode of the vCCAP on demand is explored. The Programmable vCCAP system provides an intelligent vCCAP self-generator that allows the vCCAP to be generated automatically based on the abstracted service requirements, as depicted in Figure 7.

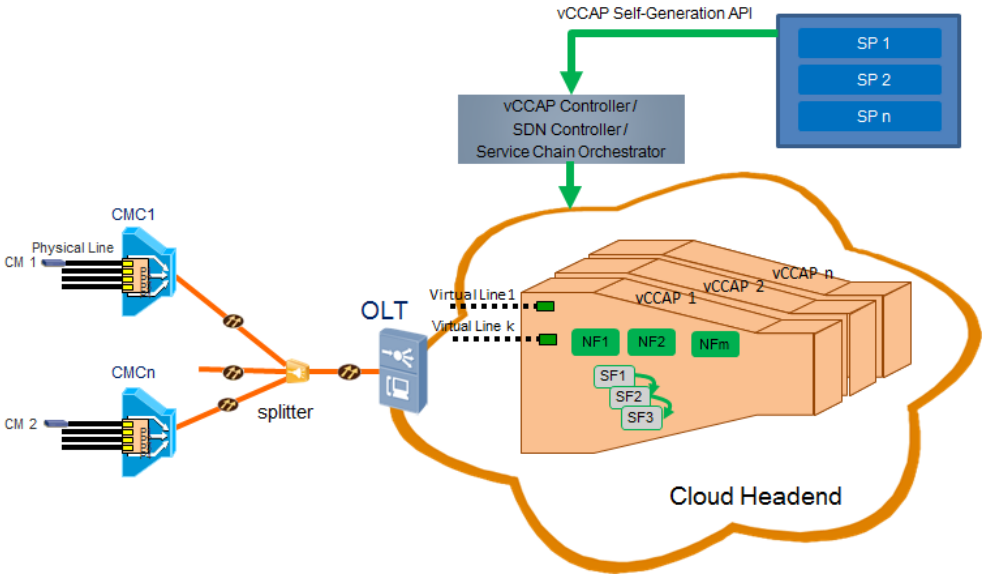

Figure 7 - Intelligent vCCAP Generation

According to business needs, the service provider presents the abstracted requirements through the vCCAP Self-Generation API. For example, a service provider that offers mobile services, requests a vCCAP to provide mobile services at a cost that does not exceed X dollars. Another service provider that offers broadband services, requests a vCCAP to provide broadband services at a cost that does not exceed Y dollars.

When the control system that consists of the vCCAP controller, SDN controller, and Service Chain Orchestrator receives the above requirements, it analyzes these abstracted requirements intelligently, and translates the abstracted requirements into network provision requirements.

In the case where vCCAPs are created for mobile services, the control system may allocate a time synchronization function, protection function and guaranteed bandwidth resources, such that, the total cost of all network resources is no higher than X dollars. On the other hand, for a vCCAP that provides broadband services, it may allocate resources for IGMP multicast network function, best-effort bandwidth resources and parental control service function, such that, the total cost of all network resources is no higher than Y dollars.

The cost of the network resources is determined by a QSN model, which consists of three items, namely, QoS, service function, and network function, as depicted in Figure 8.

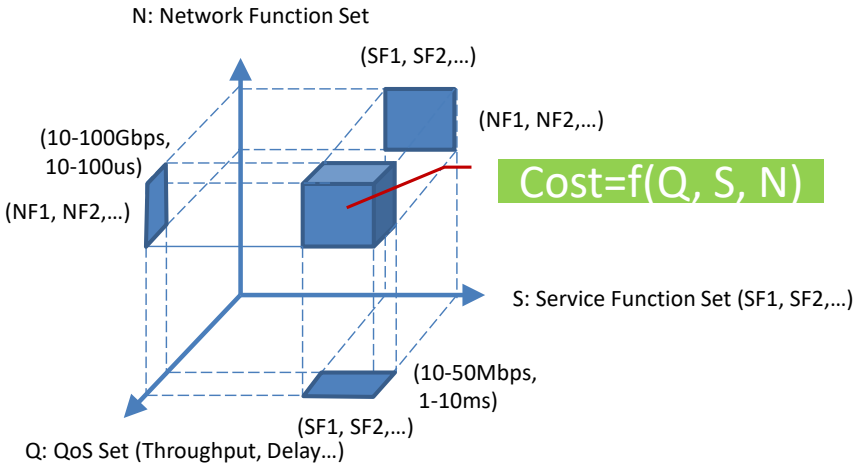

Figure 8 - QSN Model

To be more concrete, Figure 9 shows the principle of the intelligent vCCAP self-generator.

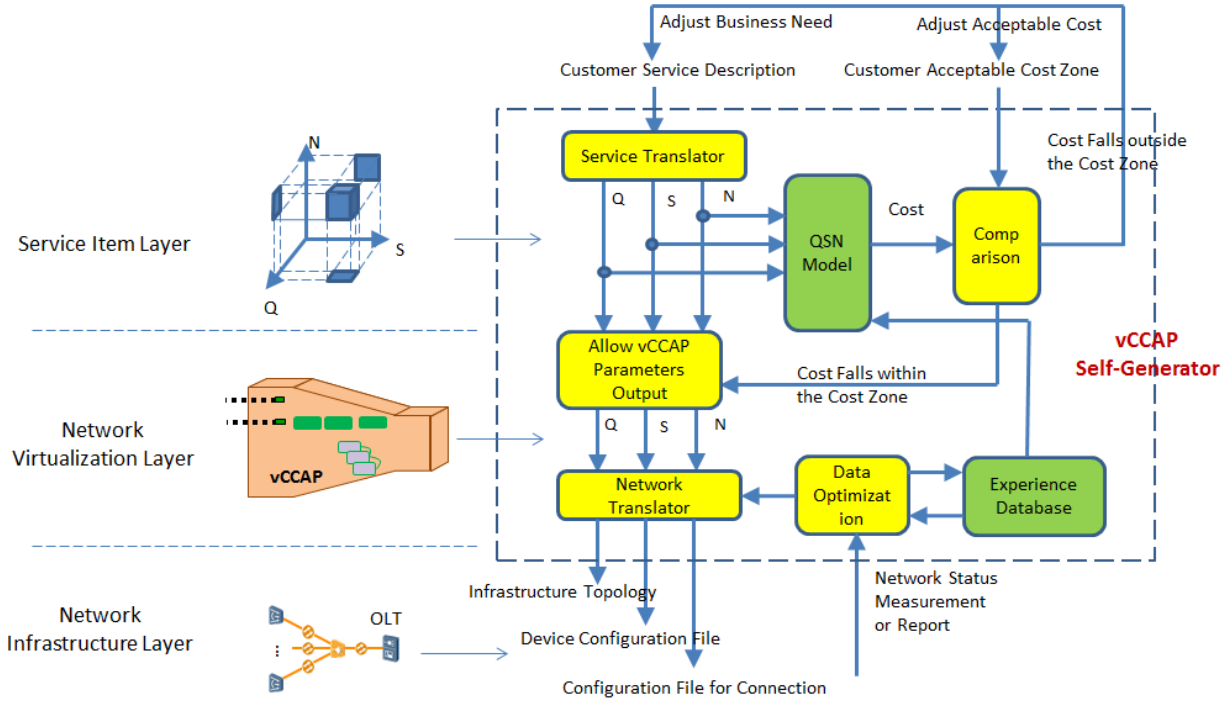

Figure 9 - Intelligent vCCAP Self-Generator Principle

A service translator translates the customer service description into vCCAP QoS (Q) requirements, service functions (S) and network functions (N). Based on the three items, a total cost for the deployment of the vCCAP is obtained by the QSN model, which is then compared with the customer's acceptable cost zone. The service provider can adjust the business needs or the acceptable cost zone to achieve a final agreement if it is necessary. Once the cost is acceptable, a vCCAP with the necessary virtual resources will be generated automatically, and a network translator will translate the QSN parameters for

infrastructure layer deployment. The infrastructure can use pure physical devices, or a mix of physical devices and virtual machines/containers running on a server. In order to enhance the intelligence of the service and network translation, a data optimization module is introduced, which uses machine learning technology and collects data from an experience database, and network status measurements or reports.

With vCCAP intelligent self-generation, the infrastructure provider can be more focused on the network infrastructure and build more functional networks to meet the needs of a richer business, while simplifying the service provider's network knowledge; the service provider's business needs can be automatically converted into network deployment.

The Value Proposition of Programmable vCCAP

The cable access network will benefit a lot with network virtualization. The key values that Programmable vCCAP can bring are summarized as follows.

7. Simple, Green and OPEX reduction

Being re-architected as a data center, the Headend can have a common infrastructure with commodity building blocks. Since the intelligence of remote nodes, e.g. complex control and management plane, is relocated to the vCCAP controller, the remote nodes can be simple and green devices without the need to support complex protocols, especially in the scenario of IoT and 5G.

Furthermore, the operator's configuration and management systems usually only need to maintain the IP address for each vCCAP instead of the IP addresses for all remote nodes. The remote node is either IP address-free or gets an auto-generated management IP address. The IP address configuration and maintenance can be simplified.

Plug and play of remote nodes is also enabled. When a network provider wants to deploy a new remote node, e.g. CMC, in the cable access network, the engineer on site installs a remote node, powers it up and connects its uplink, which comes from Headend or Hub. There is no need for the engineer to configure any parameters on the remote node, which automatically registers and connects to the vCCAP Controller. Therefore, the process of remote node installation and network configuration are simplified, and OPEX is further reduced.

8. Smooth Migration

Future access networks will have to support a whole set of technologies including DOCSIS, PON, active Ethernet, WiFi, Long-Term Evolution (LTE), 5G etcetera. Access network virtualization assures the integrity of multi-service, multi-access, diverse customized modes into a unified access network. This allows the network engineers to ignore the changes in access network topology, leading to a smooth migration from current network to a virtual access network.

Access network virtualization can abstract the common model of DOCSIS management and service provisioning. In this way, the architectural differences of traditional integrated CCAPs and distributed CCAPs can be isolated. MSOs can architect the Headend/Hub with commodity software and hardware building blocks without the need for dedicated hardware at the CCAP Core, and only leave DOCSIS MAC and PHY at remote nodes. Thus, it enables the smooth migration and transformation from Communication Technology (CT) to Internet Technology (IT) solution in cable systems. With access

virtualization technologies, coexistence and smooth migration with respect to the traditional integrated CCAP and distributed CCAP can be enabled, without impacting the MSO's configuration and management systems.

9. Network Innovation Acceleration

Thanks to the access virtualization, the remote nodes are reduced to mere programmable devices and thus decoupled from services, while the complex control and management planes are relocated to a centralized vCCAP. Remote nodes are only responsible for traffic forwarding, which minimizes complex protocol applications and configuration.

The vCCAP controller can help to build a future-proof access network that eliminates the need for hardware and software upgrades in remote nodes. With a programmable forwarding plane, the remote node is flexible and can easily cope with any subscriber session, while meeting requirements for Layer 2/Layer 3/MPLS forwarding, IPv4-to-IPv6 migration or future forwarding mechanisms. New services can be easily introduced into the cable access network, and therefore service innovation is accelerated.

10. Value-added: NaaS

Access network virtualization enables the migration from bitstream mode to a wholesale mode aka "virtual access network as a service". That means a physical cable access network can be virtualized into multiple virtual access networks, and each virtual access network can be wholesaled and be controlled and managed by third party retailers. It enables operators to break free from the simple, low-margin pipe wholesale models of the past through its support of differentiated access network offerings. In addition, MSOs can support the deployment of multi-service offerings in one physical access network, and meet the differentiated needs on the access network from different industries.

Conclusion

The rapid growth and the need for emerging requirements such as multi-access, multi-tenant and multi-service sharing in one physical network place a burden on legacy access network architectures, which find it hard to accommodate all these new technologies. In the cloud era, the access network will be transformed into a data-center based architecture. Network functions and services will run in the cloud. The Programmable vCCAP is a cloud solution with a future-proof access network architecture, which is expected to lead the way in access network evolution.

Abbreviations

5G	Fifth-generation
AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
CCAP	Converged Cable Access Platform
CDN	Content Delivery Network
CMC	Cable Media Converter
COPS	Common Open Policy Service Protocol
CPE	customer premises equipment

CT	Communication Technology
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data-Over-Cable Service Interface Specifications
FTP	File Transfer Protocol
FTTDp	Fiber to the Distribution Point
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IoT	Internet of Things
IT	Internet Technology
LTE	Long-Term Evolution
MPLS	Multi-Protocol Label Switching
MSO	Multiple System Operator
NaaS	Network as a Service
NFV	Network Functions Virtualization
O&M	Operations and Maintenance
OAM	Operations, Administration, and Maintenance
OLT	optical line terminal
OMCI	ONU management and control interface
ONU	Optical Network Unit
OPEX	Operating Expense
PON	Passive Optical Network
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
SDN	Software Defined Network
SNMP	Simple Network Management Protocol
SP	service provider
TTM	Time to Market
vCCAP	Virtual CCAP
VR	Virtual Reality

Bibliography & References

OpenFlow Switch Specification Version 1.3.5, Open Networking Foundation, https://www.opennetworking.org/.

Future access architecture: Software-defined accesss networking, Ruobin Zheng; Wenle Yang ; Jun Zhou, Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, DOI: 10.1109/CCNC.2014.6940517, 2014 , Page(s): 881 – 886.

H-MPLS: A lightweight NFV-based MPLS solution in access network, Ruobin Zheng ; Wenle Yang, Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, DOI: 10.1109/CCNC.2014.6940485, 2014 , Page(s): 887 - 892

G.984, Gigabit-capable Passive Optical Networks (GPON), ITU-T, 2003.

G.988, ONU management and control interface (OMCI) specification, ITU-T, 2010.

Technical Report, SDN Architecture for Cable Access Networks, Cablelabs, June 2015

