SDNized CABLE ACCESS NETWORKS

Karthik Sundaresan
CableLabs

Abstract

Software-Defined Networking ideas are showing a lot of value in the networking industry. SDN can transform cable access networks and simplify MSO operations.

This paper introduces an SDN architecture for Cable access networks. Data Models and South Bound Protocols are foundational tools upon which an SDN architecture is built. The controller can configure and manipulate network devices dynamically while the operator focuses on developing the services to be delivered. This architecture will apply to any underlying access technology such as DOCSIS, EPoN etc.

INTRODUCTION

Software defined networking is an evolutionary concept whose time has come. In computer programming, the focus shifted from initially writing machine-level code, then moving on to assembly language code and then progressively moving on to higher-level languages. That way programmers didn't have to worry about machine level details and instead focused on developing the algorithms and applications.

Similarly, networking is transitioning now from using manual device level commands (via CLI, etc.) for setting up the network device and the path, towards higher levels of abstraction in an SDN world, where the network and the services on top of it can be programmatically configured in a software-defined way.

SDN ideas are showing a lot of value in the networking industry. Networks are being made more programmable and are becoming virtualized. While there has been significant focus on SDN in core and data center networks, it will also provide significant benefits in the access network. It will enable quicker deployment of new services, increase flexibility for MSOs, and reduce operational expenses.

BENEFITS OF SDN PARADIGMS IN AN ACCESS NETWORK

SDN concepts have taken root in Data center environments and other self-contained networks where the operator has full control of every device. The Cable Industry can make use of the new paradigms to make the access networks more efficient.

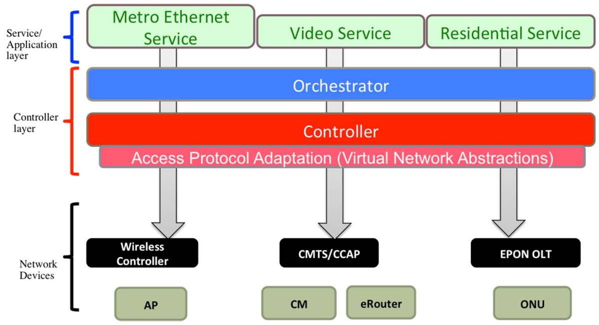
The DOCSIS Access Network is a great success story for the Cable Operators. IP High Speed Data (IPHSD) is the most important of services for the customers. Operators face a lot of challenges as the access network grows in size and the services offered over them increase day by day. Operators are managing huge numbers of devices, thousands of CMTSs and millions of Cable Modems, Set top boxes and eMTAs. The challenges of provisioning these devices, managing services, and creating interconnects becomes mind-boggling for an operator, requiring lots of people to manage and debug a network.

SDN techniques bring a new order to the chaos of service provisioning/management and streamline the MSO operations on a DOCSIS network. An SDN Controller becomes the device which talks to all the MSO network devices to configure the devices and to provision services on them. Today, operators use a disparate set of tools to manage the services on a network, including a separate vertical for provisioning and managing each new type of access technology, be it DOCSIS, EPoN or WiFi services. Services over DOCSIS need individual config files for each Cable Modem, which doesn't scale well as the number of service tiers increases. It especially doesn't scale when provisioning a service like an L2VPN circuit, where each CM needs a unique config file.

The SDN Controller will implement a common set of protocols to talk with different network devices. This allows the MSO to start focusing on creating better services to run as 'Applications' above the SDN Controller and let the controller configure or program each network device appropriately.

SDN ARCHITECTURE FOR CABLE ACCESS NETWORKS

SDN architecture for cable networks can be described in 3 layers. At the center, there is the SDN Controller. As described before this device is aware of and can talk to each of the network devices in the domain. The protocol used could be an industry standard protocol or it can be a specific protocol used by a particulare network device. This layer is shown as the Access Protocol Adaptation layer. The Adaptation layer essentially abstracts out the individual pieces of the network. The SDN controller takes the commands from the Application or service Layer and translates it to the specific devices in the network.



SDN Architecture for Cable Access Networks

Different parts of the network controlled by various SDN Controllers; the orchestrator is a higher-level entity that is used to orchestrate the services across those domains. On the top of it all sit the various applications the operator wants to deploy. In the access network, this could be IP HSD service, or L2VPN service, or setting up access for Third-party internet Access as a service.

This architecture allows for any device or access technology to be used in the access network and the same applications/services will be implemented seamlessly over each of those access networks. This is the true power of the network abstraction, which comes from the introduction of SDN and a controller device in the network.

The Access protocol Adaptation sub-Layer of a Controller is used to talk to each of network devices and it takes the form of a South-Bound Plugin on a controller device. The North-Bound programming interface used by the applications to talk to the controller becomes an NB API exposed by the controller.

The service/business logic interfaces are commonly referred to as "north-bound" of the controller, and the device-specific interfaces are referred to as "south-bound". The SDN controller exposes NB APIs to the applications; these are the "north-bound" APIs from the perspective of the SDN controller. The SDN controller enables programmatic interfaces to each of the network elements it controls, and this is the "south-bound" API.

DATA MODELS AND SOUTH BOUND PROTOCOLS

The two main enablers for a software programmable network are

- The configuration and statistics information, which is exchanged

between the SDN controller and each of the network devices
- The protocol, which carries the needed information.

An Information model or the data model needs to be developed for every network device that needs to be programmed. This data model will include all the data elements, like device settings or service settings, which need to be read by or written from a controller, to enable the devices and services across the network. It will include the elements needed to configure the device on boot-up (day-zero config). More importantly, the data model will also include the data elements which represent the creation of services over those network devices (dynamic-config).

The southbound protocol itself is independent of the data it carries back and forth. A suitable protocol choice would need to address both the day-zero config as well as the dynamic-config operations. The day-zero config requires a lightweight protocol, which is responsive to the needs of dynamic nature of setting up and tearing down of services.

For data modeling, YANG is the choice of the networking industry. NetConf and RestConf are the recommendations in terms of the protocol choices to carry the data back and forth from a controller to a network device. Any HTTP-based mechanism would also be a good choice as it is a simple stack that can be implemented by a variety of devices.

The Network Configuration Protocol (NetConf) is a network management protocol developed and standardized by the IETF (RFC 6241). It provides mechanisms to install, manipulate, and delete the configuration of network devices. Its operations are realized on top of a simple remote procedure call (RPC) layer. The NetConf protocol uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages. The protocol messages are exchanged on top of a secure transport protocol.

YANG is the data modeling language used to model configuration and state data manipulated by the NetConf protocol, remote procedure calls, and notifications. It is a "human-friendly" modeling language for defining the semantics of operational data, configuration data, notifications, and operations.

RestConf is a REST (Representational State Transfer) like protocol running over HTTP for accessing data defined in YANG, using data stores defined in NetConf. Currently it is an IETF draft that describes how to map a YANG specification to a RESTful interface. The REST-like API is not intended to replace NetConf, but rather to provide an additional simplified interface that follows REST-like principles and is compatible with a resource-oriented device abstraction.

USE CASES

IP HSD Service

High Speed Data (HSD) service is one of the most common services offered by an operator to end-users today. The current workflow for HSD using customer-provided cable modem is outlined as follows. The Customer Service Representative (CSR) is responsible for gathering customer and device information and entering that information into the BSS/OSS system. The current approach requires the CSR to be a middleman between the customer and network components such as BSS/OSS. One of the biggest issues faced by operators today is the static configuration of services using the CM configuration file. Anytime a new service is to be added, the operator needs to update the configuration file and reboot the CM. This is not scalable, causes outages, and also causes many mistakes.

An SDN controller can automate the tasks of a CSR. It will be an easy transition to an operation where managing CM configuration files becomes a thing of the past. All CMs will boot up with a basic configuration file, which essentially gets a CM online at a very low data tier. This allows the user to get online and pick his set of services from an MSO web portal. This portal interacts with the SDN controller, takes the list of services and translates them to commands to set up the services on the DOCSIS network. All the DOCSIS Service Flows, classifiers, and drop rules are set up dynamically by the SDN controller communicating with a CMTS. Essentially everything in the CM configuration file can be configured dynamically at run time. One of the big benefits of this method of operation is that whenever a user wants to change their level of service, they can do so at anytime.

L2VPN Service

MSOs offer L2VPN services to Business customers. L2VPN service is used mainly by businesses to communicate across geologically separate campuses. The process of ordering an L2VPN service on the DOCSIS network and setting up the network path from the cable modem is as follows. Currently, a new L2VPN service order requires a CSR to enter information into the BSS/OSS system. Upon receiving such an order, a network engineer will then configure the NSI path and will create a configuration file to be downloaded to the corresponding cable modems. One major issue with the current workflow model is that it comprises two disparate processes; the edge/core side where a pseudo-wire is configured and the access side where the CMTS-CM-CPE are located. This L2VPN setup takes time since separate organizations create and respond to work tickets, and this makes the process error-prone since it involves the manual exchange of data. An SDN controller improves the workflow by “orchestrating” the two sides of the network and eliminating manual interventions. The SDN controller can be used for such a service order and setup. Similar to the HSD use case, a web portal can replace the CSR and a corresponding SDN application configures the L2VPN path on the NSI side.

The SDN Controller improves the process by dynamically associating a service flow to an L2VPN pseudo-wire. This means that a cable modem does not need to be rebooted in order to activate an L2VPN service. The DOCSIS service flow would be brought up as a standard flow using the controller to talk to the CMTS via a southbound protocol (this could be PCMM) and the NSI side pseudo-wire would be set up using other commands from the controller to the appropriate device elements. The controller would bind the DOCSIS service flow to the pseudo-wire automatically, thereby achieving a dynamic setup of an L2VPN service.

Other Use Cases for SDN in the access network

The Cable operator handles various other services like setting up Internet Access for Third Party operators, Lawful Intercept for law enforcement agencies, Voice services, and Video services. In each of these services there are manual steps taken by a network engineer to set up some part of the service. All of these are candidates for automatic configuration, provisioning and management using a centralized SDN controller.

DOCSIS3.1 Profile Management

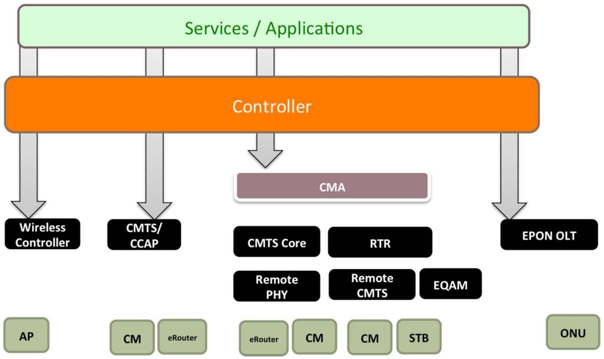
There is another class of applications that can be enabled by an SDN infrastructure which includes features that are part of the CMTS but not directly tied to the DOCSIS protocol. DOCSIS 3.1 introduces many new features into the access network. These include Variable bit loading and the use of multi-profile downstreams and upstreams, upstream probes to check the quality of the upstream OFDMA signal, etc.

The configuration, initiation logic and compute processing needed to optimize some of these functions (e.g., DS Profile setup or Load Balancing of CMs) are not a core part of the DOCSIS MAC and PHY layers itself. This allows such functionality to be moved out of a CMTS and implemented as an "application" running outside the CMTS. This application can communicate with the CMTS to gather the needed information, process the data, and make intelligent decisions to set up CMTS as needed. The various applications implemented externally communicate with the CMTS to optimize the overall network performance.

To realize this idea, again the basic steps are to develop the data models and a protocol to convey that information back and forth. As an example, to leverage the new OFDM PHY to its maximum benefit, different subcarriers use different modulation orders. Optimizing the downstream profiles will allow a downstream channe to operate with a lower SNR margin, potentially allowing a channel to operate at an overall higher throughput. The logic to achieve this can be external to a CMTS and enable innovation. For an operator, it allows uniform operation of such algorithms across different CMTS platforms. An SDN controller with the appropriate data models to represent the data, and the protocols to configure a CMTS and a northbound API to the application will enable such applications.

CCAP MANAGEMENT ABSTRACTION

The DOCSIS access networks can be integrated into an SDN world in many ways. The CMTS platform itself is evolving in the access network, from large CMTS devices to CCAP devices that are designed to provide increased EQAM and CMTS densities in a combined platform. There are also various Distributed CCAP Architectures being developed by the Cable industry. These architectures for the data transport side leave a router at the head-end and allow the CMTS MAC & PHY layers, or just the CMTS PHY Layer, to be moved down to a remote fiber node. Similarly, on the video side, all the EQAM functionality or the EQAM PHY layer can be moved to remote node.



CCAP Management Abstraction (CMA) Distributed CCAP Architectures

These various CMTS architectures can be tied into the MSO's SDNized network. The various pieces can be controlled and managed via a CCAP Management Abstraction (CMA) Layer. The CMA abstracts the various components of this distributed system into a single, cohesive CCAP platform for the OSS/BSS systems. The CMA is an application whose function is to create a container around a number of CMTS physical and virtual functions, and enable them to be managed and provisioned from existing back-office systems just like an integrated monolithic CCAP is today. Colloquially the CMA is also known as a Virtualized CCAP

APPLYING SDN ARCHITECTURE TO OTHER TYPES OF ACCESS NETWORKS

The SDN architecture described here for DOCSIS Access networks can be easily applied to other Access network technologies and pieces of network equipment on the MSO network. Take, for example, an EPoN deployment by an operator: the EPoN systems can be provisioned using the DPoE specifications. An SDN controller could essentially play that role of the DPoE System and a virtual Cable Modem, to take in DOCSIS Provisioning commands and translate them to EPoN specific commands, and send them to an existing EPoN OLT system.

In this way, legacy equipment with disparate provisioning systems can all be controlled via a Single SDN controller. Again, the key would be to create the needed data models for EPoN systems to make sure the application/service intents can be translated appropriately to the technology which is being configured. The protocol to talk from an SDN controller to the OLT could be something like RestConf or some other legacy protocol supported by the OLT, as long as the SDN controller can support that southbound protocol. This can apply to other access technologies as well, e.g., GPoN deployments, new services on top of DOCSIS or PON deployments, Wi-Fi AP provisioning and management, etc.

CONTRIBUTIONS TO OPENSOURCE CONTROLLERS

The industry needs to focus outward to the open source community, as that's where all the innovation and thought regarding SDN architecture are happening. One example is the Opendaylight (ODL) open source controller, which is an open platform for network programmability to enable SDN in networks of any scale. ODL software is a combination of components including a fully pluggable controller, interfaces, protocol plug-ins and applications. In the Helium release, the ODL platform has added a PacketCable MultiMedia plugin, which essentially enables the ODL controller to communicate to an existing CMTS platform using the COPS interface and the PCMM data protocol. CableLabs led the software effort to contribute the southbound protocol plugin and needed data models to the ODL code base. Similar efforts will be needed to enable support and management of Cable technologies by open source controllers.

FUTURE DIRECTIONS FOR EVOLUTION OF THE ACCESS NETWORK

The SDN architecture described here forms the foundation for how the MSOs will deploy and manage their networks in the future.

Once an SDN Controller is in the middle of the network, talking to the various devices and network components, then operators can start focusing on developing better applications. As newer access technologies are added, they will be integrated into this framework and the existing services will apply to them seamlessly. The customer will be happier with the same service being available on their home network or, even if they are on the road roaming, as the SDN controller will be able to set up the same services across different networks.

New concepts, such as service function chaining, are taking root within the industry. Different network functions and applications are being virtualized and being run on COTS hardware in the cloud. The SDN controller and orchestrator again are in the middle of that architecture, helping direct the traffic from the customers/access network to the appropriate VMs and services in the cloud. The SDN paradigms will bring simplicity to the MSO network operations by abstracting out the complexity of the individual network devices and their configuration.