A Proposed End-to-End SDN Architecture for MSO

A Technical Paper prepared for SCTE/ISBE by

Mohcene Mezhoudi
Principal, Bell Labs CMTS
Bell Labs Consulting
600 Mountain Avenue
Murray Hill, NJ. 07479600
908-582-2776
Mohcene.Mezhoudi@bell-labs-consulting.com

Benjamin Y. Tang
Principal, Bell Labs DMTS
Bell Labs Consulting
401 Data Drive
Plano, TX. 75024
469-910-3698
Benjamin.Tang@bell-labs-consulting.com

Jean-Philippe Joseph
Principal, Fixed Access Domain Leader
Bell Labs Consulting
600 Mountain Avenue.
Murray Hill, NJ. 07479
908-679-5798
Jean-Philippe.Joseph@bell-labs-consulting.com

Enrique Hernandez-Valencia
Bell Labs Fellow, Partner
Bell Labs Consulting
600 Mountain Avenue.
Murray Hill, NJ. 07479
908-582-3144
Enrique.Hernandez-Valencia@bell-labs-consulting.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

Introduction

The advent of Software Defined Networking (SDN) is becoming strategically critical for telecom/datacom and information/cloud Service Providers worldwide. Discussion and writing on the application of SDN in MSO networks have been limited to specific parts of the network. SDN leverages a control plane model with open programmable interfaces to enable the agile and dynamic creation of new services and the orchestrated allocation of network resources. Through this, and by bridging the SDN architectures and solutions between broadband access, hub/headend sites, metro and backbone transport, MSOs will fully leverage SDN principles and their end-end networks. Further, SDN can address the following challenges faced by many MSOs:

- Footprint – Traditional regional boundaries limit ability to provide national or global services. Recent mergers and acquisitions to expand MSO footprint may impact Service Level Agreements (SLAs) and resiliency in the consolidated network. SDN can help mitigate this through a combination of telemetry, data analytics and proactive performance/resiliency management.
- Scale/optimization– Today’s rigid network architectures increase service delivery costs. SDN provides flexibility in dynamically scaling and optimizing resource utilization across IP/optical and throughout metro and backbone networks and in broadband access.
- Growth – Offering services primarily to residential customers limits growth. MSO expansion into new markets and offering competitive new service offerings will enable new growth opportunities. SDN enables the rapid creation of new innovative, revenue-generating services by using solutions such as dynamic and automated service provisioning, network slicing and service chaining end-to-end.
- Capacity – Bandwidth growth is straining broadband access networks. New architectures and technologies such as DOCSIS® 3.1 deep fiber, node splitting, and symmetrical Full Duplex (FDX) DOCSIS will significantly increase broadband access network throughput. SDN can help manage these new complex networks to reduce migration and operations cost.
- Latency – As new ultra-delay-sensitive applications emerge there will be a need to minimize end-end latency and maximize resiliency performance and user experience. This can be accomplished by moving latency sensitive functions and applications closer to the end-user and placing them under end-to-end SDN control.

We first present an MSO future network vision with key building blocks cemented by an end-to-end SDN architecture. We propose a multi-layer end-end SDN architecture that can be achieved by implementing an SDN controlled broadband access network and extending SDN to the metro and backbone network with integrated IP/optical transport. We argue for the importance of convergence in both the broadband access and transport network, the metro portion of the MSO network, and the criticality of an SDN-based IP/Optical transport integration. Convergence and integration, which are greatly aided by network virtualization through SDN/NFV, can provide MSOs with an agile, hyper-scalable and cost-effective network fabric to enable automated management, control and optimization of network resources, and the dynamic provisioning of all revenue-generating services. The roles and functions of SDN in broadband access and metro/backbone, as well as the cost benefit of IP/optical integration – in particular, multi-layer protection, will be presented in the remainder of this paper. We conclude by presenting end-to-end SDN based service orchestration that can greatly benefit MSOs in future service delivery.

Future MSO Network Vision

We envision that the future MSO SDN-enabled metro and broadband access network will be built based on four building blocks as depicted in Figure 1.

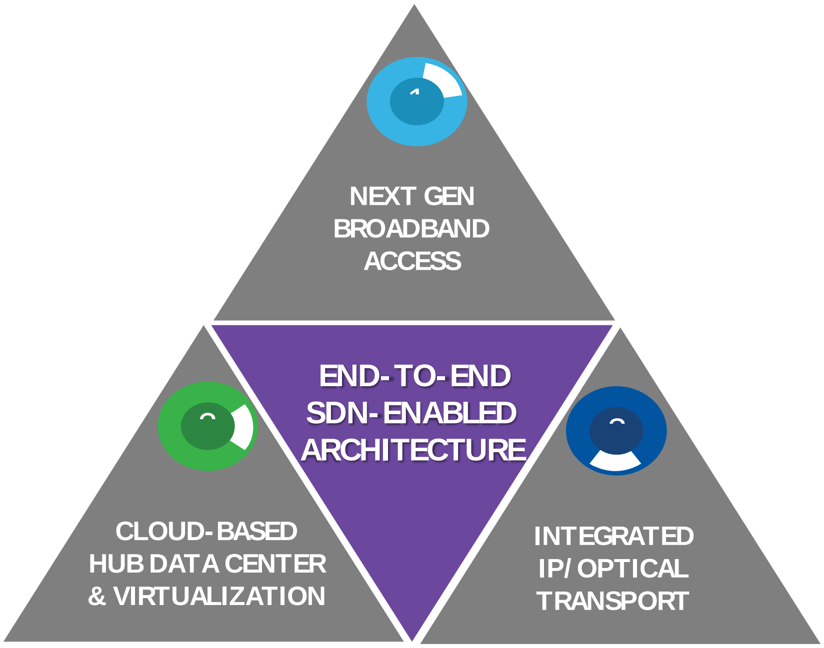


Figure 1 - Building Blocks of Future MSO Network

1. MSO Future Network Buiding Blocks

Next-Generation Broadband Access

There are multiple initiatives underway to build next generation broadband networks. A brief survey is provided here as background. The most fundamental initiative is the deployment of fiber deeper into the broadband access network and closer to end-users. This is leading to a reduction in the average number of coax amplifiers to N[1]+x, where x=6,5,4,3,2, enabling multi-Gbps downstream service access rates (in conjunction with migration to DOCSIS 3.1). Deep-fiber architectures are referred to as Distributed Access Architectures (DAA).

DOCSIS 3.1 is in deployment with many MSOs and will enable higher Upstream (US) and Downstream (DS) bandwidths through improved modulation techniques, and move the US/DS split to provide additional US capacity. Full Duplex (FDX) DOCSIS, currently under specification development, will require a N+0 (i.e., fiber node deployed at the last amplifier location) and will theoretically provide 10Gbps symmetrical bandwidth (initially FDX will operate in a reduced spectrum and provide 4-5Gbps).

---

[1] N=the fiber node

Analog spectrum is being reclaimed for use in other services such as high-speed data. Many MSOs are expanding or considering expanding outside plant (OSP) spectrum to 1 or 1.2 GHz spectrum to create additional channels used for services such as high-speed data.

MSOs are investigating providing wireless services (licensed and unlicensed spectrum) beyond Wi-Fi. In providing such services, wireless broadband access points or small cells will need to be brought to within 100 to 200 meters of end users, with fiber backhaul of traffic into the network. Similarly, DAA nodes are also brought within about 100 meters of end users, creating an ideal location for a common platform that serves both wireless and wireline access technologies [1].

Cloud-Based Hub Data Centers and Virtualization

The future MSO hub/headend locations will also evolve to a Data Center-like architecture, or edge clouds, where Virtualized Network Functions (VNF) and Physical Network Functions (PNF) will be deployed to meet the performance requirements for future applications and to offload bandwidth in the transport network. For instance, the future MSO edge cloud must be located close enough to end-users to meet low latency requirements for critical applications such as Cloud RAN fronthaul, 5G enhanced broadband, and industrial IoT.

In general, the edge cloud site will host both the mobile and fixed network functions (e.g., vRAN, vS/PGW, vOLT, vCCAP) and common applications (vDVR, vCDN, etc.), which are virtualized on Commercial Off-The-Shelve (COTS) platforms, general-purpose servers, and specialized hardware accelerators. Within the edge cloud location, leaf and spine intra-hub networking architectures are leveraged to connect servers, compute platforms and storage platforms. The edge cloud and the broadband access network elements are under the control of a Software Defined Networking (SDN) controller. SDN with its separation of control and data planes, service/resource abstraction, open interfaces and programmability, provides MSOs with great flexibility and agility to deal with dynamic applications and services and drive service innovation in the most operations efficient and cost-effective fashion.

Integrated IP/Optical Transport

A smart IP/Optical transport network interconnecting edge and core cloud sites is a fundamental component of the future MSO network vision. The benefits, enablers, and challenges of IP and Optical transport integration have been well understood by network operators [2] for some time. IP and optical integration can be achieved in multiple dimensions: data plane integration (colored interfaces), multilayer control and resilience, multilayer planning, and management. Main motivations for adopting IP/optical integration are improved network efficiency across layers, reduced resources required for protection and hence TCO savings, and optimized network management and planning. One major use case of IP/optical integration is multi-layer protection taking full advantage of available protection mechanisms from IP and optical to minimize the cost of protection/restoration.

Key technology enablers for IP/optical integration include GMPLS/GMPLS-UNI allowing tight interaction between IP and optical and an automated and switchable photonic layer. The requirement of GMPLS-UNI, however, presents a risk of vendor lock-in as the physical integration of IP and optical layers might require a single vendor in most cases. With SDN-inspired protocols such as PCE, BGP-LS, and Segment Routing (now emerging as a more promising and future proof control plane technology enabler than plain GMPLS), IP/optical integration has received renewed and growing interest from operators. These new tools largely eliminate the challenge of vendor interoperability by reducing the amount of service state maintained in the transport nodes. They also support open APIs to provide the basis for interoperability between network layers as well as between the network and orchestration layers in a multi-vendor environment. These SDN based protocols also add capabilities to rapidly instantiate multi-layer network element provisioning and turn up of bandwidths, and services, on demand. With SDN-enabled IP/optical integration, MSOs can create a scalable, reliable and cost effective tunable network fabric [3] with adaptive multi-layer resource optimization, automated network/service management, and dynamic service assurance.

2. Defining an End-to-End SDN Architecture for MSOs

SDN allows operators to effectively address multi-domain, and multi-vendor interoperability. While SDN implementation saw initial deployment in the enterprise data center space, it has quickly expanded to Next Generation Central Offices (NGCOs), the backbone and metro transport, and now the broadband access networks. Many of the benefits rendered by SDN regarding basic transport and connectivity services have been well documented. An industry survey [4] identified the top three SDN benefits sought by operators as automated service provisioning, service assurance through proactive monitoring and management, and IP/optical multi-layer optimization. Combined with segment routing, PCE, and traffic steering techniques, SDN allows for optimal allocation of network resources to meet dynamically changing service bandwidth demands and SLA requirements. For MSOs, an integrated SDN framework across broadband access, metro/backbone transport, and hub/headend (edge/core cloud) sites brings flexible end-to-end control and management of cloud-based applications and services, and hence, their agile, reliable and cost-effective interconnection.

For cable broadband access networks, the most critical benefits of SDN for an MSO – as identified by CableLabs [5] – are the extension of a common set of protocols and APIs to enable software programmability, automatic provisioning and management of network devices across broadband access and transport technologies. These new tools enable rapid creation of new services – based on the network element and service abstraction via UML and YANG data models and NETCONF procedures to manipulate the configuration of network devices, open interfaces, service chaining and intent-based networking analysis.

The proposed MSO future end-to-end network architecture, based on the building blocks described, is illustrated in Figure 2. This SDN-based architecture framework abstracts the network capabilities into “horizontal” domains such as access, metro and backbone transport, and hub/headend sites, as well as “vertical” domains – or operational layers - such as products/service, logical resources and physical resources (aka, the infrastructure).

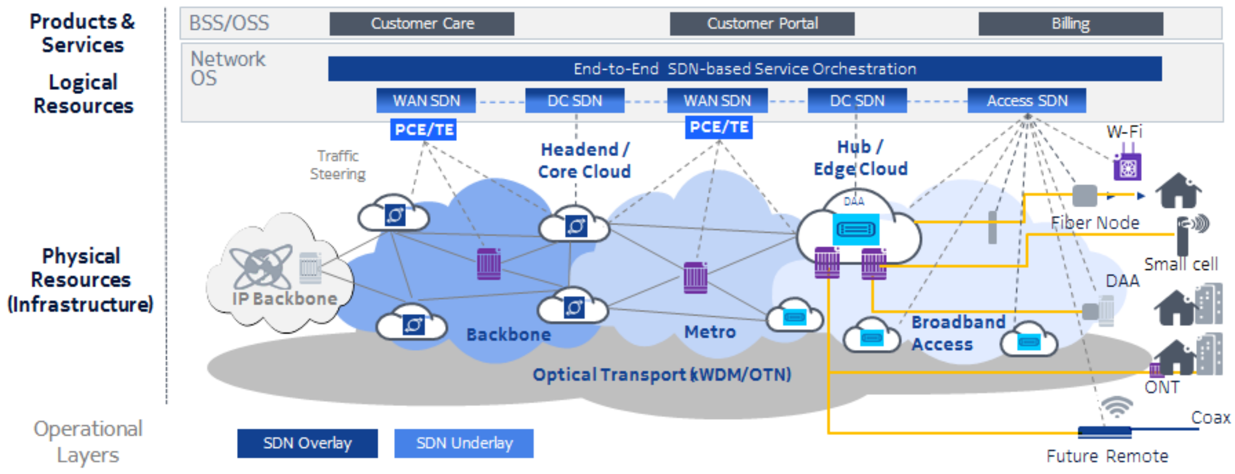


Figure 2 - MSO future SDN-based network architecture

From the network services viewpoint, a minimum of three "vertical" operational domains are envisioned:

- Physical resources: CPEs, network termination equipment (Cable modems, wireless access points), access aggregation nodes, IP edge functions, transport switches/routers and the servers/storage nodes supporting any of the network functions and applications.
- Logical resources: representing the logical abstraction of the network resources, which need also provide the ability to support "horizontal" decomposition into functional network domains such as broadband access, transport, and hub/headend sites. This functional decomposition is illustrated through the corresponding "Access", "WAN" and "DC" SDN controllers.
- End-to-end SDN network service orchestration: including any connectivity required among communicating end-users, as well as the connections to any access any network functions – physical or virtual – delivering any contracted network services.

Note that the various SDN controllers illustrated here are intended to represent logical functionality. They may be implemented as separate logical entities, or as a single integrated controller, depending on performance, scaling and administrative needs.

3. Network Decomposition and Slicing Usage of Styles

Besides network connectivity, SDN also plays a pivotal role in abstracting network services and in managing and optimizing the consumption of the resources provided by the network infrastructure. Hence, consistently with SDN principles, it is necessary for the logical components of the network architecture to support the ability to further decompose any of these vertical layers into sublayers as may be required to better integrate specific network technologies or administrative needs.

In the case of the broadband access, metro and backbone transport infrastructure, it should be possible to further decompose the physical media (fibers, coax, etc.) from the optical/wavelength links and the IP flows that constitute the ultimate physical *underlay* of the transport infrastructure. This logical decomposition, on top of these physical infrastructures, will lead to many logical *overlays*, typically instantiated through L2/L3 packet tunneling technologies that provide the logical connectivity between end-users and network function end-points, and hence, instantiated the network slices that enable flexible, dynamic and elastic delivery of services (e.g., SD-WAN, service chaining) as opposed to rigid and expensive separately built networks, as illustrated in Figure 3.

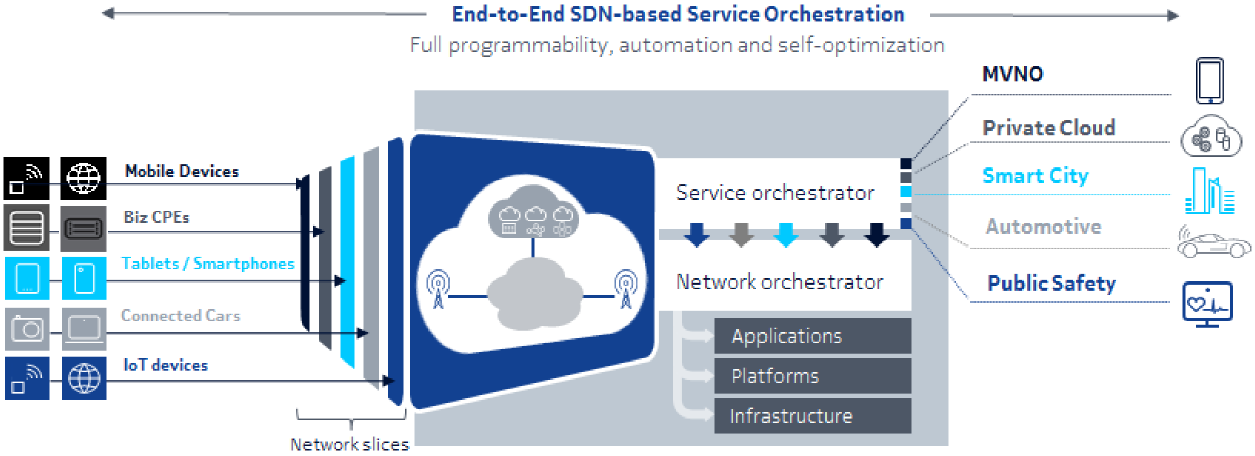


Figure 3 - Network slicing instantiated by SDN

SDN in Broadband Access

4. DSN Broadband Access Architectures

Today’s technological trends such as the industrial Internet, the Internet of Things (IoT), smart home, streaming video content, bandwidth-on-demand and app-centric, mobile-friendly personalized communications are taking roots in today’s environment - and the market competition continues to experience the entrance of service providers ready and willing to deliver these service packages to meet consumers demands.

MSOs are seriously evaluating architectural options to evolve their broadband access network to meet these trends and future demands for high bandwidth services, to improve performance, service agility, and achieve operational efficiency while reducing their overall cost structure. A key enabler of the future broadband access network is the introduction of SDN. Among the promises of SDN in the MSO’s broadband access network include the following:

- Open eco-system – Today’s broadband access network is characterized by an inflexible and closed environment with a monolithic access node, proprietary hardware and software. As a result, there is no direct access to functions, data, application and service layers, impeding flexibility and limiting scalability. The future broadband access is an SDN-enabled and open eco-system, which enables innovations and purpose-built applications in a multi-vendor and open-source environment. Further, the basic SDN architecture separates the management and control planes from the forwarding plane, thus allowing each part of the network to be independently optimized. The underlying network infrastructure is abstracted from the applications and network services, but the communication between layers is achieved with an open application layer interfaces (APIs) to allow direct programmability of each component of the network. Last, these planes can be virtualized allowing various NVFs/PNF to be distributed to different locations in the broadband access network.

- Network slicing – As the future broadband access network is multi-service, medium agnostic and programmable, the ability to create virtual slices of the network infrastructure to support wholesale, differentiated services, to dynamically allocate the network resources and expose APIs for innovative service creation, becomes critical for MSOs to evolve their business models and tap into new revenue growth opportunities.

- Node management – The ability to deliver high-bandwidth services requires the MSO to re-engineer broadband access networks and adopt a fiber-deep strategy that places smaller remote nodes closer to the customers, sharing the available bandwidth among fewer users. As a result, the number of serving nodes will significantly increase and, perhaps, by one order of magnitude relative to the current Fiber Node (FN) to achieve an amplifier-free OSP with nodes placed at the last amplifier locations (n+0). Thus, a most robust node management system is required to minimize human interventions in the OSP and allow the MSOs to reduce related OpEx. SDN will enable automation and zero-touch provisioning, and automated activation, thus drastically reducing truck rolls and OpEx.

5. I-CCAP Evolution to Distributed Architectures

The current MSO hub architecture is based on CCAP, which combines the traditional CMTS with high-speed data functions and edge QAM functions used for video (thus Integrated-CCAP or I-CCAP). The natural evolution of HFC networks is driving fiber deeper due to SG size reduction and corresponding physical FN splits. DOCSIS 3.1 is designed to enable major gains in modulation, some that require shorter coax runs with fewer or even no amplifiers in the cascade. Legacy FN technology is adequate to leverage these realities. However, the increase in the number of SGs drives a need for additional space, power and cooling in the headend and hub locations where the CMTS+EQAM and/or I-CCAP equipment resides. There is also the issue of analog optics between the hub and FN being at capacity and operational expenditure (OpEx) concern as capacity requirements on feeder fiber increase along with SG growth in an FN Serving Area (FNSA).

Distributed Access Architecture (DAA) has arisen as the next architectural advance in cable broadband access networks [6]. It considers all reasons mentioned previously as well as the conclusion that digital feeder fiber provides a ubiquitous platform which can support all fiber deeper requirements of the broadband access network, including fiber to the premise cases. A common requirement in all DAA variants is digital fiber between the headend/hub and FN location. Where DAA variants differ is in the distribution of the functional elements of I-CCAP. One variant is R-PHY or RPD, which remotes the common PHY used by all HFC-based voice, data and digital video services into the next generation FN. R-PHY leaves the MAC at the existing head-end/hub CCAP location. The other main DAA alternative remotely locates both MAC and PHY in the FN to an R-MAC/PHY or (RMD) node. The RMD alternative enables the majority of remaining CCAP functionality, which is largely implemented in software, to be placed anywhere in the cable operator network.

DAA in its different flavors is currently maturing in the specification stage at CableLabs® with product expected in 2018.

6. SDN/NFV-based Broadband Access Solution Alternatives

MSOs are considering various options to introduce SDN into the broadband access network. SDN decouples hardware (e.g., PHY layer) and software (e.g., control plane). The software can be moved to the edge cloud or instantiated wherever needed in distributed servers, independently of hardware platforms. Likewise, virtualization enables network functions to migrate from dedicated hardware to virtual machines running on general-purpose hardware and specialized hardware accelerators. Thus, SDN provides the flexibility to centrally reconfigure networks in an automated fashion. A key SDN capability is to enable automated on-demand provisioning of services in the broadband access network.

Multiple SDN broadband access solutions have been recently proposed, inspired, and stimulated by the SDN paradigm successes in data centers. SDN carries the promise of enhanced and expanded services with a more manageable operational environment. Though many standards groups and open-source projects exist, deployments remain in their infancy.

In the following, we survey a sample of these proposals with an emphasis on broadband access architectures.

CableLabs introduced in [7] the basis for an overall SDN architecture model that applies to any underlying cable broadband access technology such as DOCSIS, EPoN etc. The proposal focuses on the data models and south-bound protocols, as the foundation for how the MSOs will deploy and manage their future programmable broadband access networks. It highlights the SDN controller and orchestrator functionalities to simplify the MSO network operations by abstracting out the complexity of the network devices and their configuration. The claim is that the gain from an SDN controller which enables programmable configuration, provisioning and dynamic control of various network devices and elements, will liberate operators to focus on developing new and revenue-generating applications and integrate them with the existing services seamlessly.

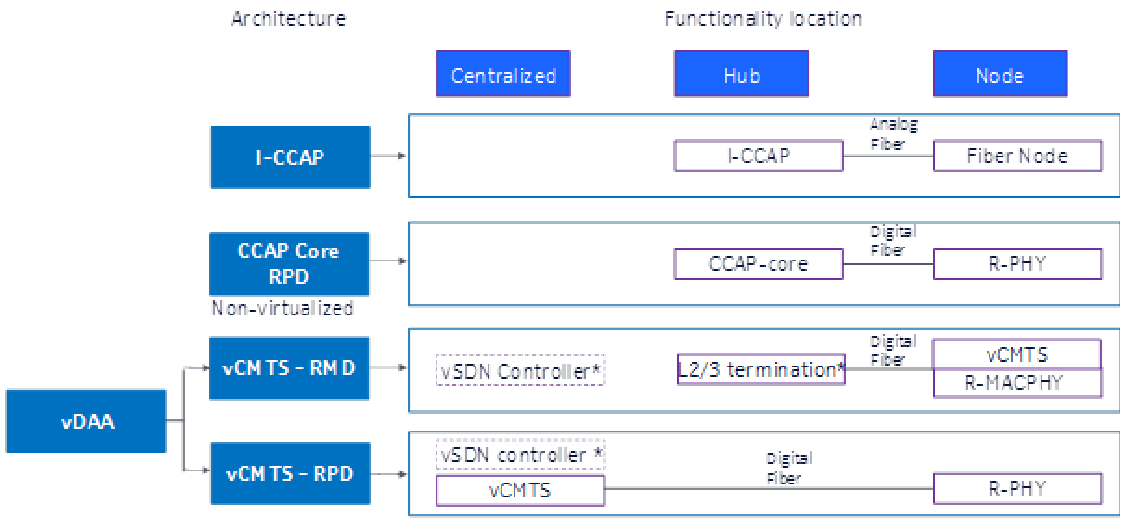
The authors in [8] emphasize that for the distinct characteristics of DOCSIS broadband networks (protocol, topology, and management capabilities), a new set of unique requirements is needed and modifications/adjustments must be applied to the existing SDN model in data centers and other networks. They present an overview of Comcast’s SDN-driven implementation of programmable Service Flows through the integration of the OpenDaylight (ODL) PacketCable® Multimedia (PCMM) plugin. They acknowledge the progress demonstrated by this platform as a control plane for the creation of DOCSIS/PCMM service flow management. However, they stress that while further development in practical and scalable, deployment/implementation and field experience are still extremely essential, the path forward for SDN in the new programmable DOCSIS network is better defined and clear.

An SDN/NFV framework is presented in [9] to enable MSOs to deliver a set of new services (network access, infrastructure, consumer services and 3rd party applications) across multiple broadband access networks technologies (DOCSIS, DPoE, PON, Wi-Fi, Mobile, etc.). They elaborate on how operators would offer and manage them. They suggest a broadband access network architecture where the broadband access technology is abstracted from the services layer, allowing the technology vendors to optimize the ASIC based solutions effectively and only migrate the services and control/management plane to a COTS platform with compute, storage and switching capabilities. This will enable both operators and vendors to offer feature parity and reuse of certain components independent of the access technology, thereby improving time to market for new services and features. In addition, they present views and assessment on what network functions can be virtualized to improve the agility of the broadband access network. And observe that while MSOs are experiencing multiple transitions (architectures, technologies, services, app-aware), they suggest that the SDN/NFV paradigm could be their means to realize synergies while addressing these transformations. They recognize SDN/NFV technology provides enormous potential benefits though it is still maturing and has achieved a lot of progress with vendors and operators actively proving its feasibility and performance capabilities and conducting real-network trials.

The integration of SDN concepts and the CableLabs DOCSIS, L2VPN, and DPoE definitions is investigated in [10]. The objective is to enable cable operators to realize fully automated end-to-end provisioning of commercial services and dynamic network reconfiguration through a single and simplified provisioning interface. The authors describe an overall broadband access architecture and its key elements. They define a set of requirements for the service provisioning API and the capabilities of DOCSIS-approach provisioning. They outline an automated DOCSIS-type provisioning framework with SDN. It is proposed that a network-layer service could be fully specified by the business systems by providing the appropriate attributes to all network elements. They assert that the model could be extended to other broadband access technologies beyond DOCSIS and DPoE technologies with further specifications of the requirements and the actions needed to be performed through the API. They supplement their approach with a description of a provisioning flow from the business service system (BSS) to the Cable Modem (CM). This involves multiple systems and human interventions. They proclaim that the proposed service provisioning framework allows the MSO to offer better-quality services at lower cost. This is achieved by reducing new services lead-time to market and eliminating manual and error-prone configuration of network equipment. Particularly for more involved business offerings where the service provisioning is reduced to a transaction rather than multiple steps with multiple complex human interaction and intervention.

The use of SDN Broadband access concepts to enable dynamic and flexible pairing of a separated MAC-PHY and R-PHY in a remote physical device (RPD) architecture is presented in [11]. The agile SDN infrastructure assigns various remote physical devices to various MAC resources (local or remote CCAP, or virtual CMTS) based on policies and network varying requirements. This results in new options for network operations savings as well as new load sharing and availability performance.

In this subsection, we focus on the introduction of SDN in the DAA-based broadband access network. Considerations pertaining to enabling SDN in an FTTH network, which MSO might deploy as an overlay network to serve their customers, are not addressed here. Among the DAA solution alternatives for the future HFC-based broadband access network, the following have gained more acceptance in the industry: non-virtualized Distributed CCAP Core (CCAP Core RPD) and virtualized DAA (vDAA). vDAA has two implementations: 1) Virtualized CMTS in a centralized location (vCMTS RPD); and, 2) Virtualized CMTS in the node (vCMTS RMD).



*Can be centralized or in a hub

Figure 4 – DAA Options

As shown in Figure 4 below, the CCAP Core RPD solution leverages a CCAP core or DOCSIS MAC in the hub location and decouples the PHY function, which is deployed as RPD nodes in the OSP.

vCMTS RMD introduces a virtualized SDN controller (vSDN), which is deployed in a centralized location, hub or headend, and remoting the combined MAC and PHY layers to an RMD node deployed in the OSP. The most obvious benefit of this solution involves trade-offs among complexity, space, and energy consumption.

vCMTS RPD leverages a virtualized CMTS (vCMTS) function that can be deployed centrally in a hub/headend to support RPD nodes. This solution provides complete flexibility to the MSOs in the DAA space. A vSDN controller is also used and can be deployed in the hub or headend location.

SDN in Metro Networks

A Bell Labs study [13] shows that consumer and enterprise traffic in the metro network is expected to grow by 3.9x from 2015 to 2020, driven by video and cloud/data center traffic. In addition, cloud-based applications (e.g., network DVR, gaming, video streaming, and future AR/VR) and dynamic placement of virtualized network functions (e.g., vCDN, vRouter, vCCAP/vCMTS) deployed in distributed edge cloud DCs will lead to a substantial change in the traffic patterns of metro networks. This increase in network flexibility coupled with the trends towards real-time user-controlled service experience - such as self-portal for dynamic change of service attributes (e.g., bandwidth and performance/SLA), and the emergence of richer IoT and 5G applications based on network slicing, will create very dynamic and elastic traffic demands. These demands are not only North-Southbound (between servers and clients) but also have East-Westbound traffic (between data centers). Delivering such large and rapid changing traffic demands will require a flexible transport network fabric, particularly across the critical metro networks. These trends will require MSOs to:

- Scale network capacity cost efficiently to sustain future traffic growth
- Allocate network resources dynamically to meet rapidly changing applications and services demands
- Automate network configuration and service provisioning in a multi-vendor, multi-layer environment
- Provide dynamic assurance of network/service performance and efficiency through use of KPIs and data analytics

IP/Optical transport integration via multi-layer protection, adaptive network resource optimization, and SDN based principles, protocols and APIs will provide MSOs a flexible and smart network fabric over which to implement an end-to-end SDN-based service delivery architecture to achieve sustainable network capacity and revenue growth. An SDN-based architecture framework further enables network programmability and automation to provide the flexibility and agility required to achieve dynamic and on-demand service provisioning and assurance.

7. Multi-layer Protection and Adaptive Resource Optimization

Several shortfalls exist today in most backbone and metro networks:

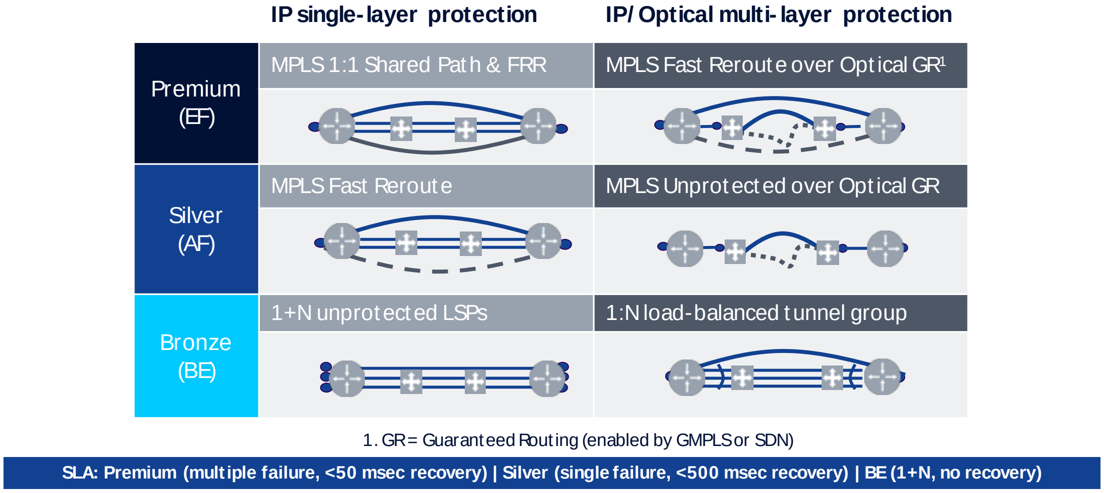
- Most operators are deploying IP and optical transport separately without taking full advantage of multi-layer protection mechanisms available – many of them are using IP protection and restoration mechanisms (MPLS, IP FRR or simply routing convergence) without leveraging optical protection capabilities. This approach risks higher cost of protection and missing critical SLA requirements (e.g., shorter failover time which can only be achieved by optical 1+1 protection).
- Furthermore, there is no differentiation of protection – traffic from all service classes is receiving the same level of protection in the IP/optical transport network, making it unnecessarily expensive for operators and results in a lost revenue opportunity for premium services with higher resiliency.
- IP and optical transport have a rigid network topology which does not adapt to dynamic traffic patterns and loads. This leads to inefficient routing and network resource utilization. For example, operators should be able to cost-effectively and dynamically establish IP shortcuts through the optical layer to address short-term and/or seasonal high-volume traffic demands more cost effectively.

Failure to address these shortfalls lead to an over-engineered network and high per-bit transport cost that is not sustainable to support future traffic growth. MSOs should develop a comprehensive strategy and solution toward multi-layer protection and optimization to achieve hyper-scalability, hyper-flexibility, and hyper-performance in its backbone and metro network. This includes:

1. A clear understanding of the business requirements for the quality of the services offered – for example, multiple classes of service (CoS), SLA and resiliency required for each CoS, as well as a business opportunity for generating additional revenue from creating additional and higher levels of CoS.
2. A well-defined differentiated, multi-layer protection solution using a mix of protection and restoration mechanisms available from IP and optical layers differently for multiple CoS options based on their SLA and resiliency requirements. An example of such a solution is given in Figure 5, where it is compared with an IP only single layer protection solution which is over-engineered

to meet the same SLA and resiliency requirements. For example, for the premium CoS, the multi-layer protection solution uses a mix of MPLS FRR (to meet < 50msec recovery time) and lower-cost optical guaranteed routing (GR) for resiliency against multiple failures, while the IP only protection requires a combination of MPLS path protection and FRR which is more expensive as the path protection would go over multiple intermediate IP nodes.

3. A set of agile IP and optical network resources made possible by emerging technologies such as segment routing (SR), path calculation engine (PCE), virtualization, CDC-F, Photonic switching, OTN switching, Variable Modulation OT's, Flexigrid and open ROADM.
4. Adaptive network resource optimization achieved by a single or hierarchy of SDN controllers capable of controlling and coordinating agile network resources across IP and optical and dynamically setting up the optimal traffic routing, network topology and resource allocation subject to the changing traffic demands so that network traffic can be optimally routed and protected at the least possible cost.



	IP single-layer protection	IP/ Optical multi-layer protection
Premium (EF)	MPLS 1:1 Shared Path & FRR	MPLS Fast Reroute over Optical GR[1]
Silver (AF)	MPLS Fast Reroute	MPLS Unprotected over Optical GR
Bronze (BE)	1+N unprotected LSPs	1:N load-balanced tunnel group

1. GR = Guaranteed Routing (enabled by GMPLS or SDN)

SLA: Premium (multiple failure, <50 msec recovery) | Silver (single failure, <500 msec recovery) | BE (1+N, no recovery)

Figure 5 – An Example of Multi-layer Protection Solution

Adaptive network resource optimization can be executed at different timescales of the network optimization cycle as indicated by Figure 6. At real-time or near real-time, the SDN controller along with PCE, SR and intelligent traffic routing algorithms [14] provide a traffic steering framework allowing MSOs to dynamically regulate admission and routing of traffic subject to specific policies and optimization goals (e.g., maximized revenue, guaranteed latency and/or resiliency) – achieving all these based on a given fixed available network capacity. At the mid-term time scale (days/weeks/months), changes in link capacity and network topology can be triggered by the shift in traffic patterns and load to optimize cost and performance. Long-term, network capacity is optimized through the operator's semi-annual or annual (or longer) capacity planning process which will involve only automatic SDN control.

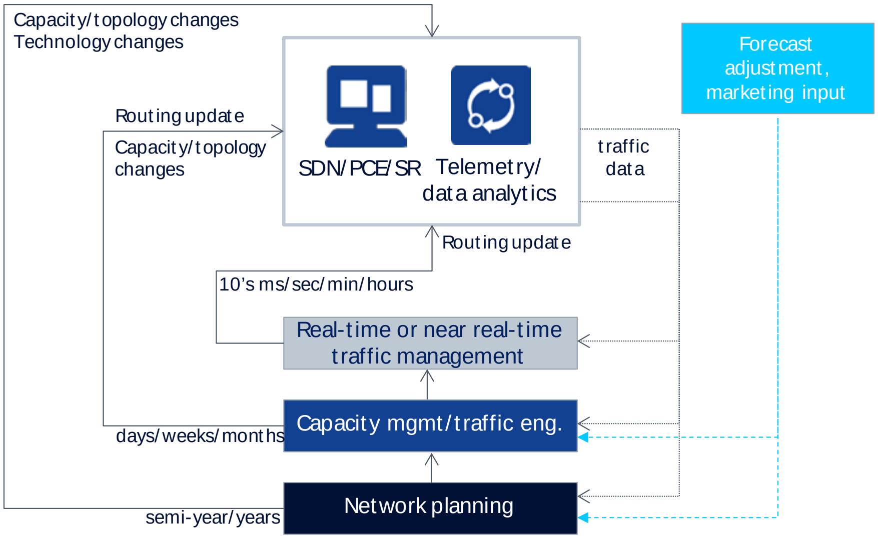


Figure 6 – Adaptive Network Resource Optimization at Various Time Scales

A Bell Labs study [15] examines SDN-enabled multi-layer protection in a typical medium-sized metro network with a mix of residential, mobile and enterprise services carried in three classes of services (Figure 7) and protected by a differentiated multi-layer protection strategy as defined in Figure 5. The study demonstrates a potential TCO savings of 30%-40% over 5 years compared to the scenario based on IP single layer protection (also described in Figure 5) in two cases where the traffic growth is driven by residential/mobile consumer services (traffic profile P1) and by enterprise services (traffic profile P2) separately. The TCO saving is due to not only better utilization of network resources for protection/restoration by using a mix of protection mechanisms from IP and optical, but also the adaptive resource optimization made possible by SDN where the IP network topology ("agile" logical topology) can be dynamically optimized to the changing traffic pattern that leads to more efficient traffic routing and further reduces the cost of protection. We depict in Figure 7 the 5-year TCO saving based on traffic profile P2 (enterprise driven) increases from 30% to 36% in the presence of a dynamically changing traffic pattern between enterprise data centers. Another metro SDN multi-layer protection case study for an MSO network operator [16] also shows a consistent 5-year TCO saving of 30%.

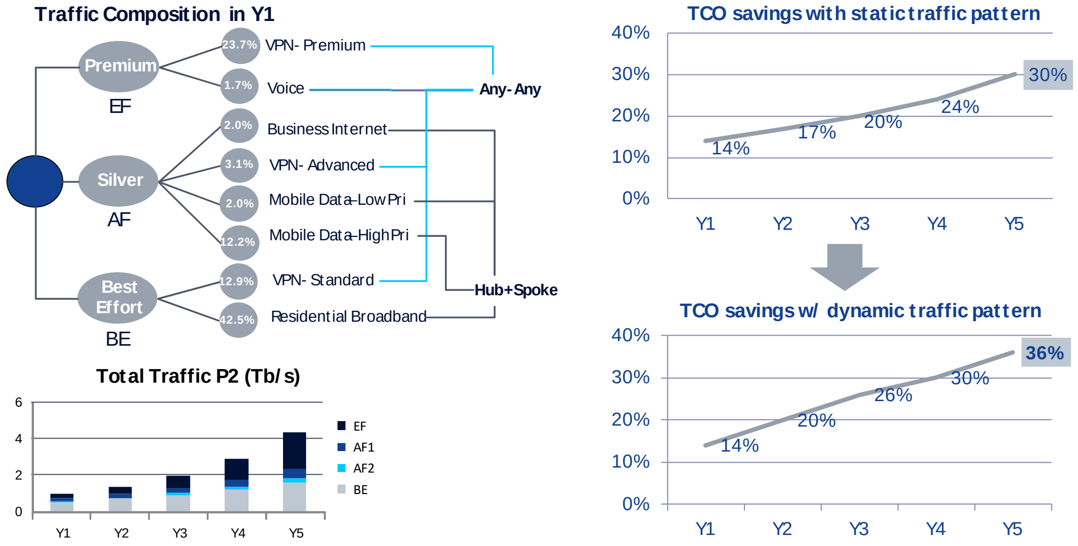


Figure 7 - A TCO Case Study of SDN-enabled Multi-Layer Protection in Metro

End-to-End SDN-based Service Orchestration

Network operators planning to implement carrier SDN expect the most important business benefits to achieve are the ability to generate more revenue from existing services and to create and deploy new services to market more rapidly. This priority is particularly driven from the perspective of a network operator's external facing product group as opposed to the network group who sees SDN primarily to improve network efficiency, cost per bit and interoperability. SDN achieves the dynamic and rapid creation of services by facilitating automated and programmable configuration and provisioning of connections and service components, which also reduces operations cost to maintain service profitability. Network automation goes beyond service orchestrating – it also addresses service assurance using monitoring and data analytics tools to detect and diagnose network problems, sometimes proactively, and respond to network demand ahead of time, delivering auto-healing and auto-scaling functionality.

These SDN benefits are of importance for MSOs as they are expanding footprint into new markets and business models where they need to quickly turn on existing and new competitive services with quality assurance at profitable operations cost.

Within the broadband access and metro/ backbone networks, MSOs are embracing the industry trend to re-architect existing hubs and data centers to centralized and edge clouds to host converged application/service platforms (e.g., SD-WAN, vDNS) and deploy a common NFV infrastructure for network functions such as vSTB, vCPE, vPVR, vCDN, vRouter and vCCAP/vCMTS. While these new capabilities promise to create more agility, cost efficiency, third-party innovation and new revenue opportunity, this cannot be accomplished without a multi-domain SDN control that orchestrates the allocation, activation, and monitoring of this virtualized services and network resources as well physical devices across the data centers and metro and broadband access network.

Multi-domain SDN orchestration in such case can be achieved through the use of underlay and overlay SDN controllers as illustrated in Figure 1. Underlay SDN controls the IP and Optical transport infrastructure layer and performs dynamic (re-)configuration of physical and virtualized forwarding network functions via network protocols such as OpenFlow, Nentconf, BGP-LS, and segment routing to create connections with required bandwidth and performance (latency, resiliency) through a programmable north-bound API to the clients requesting such connections. The utilization of network resources for establishing the connections can be optimized with the use of intelligent traffic steering algorithms and PCE by the underlay SDN. Underlay SDN is also responsible for proactively assuring quality, resiliency, and security of connections through constant data collection and analytics, and advanced support for cognitive, dynamic network control through the northbound API. Such intent-based API simplify the network knowledge required on the client side and allows the SDN control more flexibility to select and place network functions to provide the connections desired. All these underlay SDN capabilities can be implemented in a future network operating system as illustrated in Figure 8.

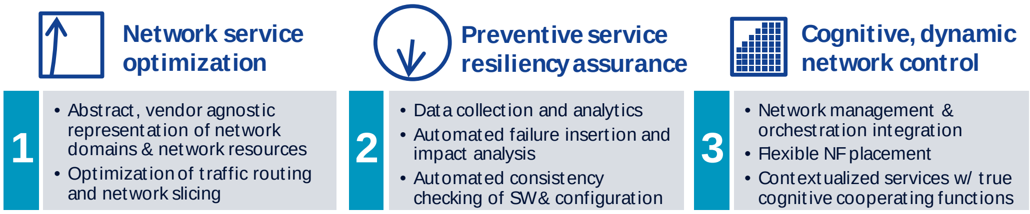


Figure 8 – Underlay SDN Implemented in a Network Operating System

8. Automated Service Provisioning and Assurance

Overlay SDN at the services layer enables flexible, dynamic and elastic allocation of required application/service functions through service chaining and policy enforcement and ties them together using the connections created by the underlay SDN. Overlay SDN is responsible for overall orchestration and delivery of services and can place requests to the underlay SDN for the elastic creation and changes of connections. This can start with customer service orders, generated by either manual tasks or customer-driven actions such as the ordering of a service through a service portal. The service ordering will then be fulfilled by the overlay SDN by identifying specific applications/services required, such as security gateway for encrypted tunnels, and determining the placement of such applications/services from a common pool of resources which may be located across multiple data centers and the connections required to stitch them together to deliver the customer's service order end-to-end. In large operator networks it is also desirable to provide the capability to segregate the provisioning and configuration of the connections among the network functions inside the data center (or hub/headend) – the intra-DC LANs - from the connections across the metro (and backbone) transport network elements. This segregation can be attained via separate DC SDN and WAN SDN controllers under the controller responsible for the End-to-End SDN-based service orchestrator. As illustrated in Figure 1, we refer to this collection of intelligent controllers and orchestrators the Network OS.

SDN orchestration with underlay and overlay SDN delivers automated service provisioning and assurance in the metro network for MSOs. The implementation of SDN orchestration includes SDN controllers and tools supporting Lifecycle Service Orchestration (LSO) which integrates orchestration, fulfillment, control, performance, assurance, usage, analytics, security, and policy of networking services.

Network operators are building up SDN controllers and tools for LSO based on open standards and open-source development such as OpenDaylight and Open Network Automation Platforms (ONAP). Contributed by both network operators and third-party developers, this offers open service creation and management platforms where concepts like microservices and service chaining are applied to create a highly scalable and extensible framework which can be used repeatedly for rolling out new services rapidly to the market in an open, multi-source environment.

Conclusion

SDN discussions and writings have focused on specific portions of MSO networks. This paper expands the application of the SDN paradigm to reconfigurable and programmable metro and access networks. This concept has been widely contextualized in the general scenario of SDN technology, with reference also to the related market place evolution. The reasons for an end-to-end SDN extension have been presented, considering the metro and access traffic evolution, the future network and business requirements, the trends of data center interconnect and edge cloud, the benefit in terms of end-user quality of experience, and the TCO savings. The buildings blocks for the future SDN networks have been reviewed.

While these building blocks are all critical to MSOs, an End-to-end SDN architecture allows MSOs to effectively address multi-domain, and multi-vendor interoperability. The SDN-based architecture framework proposed provides network abstraction capabilities into “horizontal” domains such as broadband access, metro and backbone transport, as well as “vertical” operational layers - such as products/service, logical resources, and physical resources. By deploying an end-to-end SDN architecture across metro and broadband access, MSO can automate and dynamically scale service provisioning, minimize end-to-end latency and maximize resiliency performance, optimize utilization of resources across IP/optical and throughout metro and broadband access, and create new innovative, revenue-generating services quickly using solutions such as network slicing and service chaining end-to-end. These SDN benefits are of importance for MSOs as they are expanding footprint into new markets and business models where they need to quickly turn on existing and new competitive services with quality assurance at profitable operations cost. This cannot be accomplished without a multi-domain SDN control that orchestrates the allocation, activation, and monitoring of this virtualized service and network resources as well physical devices across the data centers and metro and the broadband access network. Multi-domain SDN orchestration in such case can be achieved through underlay and overlay SDN to deliver automated service provisioning and assurance in the metro and the broadband access network for MSOs. The implementation of SDN orchestration includes SDN controllers and tools supporting Lifecycle Service Orchestration (LSO) which integrates orchestration, fulfillment, control, performance, assurance, usage, analytics, security, and policy of networking services.

Abbreviations

API	application programmable interface
BGP-LS	border gateway protocol - link state
CCAP	converged cable access platform
CDC-F	colorless directionless contentionless - flexible grid
CDN	virtual content delivery network
CMTS	cable modem termination system
DAA	distributed access architecture
FDX	full duplex
FFR	fast reroute
HFC	hybrid fiber-coax
ISBE	international society of broadband experts
MAC	media access control (layer)
MPLS	multi-protocol label switching
MSO	multi-system operator
NFV	network function virtualization
OpEx	operational expense
OT	optical transponder
OTN	optical transport network
PCE	path calculation engine
PHY	physical (layer)
PVR	personal video recorder
RMD	remote mac device
ROADM	reconfigurable optical add-drop multiplexer
RPD	remote phy device
SCTE	society of cable telecommunications engineers
SDN	software defined networks
STB	set atop box
API	application programmable interface
BGP-LS	border gateway protocol - link state
CapEx	capital expenditures
CCAP	converged cable access platform

Bibliography & References

Future Proofing Access Networks Through Wireless/Wireline Convergence, M.J. Glapa, et.al., SCTE Cable-Tech Expo 2017

IP and Optical Convergence: Use Cases and Technical Requirements, January 31, 2014

The Future X Network: A Bell Labs Perspective, Marcus Weldon, CRC Press, 2016

Delivering on the Promise of Multi-Layer Integration with SDN, Light Reading, July 2016

Virtualization and Network Evolution Open Networking – SDN Architecture for Cable Access Networks Technical Report, VNE-TR-SDN-ARCH-V01-150625, CableLabs, 2015

Optimizing Cable Access Network Evolution for Cost, Performance, and Competition, Jean-Philippe Joseph et.al. SCTE/ISBE Journal of Network Operations Volume1, Number2, 2016

SDNized Cable Access Networks, Karthik Sundaresan, 2015 Spring Technical Forum Proceedings, CableLabs, NCTA, SCTE

SDN Ground Truth: Implementing a Massive Scale Programmable DOCSIS Network, Sameer Patel et al., 2016 Spring Technical Forum Proceedings, CableLabs, NCTA, SCTE

Delivering Seamless Subscriber Aware Services over Heterogeneous Access Networks using SDN/NFV, Nagesh Nandiraju et al., 2015 Spring Technical Forum Proceedings, CableLabs, NCTA, SCTE

Software Defined Networking, DOCSIS Provisioning, and MSO Commercial Services, Kevin A. Noll et al., 2014 Spring Technical Forum Proceedings, CableLabs, NCTA, SCTE

SDN As A Matchmaker For Remote Phy Architecture, Alon Bernstein et al., 2015 Spring Technical Forum Proceedings, CableLabs, NCTA, SCTE

Virtualization and Network Evolution – Virtual Provisioning Interface Technical Report, VNE-TR-VPI-V01-170424, CableLabs

Metro Network Traffic Growth: An Architecture Impact Study, Bell Labs, 2015

Optimizing revenues with the PATH PCE – Quantifying the Benefits of Deploying a Centralized Path Computation Element*, Bell Labs, 2015

IP/Optical Integration with SDN, Ben Tang, SReXperts America, September 14, 2016

Metro Multi-Layer Protection Design, Mohcene Mezhoudi, Ben Tang, October 2016