CONSIDERATIONS FOR A SERVICE DELIVERY PLATFORM FOR OPTIMIZING THE DEPLOYMENT OF MSO BUSINESS SERVICES

RAM SRIDHARAN, STEVE DAVIDSON
NOKIA

Abstract

The business environment for MSO's commercial customers has changed; it's a disruptive world where yesterdays technology is hindering the need to accelerate towards cloud-based IT. This is particularly evident in the area of launching new business services. Traditionally, business services are tightly connected to a dedicated network infrastructure and based on a set functionality. This has forced businesses into the complex world of networking and service delivery platforms in order to achieve the network and service capabilities that match their specific business needs. Many enterprise branch locations (as well as Small and Medium Businesses - SMBs) lack the on-site technical support necessary to manage network services at these locations.

This paper examines the industry architecture concepts and delivery platform requirements for the rapid deployment of value-added cable business services that MSOs can provide to new and existing customers. The paper covers NFV (Network Function Virtualization) and SDN (Software Defined Network) -related topics focusing on tools and automation techniques both in a data center and branch office environment that would provide MSO business customers with the power to self manage and deploy their own network services.

INTRODUCTION

Cable multiple system operators (MSOs) have an unprecedented opportunity to accelerate commercial service revenues far beyond current levels by providing businesses the support they need to maximize the benefits of cloud technology.

The worldwide shift by businesses of every size and description towards greater reliance on private and public clouds for access to mission-critical applications has generated demand for lower-cost, more flexible ways to extend utilization of those virtualized resources across multiple locations and to workforces on the go. This in turn has accelerated network service providers adoption of virtualization technology to create software-defined wide area networks (SD-WANs) that greatly expand the flexibility and lower the costs of IP-based connectivity. At the same time, service providers are deploying SDN concepts within business branch offices and datacenters and embracing Network Function Virtualization (NFV) to rapidly and efficiently deploy business services across their customer base.

MSOs can take the lead in satisfying this demand by leveraging a cloud-friendly, multi-layered virtual network architecture to create a connectivity and value-added service model that far outperforms traditional service offerings. Given the growing importance of VPNs in delivering cloud-based IT applications to businesses across all their locations and to employees on the go and a platform to launch value added services, MSOs have a significant opportunity to satisfy market demand through use of SD-WAN technology to deliver software-defined VPN (SD-VPN) services to the SMB and enterprise markets.

By providing customers agile and secured access to cloud-hosted applications, MSOs can make significant inroads into a market

currently dominated by rigid VPN services that are no longer suited to the needs of SMBs or, for that matter, to new cloud-driven needs of larger enterprises. Not only will implementation of SD-VPNs and cloud infrastructure allow cable operators to provide a more flexible and scalable way for businesses to exploit the cloud; it will facilitate operators' expansion into the lucrative managed services market with the bundling of cloud-hosted applications as value-added enhancements to their connectivity services.

COST CONTAINMENT & CLOUD VIRTUALIZATION

Several recent studies underscore the impact that demand for new types of services will have on total spending for network services in the years ahead. Generally speaking, they all reflect the heavy priority businesses are placing on cost containment.

According to an annual survey of IT professionals in the U.S. conducted by Computer World, even as IT budgets are increasing, cost containment ranks as the top business priority, with 53% of respondents citing this as the top priority compared to 35% who cited growing revenue as the top priority. Other top priority items also directly relate to cost containment, including optimizing and automating business processes (47%) and accelerating business process and agility (38%). Looking at the top categories targeted for reduced spending, the survey ranked hardware spending first, followed by legacy system modernization, on-premises data center consolidation and optimization and on-premises software. All of these cost-cutting priorities point to growing reliance on cloud-friendly networks that can maximize companies' ability to leverage private and public cloud technology. With the virtualization of datacenters utilizing SDN/NFV technology, where storage, server and software applications and their backups run on a shared resource pool, efficiencies tied to use of the cloud have reoriented spending across the business landscape, extending down to the smallest SMBs.

Moreover, new developments have added to the need to virtualize the datacenter. Most notably:

- The modularization of software requires scheduling of upgrades far more frequently than in the past, greatly adding to the burden of doing things the old way.
- With the onset of big data analytics, IT teams must continually ensure they are bringing analytics systems into play across multiple workflows, requiring a level of cooperation and coordination that is difficult to sustain in the fragmented traditional operations environment.
- The traditional data center has proven to be a hospitable environment for businesses seeking to exploit opportunities in the fast-paced Internet domain, where the focus is on agility and speed-to-market amid an incessant flow of application innovation.

SOFTWARE DEFINED VPN

At the connectivity level, the worldwide pursuit of cloud-enabled cost containment is driving escalating demand for IP VPNs. Currently this is part of a VPN market dominated by incumbent local exchange carriers delivering secured IP VPNs over MPLS (Multi-Protocol Label Switching) infrastructures.

But traditional carrier VPN service options are inadequate to market needs with regard to both costs and flexibility. From an operational standpoint, manually configured VPNs impose significant constraints on a company's ability to integrate cloud services, turn up new sites and deploy and provision new IT and communications systems.

The need for a new type of VPN connectivity service applies to multiple enterprise scenarios. Companies operating in many locations linked over wide area network connections need to overcome the limitations of the traditional enterprise WAN VPN service in order to more effectively exploit the benefits of IP, the Internet and cloud technology. At the same time, for all companies, including SMBs that have traditionally not been in the market for VPNs, secure VPN connectivity to cloud-hosted apps is now essential.

An emerging need for Enterprises includes VPN connectivity for employees outside the office. Businesses everywhere want to be able to provide secure VPN connectivity to applications, data and other company resources for employees on the go, which requires that network administrators be equipped to quickly set up VPNs for secure access over mobile and Wi-Fi links by any authorized person, wherever they are.

The Advantages of SD-VPN Connectivity

All these business needs require a shift away from inflexible VPN services that do not meet the emerging needs of the new digital enterprise. MSOs, leveraging their high-capacity fiber backbones and broadband access networks, have an opportunity to provide such a cost-effective alternative with superior versatility and ease of use in comparison to legacy connectivity services.

The key to success is utilization of virtualized networking technology to create a software-defined VPN (SD-VPN) architecture, which is a subset of the SD-WAN services that are in growing use among larger enterprises. Rather than using proprietary terminals in the network and at customer premises to nail up dedicated VPN connections, network operators can leverage network functions in the cloud to orchestrate point-and-click provisioning of SD-VPNs in incremental response to customers' needs on a pay-as-you-go cost basis.

With SD-VPNs in place, MSO customers will be able to:

- Leverage the virtualized cloud to lower costs of providing backup and recovery for their storage and network-based operations;
- Expedite connectivity as they add and move branch offices;
- Steer traffic into data centers for advance service chaining use cases;
- Utilize cloud-based applications and third-party services;
- Implement unified communications and network-based collaboration;
- Easily extend VPN connectivity over wireless links to employees;
- Make better use of video for training, in-house messaging and other applications;
- Eliminate the costs of buying and upgrading proprietary CPE.

Moreover, the SD-VPN platform will allow operators to extend the reach of their customers' VPNs beyond their cable service areas to any broadband-connected locations worldwide.

OPEN PLATFORMS AND SDN

Software-Defined Networking (SDN) is a rapid shift to open source technology. Open source technologies drive down costs, reduce vendor lock-in, and accelerate innovation and development cycles. There are many points of integration between the functional layers in a cloud architecture. Adhering to standards around these points of integration enables interoperability between solutions from multiple vendors. In some cases the standard is formalized through a vendor-neutral standards group. In others a de facto standard arises due to the dominant market share of one vendor in one area that drives a large

ecosystem of partners to align with that market.

As a result, cloud technology has quickly evolved into a multi-vendor ecosystem that is commonly called a "cloud stack" (not to be confused with the cloud orchestration software from Citrix® and Apache™ called CloudStack).

A generic cloud stack that is also part of a NFV platform includes all the hardware and server virtualization, including SDN controllers and virtual networking, all the way up to the cloud orchestration software that automates the entire infrastructure of servers, storage and networking.

Looking further into the emerging cloud infrastructure, it becomes apparent how open interfaces and protocols have contributed to real multi-vendor solutions as enterprises and services have built out functioning cloud architectures. For example, SDN controller technology typically supports higher-level cloud orchestration platforms (like OpenStack®) through REST-compliant APIs (generally called northbound APIs in the controller architecture). Standardized interfaces within OpenStack also allow networking vendors to provide a standard Neutron (the networking management framework of OpenStack) plug-in, allowing any vendor to support this open source cloud orchestration system.

By comparison, a combination of long-established and new networking protocols have standardized virtual networking and overlay networks across all network vendor equipment, virtual switches and cloud management systems. Examples of such protocols include VXLAN, OpenFlow™, or control-plane protocols such as BGP.

Open source communities are playing an important role in the evolution of cloud architectures in at least two important areas: the cloud orchestration platform (both OpenStack and Apache CloudStack), as well as the SDN controller software (through OpenDaylight, Floodlight, etc). Another key open source cloud component is the Open vSwitch (OVS), which has a rapidly expanding development community and is becoming a de facto standard for Linux™ deployments.

Open source projects generally ensure interoperability between solutions from multiple vendors and can shorten development cycles. However, they are not strictly required to achieve interoperability if other interfaces and protocols have been sufficiently agreed to by vendors and between products. As a result, there is not a one-size-fits-all approach when it comes to "open" in the emerging cloud ecosystem. The cloud industry has benefited from the open source approach of OpenStack as a multi-vendor cloud orchestration platform.

NFV ORCHESTRATION

Network Functions Virtualization is the key to unlocking the true potential of the cable industry's broadband and data center infrastructure. By supporting the instantiation and delivery of any service—independent of the access and transport technologies—NFV offers MSOs a significant competitive advantage.

Management and Orchestration is a key capability that needs to be implemented on the MSO cloud infrastructure for NFV. The ETSI NFV Industry Specification Group has defined the Management and Orchestration (MANO) functional group to include three components: the virtual infrastructure manager (VIM), the VNF manager (VNFM) and the NFV orchestrator (NFVO). VIMs are responsible for controlling and managing the compute, storage and network resources. Typically there are multiple VIMs responsible

for the resources at different NFV points of presence (PoPs) or data centers.

One or more VNFMs are responsible for managing the life cycle of VNF instances including the deployment, monitoring, scaling, healing, and software upgrade processes. Finally, the NFVO has two quite different responsibilities: the orchestration of resources across multiple VIMs, and the life-cycle management of network services, which consist of one or more VNFs.

While the NFV infrastructure manages sets of compute, storage and network resources, MANO elevates this to the application level; that is, MANO understands which resources belong to specific NFV applications. MANO enables users to monitor and control the state of NFV applications. With the VNFM function, MSOs can deploy applications and execute other life-cycle actions according to pre-established recipes, reducing time-to-market and helping to reduce human error.

Arguably the most important role of MANO is service assurance; that is, it helps providers to deliver services that are at least as highly available as those delivered with traditional physical network functions. Typical production NFV deployments will be distributed across multiple NFV-PoPs to avoid single points of failure due to technical or force majeure events, but even single location events need significant assurance capabilities. MANO is responsible for collecting status information and alarms related to infrastructure resources and also those at the application level related to VNFs and network services. Unlike traditional network functions that are delivered as a bundle of hardware and software, NFV applications and the underlying infrastructure are separate elements that can fail independently. In case of a failure, a critical MANO capability is to help operators understand which infrastructure resources are used to deliver the application services (physical to virtual to application mapping) and determine the real source of the failure (root cause analysis); for example, whether the failure is caused by a problem with a server or network or whether the failure is due to an application issue.

Another aspect of service assurance is disaster recovery. In case of a catastrophic event, MANO can help restore service applications faster through automated deployment, a process that may be less prone to human error than manual restoration.
MANO is also responsible for establishing and monitoring the (virtual) networks need for internal communication among the components of VNFs or between multiple VNFs that may or may not be distributed across multiple locations.

MANO plays an important role in the security of the solution. MANO itself needs to be secured against attacks and MANO should also help to secure NFV applications against outsider and insider attacks. With role-based access control, access rights for different user roles such as cloud admin and application owner can be carefully defined, and permitted user actions should be logged to make sure that a person responsible for all actions can be identified. MANO should be protected against illicit external access using a multi-tier architecture and web application firewalls. The MANO system needs to adhere to national security requirements with the appropriate certification level. MANO should allow the definition of security zones, security groups, and security appliances to isolate applications from each other. The system should be scanned for security vulnerabilities using appropriate tools. Private keys of VNFs need to be protected. All of these functions need to be accessible through an easy-to-use user interface, typically a GUI with appropriate logging capabilities for system events and user actions.

In addition, these functions need to be available through APIs to higher layer management systems such as an operations support system (OSS)/business support system (BSS) or VNF-specific element management systems.

Model Based Orchestration

Due to the challenges of human management and procedural orchestration, a model and policy-based approach to orchestration becomes a requirement. In this approach, VNFs and NFV infrastructure are described through domain-specific languages and different engines automate a variety of operational processes based on these models. A major advantage of the model-based approach is the possibility for different engines to use the same model for their respectivepurposes.

- Deployment/placement
- Capacity management, scaling
- Healing and root-cause analysis
- Maintenance/software upgrades
- Agile development and operations (devops)

On-boarding of Virtual Network Functions (VNFs)

While the ultimate goal of NFV is the full life-cycle automation of VNFs and their management by the NFV platform, a pragmatic step-by-step approach may be required for on-boarding of VNFs. This Multi-step methodology allows for an agile, fast, initial on-boarding of VNFs, while providing a path that will ultimately realize the full benefits of NFV.

The on-boarding of a VNF is a multi-dimensional activity aiming to gradually carry out transformation in various areas such as networking, hardware, applications and their management, and also in the way the service provider is internally organized, in order to progressively take more advantage of the benefits offered by NFV. This means some VNFs are more advanced in one dimension than others.

The iterative on-boarding process allows for a gradual advancement toward the ultimate scenario of fully automated life-cycle management of the VNF. While there is no rigid path toward this progression, we can identify some typical major milestones:

• *Deployment:* At this stage, new instances of the VNF can be automatically created and deployed by the NFV Platform, which uses the information in the VNF Descriptor to fetch the software binaries from the VNF Catalog, and then instantiates and configures them over the selected NFV-Infrastructure.

• *Automated healing:* At this stage, the NFV platform can automatically handle the healing process; for example, the recovery of an application after failure of a hardware or software component. Typically, once an alarm is triggered either by the OSS or by the NFV MANO platform itself, a set of automatic actions are automatically executed to restore the application's functions. These actions can consist of the re-creation of the failed software component on a different server, the modification of the networking configuration, and other actions to connect the newly re-created software with the other components.

• *Automated scaling:* As the load on a network function varies, the network function may require more resources (or fewer resources) to be able to function without being slowed down. Therefore the resources allocated to the VNF need to be increased (scaled up) or be reduced (scaled down). At this stage of integration, the VNF platform is capable of identifying when the resources allocated to a VNF are close to being exhausted (typical example is high CPU usage due to high demand). It will then automatically allocate additional resources, create additional

instances of the software components that need to be scaled out, and most importantly reconfigure the network so that traffic is distributed over a larger pool of resources. A similar set of actions are also performed, when an application no longer requires the extra capacity allocated to it, and resources are automatically freed.

• *Automatic full life-cycle management:* The ultimate objective of NFV is to allow not only for the instantiation and automated management of an existing release of a VNF, but also to automatically update (application of patches) and upgrade (roll-out of new releases) the VNF with minimum or no outages, thus relieving the operational team from the tedious tasks that are often executed outside normal working hours. The automation of life-cycle management also protects the system from potential human errors that can happen during these critical maneuvers.

OPERATIONAL SUPPORT SYSTEM (OSS) SIMPLIFICATION

Today, there is a real opportunity for service providers to simplify their OSS by introducing a highly automated and dynamic approach to service operations. Why is this happening today?

First, the use of virtualization and other cloud software technologies inside network functions (NFV) and their deployment as applications on IT infrastructure provide the opportunity to enrich and align network operations with agile IT operations practices. Dynamic application lifecycle management principles can be leveraged from the IT world and directly applied to network functions, which allows simplification by moving from dedicated to IT standardized processes including DevOps automation processes.

Second, new flexibility is introduced by linking the OSS processes to the features of NFV orchestrators and SDN controllers as programmable networking technologies exposed using open APIs. OSS systems that are able to leverage the capabilities of such dynamic resource managers can then achieve the dynamic operations processes that are required to take full advantage of NFV and SDN.

Assuming that the introduction of new technologies will take some time, an effective evolution strategy must also consider service operations across hybrid networks consisting of both current and new technologies. In particular, the following two aspects of OSS evolution need to be addressed, sequentially or in parallel.

1. NFV readiness: The current OSS needs to be assessed with respect to its capability to move up the value chain from current to dynamic operations. This includes cleaning up current OSS service fulfillment, inventory and assurance stacks (by consolidating and automating where possible), and ensuring OSS readiness for dynamic process support. These steps are required in order to play a part in the target OSS for NFV and SDN and to be ready for dynamic operations.

2. Introduction of new operations solutions linked to NFV and SDN technologies: This includes extending or elaborating new operational processes that work across network/SDN and cloud/NFV platforms, as well as analyzing their impacts on current processes and organizations.

Abstraction is particularly useful for OSS service operation in an NFV & SDN world where highly dynamic resource management may take place in order to avoid service impacts. Abstraction between resource and service layers is key for end-to-end dynamic

operations & OSS simplification. Abstractions of underlying domain capabilities, whether technical, organizational, or geographical domains, are needed to shield the service operations OSS from resource-focused details.

These abstractions are gathered in catalogs, and become the atomic elements for easy service composition. Abstraction and composition can be repeated as often as needed to simplify end-to-end service operations. The availability of a simple information model to represent service instances with minimum information at each abstraction level is essential to this approach. This model allows the required object hierarchy to be implemented, where instances are created dynamically through service orchestration or auto-discovery, and can also be used by automated service assurance processes, thus enabling to close the current gap between fulfillment and assurance.

Hybrid service orchestration is also a key requirement while we are in this transitional state. E.g. using agile orchestration for activation of end-to-end services across Physical Network Function (PNF) and VNF based networks. The solution should allow the MSO to create a simplified and open orchestration architecture that works across networks and IT, and isolates business operations from network management.

OSS simplification should address automated assurance and dynamic operations:

- *Automated assurance*: This capability addresses customer needs by bringing customer care and network operations closer together through intelligent root cause and service impact analysis tools. This typically include analytics-driven automation of service assurance and allows you to build in proactive, automated processes that automatically identify and resolve service and network issues, and possibly avoid them through proactive measures.

- *Dynamic Operations for NFV and SDN*: This capability enables the operationalization of NFV and SDN based services by closing the loop between automated assurance and hybrid service orchestration through a common engine that spans across networks and IT and automates the discovery and reconciliation of network resources.

THE VALUE-ADDED SERVICE (VAS) OPPORTUNITY

Until now, MSOs supplying connectivity services to businesses have largely deferred to third-party CPE vendors, VARs and cloud-based managed service suppliers to provide value added services and applications over those connections that are specific to customers' needs.

But the emergence of cloud-hosted models and with the deployment of flexible networking and delivery platform for virtualized functions, MSOs can create the opportunity to tie into those models to layer robust portfolios of value-added options into their service bundles.

Virtual VPNs can open a path for MSOs into this value-added services market at a moment when access to cloud-based applications is transforming business operations. The wide-spread embrace of the benefits from lower costs, greater agility and better service availability that have softened market resistance to the cloud has made the availability of bundled value-add options a natural next step in market migration to ever greater cost savings and efficiencies.

The significance of MSO's opportunity to bundle VAS with connectivity services is reflected in a global survey of SMBs conducted by researcher AMI-Partners. The

study found SMBs prefer bundled SaaS offerings over single services by a margin of four to one.

Leveraging revenue-sharing partnerships with SaaS providers and developers, cable operators can avoid the painful experience of watching other entities use their high-speed connections to capture all the VAS business. They can up sell their connectivity customers to bundles of cloud-hosted services and applications that can be automatically provisioned through customer service representatives (CSRs) and self-help portals. With dashboard control over those apps, customer administrators can manage usage and other policies on a per-employee basis and set up access for outside collaborators as they're brought in to work on specific projects.

CONCLUSION

The MSO case for the aggressive pursuit of new commercial service opportunities through use of virtualized networking and NFV technology is clear. By deploying some of the capabilities mentioned in this paper, not only will operators be able to take the lead in providing the SD-VPN connectivity that SMBs need to maximize operational efficiency and lower costs, but also will be well positioned to build the in-house capabilities and partnerships with SaaS providers that will allow them to compete aggressively in the lucrative VAS market.

As revealed in research studies of market trends and the analysis supplied by Bell Labs Consulting, there's a vast pool of pent-up demand at all business levels for the benefits MSOs can deliver via SD-VPN connectivity and associated value added services. Costs of implementing these capabilities, unlike many new network technologies, are low enough to ensure payback on MSO investments within a very short time. With the ability to meet customers' VAS needs, MSOs will have an opportunity to drive those returns ever higher over time.

REFERENCES

1. Computer World, 2015 IT Spending Forecast, November 2014

2. AMI-Partners, SMB Cloud Playbook – Opportunities & Actionable GTM Insights, November 2014