Operationalizing SDN and NFV Networks

May 2015

Deloitte Consulting LLP

Preface

A revolution is sweeping through the telecommunications world, leading to possibly one of the biggest upheavals in the hundred plus year old industry. Telecommunication networks are migrating from traditional hardware and appliance-centric deployments to cloud-based deployments, with software as the critical component of all network functionality. At the heart of this revolution are two technologies: Network Function Virtualization (NFV), and Software Defined Networking (SDN), both of which aim at virtualizing network applications as well as the network connectivity. Both these technologies, and the interaction between them, have been undergoing trials over the past few years, and new standards as well as architecture options have begun to emerge. While most of the initial focus has centered on defining the solution architecture, the stakeholders responsible for operating these networks *viz.*, network and IT operations teams, need to still iron out operational aspects which are critical to seamless delivery of end user services. Migration from network element-centric to software-centric operations will drive fundamental changes in the network operating model across multiple dimensions, from tighter integration across network, IT, and architecture teams to new processes, and tools to manage the network. In this point of view, we present some of the leading practices for software-centric network operations, based on successful early stage implementations, that can help Communications Service Providers (CSPs) effectively manage their services and end user experience within the NFV and SDN domain.

Figure 1: Key drivers for migration to NFV and SDN

Challenge	Driver	Impact
Increased revenue to cost disparity	• Large CAPEX required to support increasing traffic volumes • Rapidly declining revenues (on a per traffic unit basis)	• Reduced service provider profitability • Continued growth in expense – both CAPEX and OPEX
Increased proprietary hardware in network	• OEM-built differentiators into proprietary hardware and software • Historically, specialized hardware has provided better performance	• Vendor lock-in leading to high costs for expansion and upgrade • Limited ability to introduce new vendors due to compatibility issues
Heavy effort to launch new services	• Custom development to ensure that proprietary hardware and software systems work together • Coordination required across multiple organizational silos to launch service	• Limited ability to challenge competition such as OTT players with disruptive offers • Increased time to catch up with competition when needed
Limited flexibility and agility	• Network resources are mostly static and tied to a geographic location • Dynamic adjustments to alleviate traffic hotspots and congestion not supported	• Networks need to be over-provisioned to handle worst case traffic scenarios • Sub-optimal utilization of network resources

Changing business dynamics and operational challenges are driving the shift to SDN/ NFV

From a CSP perspective, while user data traffic has been growing exponentially with the increase in over-the-top (OTT) and other data-centric services driving high capital investments, revenues have not kept pace. NFV and SDN are complementary technologies which leverage cloud infrastructure and can help both increase revenues with the rapid introduction of new services, and reduce expenses by shifting from expensive proprietary hardware to lower cost commodity hardware. With NFV, functionality such as firewalls, load balancers, deep packet inspection and IP Multimedia System (IMS) nodes which were traditionally implemented with hardware-based appliances, are delivered as software-based Virtual Network Functions (VNFs) on a carrier-grade cloud infrastructure. SDN, on the other hand, simplifies the connectivity between physical and virtual network elements at layer 2/3 via network virtualization protocols such as OpenFlow. NFV and SDN together offer an elegant solution for CSPs looking to address the challenges driven by business dynamics and operational considerations for today's telecom networks. Some key underlying industry and business drivers for migration towards NFV and SDN are shown in Figure 1.

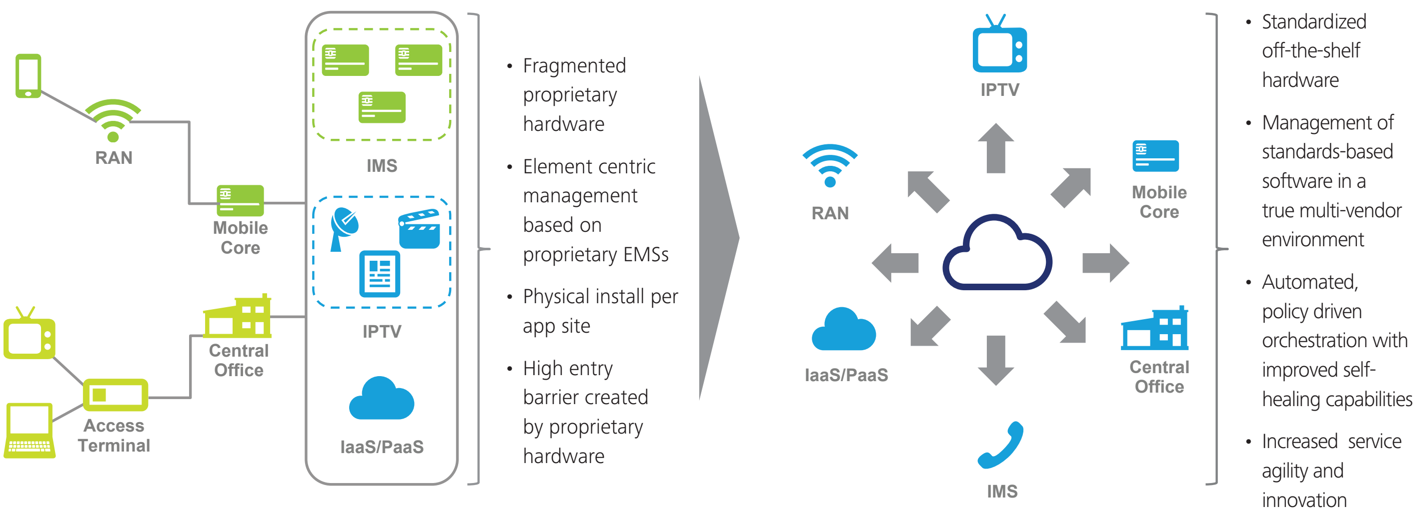
NFV and SDN will introduce a radical shift in telecom network architecture

NFV and SDN principles can be applied to most telecom access and core level network elements. Transport elements such as routers and switches in both the Local Area Network (LAN) and Wide Area Network (WAN) network segments can be replaced by commodity switches supporting SDN approaches such as OpenFlow.

Similarly, most hardware-based elements such as IMS nodes, Evolved Packet Core (EPC) platforms and Content Delivery Network (CDN) platforms, can all be virtualized on the cloud infrastructure with NFV. CSPs are also exploring alternatives to migrate hardware-based Customer Peripheral Equipment (CPE), such as Set Top Boxes (STBs), to NFV based principles. As illustrated in Figure 2, in a completely virtualized environment, most services would be based on a common cloud platform which can deliver Telco-grade capabilities.

However, the migration path towards the network shown in Figure 2 is likely to be a phased one, primarily governed by business decisions and investment lifecycles. Operations teams will be faced with the reality of needing to manage hybrid deployments, including both physical and virtual network elements, for an extended period of time, and need to be equipped with the necessary tools, processes, and skills to do so.

Figure 2: Telecom Architecture shift towards a NFV/SDN Environment



Migration to the NFV/SDN architecture will impact most operations functions

With the migration of networks to a virtualized and software-centric model, current operations functions and processes need to undergo major changes to ensure delivery of carrier grade performance. Key considerations for effective operations in NFV/SDN networks include:

- Service strategy and design needs to maintain status quo in terms of operational performance for traditional services being migrated to NFV/SDN.
- Carrier grade performance needs to be ensured by leveraging features such as dynamic creation and migration of virtual network functions to meet availability requirements.
- Operations needs to migrate to "management by exception" wherein most common errors and performance degradations are addressed via automated self-healing and self-optimization rules.
- Critical functions such as fault, outage, and performance management need to be supported with smooth handoffs across different teams which maintain physical and virtual network resources.
- The skillset of operations teams needs to be expanded to include scripting capabilities (or their equivalent via GUI-based tools) to be able to effectively create "recipes" for managing software VNFs.
- A DevOps-based model which drives closer coordination between operations and development teams needs to be introduced to improve service agility and quality.

The role of operations spans across the entire service lifecycle, and each of these stages is impacted by the introduction of NFV and SDN based networks. The entire operations model including processes, tools and technology, as well as people and organization needs to be redesigned for each functional area within Service Design and Fulfillment, Service Operations and Readiness, as well as Service Assurance.

Figure 3: Functional Domains by Service Lifecycle

Service lifecycle area	Functional domains
Service fulfillment	Activation and provisioning
Operations support and readiness	Change management
	Capacity management
	Inventory management
	DevOps
Service assurance	Performance management
	Fault management
	SLA/OLA management
	End-to-end service management

While the changes required in each operations functional domain will be operator-specific, CSPs can leverage certain leading practices which have been implemented by traditional cloud infrastructure providers and tailor them to their specific NFV/SDN deployment plan. CSPs would also be best served by leveraging these practices to first develop an operations model for the target state where all components are virtualized, and then subsequently developing a transition plan which addresses hybrid deployments.

The remainder of the whitepaper focuses on identifying these best practices for each lifecycle stage, which can help service providers manage their networks efficiently, and deliver on the promise of this network revolution.

> "The technology is the 'easy' part. Implementing SCNs (Software Controlled Networks) and maximizing business benefit will require significant planning and a healthy appreciation of what it means to overhaul network operations"

Analysis Mason, October 2014

"SDN and NFV are disruptive from a management perspective because they require a change at every level: in employee skillsets, process reengineering and automation, and new OSS capabilities"

Heavy Reading, September 2013

Leading practices for service fulfillment

Activation and provisioning

For an ideal service launch experience, it is necessary to ensure that setup and end-to-end orchestration via Management and Orchestration (MANO) happens without any errors. This can be ensured by leveraging the following practices:

- Activation and provisioning needs to be enabled via an intuitive portal which provides a simplified workflow, and pre-defined templates for standard activities such as service definition and composition, service activation, as well as service modification.
- Provisioning should be based on industry standard protocols such as YANG, NETCONF, and TOSCA – which enable end-to-end chaining of components from multiple vendors in a seamless manner. Newer protocols also include support for rollback, to enable a revert to the original configuration in case any step of the end-to-end provisioning fails.

Telefonica

- As a part of Project UNICA, Telefonica is leveraging open APIs to manage its virtual infrastructure deployment.
- YANG and NETCONF based network models are being used to define services and configure Virtual Network Functions (VNFs) from multiple vendors, implementing specific network functionality.
- Service realization consistency is ensured using standardized templates to implement defined network models.

Leading practices for operations support and readiness

Change management

One of the key benefits of implementing a SDN and NFV based network is increased agility. This is, in part, enabled by the fewer errors in change management because fewer manual steps are needed for sign-off and change implementation. The following practices can help in creating an automated change management process, which speeds up realization of the approved changes:

- A software-based workflow should be implemented to acquire approvals for changes, and automatically effect approved changes via the centralized orchestrator.
- Logically isolated test environments, built using SDN, can provide the ability to simulate multiple What-If scenarios and quantify impact of planned changes in a staging environment.

ebay

- Ebay 's focus to build its developer cloud as an extension to its production cloud, so as to minimize fragmentation caused by dedicated physical environments.
- Development, test, and production environments share infrastructure, and are logically separated using SDN.
- Production changes are deployed seamlessly from developer environments via extensive automation.

Inventory Management

In the NFV and SDN world, inventory management needs to be considered at the service, virtual network application, and resource level (Virtual Machines (VM) and physical server). With a highly dynamic virtual environment, one click access to the most up to date inventory becomes a necessity. To support these requirements, the following leading practices need to be adopted:

- Physical inventory data needs to be enhanced to include VNF and virtual network details in order to build an integrated view of utilization of logical and virtual resources across the infrastructure.
- A software repository will be needed to maintain details such as package versions and license usage.
- Auto discovery algorithms and version controlled archival systems need to be implemented which can help establish a real-time topology view and inventory reporting system. This reduces troubleshooting issues by providing the ability to identify the exact topology at the time of an event.

DevOps

To achieve improved multi-service release stability and greater deployment agility, network changes will need to be managed in a methodical and consistent way, while eliminating need for device/hardware specific scripts, and reliance on specific team members. To meet this requirement in a virtualized and software defined network infrastructure engineers need to apply DevOps principles pioneered in the enterprise cloud environment. Some leading DevOps practices are as follows:

- The network's tolerance for frequent changes needs to be increased by automating testing and deployment of changes across multiple non-production and production environments.
- Creating an automated test suite allows changes to be verified and risks to be identified through event driven triggers across multiple environments, thus, avoiding last-minute surprises.
- Operations is deeply involved with solution design and testing of end-to-end capabilities prior to the software drops in the production environment. Feedback from operations on production networks is tracked, maintained, and rolled into subsequent product sprints.

Leading practices for service assurance

Performance management

For effective management of services in the virtualized environment where performance is highly dependent on underlying cloud infrastructure, self-learning and predictive techniques must be developed to manage end-to-end service performance by intelligently correlating inputs at all levels and across locations. This can be achieved by adopting some of the leading practices as outlined below:

- New or revised KPIs/KQIs *e.g.,* Infrastructure Response Time, VNF Contention Analysis, and sophisticated algorithms need to be defined that can correlate inputs at all levels and provide insightful performance views across VNFs and virtual infrastructure.
- Predictive analytics needs to be leveraged to proactively manage resources based on predicted faults, dynamically update policies and rules based on real-time traffic characteristics. This can help minimize the occurrence of issues across the virtualized infrastructure.
- Self-optimization capabilities need to be introduced in performance management modules which can optimize configuration based on current network performance *e.g.,* scale up VMs, add new VNF instances for load balancing, configure new routes between VMs, etc..

> "A real-time network self-optimization use case replaces manual traffic engineering processes. This produces a 27% five-year total cost of ownership savings compared to manual processes"
>
> ACG Research, August 2014

Fault management

Early fault detection and mitigation is key to deliver carrier grade availability and improve end user customer experience. With the ability to proactively correlate physical and virtual level faults at a service level and performing VNF/network topology reconfiguration, Mean Time To Repair (MTTR) can be greatly reduced. Leading practices for proactive fault management include:

- The service model should be leveraged to identify all components and links impacted by a particular fault. This can be done by using the YANG model to identify which components of a service are impacted, trigger policy-based alarms, and suppress duplicate alarms.
- Policy driven self-healing strategies need to be implemented to route around faults identified via monitoring of various instances of a VNF across VMs and performing distributed failure checks.

Google

- Google supports automated failure detection based on periodic reports to its traffic engineering engine to monitor its inter-datacenter WAN.
- As demand fluctuates or unanticipated events occur, the traffic engineering engine computes options for optimal network utilization and minimal service disruption.
- The software defined network is re-programmed automatically for effective remediation with no manual intervention.

SLA/OLA management

To be able to maximize benefits from the use of virtualization, stringent Service Level Agreements (SLAs) need to be enforced onto the groups providing operations support for the underlying cloud infrastructure. This is needed to ensure that the carrier-grade requirement for availability (e.g., 5 nines) and other regulatory (e.g., NEBS) compliance requirements are met. Additionally, Organization Level Agreements (OLAs) also need to be updated to encompass all types of VNFs hosted in the network. Implementing the following practices will ensure effective SLA/OLA management:

- Carrier-grade SLA/OLAs need to be enforced on Commercial off the Shelf (COTS) hardware and software components to ensure that off-the-shelf solutions can support carrier-grade network requirements. These SLAs and OLAs also need to be enforced across organizations supporting the underlying platform on which network services are provided.
- A common SLA/OLA framework needs to be established with all vendors providing software-based VNFs or controllers. While the framework can be used to establish implementation guidelines, it must be flexible enough to support different requirements based on VNF type.
- SLAs and OLAs need to include key operational parameters such as service response time and scalability, packets lost, etc. and not be limited to the time in which an assigned ticket is acknowledged.

End-to-end Service Management

To manage and meet expectations on a per-customer basis for multiple services the focus needs to shift from merely monitoring network and node level KPIs, and turn towards analysis and correlation of performance at every layer of the network stack. The following practices will enable this correlation:

- End-to-end Service Quality Management (SQM) with integrated dashboards which provide the ability to drill down along the VNF chain all the way to the underlying virtual and physical resources and help localize issues.
- Cross domain correlation based on metrics for service accessibility, integrity, and retention which are built on new/revised KPIs/KQIs with inputs from VNFs, virtualized infrastructure, and network layers.

Conclusion

The industry metamorphosis towards NFV and SDN platforms has been gaining significant momentum over the past two years. Although 2014 has seen a focused increase in Proof of Concept and lab trials undertaken between vendors and service providers, most efforts have been focused on defining the architecture and technology with little emphasis on routine operations. A significant impact of NFV and SDN implementation will be negating the need for vendor-specific, and/or service-specific network management tools that service providers having been using to configure, monitor, and troubleshoot their networks. Service providers have made massive investments in people and processes centered on these proprietary tools and technology, thus creating multiple organizational silos. Operations will need to evolve from service/operational silos to standardized cross services operations management.

As service providers begin work to integrate NFV and SDN alongside legacy networks, appropriate operational structures will also need to be created. A renewed organizational paradigm and re-designed operations processes enabled by a flexible MANO and standardized set of tools will be key to unlocking the benefits of NFV and SDN in a traditional service provider environment.

Authors

Rahul Bajpai
Director
Technology, Media, and Telecommunications
rbajpai@deloitte.com

Sanket Nesargi
Specialist Leader
Technology, Media, and Telecommunications
snesargi@deloitte.com

Ketan Merchant
Senior Consultant
Technology, Media, and Telecommunications
kmerchant@deloitte.com

Vijay Pareek
Senior Consultant
Technology, Media, and Telecommunications
vipareek@deloitte.com

References:

- Heavy Reading, "Driving Network Agility Through A Service Orchestration Approach", April, 2014
- Tail-f, "Automating Network and Service Configuration Using NETCONF and YANG"
- ETSI, NFV ISG Whitepapers, 2013-2014
- Telefonica, "UNICA Infrastructure Experience, Mobile World Congress", 2014
- Hightech Webinar, "The SDN And NFV Gold Rush - How Will Providers Strike Gold?", September, 2013
- Google, "B4: Experience with a Globally-Deployed Software Defined WAN", 2013
- Deloitte, "Manage Your Cloud While Staying Grounded", 2011
- Analysis Mason, "Software Controlled Networking: Cloud, NFV, and SDN are important for next generation networks", September 2013
- ACG Research, "Business Case for NFV/SDN Programmable Networks", August 2014
- eBay, "OpenStack@eBay: Practical SDN Deployment using Quantum", October 2012