Understanding and Embracing SDN and NFV-Based Network Solutions to Drive Operational Efficiency

An Executive Brief Sponsored by AT&T

Roopashree Honnachari
Industry Director – Business Communication Services & Cloud Computing Services

August 2015
INTRODUCTION

The enterprise market demand for high-speed bandwidth continues to grow, driven by growing convergence of enterprise applications—Voice over Internet Protocol (VoIP), Unified Communications (UC), video, Internet and data—onto a single network. Multiprotocol label switching virtual private network (MPLS VPN), Dedicated Internet Access, Carrier Ethernet, VoIP/UC and video conferencing are all considered strategic services that represent a sizable revenue growth potential for service providers. Frost & Sullivan estimates that the total market revenue from these services will exceed $50 billion by 2020. That is a tremendous growth in revenue; and in order to tap into it, communication service providers (CSPs) need to invest in core networks that can handle the traffic growth expected from these services.

IP-based network services such as MPLS VPN and Ethernet support the movement of large amounts of enterprise wide area networking (WAN) traffic in a secure and reliable manner. However, the underlying static or monolithic nature of these network services—any changes to network in terms of bandwidth changes can take weeks or even months to provision—is a deterrent to the fast-changing bandwidth requirements of corporate WAN.

Furthermore, emergence of cloud computing is adding another dimension to the bandwidth growth, wherein the network has to be capable of handling dynamic workloads between enterprise onsite, remote and cloud hosted data centers. For service providers to support cloud usage needs, the core network must be capable of scaling dynamically, while delivering the level of performance necessary for the traffic type and end-user business requirements.

Software-defined Networking (SDN) and Network Function Virtualization (NFV) technologies hold the potential to help CSPs to shift from static or monolithic network architecture to a software-centric one. This paper presents an analysis of the following aspects within SDN and NFV-based network solutions:

▪ Enterprise market trends driving the need for SDN and NFV-based network solution
▪ Operational benefits from deploying SDN and NFV-based network solutions
▪ Key considerations for enterprises planning to deploy SDN and NFV-based solutions
▪ AT&T's Network on Demand offering, and the value proposition it brings to the market

SDN AND NFV EXPLAINED

SDN is a technology architecture that decouples the network control from the forwarding functions of the physical infrastructure. In SDN architecture, a controller determines how packets get forwarded by networking elements, separating the control and data planes within switches and routers. SDN technology does for network services what virtual machines (VM) do for servers—it enables physical network resources to be pooled together and consumed on-demand.

As shown in Exhibit 1, below, the infrastructure layer (data plane) comprises network elements, which expose their capabilities toward the control layer (controller plane) via interfaces southbound from the controller. The applications exist in the application layer (plane), and communicate their network requirements toward the
controller plane via northbound interfaces. In the middle, the SDN controller translates the applications’ requirements, and exerts low-level control over the network elements, while providing relevant information up to the applications. An SDN controller may orchestrate competing application demands for limited network resources, according to policy.

**Exhibit 1: SDN Architecture**

OpenFlow, a protocol that became an industry standard in 2011, is the primary southbound interface between the control and infrastructure layers. Along with new protocols in development, OpenFlow is designed to facilitate open communication between different vendor devices, the rest of the network, and third-party applications. The application layer is home to legacy Operations Support Systems (OSS) and Business Support Systems (BSS), other network and business applications, and the orchestration function.

Network Function Virtualization, or NFV, is a related network architecture that proposes virtualization technology to networks. The aim of NFV is to replace the multitude of proprietary network elements—hardware-based switches and routers usually contained within a CSP network—with industry standard, centrally managed commodity-based servers. In the network, NFV allows routers, switches, firewalls, load balancers, content delivery systems, end-user devices, IMS Nodes, and almost any other network function to be run as software on virtual machines—ultimately, on shared servers, using shared storage.
While SDN and NFV are complementary and mutually beneficial, they are not inter-dependent. SDN can improve NFV performance (simplify compatibility, ease operations); NFV enhances SDN via virtualization, and IT orchestration and management techniques. Although the industry consensus is that NFV and SDN are not inextricably linked at this stage in their development, Frost & Sullivan believes that the long-term and best use of these technology architectures is as complements to each other.

**MARKET TRENDS DRIVING ENTERPRISE CONSIDERATION OF SDN AND NFV-BASED NETWORK SERVICES**

The following section presents an overview of the key market trends driving enterprise consideration of SDN and NFV-based network services.

**Consumerization of IT**

The new business environment is highly mobile, and requires IT resources to be available 24/7, wherein key stakeholders—geographically dispersed teams, partners and customers—expect to do business around the clock. This means that IT must keep IT infrastructure, applications and services running at peak efficiency, with minimal interruption or downtime. While the IT team is able to access IT resources in an on-demand manner using cloud, the same is not true for network resources.

Traditional network services, while they can handle peak bandwidth demands, are not elastic enough to address the current customer needs driven by mobility and cloud-based applications. SDN-based network services enable enterprises to procure and ramp-up network resources in tandem with their cloud resources. Furthermore, the concept of bring your own device (BYOD) is enabling these mobile users to bring their own smart phones and tablets to access corporate resources, thus making it challenging for IT managers to protect corporate data and meet compliance mandates. The centralized control of network intelligence in the SDN model provides increased network reliability and security. The IT team will also have the ability to control the network at a more granular level, and apply policies at the session, user, device, and application levels.

**Exponential Growth in Video Traffic in Enterprise and Consumer Markets**

The growing penetration of video among enterprises, to increase collaboration and reduce travel costs, is a key driver for high-speed WAN services in the business market. While there is a significant base of video endpoints and infrastructure in the market, there is a growing trend towards adoption of hosted audio, Web and video conferencing services. Whether endpoints-based or hosted video conferencing services, the need for high-speed networks is critical to ensure performance quality. According to recent Frost & Sullivan estimates, the North American conferencing services market exceeded $4.5 billion in 2014. Furthermore, enterprises are increasingly evaluating hosted or cloud-based UC solutions—an integrated set of voice, data and video communications applications—which is further driving the need for reliable and dynamic, high-speed access network services.

In the consumer market, residential broadband Internet service, Internet Protocol TV service (IPTV), and VoIP are some of the services that are driving IP traffic growth on service provider networks. Broadband Internet services represent the largest share of IP traffic on service provider networks, as Internet connection speed drives the rate at which voice and video are accessed.

While cable dominates the residential video services subscriber market share today, IPTV service and Over the Top (OTT) services (dominated by Netflix, followed by Hulu) adoption has been growing as consumers cut the

---

cord. According to Frost & Sullivan’s latest research, IPTV and OTT subscribers in the U.S. multichannel video services market exceeded 13.2 million and 46.5 million, respectively, in 2014; generating revenues in excess of US $11.2 billion and $5.9 billion, respectively, for twelve months ended 2014. Exhibit 2 shows the steady increase in IPTV and OTT subscribers in the U.S. Residential Video Services Market.

**Exhibit 2:** U.S. Residential Multichannel Video Market: Subscriber Growth by Technology, 2007 to 2014

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable</td>
<td>63,529</td>
<td>62,296</td>
<td>60,950</td>
<td>58,942</td>
<td>57,810</td>
<td>57,808</td>
<td>55,726</td>
<td>54,525</td>
</tr>
<tr>
<td>IPTV</td>
<td>1,708</td>
<td>3,625</td>
<td>5,702</td>
<td>7,351</td>
<td>8,956</td>
<td>10,481</td>
<td>12,141</td>
<td>13,224</td>
</tr>
<tr>
<td>Satellite</td>
<td>30,611</td>
<td>31,299</td>
<td>32,660</td>
<td>33,356</td>
<td>33,852</td>
<td>34,140</td>
<td>34,310</td>
<td>34,330</td>
</tr>
<tr>
<td>OTT (Netflix and Hulu)</td>
<td>7,326</td>
<td>9,164</td>
<td>11,892</td>
<td>18,518</td>
<td>24,358</td>
<td>30,246</td>
<td>38,570</td>
<td>46,510</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan

As service providers continue to ramp up their networks to support the growth in subscriber base, and related traffic growth, virtualizing network elements (virtual CPE, for example) and automating network control can be of immense value. SDN and NFV technologies, combined, can enable the network to handle the video traffic—broadcast HD video content, interactive applications such as gaming, Web browsing and video on demand—efficiently, even while reducing operational costs.

**CSPs Need to Prepare for Enterprise Transformation to an IT as a Service Model**

IT as a Service (ITaaS) is a new service delivery model that delivers all of an enterprise’s compute, storage, networking, and security—as a service—running on nearly any hardware the company chooses. ITaaS is an organizational shift for the IT department: to transform itself into a service provider to the business, providing employees, partners, and customers with access to all IT resources as a service. In this way, IT shifts from the old, reactive provisioning and management organization to a proactive organization dedicated to innovation and productivity solutions.

As enterprise IT departments are looking to undergo a transformation from asset managers to service providers, they are leveraging technologies and solutions such as virtualization and hybrid cloud to deliver a range of services, quickly and cost-effectively, to their businesses. The on-demand procurement option and the pay-as-you-go billing model associated with cloud services are influencing the buying behavior of enterprises for network connectivity services. Enterprise need for on-demand network services, driven by the rapid adoption of cloud and virtualization technologies in the IT department, is a key trend driving SDN initiatives among network service providers.

The US Infrastructure as a Service (IaaS) market revenues exceeded $7 billion in 2014, indicating that despite concerns regarding data security, compliance, and application performance, enterprises are making the leap to

---


cloud to reduce their IT costs, and to manage the data growth. Furthermore, Frost & Sullivan’s recent analysis of the US Data Center Services market predicts that in 2015, IaaS revenues will surpass traditional data center services revenues. Frost & Sullivan believes that as enterprises increasingly make cloud an integral part of their IT infrastructure, they will place more emphasis on the networks that connect the various pieces (on-prem cloud, private data centers, public cloud, co-location facilities, managed hosting) of their hybrid IT deployment model.

SDN architecture enables service providers to provision universal ports, which allow enterprise customers to take advantage of the market demand for private network connectivity to cloud. These universal ports enable enterprises to provision the WAN service of their choice—Ethernet or VPN—in real-time, and pay for just the capacity they use.

**Big Data & Mobility**

Big Data applications are gaining traction across industries, driving the need for faster, more flexible and more scalable computing and network resources. Organizations are looking to big data analytics to unleash insights from their traditional data, as well as from newly acquired social data, and from IT and network operational data. Big Data analytics involves new data processing techniques applied to large amounts of data. Both the processing and the storage utilize commodity hardware in a distributed architecture, making network performance critical.

In the current highly mobile business environment, geographically dispersed teams, partners, and customers expect IT resources to be available to them around the clock. This means that IT must keep IT infrastructure, applications and services running at peak efficiency, with minimal interruption or downtime. Cloud computing is a key enabler for enterprises to extend anytime, anywhere access to mobile users. In a Frost & Sullivan Cloud survey, close to 60 percent of the respondents stated that cloud makes it easier for them to connect remote and mobile employees.

For cloud and hybrid Big Data deployments, SDN can enable enterprises to procure large amounts of on-demand bandwidth capacity, in real-time. The programmability of the network to provision network resources (and manage performance and security aspects, centrally) in a matter of minutes—as opposed to the lengthy manual chore involved in making changes to a traditionally-defined physical network—is of immense value in an increasingly cloud-centric world.

**OPERATIONAL BENEFITS FROM DEPLOYING SDN AND NFV-BASED NETWORK SOLUTIONS**

The following section details the key operational benefits to enterprises from deploying SDN and NFV-based network solutions.

**Reduced Total Cost of Ownership (TCO) and Operational Complexity**

NFV eliminates the need for proprietary hardware; and enables routers, switches, firewalls, load balancers, content delivery systems, end-user devices, IP Multimedia Subsystem (IMS) nodes, and almost any other network function to run as software on virtual machines. The ability to run these network functions on commodity servers can result in major cost savings, which the network service providers can pass on to enterprises. Today, managed customer premises equipment (CPE) services, offered with MPLS VPNs, Ethernet, and managed security services, represent a significant share of the investment that enterprises spend on networks services. NFV-based services facilitate the shift from dedicated hardware to virtual CPE, which can be provisioned in minutes, and

---

costs significantly less than physical hardware. Virtual CPE combined with SDN reduces network installation and provisioning times, simplifies network management activities for IT teams, and results in reduced Total Cost of Ownership (TCO) for the enterprise.

**Real-Time Bandwidth Scalability**

In an SDN architecture, the control plane is separate from the data plane, thus enabling physical resources to be pooled together and managed by a central SDN controller. The underlying network is automated to enable enterprise users to scale their network bandwidth in real time, similar to that of provisioning VMs. For example, if an enterprise needs to increase bandwidth on its network that connects the on-prem data center to a hosted cloud data center, for weekly backups, it could provision bandwidth on-demand for the duration required. The ability to provision bandwidth on-demand, and pay for just the amount of bandwidth consumed, not only reduces network costs, but also offers immense network procurement flexibility to enterprise users.

**Reduced Installation Times**

Installation intervals or delivery times promised with traditional network architectures can range from 30 to 90 days, or more in some scenarios. The lengthy cycle time is attributed to a number of factors, including evaluating customer site readiness, ensuring that all the required network elements are in place, and, if not, sending a truck out to install the necessary hardware at customer site, and configuring the circuit. SDN as a capability automates the network provisioning steps and processes. Combining NFV with SDN, a virtual CPE can be instantiated, and network resources can be provisioned in near real time, as opposed to months, as is the case in traditional network architectures. Hence, by choosing a software-centric network solution, enterprises can provision network resources faster, as demanded by their business needs.

**Security Aspects Built into the Network Solution**

In software-centric network architecture, the SDN controller abstracts the logic from the infrastructure layer and puts it in the global centralized layer, making security inherent or native to the SDN controller, as it is included in the software mix in the early stages. The SDN controller makes it easier to apply uniform security policies across services, and deploy additional security measures, in real-time, as everything is in the virtual machines. Key security aspects of an SDN and NFV-based network solution include:

- Enterprise IT department can choose to deploy modular security solutions by spinning up VMs to combine security solutions from multiple vendors. For example, users can deploy a virtual Juniper firewall with a set of additional features from other vendors.
- Automated security patching, as network administrators can set up policies for patching updates to happen at scheduled times.
- Reduced administration and management burden for the enterprise IT teams, as it is a lot easier to deal with VMs compared to physical appliances or hardware.
- The traditional perimeter security measures are still prone to highly sophisticated security threats. Using an SDN controller, enterprise network administrators can introduce security at a VM level, to ensure a deeper level of security measures on enterprise applications.
- In the event of a distributed denial of service (DDoS) attack on the SDN controller, VM, or a virtual network function VM (for example, a router or a firewall), the affected VM can be quickly detected,
isolated, shut down, quarantined, and replaced by another dynamically instantiated VM. The threat then can be quickly resolved by applying security patches to fix the code vulnerability. Enterprise IT teams can quickly spin-up identical VMs in a different location to restore and ensure resiliency and reliability of infrastructure.

**KEY CONSIDERATIONS FOR ENTERPRISES WHILE TRANSITIONING TO SDN AND NFV-BASED NETWORK SOLUTIONS**

SDN and NFV technologies are new to enterprises, with varying levels of understanding among IT decision makers. While some enterprises have a deep understanding of these technologies, and are ready to implement SDN and NFV, others are less familiar with the benefits of these solutions. Slow evolution of industry standards, and limited implementation of SDN and NFV in service provider networks are factors deterring enterprise interest in these technologies. Additionally, even when enterprises understand SDN and NFV, they are not sure of what steps to take while transitioning to SDN and NFV based solutions.

The following section details the key considerations for enterprise IT decision-makers that are looking to deploy SDN and NFV-based network solutions in the near future.

**Strategic Technology Roadmap and Planning**

The first step in implementing SDN and NFV-based network solutions, as in most IT implementations, is to have a clear technology roadmap. Create a roadmap that clearly defines the key phases of SDN and NFV deployment strategy, which could include aspects such as:

- Transitioning from TDM to IP networks
- Consolidating multiple data centers to fewer, but more efficient ones
- Deploying a private Ethernet-based network along with multisite VPNs, to connect distributed customers, partners, suppliers, and employees.

Most large companies have multiple networks from different vendors, which make it difficult to transition to a software-centric model without proper inventory management. With a detailed technology migration roadmap in place, the next step is to take stock of the inventory of existing vendor agreements. It is critical that enterprises factor in the disparate networks that are in place before introducing SDN and NFV into their network infrastructure; as a piecemeal approach to deploying SDN and NFV-based network solutions will not yield all the operational benefits of these technologies. Considering the transition to a software-centric network infrastructure will be a multi-phased process. Having a clear technology roadmap will help enterprises transition in small increments, with minimal disruption to their business goals. Enterprises that have sophisticated IT teams can either follow a do-it-yourself approach to develop a clear SDN and NFV deployment strategy, or work with a trusted service provider partner that can help them plan, deploy and manage the solutions.

**End-to-end Program Management and Management Tools**

The second step, after developing a strategic technology roadmap to deploy SDN and NFV-based solutions, is the end-to-end program management of the transition plan, which cuts across multiple organizations or layers of the company. As noted, enterprise networks could be a mix of various vendor networks spanning wireline and wireless services, and TDM and IP-based services, to list a few. A strong program management plan to evaluate
existing services configurations, prioritize the sequence in which the transition will occur, and train resources to facilitate SDN and NFV-based network solutions, is key to ensuring the overall progress of the technology roadmap.

Management tools are crucial to performance management of network solutions. Enterprises have historically either deployed their own application performance and network management tools, or used the ones offered by their WAN service providers. With the emergence of SDN, some large companies have created their own SDN-like platforms, which have functionality and orchestration capabilities that not only work across networks, but also across application and cloud environments. For enterprises that have a basic understanding of SDN and NFV technology, it is imperative to consider service provider offerings with application programming interfaces (APIs), which can integrate with their own existing orchestration and management platforms.

**Program Governance and Ongoing Innovation**

The third and final step in the transition to SDN and NFV solutions is post-implementation program governance and on-going management of solutions, as these technologies are new, and changes need to integrate as they emerge.

As bandwidth scalability in real-time is a key feature of SDN and NFV-based network solutions, an important element of program governance is aligning existing processes and policies to limit access control to certain personnel for making bandwidth changes. Policy control ensures that enterprise IT decision makers can take advantage of the flexibility of network solutions without any adverse financial impact due to unauthorized personnel making changes to the network.

The ongoing innovation in the SDN and NFV solutions arena can make it difficult for enterprises to keep up. Working with a service provider that has deep expertise in offering managed services can be beneficial to enterprise customers. Alternatively, enterprises with in-house expertise to manage SDN and NFV-based solutions could use service provider platforms—which provide the necessary tools and levers to perform bandwidth changes, and gain visibility into network SDN controllers and infrastructure, etc—and integrate their internal business applications and performance management tools into the platform.

**AT&T’s Network on Demand Offering: Redefining Network Connectivity**

AT&T’s Network on Demand offering is part of the company’s “Software Defined Architecture” initiative to modernize and simplify its WAN services using SDN and NFV. AT&T is the first and only US-based network service provider, so far, to have deployed SDN and NFV technologies at a large scale. AT&T’s Network on Demand capability is currently operational, with AT&T Switched Ethernet (ASE) services across its 21 state network footprint. The Network on Demand offering comes backed by all the business benefits of SDN and NFV-based network solutions—faster network provisioning, granular bandwidth, and deep security features—discussed throughout this document.

The following section details the key features and benefits of AT&T’s Network on Demand offering.

**Market Availability and Pricing Structure**

AT&T’s Network on Demand capability is operational with AT&T switched Ethernet services; and this capability is currently available across its 21-state footprint. Enterprises can procure Network on Demand on AT&T’s intra LATA (intra city) and inter LATA (intercity) Ethernet footprint.
AT&T's Network on Demand service pricing structure consists of fixed and variable components that include:

- A one-time charge for any wiring required, and port installation
- Fixed monthly recurring fees for the provisioned port
- Variable or usage-based bandwidth fees for the network capacity procured on demand

**Ease of Network Procurement and Management**

AT&T Network on Demand enables business customers to order network services on-demand. Customers use a self-service portal to choose and order network capacity, as needed. The company has implemented high levels of automation into the process, from service ordering to port and bandwidth provisioning, to billing and management. This reduces enterprise user complexity of ordering, and speeds-up delivery time. Bandwidth can be provisioned in real time (for ports and physical circuits already in place), as opposed to days (new circuits where physical wiring is required can take 3 to 5 days to be provisioned). Cost of ownership is lowered for customers, as they only pay for what they use, instead of fixed monthly recurring charges.

The capability comes packaged with five different classes of service. Customers can choose from 14 different port speeds (varying from 2 Mbps to 1 Gbps) to configure bandwidth capacity. The bandwidth change will be, initially, limited to one change per day.

**Ability for Existing AT&T Switched Ethernet Customers to Create Hybrid Networks**

The Network on Demand offering takes into consideration the needs of existing AT&T switched Ethernet customers by providing customers the option to create hybrid networks. Existing ASE customers can add new sites on Network on Demand; while AT&T ensures that all sites can communicate with each other. This way, customers can trial Network on Demand before making the switch completely, when they are ready. For example, if an existing ASE enterprise customer is opening a new business location, it can procure Network on Demand at that site, to create a hybrid network. Enterprise IT teams can further monitor the hybrid network via a self-service portal to track network inventory. Business drivers for enterprises to use Network on Demand are the quick turn-up time, simplified ordering process, and the ability to scale bandwidth up and down, as needed.

**“Sell & Deploy” Approach to Transition Potential Customers in the AT&T Footprint to the Network on Demand Offering**

AT&T’s “sell and deploy” initiative allows sales personnel to sell the Network on Demand offering to business locations that are already inside or close to a fiber lit building in the AT&T network footprint—but without SDN equipment installed. For such customers, AT&T will send out a technician to the customer site within eight business days, to assess whether the site is Network on Demand-capable, and to determine the delivery intervals associated with provisioning a new circuit. The delivery interval varies based on one of four scenarios requiring AT&T to 1) add a new customer terminating device; 2) add a cable; 3) carry out some construction; or 4) extend fiber under feeder. AT&T’s “sell and deploy” initiative aims to fast-track rollout of SDN capabilities across its fiber network footprint.
THE LAST WORD

SDN and NFV hold the potential to enable enterprise network transformation from a traditional monolithic architecture to that of a software-centric architecture. In an increasingly cloud-centric world, the programmability of the network—ability to provision bandwidth in real time, and manage performance and security aspects, centrally—is of immense value. In addition, the consumption-based pricing model for bandwidth, as in the cloud model, makes it easier for enterprises to better manage their overall IT and network costs. AT&T’s Network on Demand is an example of the SDN and NFV-based network solutions that enterprises could readily deploy to kick-start their journey to software-centric network architecture.

Roopashree (Roopa) Honnachari

Industry Director –
Business Communication Services & Cloud Computing Services
Frost & Sullivan
rshree@frost.com

Share this with your peers
ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041