

UTILIZING NETWORK FUNCTION
VIRTUALIZATION FOR AN AGILE
ENTERPRISE WAN

F R O S T  S U L L I V A N

An Executive Brief Sponsored by AT&T

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

July 2016

INTRODUCTION

The enterprise wide area networking (WAN) space is undergoing a major transformation, primarily driven by the increased penetration of cloud services. The on-demand, agile architecture of cloud services is dictating the need for WANs that can scale in real-time to take advantage of cloud services. Network Service Provider (NSP) initiatives around Software Defined Networking (SDN) are addressing the need for on-demand bandwidth.¹

While SDN is enabling the transformation of WAN from a static, inflexible architecture to that of an agile and flexible software-centric one, enterprise data centers (and branch locations) are still crowded with multiple hardware devices for separate network functions. For example, it is common to have a firewall appliance and a WAN optimization device alongside routers. As the number of sites in an enterprise WAN grows, so do the number of hardware appliances required for separate functions, thus increasing network operational costs and complexity. What if these various network functions could be consolidated into a single device, and run as software?

Network Function Virtualization, or NFV, is a network architecture that can help achieve virtualization in the WAN. The aim of NFV is to replace the multitude of proprietary network elements—hardware-based switches and routers—with industry standard, centrally managed commodity-based servers. NFV allows routers, switches, firewalls, load balancers, content delivery systems, end-user devices, IMS nodes, and almost any other network function to run as software on virtual machines (VMs)—ultimately, on shared servers, using shared storage.

NSPs are increasingly deploying NFV along with SDN, as they are complementary and mutually beneficial. SDN can improve NFV performance (simplicity, compatibility, ease of operations); and NFV enhances SDN via virtualization, IT orchestration and management techniques. As NSPs deploy these technologies, enterprises can benefit as well. NSPs are evaluating and deploying SDN and NFV to reduce their overall operational expenditure on networks, and to deliver new services to enterprises. While the value proposition of these complex technologies may not be immediately apparent to enterprises, there are clear business benefits to working with an NSP that has a roadmap in place to embrace SDN and NFV.

In this paper, we compare and contrast traditional network approaches with NFV, and detail the business benefits of deploying NFV-based services or virtual network functions (VNFs). We also evaluate AT&T's NFV-based offering—Network Functions on Demand—and the value proposition it brings to the market.

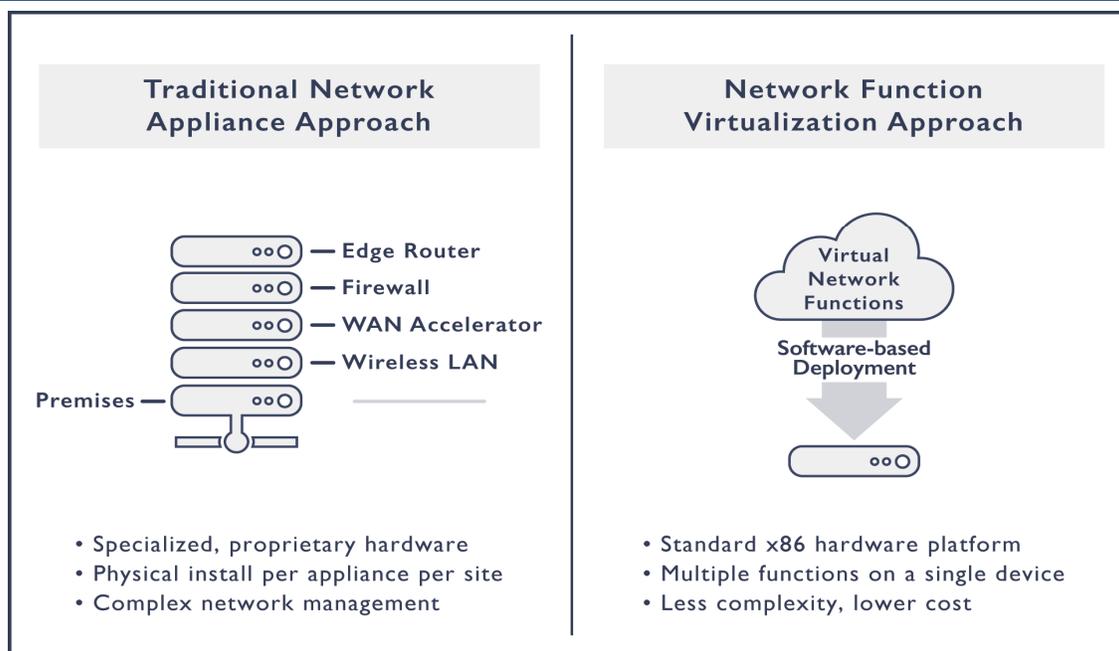
¹ SDN is a technology architecture that decouples the network control from the forwarding functions of the physical infrastructure. In SDN architecture, a controller determines how packets are forwarded by networking elements, separating the control and data planes within switches and routers. SDN technology does for network services what virtual machines (VM) do for servers—it enables physical network resources to be pooled together and consumed on-demand.

WHY SHOULD ENTERPRISES CARE ABOUT NFV-BASED SERVICES?

The benefits of NFV that service providers are realizing—reduced hardware cost, faster deployment of network functions, automated service chaining,² reduced network operational expenditure, and the enhanced ability to launch new services—are the same benefits that enterprise can also realize by choosing NFV-based solutions. NFV-based solutions translate to virtual network functions (VNFs) for enterprises. Using VNFs, enterprises can achieve enhanced control over their networking functions, with dramatically improved provisioning cycle times; and deploy new applications and services in a matter of hours or days. Following is a list of traditional network challenges addressed by adopting VNFs.

The enterprise WAN consists of multiple proprietary hardware devices—routers, WAN optimization controller (WOC), Application Deliver Controller (ADC), firewalls, etc—that are expensive to deploy and manage. NFV uses virtualization techniques to deploy network functions in software—virtual network function (VNF)—running on commodity hardware. Exhibit I depicts the comparison of a traditional network approach with the NFV approach.

Exhibit I: Traditional Approach vs. NFV



Source: Frost & Sullivan

With NFV, the enterprise WAN equipment is replaced by virtualized universal customer premises equipment, or uCPE, which can be installed in a Telco closet or a datacenter. The uCPE is a plug-and-play device that can be effortlessly set up by the enterprise IT team. The device, once plugged in and booted up, connects to the NSP cloud, downloads the necessary VNFs, and installs and activates the software. For example, separate VNFs could be launched for each network function—one VNF for WAN optimization, and one for firewall—instead of deploying multiple hardware devices.

² Service chaining is a series of network services, such as WAN accelerators or firewalls, which are interlinked through the network to support an application.

Faster Deployment Cycles with Reduced Operational Costs

In the traditional network approach, every network function runs on proprietary hardware appliances that are physically deployed, and maintained separately. When all of the network functions that enterprises have at each site are multiplied by the number of locations, it quickly adds up to hundreds or thousands of boxes to manage in the network. With NFV, VNFs can be deployed on a premises-based x86 based white box or in the cloud, thus reducing the amount of hardware equipment in the enterprise WAN; which means less hardware costs, less moving parts, less things that could go wrong, and less maintenance for the IT team due to reduced overall operational scale.

Furthermore, VNFs can be instantiated on-demand, and can be programmed and managed remotely, leading to dramatically shorter delivery cycles, as services can be deployed in minutes, rather than days, as previously required in the traditional hardware-based approach.

Improved WAN Efficiency

As VNFs run on a virtualized uCPE, the number of devices that need physical maintenance is limited. In the traditional network approach, if a device failed, the NSP had to replace the hardware for each function. In the case of VNFs, the network administrators can just rip and rebuild that function, as everything is in software. The VNF download and storage configuration can be up and running in a matter of minutes, as opposed to days in the hardware-centric approach. Furthermore, NSPs offer service level agreements that typically include shipping of a replacement uCPE in 4-6 hours, in case the physical device fails.

The software-centric nature of VNFs also makes it easy for network administrators to carry out on-going maintenance of WANs. In the traditional network approach, for any changes to the network functions, a technician had to be sent to carry out the reload on the equipment for enterprises. With VNFs, the NSP's support team can remotely access the VNFs to make periodic changes and updates. The cost savings, in terms of maintenance cost alone, could result in 10-15% savings for enterprises.

Ability to Deploy Enhanced Security Features in a Modular Fashion

NFV-based solutions make it easier to deploy additional security measures, in near real-time, as everything is in the virtual machines. Enterprise IT departments 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 firewall from one vendor, and then add a set of additional features from other vendors. In the event of a distributed denial of service (DDoS) attack on the VM or a VNF, the affected VM can be quickly detected, isolated, shut down, quarantined, and replaced by another dynamically instantiated VM. The threat can then 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. The VNF approach also reduces network administration and management burdens for the IT teams, as it is a lot easier to deal with VMs compared to physical appliances or hardware. For example, software policies can be set-up for patching updates to happen at scheduled times.

Catalog-based Multi-Vendor Approach Fosters Innovation

With NFV, NSPs can aggregate multiple vendors' solutions, and provide enterprises the ability to choose VNFs from various vendors. Enterprises can choose from a catalog of VNFs, which simplifies vendor management, as they do not have to deal with multiple vendors for each network function. The NSP takes on the burden of vetting the solution vendor, and managing relationships with them for the end customer.

The catalog-based multi-vendor approach enables the enterprise IT teams to innovate faster, as they can now choose best of breed solutions from different vendors without going through the CAPEX investment required in the traditional approach. For example, if they want to use a Juniper router instead of Cisco, they can do so, as it is only a matter of downloading the software, and configuring it. Alternatively, if they have always used Cisco, but want to try out a product from a start-up, they can do so using the VNF approach.

As VNFs enable network administrators to cut down the time spent on deploying and managing hardware boxes, they can focus on strategic initiatives of the company. Network and IT teams can now spend time doing real IT and networking versus administrative or supply chain functions that keep them from having the time to be innovative in their real jobs.

Fulfills “Green” Requirements by Reducing Hardware Sprawl

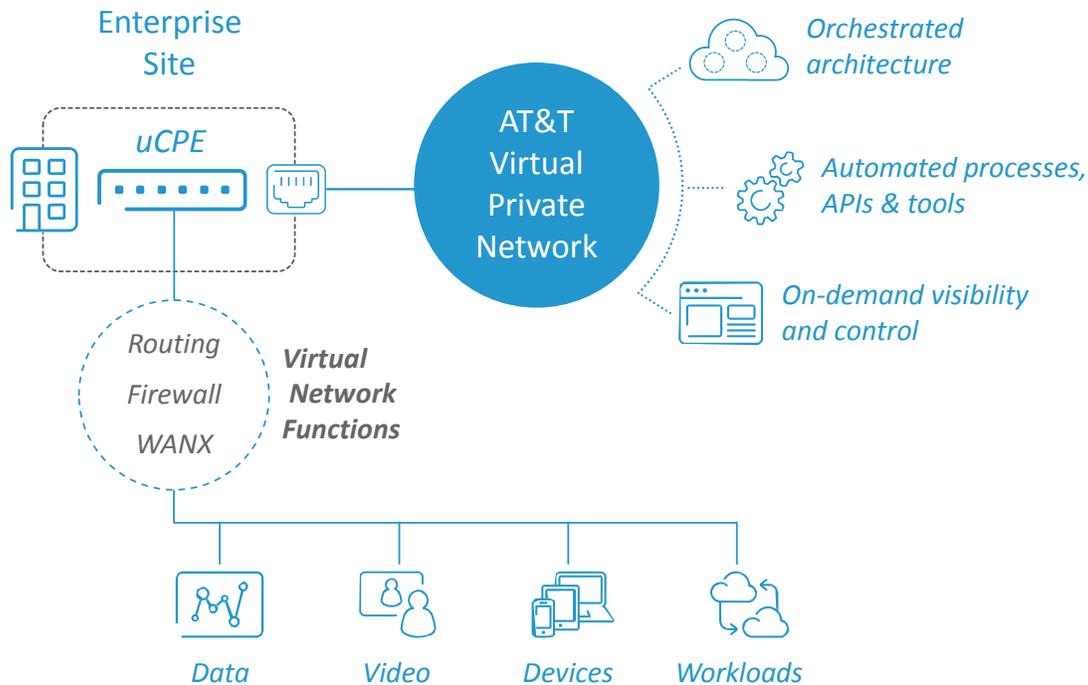
The uCPE typically has a thin profile and is racked, which eliminates the need for separate hardware for each function, enabling up to four VNFs to be delivered using a single device. From an environmental perspective and cost standpoint it uses less power, so enterprises can adhere to “green” initiatives they have in place. The uCPE also eliminates hardware sprawl, and hence reduces organizations' carbon footprint, and power and cooling expenses needed for telecom closet and data centers.

OVERVIEW OF AT&T'S NFV-BASED OFFERING

AT&T is an early adopter of SDN & NFV technologies. In 2013, the company launched its “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 technology on a large scale. The company has already made great progress by implementing an SDN controller into the network architecture, to automate network provisioning, and orchestrate changes across devices, locations and services.³

As a next step to its network simplification strategy, AT&T has embraced NFV to move network functions from hardware to software elements. The company's Network Functions on Demand solution is targeted towards enterprises to help them procure network functions on demand, which can be dynamically instantiated on a common infrastructure, when and where needed. Exhibit 2, below, depicts the NFV-enabled enterprise WAN.

³ For a detailed analysis of AT&T's SDN-enabled solutions please read the whitepaper: [Understanding and Embracing SDN and NFV-Based Network Solutions to Drive Operational Efficiency](#)

Exhibit 2: NFV-enabled Enterprise WAN

Source: AT&T

Service Availability

The Network Functions on Demand solution became available in the first half of 2016, with AT&T's VPN services. Existing AT&T VPN customers are able to access the VNFs through a uCPE, which is a plug-and-play device. The uCPE requires limited technical expertise, and can be quickly installed by any network administrator. The uCPE connects to the AT&T Cloud, downloads specified virtual functions (e.g., virtual router, virtual firewall), and installs and activates the software. Once the installation is complete, the uCPE assumes the identity of downloaded virtual network functions, and can be managed by AT&T or customers in near real time.

The current Network Functions on Demand solution includes a medium uCPE that supports up to 4 VNFs and a catalog of 4 VNFs—Juniper and Cisco virtual routers, a Fortinet virtual firewall, and a Riverbed WAN accelerator. The service is available in 76 countries around the globe.

Deployment Options

Network Functions on Demand solution can be deployed flexibly, using different models: on customer premises today, and in the AT&T Integrated Cloud (AIC), or both, in the near future. While some applications can be implemented in either location, others are better suited for a specific location. For example, a customer could choose to implement a WAN acceleration application on the premises, but want the virtual DDoS protection to be implemented in the AIC. Applications on the premises are dedicated to a specific site; but applications in the cloud can be shared by many sites, with throughput currently limited to 1 Gbps.

Pricing Structure

The pricing structure for Network Functions on Demand consists of monthly recurring charges (MRC) for the universal CPE, and separate charges for VNFs. For example, if an enterprise buys VNFs for router and firewall, it would incur two charges: MRC for the uCPE, and MRC for the two VNFs.

Phased Approach to Technology Refresh

The uCPE is easy to phase into existing WAN networks, and is more efficient in multi-site, mixed-vendor environments than proprietary equipment. AT&T's Network Functions on Demand solution allows customers to embrace VNFs in a phased approach. For example, a customer could deploy the uCPE as a router with an existing hardware-based firewall. When the firewall reaches its end of life, the customer can simply download a firewall VNF onto the uCPE, and run both functions there.

Customers whose network appliances are approaching a technology refresh cycle across multiple locations, and those with a conglomeration of acquisitions, for example, will benefit particularly from the NFV-enabled uCPE approach, as they attempt to simplify their infrastructures or integrate many disparate hardware platforms.

Future Roadmap

AT&T continues to invest in building VNF services with an eco-system of best-in-class vendors, as enterprise needs vary and there is no one-size-fits-all. AT&T has announced vendor relationships with Juniper, Fortinet, Cisco, Brocade, and Riverbed. In the future, customers will be able to pick the networking technology and the VNFs of their choice from a catalog of multiple vendors.

CONCLUSION

The enterprise WAN is transforming owing to the impact of cloud computing. The networks connecting various IT deployment models (on-premises servers, managed hosting, private cloud, public cloud, hosted private cloud) and users to cloud-based applications need to become more agile, to scale in accordance with the needs dictated by applications. The traditional hardware-centric approach to deploying network functions is time-consuming, as proprietary networking equipment needs to be deployed and configured. The inability to build and scale network infrastructure quickly has hindered enterprises' attempts to be more nimble in responding to business and customer demands. Embracing NFV-based solutions and VNFs can change that, as detailed throughout this paper. The ability to procure VNFs greatly simplifies WAN deployment and management functions. As your organization evaluates NFV based solutions, AT&T's Network Functions on Demand solution could be the right choice for you.

Roopa Honnachari

Industry Director – Business Communication Services & Cloud Computing

Frost & Sullivan

rshree@frost.com

Silicon Valley

331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio

7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London

4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
<http://www.frost.com>

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

Auckland

Bahrain

Bangkok

Beijing

Bengaluru

Buenos Aires

Cape Town

Chennai

Colombo

Delhi / NCR

Detroit

Dubai

Frankfurt

Iskander Malaysia/Johor Bahru

Istanbul

Jakarta

Kolkata

Kuala Lumpur

London

Manhattan

Miami

Milan

Moscow

Mumbai

Oxford

Paris

Rockville Centre

San Antonio

São Paulo

Sarasota

Seoul

Shanghai

Shenzhen

Silicon Valley

Singapore

Sophia Antipolis

Sydney

Taipei

Tel Aviv

Tokyo

Toronto

Warsaw

Washington, DC