The Re-emergence of Network Functions Virtualization in Enterprise WAN, and Why It Matters Now More Than Ever

Custom Research by ISG, Sponsored by AT&T Business

APRIL 2023

Introduction

COVID-19 has forced global organizations to fast-track their digital transformation initiatives. Cloud computing, edge computing, unified communications, and Internet of Things (IoT) are top-of-mind technology priorities for IT decision makers. As enterprise applications get increasingly distributed among hybrid cloud environments, enterprise WAN plays a critical role in optimally connecting distributed users (due to rise in remote/hybrid working trend) to distributed applications.

The enterprise WAN is evolving to a software-centric approach with software-defined networking (SDN), network function virtualization (NFV) and software-defined WAN (SD-WAN) technologies to support distributed users and applications. An SD-WAN architecture uses SDN principles to separate the data plane from the control plane in the WAN. It abstracts the underlying transport networks (MPLS, ethernet, wireless, satellite) and shifts control intelligence from edge devices into a centralized, software-based controller. SD-WAN technology brings the much-needed agility and flexibility to connect hybrid IT deployments in an effective manner. For example, the SD-WAN appliance (deployed in physical or virtual format) can automatically route traffic bound to cloud on internet links and to corporate datacenters on private links based on predefined policies by network administrators.

As SD-WAN deployments increase, businesses are quickly realizing that a holistic approach to enterprise WAN virtualization is critical, and several aspects of traditional WAN edge or branch infrastructure will need to change to make the WAN truly agile. The WAN network functions residing in businesses' branch locations — router, SD-WAN, firewall, LAN switches, end-to-end network visibility, etc. are still hardware centric, making them time consuming and expensive to deploy and manage. NFV-based approaches use virtual universal customer premises equipment (uCPE) that can host multiple virtual network functions (VNF). NFV brings immense operational and cost efficiencies by consolidating multiple functions on a single device and allowing network administrators to centrally manage and orchestrate the WAN.

While NFV-based virtual network services have been available in the market since 2016, market adoption has been slow due to several factors: cost of the uCPE, complexities involved in service chaining and orchestrating multiple VNFs across multiple domains, lack of clear understanding among network decision makers on the true value of uCPE approach, to list a few. However, virtual network services have evolved greatly in the last couple of years to address the past challenges and offer several benefits over the previous offerings. Most importantly, the supply chain issues in the telecom equipment space, owing to chip shortage during COVID-19 is another big reason to consider a software centric approach to deploying network functions that are heavily dependent on specialized hardware today.

As your organization deploys SD-WAN, it is critical to closely evaluate all other network functions that are important to ensure a cohesive WAN. Deploying an uCPE platform that can host multiple VNFs, including SD-WAN solutions from multiple vendors, addresses WAN virtualization in a holistic manner while giving your network administrators the freedom to pick and choose vendor solutions.

NFV Value Proposition to Enterprise WAN

The traditional enterprise WAN is laden with multiple specialized hardware devices — routers, switches, 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. 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.

With NFV, the enterprise WAN equipment is replaced by virtualized customer premises equipment that can run multiple VNFs and is called the universal CPE or uCPE. The uCPE 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 network service provider (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.

NFV Dramatically Reduces Deployment Cycles

In the traditional network approach, every network function runs on proprietary hardware appliances that are physically deployed and maintained separately. When all 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 lesser hardware costs, fewer moving parts, fewer 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.

NFV Delivers Superior Operational Efficiencies For WAN

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 to 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% to 15% savings for enterprises.

NFV Enables Network Administrators to Deploy Enhanced Security Features

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 protect 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.

NFV Offers Enterprises the Choice to Deploy Best-of-breed Solutions

The emergence of secure access service edge (SASE) frameworks is influencing businesses' decision to choose a single vendor solution for networking and security. However, several global organizations still prefer a best-of-breed approach that offers them the choice to work with multi-vendor solutions. 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. 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.

NFV enables Businesses to Fulfill "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 multiple 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.

NFV is Integral to Network-as-a-Service Trend Becoming a Reality

NaaS in its current form allows businesses to buy network hardware, software, and services in a subscription model. SDN and NFV are highly critical for NaaS model to become a reality. SDN enables true network flexibility and scalability, and NFV allows related network functions (routers, firewalls, VPN concentrators, WAN optimization devices, session border controllers and others) to be deployed as software. The subscription-based billing model of NaaS offers enterprises freedom from investing large amounts of their technology budget in network hardware and static connectivity services. With NFV at its core, network functions can be instantiated quickly on a premises-based uCPE or in the cloud. Currently, enterprise networks currently contain a great deal of hardware, hence NaaS contracts are typically longer than traditional contracts since hardware costs take longer to amortize. By integrating NFV based virtual network services into NaaS offerings, service providers can offer flexible contracting terms and lower penalties for changes on the uCPE.

Market Trends Driving Demand for NFV-based Virtual Network Services

SD-WAN Adoption Sets the Stage for Holistic WAN Virtualization

Cost-effective branch site connectivity, fast deployment times, centralized network management, and optimized cloud connectivity are the factors driving SD-WAN adoption among businesses. As SD-WAN gains traction, businesses understand that to fully realize the potential of a software-centric architecture, multiple WAN functions need to be agile. Using the uCPE model, businesses can consolidate and orchestrate functions such as routing, WAN optimization, security, and session border controllers from a single appliance. Hence, while the SD-WAN appliance offers some inbuilt routing, security, and WAN optimization features, it is prudent that businesses evaluate the uCPE model that supports multiple VNFs and offers the flexibility to choose from a catalog of vendors while architecting their WANs.

Hybrid Cloud Networking Trends

As enterprise applications are distributed across hybrid IT architecture, SD-WAN enables enterprise IT to predefine business policies through the SD-WAN controller to specify which cloud applications are suitably accessed directly through the Internet versus backhauled to a hub site. SD-WAN solutions have predominantly been deployed in the branch sites and cloud data centers so far. To implement a successful hybrid cloud strategy network managers need to ensure on-prem data centers, colocation data centers, cloud POPs and edge compute nodes all support the same infrastructure as a branch site. Virtual network services have evolved significantly to support multi-service orchestration across domains and offer enterprises the agility and flexibility to deploy VNFs at all these connection points.

Businesses Demand Fast Time-to-market to Retain Global Competitiveness

As organizations look to expand globally and bring new local sites online quickly it may not always be evident which global regions make business sense without testing the markets. With virtual network services, businesses can test new markets in an inexpensive way before investing CAPEX on branch locations. The COVID-19 pandemic has further highlighted the limitations of hardware-centric branch architectures. The fact that large portions of the workforce had to transition almost overnight to a remote working environment has escalated the challenges of shipping, deploying, configuring, and managing physical network appliances. As businesses embrace long-term remote working trends, optimizing and securing user connectivity to cloud-based applications requires local presence. To enable seamless access to cloud-based applications, businesses can deploy virtual network services at locally situated third-party data centers (for example, Equinix). Traditional branch site expansion involves tedious and time-consuming process that limits businesses' ability to compete effectively. With virtualized WAN (using a uCPE platform) global presence can be established in a fast and efficient manner.

AT&T NFV Based Virtual Network Services

AT&T Network Functions Virtualization solution targets businesses of all sizes to help them procure VNFs, which can be dynamically instantiated on a common infrastructure when and where needed. AT&T NFV solution is part of the company's overall software defined solutions (SDS) portfolio, consisting of SD-WAN and software defined core to support bandwidth on-demand services.

Seamless Evolution from SD-WAN to NFV
AT&T SD-WAN solution is delivered on vendor-specific appliances and a good fit for some customer requirements. However, deploying a single function appliance is expensive and does not support a holistic approach to WAN virtualization. AT&T NFV solution using a uCPE allows businesses to deploy multiple network functions on a single appliance. The virtual network services are supported on white boxes that range from extra-small (supports 2 VNFs) to extra-large (supports 12 VNFs) and cater to businesses' various edge requirements. AT&T NFV solution is both transport- and carrier-agnostic, which means it supports a wide scope of transport options including MPLS, Internet, Ethernet, and TDM services.

Extensive VNF Support across Multiple Environments
AT&T Network Function Virtualization solution supports a broad range of certified VNF vendors across routing, WAN optimization, firewall, application visibility, and SD-WAN applications. Notable among the vendors supplying VNFs include Cisco, Juniper, VMware, Aruba HPE, Fortinet, Accedian and Palo Alto. Some of these vendors offer multi-function VNFs (e.g., Fortinet, whose VNF includes security, SD-WAN, and routing), which when deployed on a uCPE are much more cost-competitive and easier to manage compared to single function VNFs. AT&T certified VNFs can be deployed on-premises, in the public cloud (Microsoft Azure, Google Cloud Platform, and AWS), and in third-party data centers such as Equinix and TAO. The support for multi-environment VNFs is extremely critical for businesses to succeed in their hybrid cloud strategy, and AT&T NFV solution delivers that.

Best-of-breed Solutions and Multi-vendor Orchestration
With AT&T NFV solution, enterprises can choose best-of-breed solutions that best fit their requirements, while enabling IT teams to innovate faster as they can deploy solutions from different vendors without investing in the capital expenditure (CAPEX) as required in the traditional approach. For example, you could deploy routing from Juniper, SD-WAN from VMware, and firewall from Fortinet. Network decision makers can choose from a catalog of certified VNFs, which simplifies vendor management by eliminating the hassle of dealing with multiple vendors for each network function. AT&T takes on the responsibility of vetting and certifying the solution vendor and managing relationships with it for the end customer.

One of the challenges to NFV adoption is the complexity of service chaining multiple VNFs and orchestrating these VNFs across different devices, networks, and applications. To address this challenge, AT&T NFV solution is backed by a multi-domain orchestration platform (from Ericsson) that greatly simplifies service chaining and offers immense design flexibility in terms of move, add, change, and delete requests.

High-speed and High-availability Options across Geographies

A critical challenge to uCPE adoption has been the limitation of bandwidth speed options (most supported less than 1G speed) on these devices, which makes them unsuitable for data center and hub sites. Businesses gravitated to high-speed SD-WAN appliances instead to fulfill the need for high speed appliance at data centers and hub sites. AT&T NFV solution includes appliances that support up to 10G speeds to allow customers the ability to deploy uCPE devices across their WAN edge locations (on-premises, public cloud, private cloud and third-party data centers).

As businesses adopt the software-centric architecture, it is prudent that they consider resiliency options to ensure continuity of operations. For instance, AT&T NFV solution is available in high availability options of dual uCPE devices and dual transport options. Customers can choose from service chaining combinations for firewall + SD-WAN and routing + firewall, in an active/passive model. Further, traffic can be set up to re-route over AT&T Network-Based IP Remote Access (ANIRA) or via customer-configured wireless routers.

Service Availability and Pricing Structure

AT&T Network Functions Virtualization solution is available in more than 200 countries and territories. Pricing structure allows for subscription-based pricing for the AT&T NFV solution, thus enabling businesses to move toward an OPEX model.

Conclusion

The traditional static, hardware-centric approach to building WAN architecture is complex and time-consuming, which hinders enterprises digital transformation efforts. SD-WAN technology, since its inception in 2014, has addressed some of the challenges of traditional networking in terms of network agility and automated network selection. However, with evolving enterprise needs and the maturity of SDN and NFV technologies, deploying single function SD-WAN appliances can be less than optimal. AT&T's NFV solution can help businesses truly realize the potential of a software-centric architecture by addressing the entire gamut of network functions, by offering best-of-breed solutions from multiple vendors. AT&T NFV solution is agile, carrier-and-transport agnostic, available in fully managed or co-managed options, allowing your organization flexibility in terms of how you architect your WAN.

To learn more about AT&T Network Function Virtualization, please visit: **www.att.com/nfv**

About the Author

Roopa Honnachari
Director
ISG
roopa.honnachari@isg-one.com

Roopa is ISG's subject matter expert in next-generation intelligent services such as SD-WAN, SDN, NFV, Cloud and Edge Networking, and established WAN services such as MPLS VPN, Ethernet, DIA and Waves. As part of the Network and Software Advisory team, Roopa assists clients in transformation initiatives around networking, security and enterprise solutions.

Roopa has been involved in global consulting engagements that are grounded in complex network and Information Technology transformation. Roopa has orchestrated transformations including SD-WAN, SDN, NFV based virtual network services, cloud services, UCaaS, and SIP trunking. Roopa's strong research background and in-depth knowledge on telecom technologies has helped her be part of engagements that include strategy assessments, RFP development, contract negotiations, transformation, and change management.

About ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,600 digital-ready professionals operating in more than 20 countries— a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit www.isg-one.com.