FROST & SULLIVAN

Software Define Your Enterprise WAN with Virtual Network Services

FROST & SULLIVAN WHITEPAPER

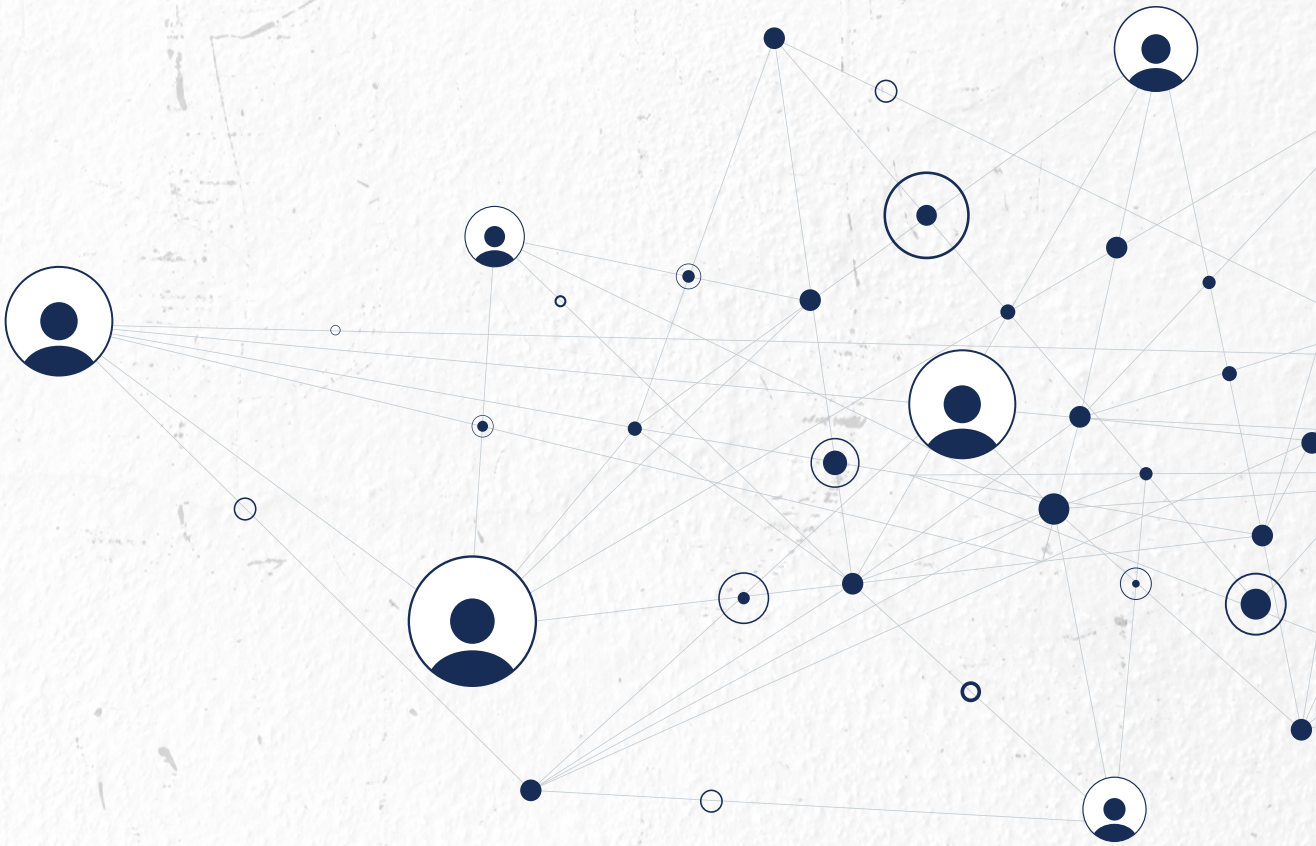
frost.com

Sponsored by

AT&T Business

Juniper driven by Mist AI

CONTENTS



Introduction

As businesses across verticals embrace hybrid cloud, Internet of Things (IoT), remote working, and edge computing trends, it is imperative to ensure the wide area network (WAN) being used is agile, flexible, and highly secure. While software-defined WAN (SD-WAN) solutions in the market today come integrated with some of these network functions—routing and security functions, for example—the network function virtualization (NFV)-based approach uses virtual universal customer premises equipment (uCPE) that can host multiple virtual network functions (VNFs). When an organization deploys SD-WAN, it is critical to closely evaluate all other important network functions to ensure a cohesive WAN. Deploying a uCPE platform that can host multiple VNFs, including SD-WAN, addresses WAN virtualization holistically while giving network administrators the freedom to pick and choose vendor solutions.

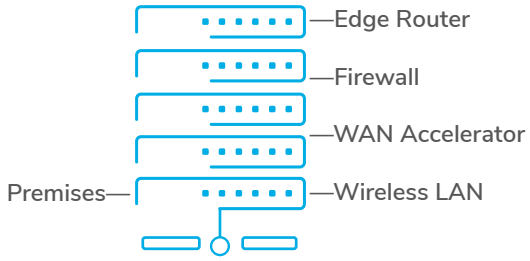
NFV-based virtual network services have been available in the market since 2016, but they have experienced slow adoption due to several factors: cost of the uCPE, complexities involved in service chaining and orchestrating multiple VNFs across multiple domains, and lack of clear understanding among network decision-makers on the true value of a uCPE approach, to list a few. However, virtual network services have evolved greatly in the last couple of years to address those challenges and extend several benefits not possible from previous offerings. In this paper, we summarize the greater benefits of virtual network services when compared to a traditional hardware approach, look at market trends driving the need for a platform-centric architecture to WAN virtualization, and offer insight into AT&T's virtual network services portfolio, AT&T Network Functions Virtualization, in collaboration with Juniper Networks.

Why Should Enterprises Care About NFV-based Services?

The enterprise WAN consists of multiple proprietary hardware devices—routers, WAN optimization controller (WOC), application deliver controller (ADC), firewalls, application visibility—that are expensive to deploy and manage. In contrast, NFV uses virtualization techniques to deploy network functions in software—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. The following list describes traditional network challenges addressed by adopting VNFs. Exhibit 1 compares a traditional network approach against an NFV approach.

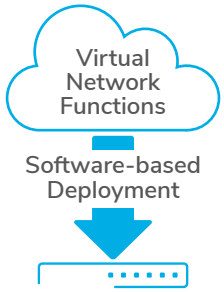
Exhibit 1: Traditional Approach vs. NFV Approach

Traditional Network Appliance Approach



- Specialized, proprietary hardware
- Physical install per appliance per site
- Complex network management

Network Function Virtualization Approach



- Specialized x86 hardware platform
- Multiple functions on a single device
- Less complexity, lower cost

Source: Frost & Sullivan

With NFV, enterprise WAN equipment is replaced by virtualized customer premises equipment that can run multiple VNFs and is called universal CPE, or uCPE. The uCPE can be installed in a telco closet or a data center. The uCPE is a plug-and-play device that an enterprise team can effortlessly set up. 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.

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 white box or in the cloud, thus reducing the amount of hardware equipment in the enterprise WAN; which means reduced hardware costs, fewer moving parts, less chance for things to go wrong, and limited maintenance for the IT team due to reduced overall operational scale. Furthermore, VNFs can be instantiated on-demand and programmed and managed remotely, leading to dramatically shorter delivery cycles—as services can be deployed in minutes rather than days—than what is required by 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 fails, the NSP must replace the hardware for each function. In the case of VNFs, network administrators can simply rip and rebuild that function, as it is deployed as 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 the shipping of a replacement uCPE within 4 to 6 hours if the physical device fails.

Moreover, the software-centric nature of VNFs 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 is deployed to physically 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 alone, could result in 10 to 15% 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, because everything is in the virtual machines (VMs). Enterprise IT departments can choose to deploy modular security solutions by spinning up VMs to combine 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 swiftly 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 the resiliency and reliability of infrastructure. In effect, the VNF approach reduces network administration and management burdens for the IT teams as it is a lot easier to deal with VMs than 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 Offers Superior Vendor Choices

With NFV, NSPs can aggregate multiple vendors' solutions and provide enterprises the ability to choose VNFs from various vendors. The NSP takes on the responsibility of vetting and certifying the solution vendor and managing relationships with it for the end customer. The catalog-based multi-vendor approach enables enterprise IT teams to innovate faster because they can now choose best-of-breed solutions from different vendors without investing in the capital expenditure (CAPEX) required from the traditional approach. If they have always used one vendor's hardware, but want to try a product from another, they can do so using the VNF approach.

> Enterprises can choose from a catalog of VNFs, which simplifies vendor management by eliminating the hassle of dealing with multiple vendors for each network function.

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 and enables multiple VNFs to be delivered using a single device. From an environmental perspective and cost consideration it uses less power, so enterprises can adhere to any "green" initiatives they have in place. The uCPE also eliminates hardware sprawl, and hence reduces organizations' carbon footprint as well as the power and cooling expenses needed for maintaining telecom closets and data centers.

Market Trends Driving the Need for Virtual Network Services

Businesses Ramp-up Digital Strategy Efforts

The COVID-19 pandemic has forced many businesses to fast-track their digital strategy. As organizations emerge from the pandemic, they are increasingly looking to deploy technologies to optimize resources, increase operational efficiency, and enhance business continuity. Frost & Sullivan research shows that hybrid cloud, unified communication as a service (UCaaS), SD-WAN, and network and application security are some of the areas in which businesses continue to invest. Virtual network services can dramatically reduce a business's hardware costs as multiple network functions can be consolidated into a single virtual uCPE. Furthermore, the software-centric approach enables VNFs to be instantiated effortlessly at the branch, data center, or cloud location, making it easy to deploy and manage network functions on the go.

Rise in SD-WAN Adoption

In the recent Frost & Sullivan SD-WAN survey, 27% of the respondents indicate they have deployed or have an SD-WAN deployment underway, and another 15% indicate they are extending SD-WAN to additional locations. Cost-effective branch site connectivity, fast deployment times, centralized network management, and optimized cloud connectivity are some of the drivers for managed SD-WAN adoption among businesses. As SD-WAN adoption gains traction, businesses understand that to fully realize the potential of a software-centric architecture, several WAN functions must be agile. Routing, WAN optimization, security, and session border controllers are some of the functions that the uCPE model helps businesses consolidate and orchestrate from a single appliance. Therefore, although the SD-WAN appliance offers some in-built routing, security, and WAN opt features, it is prudent that businesses select the uCPE model that supports multiple VNFs and offers the flexibility to choose from a catalog of vendors when architecting WANs.

Frost & Sullivan estimates North American **market revenues exceeded $2.7 billion in 2021**, with more than 280,000 operational sites.

Hybrid Cloud Networking

In Frost & Sullivan's 2021 Global Cloud Survey, 53% of the respondents say they have deployed cloud infrastructure as a service (IaaS), and 41% currently use hybrid cloud. Moreover, 43% of the respondents indicate they plan to deploy hybrid cloud in the next two years. As enterprise applications get distributed across hybrid IT architecture, SD-WAN enables enterprise IT teams to predefine business policies through the SD-WAN controller and to specify which cloud applications are suitably accessed directly through the Internet versus backhauled to a hub site. So far, SD-WAN solutions have predominantly been deployed at branch sites and cloud data centers. For businesses' hybrid cloud strategies to be successful, network managers must ensure on-premises data centers, colocation data centers, cloud points of presence (POPs), and edge compute nodes all support the same infrastructure as supported at a branch site. Ultimately, a uCPE offers the agility and flexibility to deploy VNFs at all of these connection points.

Multi-vendor Approach Provides Wider Choice

Customers of traditional hardware-centric WAN have struggled with its lack of agility and flexibility, which has created strong vendor lock-in. Virtual network services shift the entire architecture to become software-centric, where network functions deploy in a virtual format. The software-centric architecture not only brings great agility for VNF deployment, but also brings immense flexibility and choice for businesses during vendor selection. The NFV-based approach offers network functions on-demand through a catalog of best-of-breed solutions from multiple vendors. This means businesses have vendor independence to an extent (considering the catalog is still limited to the VNFs supported by the service provider), allowing customers to conduct technology bake-offs before deciding on which vendor to use. The traditional hardware-based WAN edge design does not support this kind of flexibility in vendor selection or deployment speed when designing or redesigning the WAN.

Enhance Global Competitiveness through Fast Deployment

As organizations look to expand globally and bring new local sites online quickly, understanding which global regions make business sense is not always evident without testing the markets. With virtual network services, businesses have a cost-effective way to test new markets before investing CAPEX in branch locations. In fact, the COVID-19 pandemic aptly highlights the limitations of hardware-centric branch architectures, and as most of the workforce (wherever applicable) had to transition to a remote working environment, almost overnight, the challenges of shipping, deploying, configuring, and managing physical network appliances escalated. Businesses can deploy virtual network services at third-party data centers (e.g., Equinix) to establish themselves in local markets near their users and enable seamless access to cloud-based applications. Whereas traditional branch site expansion involves a tedious and time-consuming process that limits businesses' ability to compete effectively, a virtualized WAN (using uCPE platform) approach creates a fast and efficient way for competitors to establish a global presence.

> As businesses adopt long-term remote working trends, a local presence is needed to optimize and secure user connectivity to cloud-based applications.

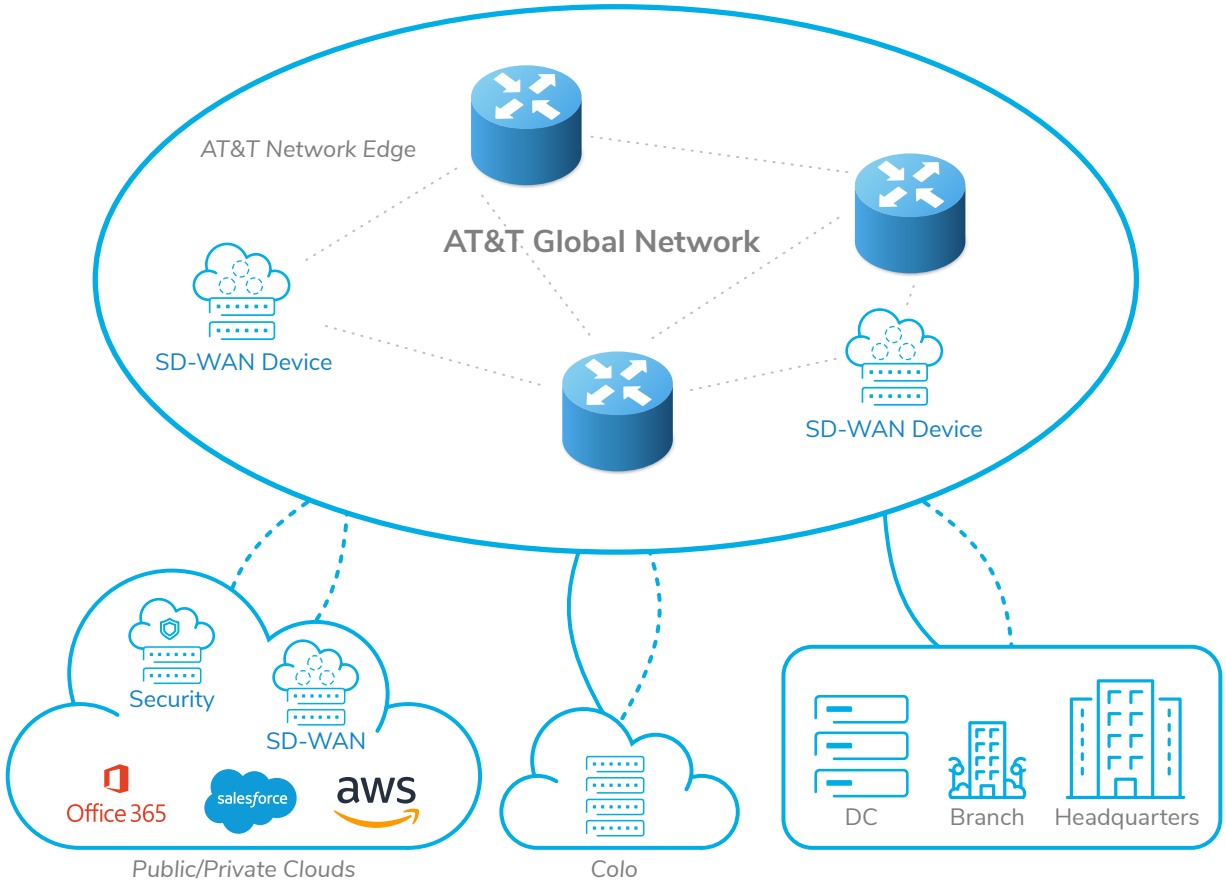
AT&T Network Functions Virtualization

In 2016, AT&T became the first service provider to launch commercial virtual network services—AT&T Network Functions Virtualization, in collaboration with Juniper Networks—for the enterprise market. The 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 Network Functions Virtualization 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. The virtual network services are supported on AT&T Network Functions Virtualization Devices that range from extra-small (supports 1 VNF) to extra-large (supports 12 VNFs) and cater to businesses' various edge requirements. AT&T Network Functions Virtualization is both transport- and carrier-agnostic, which means it supports a wide scope of transport options including MPLS, Internet, and Ethernet.

Extensive VNF Support across Multiple Environments

AT&T Network Functions Virtualization supports a broad range of certified VNF vendors across routing, WAN optimization, firewall, application visibility, and SD-WAN applications. Some 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 Network Functions Virtualization delivers that.



Multi-vendor Orchestration

Although virtual network services have been available since 2016, market adoption has been slower than expected for several reasons. Key among them is the complexity of service chaining multiple VNFs and orchestrating these VNFs across different devices, networks, and applications. To address this challenge, AT&T Network Functions Virtualization 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

Another 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 appliances at data centers and hub sites. AT&T Network Functions Virtualization devices 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).

AT&T Network Functions Virtualization comes in high availability options of dual AT&T Network Functions Virtualization 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.

As businesses adopt the software-centric architecture, it is prudent that they consider resiliency options to ensure continuity of operations.

Service Availability & Pricing Structure

AT&T Network Functions Virtualization is available in more than 200 countries and territories. The pricing structure includes subscription-based pricing for the AT&T Network Functions Virtualization service, 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. While SD-WAN technology offers some agility, it addresses only the automated network selection part of WAN. For businesses to truly realize the potential of a software-centric architecture, the related network functions must also be agile. The convergence of SD-WAN, SDN, and NFV technologies is making it possible to deploy a dynamic WAN because businesses can use SD-WAN technology to route traffic based on pre-defined policies, change the underlying bandwidth in real time, and deploy network functions on a uCPE. As an organization transitions toward software-defined solutions, it is imperative that it consider a platform-centric approach that addresses WAN virtualization in a holistic manner.

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

GROWTH IS A JOURNEY. WE ARE YOUR GUIDE.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion

FROST & SULLIVAN