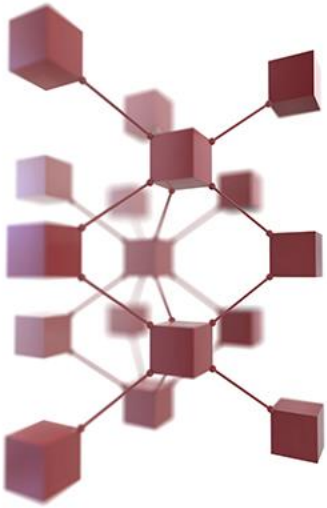
www.pipelinepub.com
Volume 16, Issue 9

NFV Still Matters: Here's Why

By: Dean Campbell



While lacking the populism, cachet, and rate of adoption of its closely related technology 'cousin' Software Defined Networks (SDN), Network Function Virtualization (NFV) is finally ready to come into its own. The proof is in the numbers and the reasoning behind it.

First, the numbers. According to a report by ResearchandMarkets.com "The global NFV market is expected to grow from USD 12,949 million in 2019 to USD 36,324 million by 2024, at a Compound Annual Growth Rate (CAGR) of 22.9 percent during the forecast period."

Next, the reasoning. It's no secret that telecom and cloud service providers have implemented NFV to optimize their networks. The architecture and technologies of these networks need answers that address their current and possible future limits and needs, not what's come previously. NFV also offers additional capacity for Internet of Things (IoT) applications and is especially vital to service providers that continue to rely on NFV as they increase connectivity speeds in the age of 5G.

Moreover, McKinsey estimates that operators who add NFV to any cloud or any 5G network will lower capital expenditures by 40 percent.

So, NFV is not going away. There are many benefits, including lower costs, better agility, faster speeds, and increased security. This article addresses these (and others) in more depth and examines how NFV will parallel the growth of other complementary technologies to support today's next-generation networks.

What NFV is—and what it's not

NFV is a change from using purpose-built hardware (e.g., routers, firewalls, etc.) to using generic/COTS server hardware to run applications that provide the infrastructure "functions" and run them in a virtual environment. As a result, it is frequently confused or lumped in with other virtualization uses cases like:

> **Edge Compute**: Running user applications near the edge of the network to provide customer services and improved performance (latency).
>
> **Software-Defined Networking**: Although application- and software-based, NFV focuses on providing individual network functions (e.g., jobs the network infrastructure needs performed in order to manage traffic), whereas SDN is an overall "management" of the network elements themselves, of which NFV instances can be a part.

Additionally, SDN has changed the industry by decoupling network controls from hardware and allowing the network to be managed by a much more flexible software layer. SDN-deployed networks utilize intelligent network automation to adapt to changing conditions, such as auto-detecting new networks or changes to the network, without the need for human intervention. NFV complements SDN and focuses on optimizing the network services through virtualized network applications such as switching, routing and firewalls.

According to ETSI, the European Telecommunications Standards Institute, the goal of NFV is to "transform the way that network operators architect networks by evolving standard IT virtualization technology to consolidate many network equipment types on to industry standard high-volume servers, switches and storage, which could be located in the data center, in the network or at end-customer premises." NFV replaces traditional, custom-designed network

equipment (think black boxes) that continues to dominate the installed base of networks.

The clear benefit of this is to avoid using custom hardware devices for each network function. As a result, load balancers, firewalls, IDS/IPS, and WAN accelerators can now run as a software function, without generic hardware.

NFV Innovators: Cloud, Communication and Content Service Providers

Operators embracing NFV, SDN and open interfaces can offer extremely fast timelines to install and turn up new services, achieving a competitive edge through service agility. Complementing NFV with SDN and programmable hardware can optimize data forwarding and underlying connectivity, providing high performance and assured communications between virtual appliances.

The ability to deploy services as software downloads to the CPE enables service providers to roll out new services across a customer's entire organization without the need to dispatch engineers and install new equipment. Service providers can offer "try before you buy" promotions and short-term leases for special events. The model can also be extended to allow field sales executives to take an order at the customer site and have it turned up automatically via orchestration.

NFV and SDN together can help service providers to transition from legacy solutions to new VNF-based business service models. These new models incorporate simplified connectivity networks and virtual appliances hosted at the customer premises or in the service provider's network. Cloud service providers offering network storage and compute facilities in their data centers can also explore new business models. They can supply end customers with CPE-based VNF hosts. They can improve the end-user quality of service and quality of experience by mobilizing the location of virtual functions on-demand and installing VNFs in an elastic fashion to the customer premise.

The enterprise benefit

An immediate benefit to enterprises is the simplification of IT infrastructure. This is accomplished through the adoption of a flexible and programmable L2/L3 forwarding device complemented by virtualization of appliances, such as routers,

deep packet inspection, firewall, WAN optimization, intrusion prevention systems and network performance monitoring, with models supporting VNFs hosted locally or in a private cloud.

Many enterprises are considering NFV within their own and often distributed network infrastructure to unburden network operations and focus on immediate business activities. Additionally, enterprises can rapidly test and turn up new services using NFV and create architectural blueprints in software containers.

As NFV matures, appliances relevant to specific industrial verticals will emerge in VNFs targeted; for example, at mobility of the end-user and telemetry collection in the Internet of Things.

The combination of SDN/NFV with SD-WAN, edge computing and 5G has become a critical enabler of IoT. For example, 5G ensures that all IoT devices can be connected without a reliance on wires.

Edge computing has proven to meet the needs of applications for reliable, secure, real-time high performance, yet it also introduces a new level of complexity with the amount of computing, storage allocation and open-source third-party applications. This is where SDN and NFV come into the picture, simplifying the network management by supporting an open environment that allows for tools and software across many hardware platforms to connect to IoT more effectively and ensure a fast, flexible, and secure network.

Additionally, 5G needs NFV. The service components of the 5G infrastructure (CU, RU, DU) have been virtualized into a CRAN (Cloud RAN) architecture. In order to dynamically support changing load conditions in a 5G network and changing demands regarding latency (network delay), NFV will be required. The ability to "spin up" additional instances of CUs or DUs in order to support additional or temporary loads, and the ability to move them between locations (closer to RU to support lower latencies) are critical to allow the next-generation network to process and transport 5G traffic**.**

In fact, research suggests that the digital transformation of networks through NFV and 5G could unlock $2 trillion in value for the telecom industry, consumers, and society by 2025.

Clearly, NFV still matters. The following six use cases demonstrate how NFV is being used today to address a range of challenges—as well as provide enhanced solutions to these and other networking hurdles to enhance services.

Six use cases

Microsegmentation. The ability to run many small (virtual) instances of a function (routing, encryption, etc.) for each customer allows for faster deployment (a small router setup rather than adding more rules to one, monolithic router), scalability (as each router is its own separate process – as there is no single "scaling point"), and flexibility (instances or customers can use different versions or vendors for their instance).

Efficiencies in a provider cloud, or on customer prem (mini-cloud or edge-cloud). The operator can run a firewall, for example, on a small customer prem device that supports virtual application instances or in their own private cloud or data center environment. The choice can be made based on which is most efficient for processing power and provides the required latency.

Easier to roll out new applications. Because there is no physical infrastructure or hardware required to roll out, add or remove applications if the service provider already offers managed managed firewalls, for example, then rolling out an encryption application is simple. Just add the application to the virtual environment management tools. No additional hardware, testing, or truck rolls; only some configuration in the software tools and the application is ready to roll out to customers.

Easier to manage updates, security, patches, etc. Virtual instances are managed from a central location. If a zero-day exploit is uncovered, the operator can quickly apply security patches from the central management location without the need for truck rolls to individual locations.

Performance management or dynamic response to changing conditions. Virtualization can help by allowing the operator to provide more processing power (such as spinning up additional compute resources or additional instances of the network function application) in order to respond to dynamic load

conditions. These additional computing or application resources can be "spun up" in the specific area of the network where required. Alternatively, if there are no constraining latency or traffic concerns, lesser user resources (perhaps in more remote parts of the network) can be leveraged to support higher load conditions in other parts of the network.

Eliminate vendor lock-in. Leveraging open interface standards allows customers to pursue a best-of-breed approach without vendor lock-in on the hardware or software side. With no "hardware" in place (other than servers supporting the functions), the operator can change application versions—and even vendors—as simply with one click from the management interface. No longer does an operator have to look at hardware sunk costs forcing them to continue with a specific vendor; they can change and start deploying a new vendor whenever desired. Replacement strategies, or cap-n-grown are both supported easily when the functions are virtualized (all software or licenses) and there are no underlying hardware changes to worry about.

Orchestration, flexibility, and a look forward

In today's world, the emphasis is on how to manage network elements more programmatically — to "orchestrate" processes that maintain, provision or troubleshoot network functionality.

Adding NFV provides a significant amount of flexibility. There is no longer a need to deploy different physical hardware. Applications, or NFV instances, can be updated immediately through the virtual environment. However, in order to take full advantage of NFV, network operators need to focus on the management infrastructure that manages the "instances" of NFVs, in addition to the normal management and orchestration of the elements or functions themselves. Still, the upside from enabling this management and functionality provides a solid return on investment.

The evolution to a software-centric network requires a network transformation with a pace determined by operational and organizational changes rather than technological developments. An approach allowing a seamless, stepwise introduction of NFV is essential to benefit from efficiency gains in the short term

while implementing the transformation steps necessary for the longer term. Open interfaces and open software are key, as they prevent vendor lock-in and cause least disruption when moving from the present to a future mode of operation.

NFV does require investment in another layer of network management: it requires you to build additional skills as you need to be able to manage the VNFs – the virtual element – in addition to managing as you do now with the functions they already provide. Even so, NFV is a meaningful way to build a truly dynamic network.

And, ultimately, when you come right down to it, that's why NFV matters.