Channel Guide to NFV: Faster, Better, Higher-Margin Services

By Kurt Marko

Channel Partners™

FEBRUARY 2017 | US$25 | S040217

Channel Guide to NFV: Faster, Better, Higher-Margin Services

By Kurt Marko

FEBRUARY 2017 | US$25 | S040217

Channel Partners™

Table of Contents

A Burgeoning Market 5
NFV 101 7
Brief Intro to Network Virtualization 8
Virtual Networks, New Possibilities 9
Beware the Scale 9
Chain Chain Chain 10
Channel Business Opportunities 11

Channel Partners™

About the Author

linkedin.com/in/krmarko
@krmarko

KURT MARKO is an IT industry analyst, consultant and regular contributor to a number of technology publications, pursuing his passion for communications after a varied career that has spanned virtually the entire high-tech food chain from chips to systems. Upon graduating from Stanford University with bachelor's and master's degrees in electrical engineering, Marko spent several years as a semiconductor device physicist, doing process design, modeling and testing. He then joined AT&T Bell Laboratories as a memory chip designer and CAD and simulation developer. Moving to Hewlett-Packard, he started in the laser printer R&D lab doing electrophotography development, for which he earned a patent, but his love of computers eventually led him to join HP's nascent technical IT group. Marko spent 15 years as an IT engineer and was a lead architect for several enterprisewide infrastructure projects at HP, including the Windows domain infrastructure, remote access service, Exchange email infrastructure and managed web services.

Channel Guide to NFV: Faster, Better, Higher-Margin Services

The software-defined trend is changing everything, from how we provision WANs to how we sell firewalls to how we build data centers. As dedicated servers and purpose-built hardware are replaced by virtual machines, storage volumes and networks, the opportunities are endless. Analysts say that the network functions virtualization (NFV) market is set to explode, growing at a compound annual growth rate of 42 percent and reaching $15.5 billion by 2020.

That business is coming straight out of MPLS and hardware appliance sales: Ciena says its market research and customer discussions show that 20 percent to 30 percent of managed services, including enterprise routing, security, WAN optimization, network analytics and session border controls that are currently delivered via physical appliances are on pace to move to software.

No wonder, given business execs' hunger for agility. The marquee promise of SDN is its ability to automate the setup and management of physical networks. Replacing static configurations and topologies with a dynamic fabric, under the direction of an intelligent controller that can react quickly to demand spikes, delivers unprecedented flexibility.

From a partner sales perspective, as we've discussed, a physical appliance will be changed out every three to five years. But it's feasible to sell NFV-based services much more frequently, since customers are not limited by big hardware investments. Virtualized network services are much easier to update with security patches, bug fixes or new features, lessening the staff time spent on these tasks. NFV will also make it easier

NFV at Your Services

Verizon announced in Q3 a menu of new virtual network functions to provide WAN optimization, SD-WAN and security in an as-a-service model in three configurations: universal CPE, cloud-based virtual CPE services and hybrid services where on-premises- and cloud-based deployment models are mixed and matched.

"The way in which network services are delivered is going through an unprecedented shift — the biggest we've seen since the broad adoption of MPLS," said Shawn Hakl, vice president of networking and innovation at Verizon. Partners need to take notice and understand various strategies.

to sell higher-end managed services to small companies and capex-constrained verticals, to expand your own geographic footprint and to empower customers to support remote and branch offices.

Regardless of how SDN is implemented at a customer site — whether via a full-stack controller that manages low-level (Layer 2/Layer 3) network flows or using a virtual network overlay on an existing Ethernet fabric — it enables network function virtualization that allows applications and services to interact with the physical network.

Such programmability has monumental implications for your suppliers, too. Carriers, ISPs and cloud service providers have made SDN a centerpiece of their strategies, and hardware vendors from Cisco to HPE are looking to stake out their positions in a post-appliance world.

A Burgeoning Market

The technology development and business direction of SDN and NFV are largely being shaped by a number of open standards projects and industry groups (see "Standards Bingo," below).

Demand for standardization is coming through loud and clear from large network operators. In fact, the ONUS mission statement declares that it's a project designed to "enable service providers to build real software defined networks."

Standards Bingo

If you want to dig into the nuts and bolts of SDN and NFV, the best bet is one of the various standards bodies.

- **NFV in ETSI** was founded in 2012 and has now released some 45 publications and is at Release 3 of its detailed specification. The group has nearly 300 members.
- **The Open Networking Foundation** has as its mission the promotion and adoption of SDN through open standards development. Its resource page is the place to go for SDN learning.
- **The Open Networking User Group** runs ONUG conferences in the spring and fall, with a business value focus. Its goal is to advocate for open, interoperable hardware and software-defined infrastructure solutions that span the entire IT stack. Members include Cisco, Huawei, HPE and Verizon.
- **OpenDaylight** maintains the open-source OpenDaylight platform (ODL) SDN controller under the Linux Foundation. It's popular with universities, state and local governments, and researchers.
- **The Open Network Operating System** is a highly scalable SDN platform aimed at service providers. AT&T, Comcast, Google, NTT and Verizon are on the board.
- **Open Platform for NFV** is an open NFV reference architecture now on its third release, code-named Colorado, that has new security, IPv6, VPN and other capabilities.

With several years of pilot experience behind them, carriers and service providers are moving quickly with production-scale NFV implementations. That will have a profound effect on the network equipment market. As we mentioned, the latest estimate by IHS Market says the NFV market will grow at 42 percent annually through 2020, reaching that $15.5 billion number. The vast majority of these sales, 80 percent, will be for software, not hardware, as you might expect.

Splitting out sales a different way, IHS expects only 16 percent will come from infrastructure — the servers, storage and switches that have been so lucrative for VARs. Going forward, 73 percent of sales will come from virtual network functions and applications that will deliver recurring revenue. Just as Microsoft has aggressively pushed its partners to sell Office 365 and Azure, IHS says service providers' desire for service agility and operational efficiency will drive them to move their channels to NFV.

Last year, an IHS Markit survey found that 100 percent of service provider respondents said they will deploy NFV at some point, with 81 percent expecting to do so by 2017. Most, 59 percent, had already deployed.

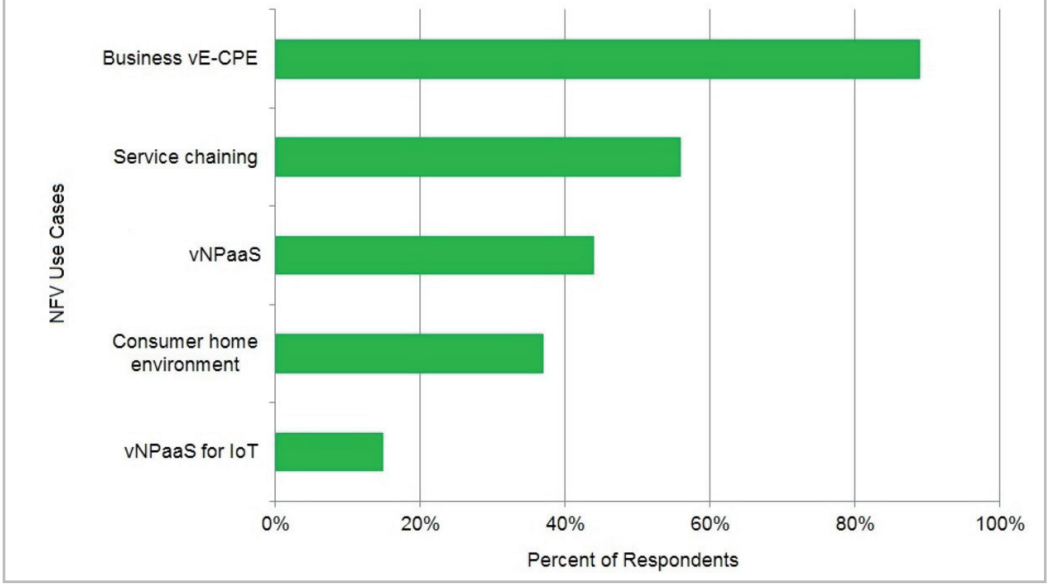
A look at exactly *how* carriers plan to use NFV highlights the opportunities for partners as the technology becomes more prevalent and easy to use:

- About 90 percent use NFV to replace business CPE with virtualized network services;
- Over half plan to chain multiple virtual services together to provide new capabilities and dynamically respond to changing network conditions; and
- More than 40 percent are creating virtual network application platforms (vNPaaS) to enable customers or partners to create their own virtual services.

Agents in particular should make no mistake: Your key carriers and ISPs are wholly committed to NFV. It's time for you to investigate the technology and prepare a business case to move customers into software-defined network services.

Top Use Cases for NFV

Service providers named their most important NFV use cases for revenue generation.



Source: IHS

NFV 101

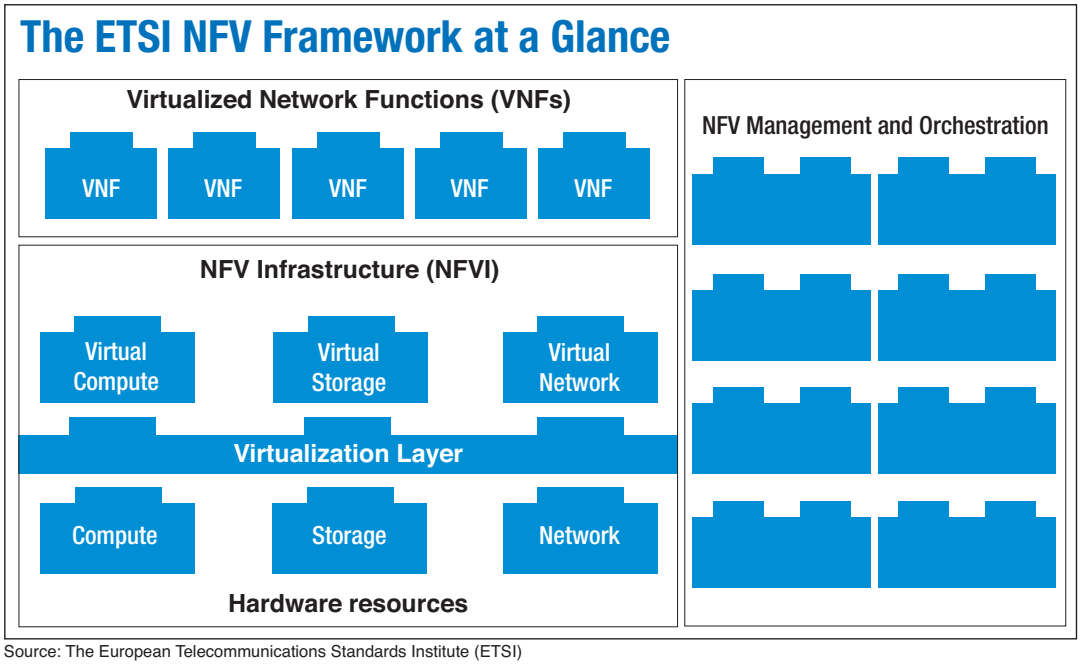
It's easy to get overwhelmed by new acronyms and terms thrown around the NFV discussion. One of the first sources of confusion is the conflation of NFV with virtual network functions (VNF). For our purposes, they describe the same concept, which is why they are so often interchanged. However, according to the ETSI standard, they represent distinct ideas.

"NFV" is an umbrella term describing the entire framework of virtual network infrastructure and services. It is composed of:

- **NFV infrastructure (NFVI)**, the underlying virtual infrastructure including servers, storage and networks (SDN)
- **Virtualized network function (VNF)**, the virtualized, software-only implementation of a network service that runs atop NFV infrastructure
- **Management and automation** software used for service deployment and to operate the infrastructure

As the ETSI architectural description puts it: "The NFV framework enables dynamic construction and management of VNF instances and the relationships between them regarding data, control, management, dependencies and other attributes."

VNFs represent the business opportunity for partners and MSPs, but they are impossible to deploy without underlying virtual infrastructure and management automation software. Thus, although we might interchange the terms, we will specify "VNF" or "virtual services" when discussing a salable network service or component, such as IPv6 NAT or a web proxy that can be chained with other functions to create a service.



Source: The European Telecommunications Standards Institute (ETSI)

Brief Intro to Network Virtualization

An NFV infrastructure is built on familiar components from a virtual machine stack (vSphere/vCenter, Windows Server/System Center) paired with a virtual network platform that might be new to partners. The combination comes in many forms; however, the ETSI NFV standard is careful not to specify particular types or product implementations for virtualized infrastructure:

"Rather, NFV expects to use virtualisation layers with standard features and open execution reference points towards VNFs and hardware (computation, network and storage). …. Nonetheless, in NFV, VMs shall always provide standard ways of abstracting hardware resources without restricting its instantiation or dependence on specific hardware components."

Translated: Use whatever virtual computing and storage platform you are familiar with or feel is best for the job. Components of NFV might even be split into a hybrid infrastructure, with some elements running on customer premises or at the partner's network gateway and others on the public cloud.

Again, ETSI does not prescribe a particular network virtualization technique, only that the network provide connectivity among VMs comprising a VNF, and/or between different VNF instances.

There are several ways to go about this. The standard points out alternative technologies, including virtual LANs (VLANs), virtual private LAN services (VPLSes), overlay and tunnel protocols like VXLAN or NVGRE, and the full decoupling of a centralized network controller with a distributed data plane using something like OpenFlow.

The least disruptive option is the use of a network overlay like VMware NSX or Microsoft Hyper-V Network Virtualization (HNV) to create a virtual network on top of a customer's existing Ethernet routers and switches.

Regardless of the implementation, Verizon's SDN-NFV reference architecture has some useful guidance on physical compute and network layer characteristics:

- Uses **modular, extensible hardware** that shares communication fabrics, power supplies, cooling units and enclosures
- Is **redundant**, with no single point of failure for the network fabric (NICs, switches and interconnect), servers, power or cooling
- Uses a **non-blocking network fabric** with out-of-band management
- Supports **hardware virtualization and APIs** such as single root I/O virtualization (SR-IOV) and data plane development kit (DPDK)

Verizon bases its NFV project on OpenStack.

Exploiting the dynamic configurability and extensibility of virtual networks also requires a management software backplane that can automate routine operations and consistently set network configuration and security policies according to established templates and rules.

Software interfaces and APIs enable you to automatically tie VNFs to particular applications, with different network policies linked to individual users or groups. Policy-based network delivery allows services such as firewalls, WAN optimizers or UC features to follow applications and users, and not be tied to specific physical infrastructure.

Virtual Networks, New Possibilities

VNFs are essentially software appliances that can be configured and deployed on the fly. However, automating their management and integration requires some standardization of network and software interfaces (APIs) and metadata.

Essentially, as with any offering, you don't want to reinvent the wheel for each customer.

It's well worth some upfront planning with technical staff or your carrier partners. As software constructs, VNFs open up possibilities not present with hardware-based devices, notably service composition, decomposition and chaining.

Breaking down VNFs into smaller functional modules, such as a Layer 3 stateful packet inspection engine or a Layer 7 application proxy, is attractive for the same reasons developers have gravitated to containerized microservices to build cloud-native applications: It allows the same code to be reused for different services, increases scalability, reduces development time and improves security by exposing a smaller attack surface.

Conversely, VNF composition and chaining allows microservices to be mixed and matched into complex services tailored for specific customers or industries.

Beware the Scale

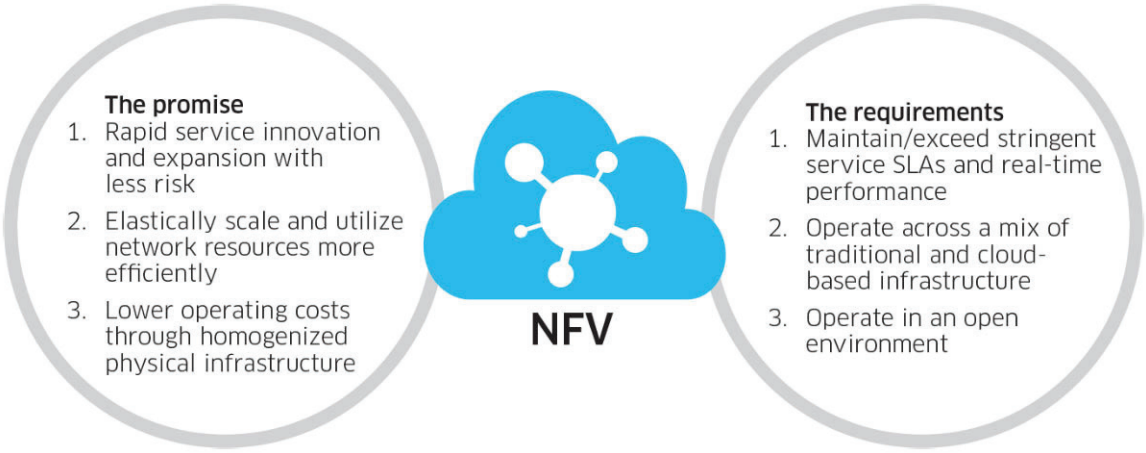
For all of NFV's upsides, network service providers with large portfolios and heterogeneous systems may find that abstracting network services from the underlying hardware creates new problems. As ETSI points out, management challenges include:

- Mapping services to the physical infrastructure using infrastructure management software that may not be up to the task
- Deploying VNFs to the appropriate network locations, which are typically scattered across a WAN
- Allocating and scaling hardware resources to meet capacity demands could incur capex. Hyperconverged infrastructures, **such as from channel-focused provider Nutanix**, are often cited as a way to ease the hardware problem.
- Logically and physically tracking VNFs by user/customer and location, for billing and patching.
- Troubleshooting when the root cause of a problem may be hardware, software or a combination of both

Ideally, VNF management will eventually be handled by a packaged product. However, to the extent that there is a market for such VNF management software, it is immature and changing.

Fortunately, orchestrating network services across a wide variety of network equipment from myriad manufacturers requires standardization, and that need has spawned a couple of important multivendor projects in addition to the standards bodies we discussed earlier.

NFV for Enabling Network Agility



Source: Nokia

NFV-MANO is ETSI's approach and consists of a virtual infrastructure manager (VIM) that controls the NFV infrastructure and collects performance, security and error measures; NFV orchestrator (NFVO) that deploys VNF packages and handles service management including instantiation, scaling, performance monitoring, event correlation and service termination; and a VNF manager (VNFM) that acts as a bridge between the VIM and NFVO to provide control of VNFs and reporting to a (physical) network management system.

The ETSI NFV group now has more than 200 member and participant companies, including Broadcom, Cablelabs, HPE, Oracle, Sprint and VMware. An alternative standard, ECOMP (Enhanced Control, Orchestration, Management and Policy) provides similar capabilities, with added features designed for carriers. ECOMP was recently open sourced and adopted as a Linux Foundation project, so partners should expect to see compliant products from member companies including some of the largest equipment vendors and carriers — AT&T, Bell Canada, Brocade, Ericsson, Huawei, IBM, Intel and Orange.

Chain Chain Chain

VNFs can replace almost any traditional network service. The most popular use cases now tend to be replacements for hardware appliances such as firewalls, load balancers, VPN gateways, WAN optimization accelerators and application delivery controllers. Besides those, consider:

- Campus or branch network virtualization that partitions a physical network into logical pieces that can be allocated to different business units, customers (think a mall with dozens of retailers), applications or security needs
- Virtualization of CPE and associated provider edge (PE) equipment to replace multiple on-premises appliances with software applications and migrate some network functions from on-premises hardware to remote, in-cloud virtual infrastructure

- SD-WAN and dynamic interconnects that can change and optimize network connections between locations based on physical link performance and customer demand
- Network access control to handle and authenticate remote connection requests, assess a client's compliance with local security policies and dynamically connect clients to the appropriate network based on the user identity and device type, and the device's security profile

As mentioned, a potent feature of NFV is the ability to dynamically link virtual services into a service chain. As Verizon's NFV reference architecture describes it, a service chain steers traffic through a set of functions in a set order. The reverse path traverses the same service functions as the forward path, typically in reverse order. Thus, if a customer edge chain included a stateful firewall, video traffic optimization and a network address translation (NAT) gateway, egress traffic would first hit the NAT, before passing through the video optimizer and firewall.

Carriers commonly use NFV service chains to provide the mobile S/Gi-LAN; partners will find them useful to provision a virtual CPE in which VNFs are delivered from the core network to an on-premises thin client device.

Channel Business Opportunities

NFVs and virtual services can be profitable for partners for many of the same reasons carriers are implementing them, as this article from Ciena highlights.

Besides incremental revenue from selling new virtual services to existing customers, you can significantly expand your geographic reach, adding customers without concern over having to roll a truck to install hardware. Much like Tesla can introduce significant new features such as autonomous driving via an overnight software download, partners can generate new revenue streams by adding new virtual services.

Customers will enjoy lower costs, both capex and opex, by replacing expensive hardware with software, and partners will lower error rates by replacing manual processes with programmable automation.

Then there's speed. For suppliers, no dedicated appliances means no more hardware evaluation, testing and unforeseen problems with software configuration. Partners will see faster service installations. Ciena's case studies show a 40 percent increase in revenue by turning up virtual services within hours instead of days or weeks.

Our take is that NFV provides partners with significant new service opportunities that are both highly adaptable and profitable. Look at carrier partner programs like this from Verizon that can bootstrap the launch of new network services.

As a first step, talk to your carriers and vendor suppliers to get a handle on their SDN and NFV strategies and VNF portfolios. Inventory your existing network services and identify good candidates for virtual disruption — WAN optimization, SD-WAN, branch firewalls and UC services are great places to start.

See what else your carrier partners are doing with SDN and virtual services, and think how you might exploit these in your product suite. And, look for innovative new suppliers where you find gaps. For example, as we profiled last July, Masergy Communications has a virtual platform designed specifically for resellers.