STRATEGIC WHITE PAPER | NFV INSIGHTS SERIES

The what and why of NFV orchestration

2015 is the year of the first Network Function Virtualization (NFV) deployments and many service providers are working out the details of their NFV introduction plans. The question is no longer whether NFV is to be deployed, but how to do it to obtain the greatest short-term and long-term benefits. NFV will not be introduced in a “big bang” approach, but pragmatically with carefully selected initial applications. One of the key questions in this context centers on the kind of NFV platform that should be deployed to support initial applications. As well, service providers are considering how to evolve from such first deployments toward a powerful NFV environment that will bring the concept of NFV to full fruition with a new level of service agility, streamlined operational processes, and a cost base comparable to over-the-top competitors.

About the NFV Insights Series

NFV represents a major shift in the telecommunications and networking industry. NFV applies virtualization and cloud principles to the telecommunications domain. Until recently, this approach appeared to be impossible due to the stringent performance, availability, reliability, and security requirements in communication networks. Many service providers are now keen to implement NFV to help them gain an advantage through automation and responsiveness in order to deliver an enhanced customer experience while reducing operational costs. This series of whitepapers addresses some of the key technical and business challenges on the road to NFV.

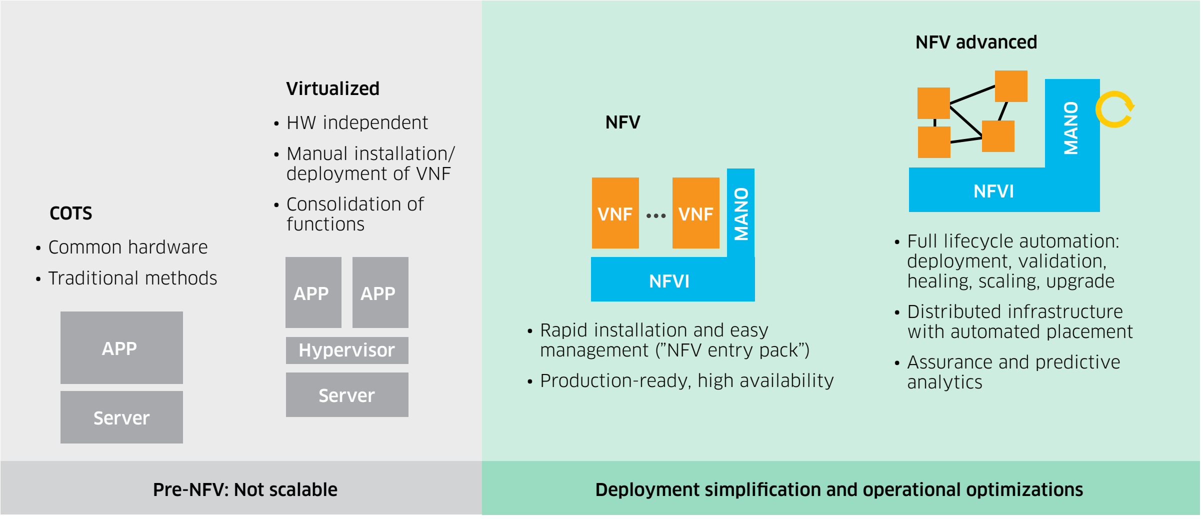
Alcatel·Lucent

Table of contents

The path to NFV

A fundamental assumption of NFV is that network functions run on commercial off-the-shelf (COTS) servers. Moreover, modern virtualization technologies enable multiple virtual network functions (VNFs) and their components to share server, storage and networking resources, resulting in a better utilization of these resources. Figure 1 shows different levels of NFV introduction.

Figure 1. The path to NFV


COTS
• Common hardware
• Traditional methods
APP
Server
Virtualized
• HW independent
• Manual installation/ deployment of VNF
• Consolidation of functions
APP
APP
Hypervisor
Server
NFV
VNF
VNF
MANO
NFVI
• Rapid installation and easy management ("NFV entry pack")
• Production-ready, high availability
NFV advanced
MANO
NFVI
• Full lifecycle automation: deployment, validation, healing, scaling, upgrade
• Distributed infrastructure with automated placement
• Assurance and predictive analytics
Pre-NFV: Not scalable
Deployment simplification and operational optimizations

However, these first two levels — COTS and Virtualized — are limited in their benefits and are not scalable toward a real NFV solution. To realize the benefits of NFV, a more efficient, production-ready solution is required. The main drivers for such production-ready solutions are not only efficiency but also the ability to deliver manageable, highly reliable and secure services to customers.

Two elements are critical to meet these goals: NFV infrastructure and an NFV management and orchestration (MANO) system.

The NFV infrastructure comprises the hardware with servers, storage, and network switches and a software package with operating systems, hypervisor, and virtual switches. Other features are required as well — operational and administrative capabilities such as automated installation and commissioning, hardware cluster and software monitoring and alarming, and virtualized resource management.

The second element and the main focus of this document is the NFV MANO. The concept of orchestration has been frequently discussed and there is much uncertainty about it in the industry. Let us take a deeper look now at what is really the role of the orchestration in NFV solutions.

NFV management and orchestration

The ETSI NFV Industry Specification Group has defined the Management and Orchestration (MANO) functional group to include three components: the virtual infrastructure manager (VIM), the VNF manager (VNFM) and the NFV orchestrator (NFVO). VIMs are responsible for controlling and managing the compute, storage and network resources. Typically there are multiple VIMs responsible for the resources at different NFV points of presence (PoPs). One or more VNFMs are responsible for managing the life cycle of VNF instances including the deployment, monitoring, scaling, healing, and software upgrade processes. Finally, the NFVO has two quite different responsibilities: the orchestration of resources across multiple VIMs, and the life-cycle management of network services, which consist of one or more VNFs.

While the NFV infrastructure manages sets of compute, storage and network resources, MANO elevates this to the application level; that is, MANO understands which resources belong to specific NFV applications. MANO enables users to monitor and control the state of NFV applications. With the VNFM function, operators can deploy applications and execute other life-cycle actions according to pre-established recipes, reducing time-to-market and helping to reduce human error.

Arguably the most important role of MANO is service assurance; that is, it helps providers to deliver services that are at least as highly available as those delivered with traditional physical network functions. Typical production NFV deployments will be distributed across multiple NFV-PoPs to avoid single points of failure due to technical or force majeure events, but even single-location events need significant assurance capabilities. MANO is responsible for collecting status information and alarms related to infrastructure resources and also those at the application level related to VNFs and network services. Unlike traditional network functions that are delivered as a bundle of hardware and software, NFV applications and the underlying infrastructure are separate elements that can fail independently. In case of a failure, a critical MANO capability is to help operators understand which infrastructure resources are used to deliver the application services (physical to virtual to application mapping) and determine the real source of the failure (root cause analysis); for example, whether the failure is caused by a problem with a server or network or whether the failure is due to an application issue.

Another aspect of service assurance is disaster recovery. In case of a catastrophic event, MANO can help restore service applications faster through automated deployment, a process that may be less prone to human error than manual restoration.

MANO is also responsible for establishing and monitoring the (virtual) networks needed for internal communication among the components of VNFs or between multiple VNFs that may or may not be distributed across multiple locations.

MANO plays an important role in the security of the solution, an area where Alcatel-Lucent has contributed as leader of the ETSI SEC working group and has helped to identify attack vectors specific to NFV.[1] MANO itself needs to be secured against attacks and MANO should also help to secure NFV applications against outsider and insider attacks. With role-based access control, access rights for different user roles such as cloud admin and application owner can be carefully defined, and permitted user actions should be logged to make sure that a person responsible for all actions can be identified.

MANO should be protected against illicit external access using a multi-tier architecture and web application firewalls. The MANO system needs to adhere to national security requirements with the appropriate certification level. MANO should allow the definition of security zones, security groups, and security appliances to isolate applications from each other. The system should be scanned for security vulnerabilities using appropriate tools. Private keys of VNFs need to be protected.

All of these functions need to be accessible through an easy-to-use user interface, typically a GUI with appropriate logging capabilities for system events and user actions.

In addition, these functions need to be available through APIs to higher layer management systems such as an operations support system (OSS)/business support system (BSS) or VNF-specific element management systems.

Advanced MANO

Some of the MANO functions create value specifically for larger NFV solutions with many distributed PoPs and many different applications running on them. In such an environment, life-cycle management operations that used to be triggered by human operators will increasingly become automated. Operators retain control of the automated process through policies that can be configured into the MANO component. Such automation requires intelligent placement and resource management algorithms that determine the PoPs and resources to be allocated that best utilize available capacity while complying with service provider policies. Advanced MANO solutions support infrastructure capacity management, through trend analysis, for example.

Use cases

Alcatel-Lucent is working with numerous service providers on proof-of-concept and production deployment projects. Most production projects are centered on the introduction of specific VNFs and services along with an NFV platform. Most service providers choose their first-off project pragmatically, for example, end-of-life replacement for a simple application, such as domain name system (DNS) or authentication, authorization and accounting (AAA), or greenfield deployment of a more complex application such as virtualized IP multimedia subsystem (IMS). While the immediate focus of these projects is the delivery of a particular service with NFV technology, service providers are keen to add additional applications going forward; thus, there should be a smooth evolution path to a shared solution capable of delivering the full scope of NFV benefits.

One customer is in the process of replacing a traditional Diameter router solution with the next-generation Diameter router now available as a VNF. The solution will be distributed across two sites. Due to virtualization, the new solution better utilizes server resources — freeing up servers for additional applications, such as another instance of the Diameter router solution serving a subsidiary in a different country. While not originally interested in an orchestrator (MANO), the customer will now be using the orchestrator to manage the different sites as well as the different application instances. With the orchestrator, the customer benefits from an application view, the zoning capability with anti-affinity, hardware and software monitoring, analytics capabilities to correlate between hardware, software and application layers. The solution is highly available both at the application level and at the NFV platform level.

Another service provider will install a new, efficient DNS/Dynamic Host Configuration Protocol (DHCP) solution as a replacement for a traditional solution based on physical network functions. This customer needs a geo-redundant, distributed solution with three PoPs hundreds of kilometers apart with a capability to manage the solution remotely from a centralized location. (It is not practical to send people to the location for every failure.) The service provider uses MANO for automated deployment, centralized hardware and software monitoring (including fans and processor temperature) and resiliency. As this will be a production service, the solution needs to support software upgrades without service interruption.

A third service provider is deploying a vIMS solution to deliver a state-of-the-art Voice over LTE (VoLTE) service. The NFV platform should be ready for future applications, such as virtualized evolved packet core (vEPC) and service chaining. The provider chose an NFV solution to overcome the slow process of traditional application deployment and to gain freedom of choice for the hardware. Key requirements of the service provider are stability, high availability, automated deployment and in-service upgrades. The role of MANO is to support automated deployment with co-managing capability, centralized extended infrastructure monitoring and multiple NFV application management.

Business case

The business case for NFV is not a simple calculation and will greatly depend on the specifics of each project. The following case may or may not be indicative for other service providers and applications. Alcatel-Lucent has done an in-depth business case study for a virtual DNS server solution with a Tier 1 service provider.[2] In this case, the study showed how even a simple application like DNS can benefit greatly from running on an NFV platform, even though it was used only for that single application. The study found lead-time reductions for several MANO-controlled processes — scaling: -98 percent; software upgrade: -77 percent; healing: -81 percent to -96 percent. These lead-time reductions allow allocating human resources to more productive activities such as introduction and continuous improvement of new services (this effect has not been quantified in the business case).

MANO-based automation helps service providers to focus their attention on generating more revenue with the introduction of new services, such as advanced communication services [3] as well as on more rapid service evolution to reduce customer churn and foster churn-in from competitors. Services implemented through VNFs simplify the procurement, planning and deployment process while other activities, such as BSS integration and promotion, may benefit to a lesser extent. The acquisition, shipment and installation of hardware are eliminated, which can be an even greater advantage for international deployments. Service providers can reduce risk by testing services and scaling them up quickly in case of growing customer demand or shut down the service and replace it with a different one (fail fast). NFV also supports a continuous service improvement process through easy and automated software upgrades leading to earlier feature availability.

Summary

The MANO component of the NFV architecture contributes not only to large, massively distributed and multi-application NFV solutions, but also to NFV projects with one or a few applications. A fundamental capability of MANO is to help assure an efficient, well-defined operational process in an environment where roles and responsibilities are becoming newly defined. MANO helps to build a production quality platform with the required service availability, ability to quickly respond to failures and simple provisioning of a coherent, centralized view of the NFV infrastructure with the applications running on it. Service providers should also carefully evaluate how their NFV platform is secured against internal and external errors and attacks, as well as outages and disasters. The higher level of automation streamlines traditional operational processes and allows operators to focus their human resources on service innovation and other activities more critical to the success of the business.

For further reading

[1] NFV Insights Series: Providing security in NFV – challenges and opportunities, http://resources.alcatel-lucent.com/?cid=178552

[2] NFV Insights Series: Business case for moving DNS to the cloud, http://resources.alcatel-lucent.com/?cid=178476

[3] Alcatel-Lucent Advanced Communication Services win 2015 GSMA Global Mobile Award: Best Mobile Network Product or Solution for Serving Customers, http://www.gsma.com/newsroom/press-release/winners-2015-global-mobile-awards/

Alcatel·Lucent