White Paper

Decoding the Management & Orchestration Architecture for Network Functions Virtualization

Prepared by

Caroline Chappell
Senior Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of

www.cyaninc.com

February 2014

Executive Summary

As the seminal ETSI white paper points out, network functions locked into proprietary hardware are a source of high cost and service delivery delay. Virtualizing network functions, which means running them on commercial-off-the-shelf (COTS) servers with industry-standard chipsets and IT virtualization technology, promises to deliver large benefits in the form of capex reduction and service agility.

This paper identifies three approaches to network functions virtualization taking place under the banner of ETSI network functions virtualization (NFV): bare metal implementation of network functions on COTS hardware; virtualization of network functions on specific COTS servers equipped with hypervisors; and cloudification, the complete decoupling of network function and hardware layers. Operators are implementing different virtual network functions (VNFs) using each of these three approaches depending on the function's internal and the operator's business requirements.

The siloed nature of the management systems (OSS) associated with each proprietary hardware-based network function adds further recurring cost to a network operator. Virtualizing network functions has a large impact on this cost because it breaks down OSS silos, de-duplicating expensive management functions and making it easier to compose and manage VNF-based services end-to-end. Operators can more flexibly move and change VNFs, they can manage multiple VNFs with a common system and they can separate management concerns for greater simplicity and efficiency. For example, the COTS-based server infrastructure can be managed independently from VNFs themselves.

To achieve NFV benefits, operators must introduce new management capabilities. Existing OSS are unlikely to be able to deal with VNFs without significant augmentation. The ETSI NFV Industry Specification Group (ISG) has described a Management and Orchestration (MANO) stack that contains the spectrum of new capabilities for managing NFV. These include the Virtualized Infrastructure Manager (VIM), which manages virtual compute, storage and networking resources, and which operators are typically implementing with OpenStack.

Because NFV MANO separates management concerns, it also describes the requirement for VNF management and orchestration functions. This paper distinguishes between service orchestration, which composes VNFs into service chains, and VNF deployment and management orchestration.

In real world networks, service orchestration needs to orchestrate proprietary hardware-based network functions and VNFs together. Thus operators need multi domain service orchestrators (MDSOs) that sit above the MANO stack. An existing OSS may be able to play the role of an MDSO, providing it has a VNF deployment and management orchestrator beneath it to manage participating VNFs.

This paper details the critical role of a VNF deployment and management orchestrator, which provides a common management layer for any or all VNFs, regardless of the virtualization approach that has been applied. The VNF deployment and management orchestrator is responsible for deploying VNFs at the right location, with the right resources and mediating between VNFs, the VIM and external B/OSS, multi-domain service orchestrator.

The paper also offers recommended steps operators need to take in implementing NFV.

Section II looks at the industry changes that are driving the need for network transformation through NFV.

Section III describes the architecture needed to manage VNF and discusses implementation approaches.

Section IV makes recommendations for migrating to NFV in an evolutionary way, enabling new management and orchestration functionality to co-exist with existing management systems without the need to rip and replace them.

Industry Drivers for NFV

NFV Addresses Key Industry Challenges

That 12 operators joined together so quickly in 2012 to publish a white paper on NFV is testament to the severity of the challenges they face. The NFV white paper paints an eloquent picture of lack of service agility and rising network costs as a result of the proliferating range of proprietary physical appliances that telcos need to add to their networks.

A key source of expense was not explicitly highlighted in the seminal NFV white paper: the management of all those physical devices. Although many operators have made strides toward a single management view at the highest level of operational abstraction – end-to-end service – physical device management remains largely proprietary and manual down at appliance level.

Device-specific operational silos contribute heavily to the total cost of ownership (TCO) of physical appliances. They also make it extremely time-consuming and complex to launch new services that cross multiple silos. Different management stovepipes must be integrated and orchestrated – a costly process that must be carried out on a custom basis and regression-tested, due to complex service and network dependencies. As a result, network services typically take months to deliver in a world that increasingly expects service delivery in days or even minutes.

Subsequent papers emerging from what is now the ETSI NFV ISG have acknowledged that network management is a critical issue. Since the main aims of ETSI NFV are to drive down cost and accelerate time to market for new services, they apply not only to the form factor in which network capabilities (functions) are delivered, but also the management of those functions. Decoupling network function that can be realized in software from proprietary hardware and virtualizing it will only take operators so far toward NFV goals. To gain the full benefit of NFV-based network transformation, they eventually need to transform their operational processes and systems, too.

The Roadmap to NFV

A key principle of NFV is that network functions should be decoupled from proprietary hardware and run instead on industry-standard servers equipped with standard IT virtualization technology. Operators interpret industry-standard servers to mean COTS servers with industry-standard chipsets, as shown in **Figure 1**.

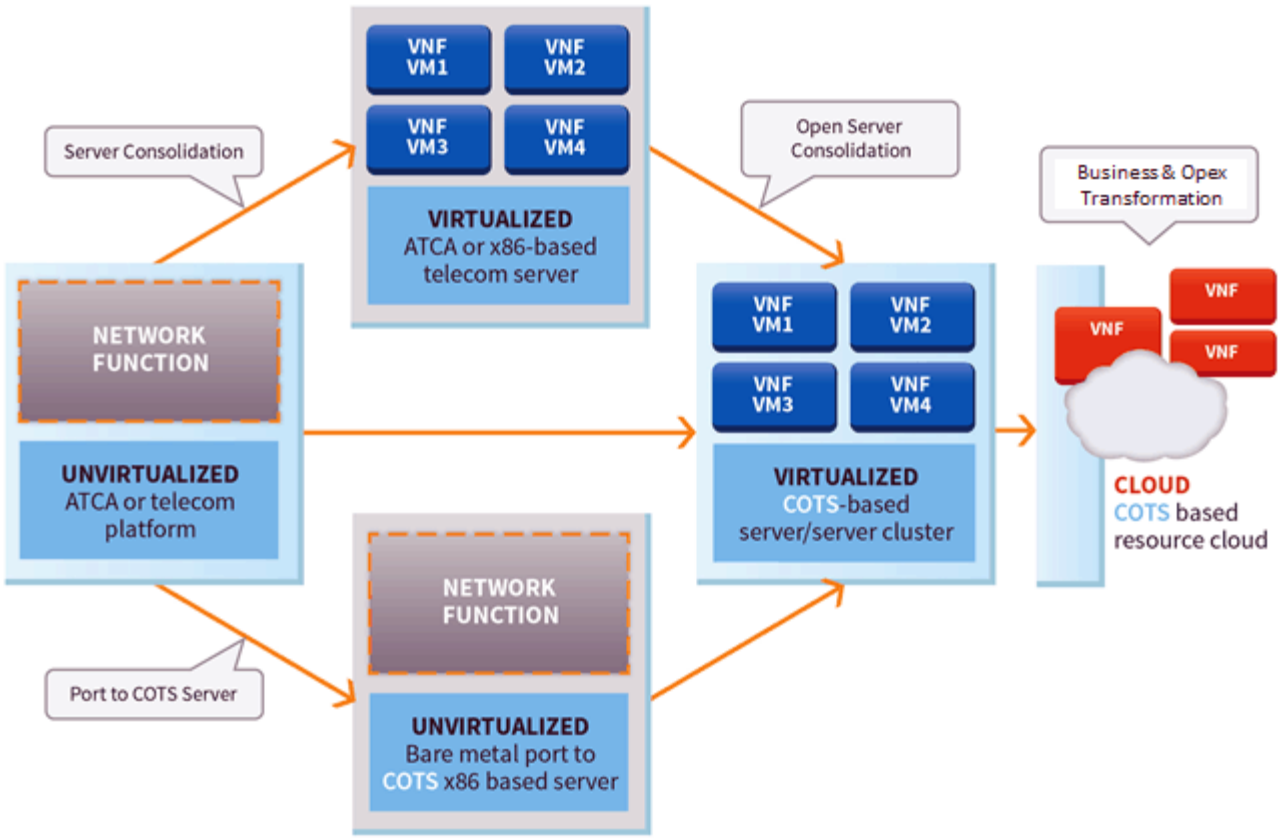
Heavy Reading has identified three key approaches to network functions virtualization that operators and vendors are taking:

- **Bare metal implementation:** Moving network functionality off proprietary hardware and onto a COTS server without a hypervisor. We classify this as "NFV" even though there is no virtualization involved, because server standardization means functions can be moved flexibly within a COTS server environment.
- **Virtualization:** Moving network functionality onto a COTS server with a hypervisor. Functions may still be located on specific servers or server clusters, but the operator can run multiple instances of a function, or multiple functions, on the same server/cluster, reducing equipment costs

- **Cloudification:** Moving network functionality into a cloud environment. In the cloud environment network functions are "untethered" from physical servers and, theoretically, any network function may run on any server anywhere in the cloud at any given moment.

These approaches are not mutually exclusive and may be used in combination. We envisage that different network functions will be implemented using each of these three approaches depending on their internal and operator requirements. For example, some network functions are not suitable candidates for virtualization but can be moved to COTS bare metal servers. Others may already sit on COTS bare metal servers but represent a large investment that an operator is not yet ready or able to replace with virtualized equivalents. A few operators may take network functions straight to the cloud. Some functions may follow a linear progression from bare metal migration to cloudification over time.

Figure 1: The Virtualization Roadmap



Source: Heavy Reading

For ease of reference, this paper will call all network functions running on COTS servers, regardless of level of virtualization, **virtual network functions** (VNFs).

Network functions that remain on proprietary appliances, tightly coupled to specific hardware, will be referred to as **physical network functions** (PNFs).

Cloudification is the end goal of NFV, but few network functions run in the cloud today. For a long time to come, operators will need to manage and orchestrate a mixed set of bare metal, virtualized and cloudified network functions. In fact, the challenge is wider than this: to manage all types of VNFs together with PNFs in order to deliver network services.

Virtualization Creates New Opportunities for Management

VNFs on industry standard servers can be faster and less costly than PNFs to deploy and manage. Operators gain:

- **Choice of where to run the function(s**) in their infrastructure. Even if a function is not virtualized, it can potentially be placed on any COTS server in any location because the server environment is standardized.
- **Commonality of management across VNFs**. When network functions are locked into proprietary physical appliances, each appliance has to be managed differently. When VNFs run in a common environment, there is a large opportunity to manage their deployment in a consistent and standardized way
- **Separation of management concerns**. NFV separates the management of resources (physical and virtual) from the management of applications (VNFs). To a VNF, resources are abstractions – virtual resources – and a different management layer takes care of them. This contrasts with traditional network management systems (NMS/OSS) that manage the application logic and the hardware together in a proprietary physical appliance (PNF).

The common management environment needs to take account of cloudified, virtualized and bare metal VNFs. Existing OSS can manage bare metal and even virtualized VNFs, but they have two drawbacks: (1) they typically manage individual VNFs in silos; and (2) they can't manage cloudified VNFs at all. Current OSS will need significant augmentation if they are to provide the common management environment needed for NFV.

It is important that operators lay the right foundations for managing the NFV-enabled network. The industry has a once-in-a-generation chance to design, from the ground up, a management architecture that can provide order of magnitude improvements in the cost and agility of their network operations. This architecture needs to deliver the full value of the NFV vision across the three "virtualization" models we have identified.

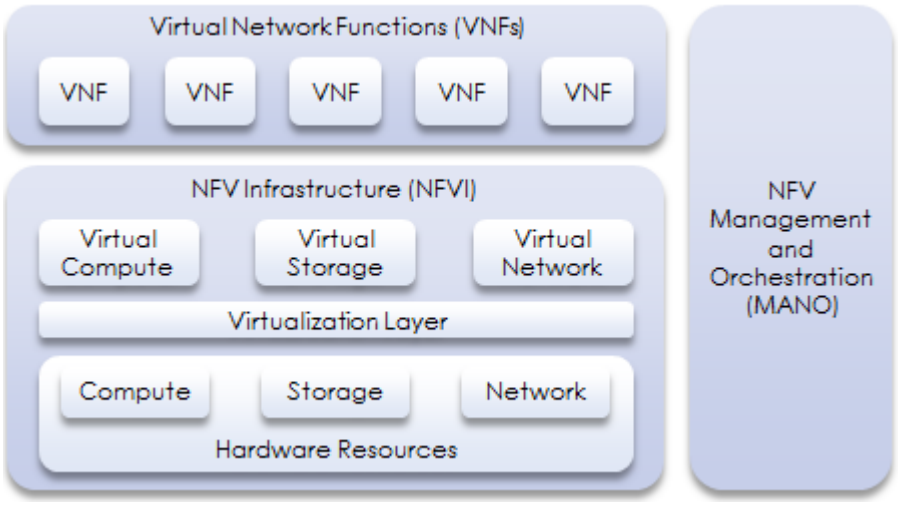
NFV Management Architecture Considerations

The NFV Architecture & VNF Management

The architecture defined by ETSI NFV ISG highlights the separation of infrastructure and application domains. It has three major components (see **Figure 2**):

- The **NFV Infrastructure** (NFVI), which consists of physical resources, the virtualization layer that abstracts them and the virtualized versions of those resources. Operators may choose to implement multiple NFVIs, for example, at different locations within their infrastructure (in data centers, central offices, radio base stations, etc.) and/or with different characteristics. NFVIs may vary according to the compute, storage and network hardware combinations they provide, their memory availability, the service-level agreements (SLAs) they offer around latency and high availability, their level of resilience (for example, whether or not they support multiple attachment points to the WAN) and other factors.
- **Virtual Network Functions.** NFV envisages the NFVI(s) supporting multiple VNFs from multiple vendors. This is desirable if operators are to gain the full benefits of moving network functions onto standard hardware and breaking operational silos with common management. These benefits include location flexibility, scalability, high infrastructure utilization rates and operating costs spread across multiple VNF workloads.
- **Management and Orchestration (MANO).** The MANO stack describes the common management environment needed for VNFs. In the ETSI NFV architecture, MANO's primary focus is on managing and orchestrating virtualized and cloudified VNFs and infrastructure, but this paper will argue that it is possible, and in fact desirable, to be able to manage and orchestrate all three types of VNF, including those running on industry standard bare metal environments.

Figure 2: Three Pillars of the ETSI NFV Architecture

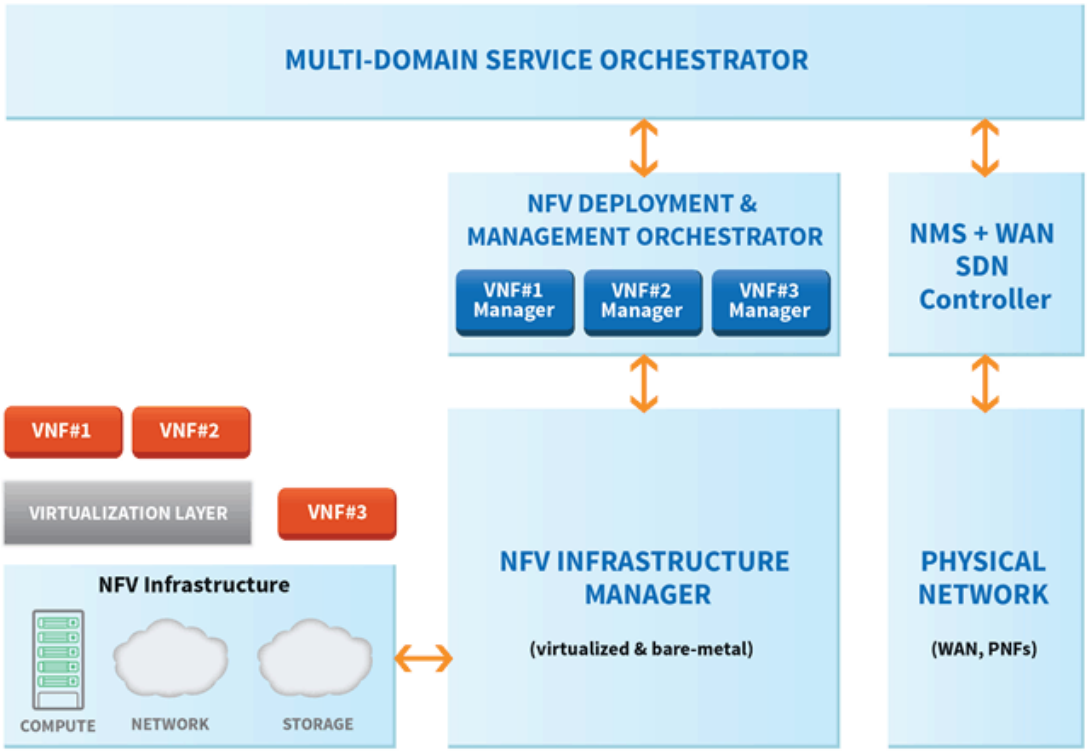


Source: ETSI NFV ISG

MANO Components

The MANO stack is a work in progress and certain aspects of it are open to interpretation, especially around VNF management. **Figure 3** shows how NFV MANO stack components might co-exist with existing network management systems and network infrastructure.

Figure 3: An End-to-End View of Physical & Virtual Network Function Management



Source: Cyan

NFVI Management

The best-defined area of the MANO stack is the lowest level: the management and orchestration of the physical and virtual compute, storage and connectivity resources that make up the NFVI. This is carried out by a **Virtualized Infrastructure Manager** (VIM). The VIM deploys and manages NFVI(s) and serves up compute, storage and networking resources on-demand.

There are multiple candidates for the VIM. OpenStack is a popular choice for many telcos and vendors because its open source status is seen as protection against vendor lock-in.

VNF Orchestration

At the highest level of the stack, sits the **orchestrator**. Within MANO as it is currently defined, the orchestrator plays two roles.

The first is a **service orchestration** role, assembling network functions into services that can be consumed by higher-level services (products) and/or directly by end users. This is known as **service chaining**, or, where a service consists exclusively of VNFs, **forward graphing**. Since operators will, for a long time to come, have a mix of virtual (VNFs) and physical, appliance-based functions (PNFs) in their networks, most services for the foreseeable future will consist of a mix of VNFs and PNFs. This means service orchestration must take place above the MANO stack, where both virtual and physical functions can be "stitched" together into service chains.

There is a need for a **multi-domain service orchestration capability** that is currently beyond the scope of the NFV MANO architecture. The multi-domain service orchestrator will need to speak to the VNF deployment and management orchestrator within the MANO stack (see below) that will deploy the VNFs and instantiate the VNF forward graphs participating in service chains. The multi-domain service orchestrator will also need to interact with all the OSS management domains responsible for the PNFs that are part of the chain. Some existing OSS may be candidates to implement the multi-domain service orchestration (MDSO) capability once they have been extended and integrated with an NFV deployment orchestrator. Or operators may choose a new product for this role.

The second is a **VNF deployment and management orchestration** role. The VNF deployment and management orchestrator provides a common management layer across any or all VNFs, regardless of the NFV approach (bare metal, virtualization, cloudification) that has been applied.

Figure 4: VNF Deployment & Management Orchestrator Functions

FUNCTION	DESCRIPTION
Global view of resources	Visualization of all resources across multiple NFVIs and bare metal environments. This supports efficient resource management across NFV infrastructure(s).
Policy-driven placement of VNFs	Placement of appropriate resources/NFVI(s) in optimal location(s) according to the policy requirements (e.g., security, isolation) of individual VNFs. Automatic, manual and semi-manual placement should be supported.
KPI monitoring, analysis and presentation and event handling	Monitoring of both virtual resource and VNF key performance indicators (KPIs) and event triggers/alerts for breaches of KPI thresholds.
VNF lifecycle management	Support for VNF deployment, scaling up, down, in and out of virtual resources and resilience and recovery actions.
Auditing and reporting	Audit trails of, e.g., scaling requests and events, policy enforcement, resource usage, SLA breaches, etc.
Deployment of VNF forwarding graphs	Coordination of VNFs participating in forwarding graphs.
OSS and multi-service domain orchestration integration	Ability to: • Send NFV state-related and accounting and usage information to B/OSS • Accept/report on policy management, data analytics triggers from/to B/OSS • Handle NFVI capacity/information exchanges with B/OSS (systems of record) • Accept deployment instructions from multi-domain service orchestrator

The VNF deployment and management orchestrator is responsible for deploying VNFs at the right location, with the right resources and mediating between VNFs, the VIM(s) associated with NFVI(s) and systems external to the MANO stack (B/OSS, multi-domain service orchestrator) over the lifecycle of the VNF.

MANO-based VNF deployment and management orchestration replaces the months-long hardware procurement cycle needed to deploy network functions in the physical world with the almost instantaneous provision of appropriate virtual resources created and maintained within the NFVI.

Prerequisites for VNF Deployment & Management Orchestration

The alternative to an orchestrated approach to VNF deployment is for every VNF to be responsible for deploying itself on an NFVI and for managing its own needs for virtual resources. This would require each VNF, every time it wants to scale up/out or turn off resources, to talk directly to the Virtualized Infrastructure Manager (VIM). There is widespread agreement that allowing VNFs individual access to the VIM is a recipe for chaos.

Individual VNFs do not have a global view of available resources. They lack the knowledge of different NFVIs and their resource topologies and properties and they have no awareness of the needs of other VNFs. Without an orchestration function, individual VNFs are likely to create resource contention, "noisy neighbor" and affinity problems that will threaten the stability, availability and performance of the shared NFV infrastructure and all the applications running on it.

The volume of VNF requests hitting the VIM – without any kind of intelligent triaging of requests to determine which are the most urgent and should have priority – could overwhelm the VIM. This is why it is important to have a VNF deployment and management orchestrator that mediates between the VNFs and the underlying resource layer.

But VNF vendors need to do their part. They will need to create deployment templates for their VNFs that can be consumed by the VNF deployment and management orchestrator and acted upon. The VNF deployment template, which should be based on an industry standard, such as OpenStack Heat or OASIS TOSCA, expresses the VNF's deployment requirements and policies. For example, the template should express the VNF's memory, compute, storage, networking, security and geolocation needs. The VNF deployment and management orchestrator feeds these policies into its placement algorithm to determine where and how to deploy VNF workloads and then instructs the VIM to provide the necessary resources in the right place(s).

The template can also expose the VNF's key performance indicators (KPIs), for example, its memory and CPU usage, which the VNF deployment and management orchestrator can monitor to determine when to provide additional resources. The orchestrator can use the KPIs to monitor the performance of each VNF and remediate any problems by sending instructions to the VIM to reconfigure the NFVI.

Alternatively, it may be appropriate in the case of large and highly complex VNFs that the VNF's own management system (VNF Manager) should monitor these KPIs internally and send requests for new resources to the VNF deployment and management orchestrator. The VNF deployment and management orchestrator is

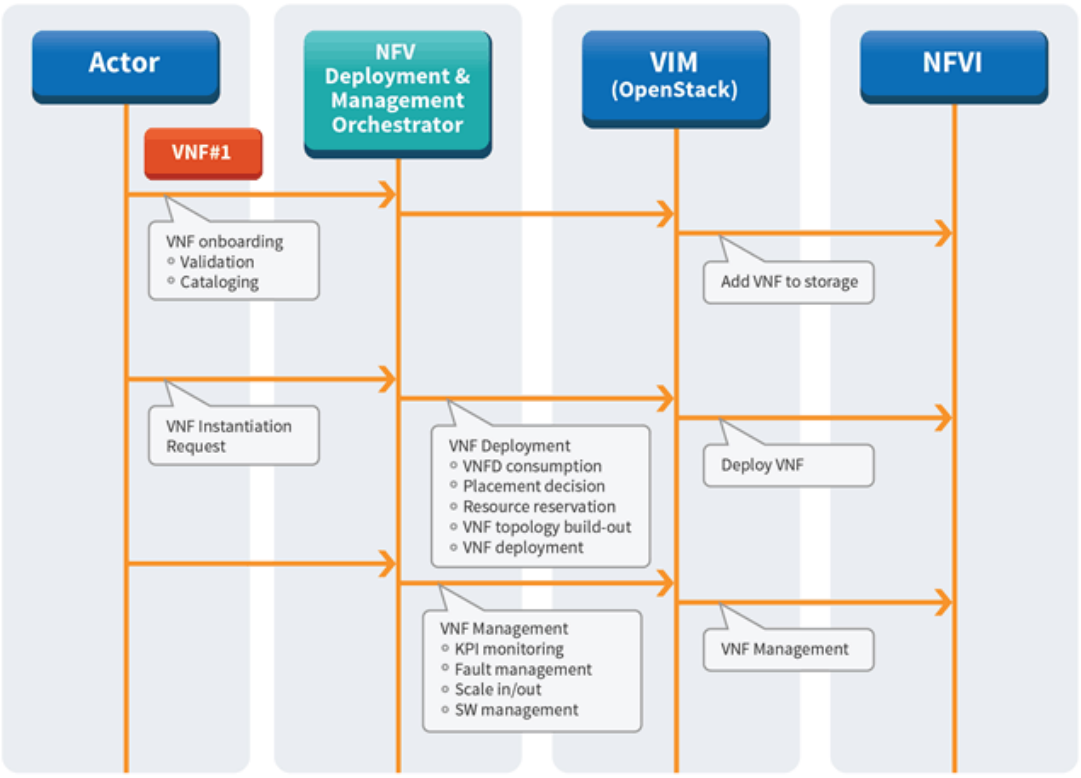
still needed to mediate these requests to avoid the problems that would arise if a VNF Manager gave direct instructions to the VIM.

Once the VIM has responded to the VNF deployment and management orchestrator's request for new NFVI resources, the orchestrator can perform the necessary tasks to deploy the additional virtual resources.

The VNF deployment and management orchestrator/VNF template approach closely follows the "DevOps" approach in the IT cloud. This leverages the management intelligence that can be baked into a global orchestration capability. A DevOps approach reduces the management burden on each VNF developer and lowers operational cost by de-duplicating "stovepiped" VNF management function.

Figure 5 illustrates the process for deploying VNFs using a VNF deployment and management orchestrator.

Figure 5: Steps in the VNF Deployment Process



Source: Cyan

Recommended Steps on the Path to NFV

Operators are considering the migration steps needed to integrate NFV into their existing operational environment. The following recommendations are based on current operator best practice.

Select candidate VNF(s). Operators are progressing with NFV one function at a time to build up knowledge and experience. So their first challenge is to identify a network function(s) for which there is a strong business case for some level of virtualization.

Operators should factor into the business case the NFV approach they wish to take, for example, function migration to a bare metal COTS server, virtualization or cloudification. Typical drivers for the business case include lower cost of implementation and faster, more ubiquitous deployment of a function.

VNF selection must consider whether there are mature vendor implementations of the function(s) at the operator's required level of virtualization; the operator's skillset and capabilities for handling an NFV version of a particular function; the geographical scope of the VNF deployment, e.g., in a specific metro network or data center; and the VNF's other environmental and management requirements.

Select/design a future-proof NFVI. The first VNF will be an anchor tenant of the NFVI, but most operators expect their NFVI to run multiple functions over time. Since an operator may want to support all three of the NFV approaches this paper has identified, the NFVI should be designed with the end goal of cloudification in mind, even if initially, it only runs VNFs on COTS bare metal servers. In other words, the NFVI should be future-proofed to handle all phases of NFV.

Leading operators are trying to standardize on hardware, virtualization platform, storage and networking fabric within their NFVI, but some envisage running different NFVIs in different environments, such as a data center NFVI and a base station NFVI. Some NFVI nodes may be better suited for high-performance, high availability VNFs and others for VNFs that are less mission critical.

In the future, an NFVI may be "assembled" dynamically to meet the deployment needs of a particular VNF. This will be achieved through the orchestration of software interfaces to NFVI building blocks. In designing an NFVI, operators should be aware of the industry megatrend toward "software-defined" infrastructure as exemplified by the Open Compute initiative.

Audit existing OSS to understand management gaps for VNFs. Is there a candidate for a multi-domain service orchestrator that will be able to orchestrate the fulfillment of services consisting of both PNFs and VNFs? If not, the operator will need to consider how it will plug this management gap.

In most cases, existing OSS will lack VNF deployment and management orchestration or VIM support as such management functionality has not previously been required in the physical network environment. So operators will find they have work to do to augment existing OSS with these capabilities or acquire a new system that provides deployment orchestration functionality.

The VNF deployment and management orchestration capability/augmented OSS will need to interface to the operator's selected VIM interface for its NFVI (for example, OpenStack).

Integrate data and metrics from the VNF deployment orchestration/NFVI environment with OSS systems of record. Operators should bear in mind the effort and cost required to extend operational systems designed to manage the physical network with the very different functionality required to manage and orchestrate VNFs and the NFVI.

Existing inventory systems, for example, would need to be completely overhauled to manage the data center equipment types, software, scale and virtual to physical application and resource mapping needed to understand and orchestrate deployment of a VNF in an NFVI. It may be more cost-effective to bring in a new VNF deployment and management orchestration tool that is fit for purpose rather than attempt to re-engineer an existing system.

However, operators are not likely to rip and replace existing OSS and they may retain them as systems of record for both PNF and VNF management. This gives them a "single pane of glass" view, for example, for isolating and troubleshooting network issues. Operators will need to identify the integrations needed with their existing OSS environment to enable coherent management across physical and virtual functions.

Work with VNF vendors to produce deployment templates that can be consumed by the VNF deployment and management orchestrator and implemented on the NFVI. Operators should encourage their selected VNF vendor(s) to supply a standardized deployment template that defines the VNFs deployment requirements and policies and that exposes the thresholds at which a VNF deployment and management orchestrator needs to provide or withdraw resources.

At present, an operator needs to work with its selected VNF supplier so that the vendor can understand both the VNF management capabilities and the NFVI characteristics the operator's NFV environment will provide. This helps the vendor to tune VNF performance and reduce management overhead for a specific operator implementation. The use of a standard templated approach future proofs both operator and vendor.

Develop the new operational mindset and skills needed to drive NFV results. As we have said, NFV delivers operational benefits, including choice over where to run functions, common management across multiple VNFs and the separation of management concerns. A hardware failure in the NFVI, for example, has no impact on the service availability of a VNF since the VNF deployment and management orchestrator simply spins up a new instance of the VNF in a non-affected part of the NFVI. The hardware failure needs to be traced for replacement purposes, but the impact on service downtime is negligible compared to the effect there would be on a service comprised of PNFs.

Acclimatizing to such a new operational mindset and a DevOps approach takes time. However, if operators really want to drive cost out of their networks and benefit from the power of NFV, they must make this adjustment. Operators should invest in new skills and tools rather than import legacy network management processes and systems into the NFV environment.

About Cyan Inc.

Cyan enables network transformation. The company's software-defined network (SDN) solutions deliver orchestration, visualization and scale to networks that, until now, have been static and hardware-driven. Cyan's open platforms provide multi-vendor control and visibility to network operators, making service delivery more efficient and profitable. Cyan's ground-breaking Blue Planet SDN Platform and innovative Z-Series packet-optical hardware support hundreds of deployments across North America, Europe, South America and Asia, ranging from large carriers, fiber operators and wireless backhaul providers to enterprises, data centers and government agencies.

Cyan's focus on innovation and product excellence has resulted in numerous awards for its platforms. Most recently, Cyan's Blue Planet SDN Platform won *Light Reading*'s 2013 Leading Lights Award for Best New Telecom Product and Telecom Asia's 2013 Innovation and Reader's Choice Award for SDN Innovation of the Year. Led by a seasoned management team with extensive telecom, networking and software expertise, Cyan is headquartered in Petaluma, California, USA.