TEAM-KINETIC

BY

MQWALA V

HLAULA M

TYOTYO P

BACKGROUND

NFV originated within the highly competitive service provider community, as they looked for ways to cut costs and accelerate the roll out of profitable services to better monetize their networks and grow their revenues. Hardware-based network appliances, which are typically expensive and complex to deploy and manage, were limiting the providers’ ability to consolidate functionality and quickly trial new services. Within an increasingly virtualized environment, providers wanted to be able to deploy network functionality whenever and wherever it was needed; they didn’t want to be tied to the capabilities of a specific appliance or topology. They felt if they could decouple the network services from the hardware, it would allow them to deploy networking components that could truly fit and support a fully virtualized infrastructure, including servers, storage and even other networks. A few providers came together, within the European Telecommunications Standards Institute’s (ETSI) and created the Industry Specification Group (ISG) for NFV to accelerate the progress of virtualizing network functions. Launched in January of 2013, the ETSI ISG for NFV has been working to develop the requirements and architecture of virtualized network functions in a telecommunication’s network. In September of 2014, the Linux Foundation announced the Open Platform for NFV Project (OPNFV), which is an open source, carrier-grade integrated platform that aims to help bring new NFV products and services to the industry faster. The goal is to make the recommendations and standards that come out of the ETSI ISG a reality, by leveraging the cumulative resources of the open source community. ETSI ISG for NFV and OPNFV will work closely to advance NFV concepts and technologies. We are starting to see some of the fruits of the industry’s labor, with NFV trials

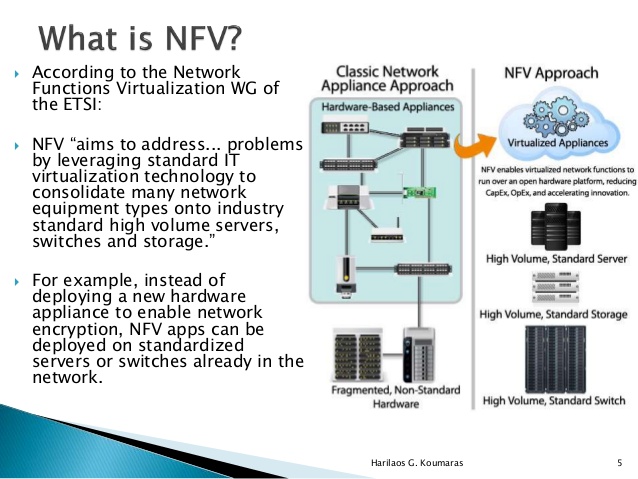
Introduction of network function virtualization

Network operators’ networks are populated with a large and increasing variety of proprietary hardware appliances. To launch a new network service often requires yet another variety and finding the space and power to accommodate these boxes is becoming increasingly difficult; compounded by the increasing costs of energy, capital investment challenges and the rarity of skills necessary to design, integrate and operate increasingly complex hardware-based appliances. Moreover, hardware-based appliances rapidly reach end of life, requiring much of the procure design-integrate-deploy cycle to be repeated with little or no revenue benefit. Worse, hardware lifecycles are becoming shorter as technology and services innovation accelerates, inhibiting the roll out of new revenue earning network services and constraining innovation in an increasingly network-centric connected world.

Network Functions Virtualization (NFV) is a core structural change in the way telecommunication infrastructure gets deployed. This in turn will bring significant changes in the way that applications are delivered to service providers. NFV will bring cost efficiencies, time-to-market improvements and innovation to the telecommunication industry infrastructure and applications. NFV will achieve this through disaggregation of the traditional roles and technology involved in telecommunications applications

Definition

Network Functions Virtualization aims to transform the way that network operators architect networks by evolving standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacenters, Network Nodes and in the end user premises, as illustrated in Figure 1. It involves the implementation of network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need for installation of new equipment.



What Makes NFV Different?

While PC-based network devices have been available since the '80s, they were generally used by small companies and networking enthusiasts who didn't or couldn't afford to buy a commercial-based solution. In the last few years many drivers have brought PC-based networking devices back into the limelight, including: Ethernet as the last mile, better network interface cards, and Intel's focus on networking  
processing in its last few generation of chips. Today many vendors are producing PC-based network devices. Advancements in packet handling within Intel's processors, allowing processor cores to be re-programmed into network processors, allow PCbased network devices to push 10's or even 100's of Gbp/s. Values of NFV  
Some of the values to the NFV concept are speed, agility, and cost reduction. By centralizing designs around commodity server hardware, network operators can:

· Do a single PoP/Site design based on commodity compute hardware;

Avoiding designs involving one-off installs of appliances that have different power, cooling and space needs simplifies planning.

Utilize resources more effectively;

Virtualization allows providers to allocate only the necessary resources needed by each feature/function.

Deploy network functions without having to send engineers to each site; “Truck Rolls” are costly both from a time and money standpoint.

Achieve Reductions in OpEX and CapEX; and,

Achieve Reduction of system complexity i.e Deliver Agility and Flexibility: quickly scale up or down services to address changing demands; support innovation by enabling services to be delivered via software on any industry-standard server hardware

Accelerate Time-to-Market: reducing the time to deploy new networking services to support changing business requirements, seize new market opportunities and improve return on investment of new services. Also lowers the risks associated with rolling out new services,allowing providers to easily trial and evolve services to determine what best meets the needs ofcustomers.

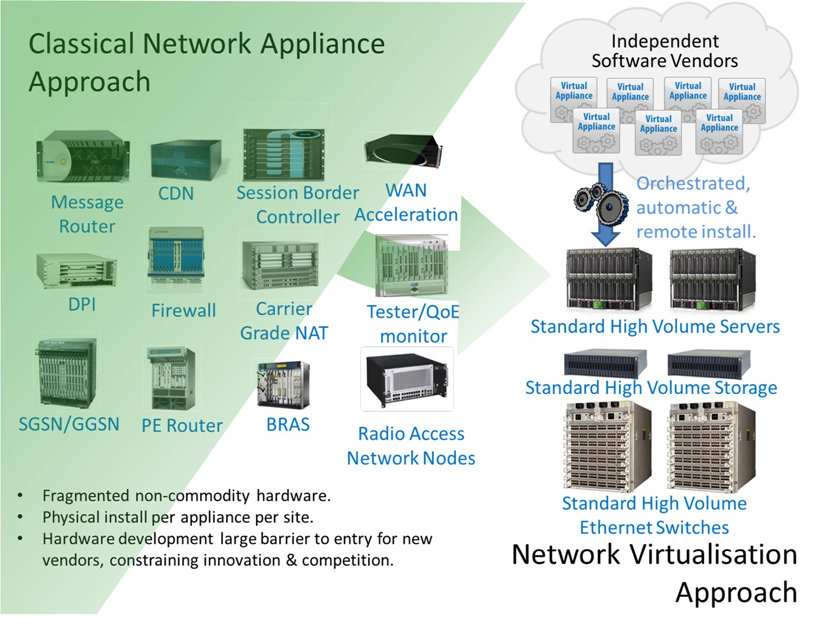
Error resilience : Ensuring the appropriate level of resilience to hardware and software failures.

Scale: Network Functions Virtualization will only scale if all of the functions can be automated.

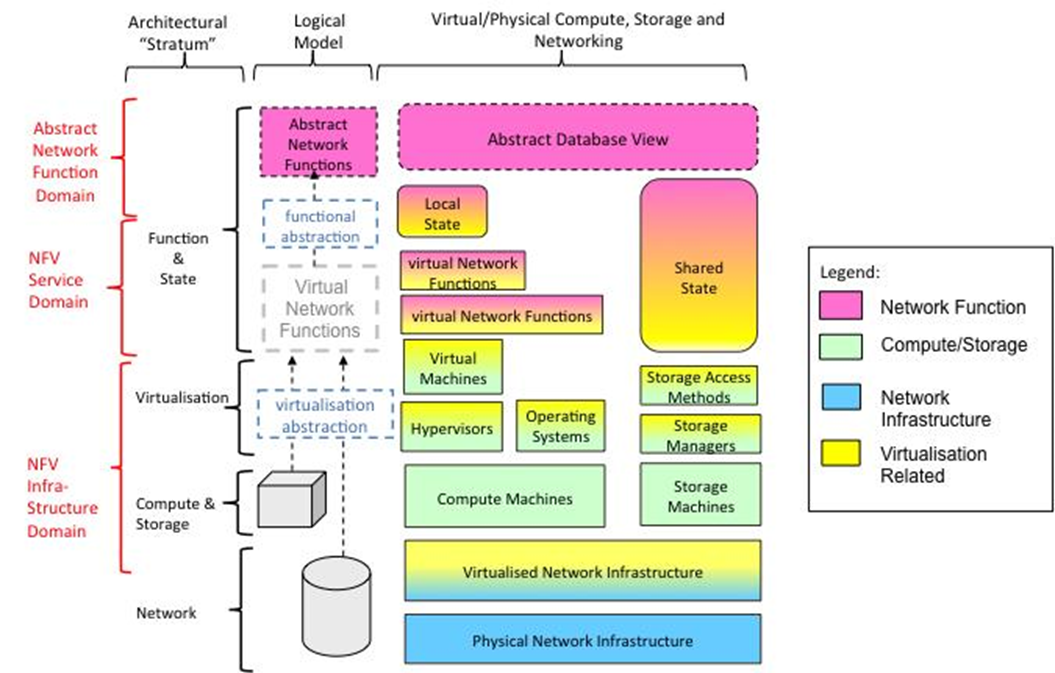
Overview of the ETSI NFV ISG

The ETSI Board approved foundation of the NFV ISG in time for publication of our first white paper last October. ETSI is a global organisation and has proved to be an excellent environment in which to Network Functions virtualization progress our work and we extend our thanks to the Director General and the ETSI Board for their accommodation and support. Although ETSI is a Standards Development  
Organisation (SDO), the objective of the NFV ISG is not to produce standards. The key objectives are to achieve industry consensus on business and technical requirements for NFV, and to agree common approaches to meeting these requirements. The outputs are openly published and shared with relevant standards bodies, industry fora and consortia to encourage a wider collaborative effort. The NFV ISG will collaborate with other SDOs if any standardization is necessary to meet the requirements. The NFV ISG also provides an environment for the industry to collaborate on Proof of Concept (PoC) platforms to demonstrate solutions which address the technical challenges for NFV implementation and to encourage growth of an open ecosystem

NFV:Vision



NFV architecture Model

1. Network operators have proven NFV feasibility via proof of concept test platforms
2. Network operators and vendors have identified numerous “fields of application” spanning all domains (fixed and mobile network infrastructures)
3. Significant CAPEX/OPEX benefits, leveraging also the economies of scale
4. Emerging virtual network appliance market
5. Novel ways to architect and operate networks, spawning a new wave of industry wide innovation
6. Network Functions Virtualization can dramatically change the telecom landscape and industry over the next 2-5 years

Why NFV is the future?

Recent tests by network operators and vendors have demonstrated that network functions can operate at the level of several millions of packets per sec, per CPU core

Demonstrates that standard high volume servers have sufficient processing performance to cost-effectively virtualized network appliances o The hypervisor need not be a bottleneck o The OS need not be a bottleneck

Total Cost of Ownership advantages are a huge driver – could be scenario specific but expect significant benefits, e.g., energy savings

Advances in virtualization & server technologies have propelled the importance and use of software in many applications and fields

A concerted industry effort is underway to accelerate this vision by encouraging common approaches which address the challenges for NFV

Benefits of NFV

We believe the application of Network Functions Virtualization brings many benefits to network operators, contributing to a dramatic change in the telecommunications industry landscape. Benefits we foresee include (not in any particular order):

* Reduced equipment costs and reduced power consumption through consolidating equipment and exploiting the economies of scale of the IT industry (~9.5M Servers shipped in 2011 compared with ~1.5M routers forecast for 2012).[1,2]
* Increased velocity of Time to Market by minimizing the typical network operator cycle of innovation. Economies of scale required to cover investments in hardware-based functionalities are no longer applicable for software-based development, making feasible other modes of feature evolution. Network Functions Virtualization should enable network operators to significantly reduce the maturation cycle.
* The possibility of running production, test and reference facilities on the same infrastructure provides much more efficient test and integration, reducing development costs and time to market.
* Targeted service introduction based on geography or customer sets is possible. Services can be rapidly scaled up/down as required. In addition, service velocity is improved by provisioning remotely in software without any site visits required to install new hardware.
* Enabling a wide variety of eco-systems and encouraging openness. It opens the virtual appliance market to pure software entrants, small players and academia, encouraging more innovation to bring new services and new revenue streams quickly at much lower risk.
* Optimizing network configuration and/or topology in near real time based on the actual traffic/mobility patterns and service demand. For example, optimization of the location & assignment of resources to network functions automatically and in near real time could provide protection against failures without engineering full 1+1 resiliency.
* Supporting multi-tenancy thereby allowing network operators to provide tailored services and connectivity for multiple users, applications or internal systems or other network operators, all co-existing on the same hardware with appropriate secure separation of administrative domains.
* Reduced energy consumption by exploiting power management features in standard servers and storage, as well as workload consolidation and location optimization. For example, relying on virtualization techniques it would be possible to concentrate the workload on a smaller number of servers during off-peak hours (e.g. overnight) so that all the other servers can be switched off or put into an energy saving mode.[3]

Improved operational efficiency by taking advantage of the higher uniformity of the physical network platform and its homogeneity to other support platforms:

IT orchestration mechanisms provide automated installation, scaling-up and scaling out of capacity, and re-use of Virtual Machine (VM) builds.[4]

Eliminating the need for application-specific hardware. The skills base across the industry for operating standard high volume IT servers is much larger and less fragmented than for today’s telecom-specific network equipment.

Reduction in variety of equipment for planning & provisioning. Assuming tools are developed for automation and to deal with the increased software complexity of virtualization.

Option to temporarily repair failures by automated re-configuration and moving network workloads onto spare capacity using IT orchestration mechanisms. This could be used to reduce the cost of 24/7 operations by mitigating failures automatically.

The potential to gain more efficiency between IT and Network Operations.

The potential to support in-service software upgrade (ISSU) with easy reversion by installing the new version of a Virtualized Network Appliance (VNA) as a new Virtual Machine (VM). Assuming traffic can be transferred from the old VM to the new VM without interrupting service. For some applications it may be necessary to synchronize the state of the new VM with the old VM.

The Changing Telecoms industry landscape

Although Network Functions Virtualization brings many advantages to the telecommunications industry it is likely to transform the vendor landscape. Each player will need to position/re-position itself in the new Network Functions Virtualization market.

This is not as disruptive as it may seem because network equipment vendors already implement some of their solutions by combining their proprietary software with industry standard hardware and software components, but in a proprietary way. Enabling their proprietary software to run on industry standard hardware in a standardized way may be a significant opportunity for existing players because their software and networking know-how is where the real value is in many cases. Some major industry players are already moving in this direction by offering virtualized versions of their products. The challenge for network operators is how to migrate their operations and skill base to a software based networking environment while carefully re-targeting investment to maximize reuse of existing systems and processes.

Enablers for network function virtualization

Several recent technology developments make the goals of Network Functions Virtualization achievable. This section describes these enablers and briefly discusses relevance.

Cloud computing

Network Functions Virtualization will leverage modern technologies such as those developed for cloud computing. At the core of these cloud technologies are virtualization mechanisms: hardware virtualization by means of hypervisors, as well as the usage of virtual Ethernet switches (e.g. switch) for connecting traffic between virtual machines and physical interfaces. For communication-oriented

functions, high-performance packet processing is available through high-speed multi-core CPUs with high I/O bandwidth, the use of smart Ethernet NICs for load sharing and TCP Offloading, and routing packets directly to Virtual Machine memory, and poll-mode Ethernet drivers (rather than interrupt driven, for example Linux NAPI and Intel’s DPDK).

Cloud infrastructures provide methods to enhance resource availability and usage by means of orchestration and management mechanisms, applicable to the automatic instantiation of virtual appliances in the network, to the management of resources by assigning virtual appliances to the correct CPU core, memory and interfaces, to the re-initialization of failed VMs, to snapshot VM states and the migration of VMs.

Finally, the availability of open APIs for management and data plane control, like Open Flow,

OpenStack, Open Naas or OGF’s NSI, provide an additional degree of integration of Network Functions Virtualization and cloud infrastructure.

Industry Standard High Volume Servers

The use of industry standard high volume servers is a key element in the economic case for Network Functions Virtualization. Network Functions Virtualization leverages the economies of scale of the IT industry. An industry standard high volume server is a server built using standardized IT components (for example x86 architecture) and sold in the millions. A common feature of industry standard high volume servers is that there is competitive supply of the subcomponents which are interchangeable inside the server.

We believe that Network Appliances which depend on the development of bespoke Application Specific Integrated Circuits (ASICs) will become increasingly uncompetitive against general purpose processors as the cost of developing ASICs increases exponentially with decreasing feature size.[5] Merchant silicon will still be applicable for commodity functions implemented at scale, and ASICs will still be applicable for some types of very high throughput applications.

Challenges for Network Functions Virtualization

There are a number of challenges to implement Network Functions Virtualization which need to be addressed by the community interested in accelerating progress. How this effort could be progressed is described later in this document. Challenges we have identified are (not in any particular order):-

* Portability/Interoperability. The ability to load and execute virtual appliances in different but standardized datacenter environments, provided by different vendors for different operators. The challenge is to define a unified interface which clearly decouples the software instances from the underlying hardware, as represented by virtual machines and their hypervisors. Portability and Interoperability is very important as it creates different ecosystems for virtual appliance vendors and datacenter vendors, while both ecosystems are clearly coupled and depend on each other. Portability also allows the operator the freedom to optimize the location and required resources of the virtual appliances without constraints.
* Performance Trade-Off. Since the Network Functions Virtualization approach is based on industry standard hardware (i.e. avoiding any proprietary hardware such as acceleration engines) a probable decrease in performance has to be taken into account. The challenge is how to keep the performance degradation as small as possible by using appropriate hypervisors and modern software technologies, so that the effects on latency, throughput and processing overhead are minimized. The available performance of the underlying platform needs to be clearly indicated, so that virtual appliances know what they can get from the hardware. The authors of the white paper believe that using the right technology choice will allow virtualization not only of network control functions but also data/user plane functions.
* Migration and co-existence of legacy & compatibility with existing platforms.
* Implementations of Network Functions Virtualization must co-exist with network operators’ legacy network equipment and be compatible with their existing Element Management Systems, Network Management Systems, OSS and BSS, and potentially existing IT orchestration systems if Network Functions Virtualization orchestration and IT orchestration are to converge. The Network Functions Virtualization architecture must support a migration path from today’s proprietary physical network appliance based solutions to more open standards based virtual network appliance solutions. In other words, Network Functions Virtualization must work in a hybrid network composed of classical physical network appliances and virtual network appliances. Virtual appliances must therefore use existing North Bound Interfaces (for management & control) and interwork with physical appliances implementing the same functions.
* Management and Orchestration. A consistent management and orchestration architecture is required. Network Functions Virtualization presents an opportunity, through the flexibility afforded by software network appliances operating in an open and standardized infrastructure, to rapidly align management and orchestration North Bound Interfaces to well defined standards and abstract specifications. This will greatly reduce the cost and time to integrate new virtual appliances into a network operator’s operating environment. Software Defined Networking (SDN) further extends this to streamlining the integration of packet and optical switches into the system e.g. a virtual appliance or Network Functions Virtualization orchestration system may control the forwarding behaviors of physical switches using SDN.
* Automation. Network Functions Virtualization will only scale if all of the functions can be automated. Automation of process is paramount to success.
* Security & Resilience. Network operators need to be assured that the security, resilience and availability of their networks are not impaired when virtualized network functions are introduced. Our initial expectations are that Network Functions Virtualization improves network resilience and availability by allowing network functions to be recreated on demand after a failure. A virtual appliance should be as secure as a physical appliance if the infrastructure, especially the hypervisor and its configuration, is secure. Network operators will be seeking tools to control and verify hypervisor configurations. They will also require security certified hypervisors and virtual appliances.
* Network Stability. Ensuring stability of the network is not impacted when managing and orchestrating a large number of virtual appliances between different hardware vendors and hypervisors. This is particularly important when, for example, virtual functions are relocated, or during re-configuration events (e.g. due to hardware and software failures) or due to cyber-attack. This challenge is not unique to Network Functions Virtualization. Potential instability might also occur in current networks, depending on unwanted combinations of diverse control and optimization mechanisms, for example acting on either the underlying transport network or on the higher layers’ components (e.g. flow admission control, congestion control, dynamic routing and allocations, etc.). It should be noted that occurrence of network instability may have primary effects, such as jeopardizing, even dramatically, performance parameters or compromising an optimized use of resources. Mechanisms capable of ensuring network stability will add further benefits to Network Functions Virtualization.
* Simplicity. Ensuring that virtualized network platforms will be simpler to operate than those that exist today. A significant and topical focus for network operators is simplification of the plethora of complex network platforms and support systems which have evolved over decades of network technology evolution, while maintaining continuity to support important revenue generating services. It is important to avoid trading one set of operational headaches for a different but equally intractable set of operational headaches.
* Integration. Seamless integration of multiple virtual appliances onto existing industry standard high volume servers and hypervisors is a key challenge for Network Functions Virtualization. Network operators need to be able to “mix & match” servers from different vendors, hypervisors from different vendors and virtual appliances from different vendors without incurring significant integration costs and avoiding lock-in. The ecosystem must offer integration services and maintenance and third-party support; it must be possible to resolve integration issues between several parties. The ecosystem will require mechanisms to validate new Network Functions Virtualization products. Tools must be identified and/or created to address these issues.

Recommendations/Call for Action

Network Functions Virtualization is already occurring. In a few years, we can expect the communications industry to look and feel similar to the IT industry. There will be a wider range of business models more suited to a software industry. Operations complexity will be abstracted away by more automation and self-provisioning will be more common. As detailed in this white paper, Network Functions Virtualization will deliver many benefits for network operators and their partners and customers whilst offering the opportunity to create new types of eco-systems (alongside traditional supply models based on preferred strategic partners) which will encourage and support rapid innovation with reduced cost and reduced risk. To reap these benefits the technical challenges, as described above, must be addressed by the industry.

The authors of this white paper believe that solutions to these technical challenges are available (or could be made available) and recommend that the IT and Network industries combine their complementary expertise and resources in a joint collaborative effort to reach broad agreement on standardized approaches and common architectures which address these technical challenges, and which are interoperable and have economies of scale.

To accelerate progress, a new network operator-led Industry Specification Group (ISG) with open membership is being setup under the auspices of ETSI to work through the technical challenges for Network Functions Virtualization as outlined in this white paper. The formal creation process of this ETSI ISG has been started and is expected to be completed by mid-November 2012.

While ETSI will provide the organization for this initiative, the ISG will downstream its work to all relevant organizations and seek to encourage convergence of IT and Network Standardization efforts in this space.

The key objectives, activities and outputs of the ISG are expected to be:

* The ISG will initiate joint studies which address the technical challenges for Network Functions Virtualization as documented in this white paper. With consensus outputs detailed in white papers openly published to the wider industry. It is expected that study items would be identified in a “Network Operator Requirements” white paper prepared by the ISG as an initial deliverable.
* Although parented under ETSI, the ISG will not be a Standards Development Organization (SDO) in itself; it will reference the work of existing SDOs where applicable. Where there are gaps, it will encourage member contributions to SDOs requesting them to take into account the recommendations of the ISG (i.e. requesting updates to existing standards, or to create new standards if appropriate).
* The ISG will identify other expert bodies that could assist with this work, and request that they undertake studies related to their scope to help move the industry forward.
* The ISG will facilitate members to share technical learning in a collaborative way which does not compromise confidentiality.
* The first meeting of the ISG will take place in January 2013. Details will be announced as soon as possible after publication of this white paper.
* In order to chart the way forward for Network Functions Virtualization, the wider industry is asked to provide feedback:
* Network Operators: To state their interest in joining the ISG, thus subscribing to the targets and approach as outlined in this white paper.
* Existing organizations and forums: To state if they see themselves being impacted by the work addressed in the ISG, and to provide information on how they would like to interact with it.
* Vendors: To state their interest in joining the ISG. Vendors are furthermore requested to state the study items in which they are most interested.

MANO Functional Blocks

**NFV Orchestrator:**

– On-boarding of new Network Service (NS), VNF-FG and VNF Packages

– NS lifecycle management (including instantiation, scale-out/in, performance measurements, event correlation, termination)

– Global resource management, validation and authorization of NFVI resource requests

– Policy management for NS instances

**VNF Manager:**

– Lifecycle management of VNF instances

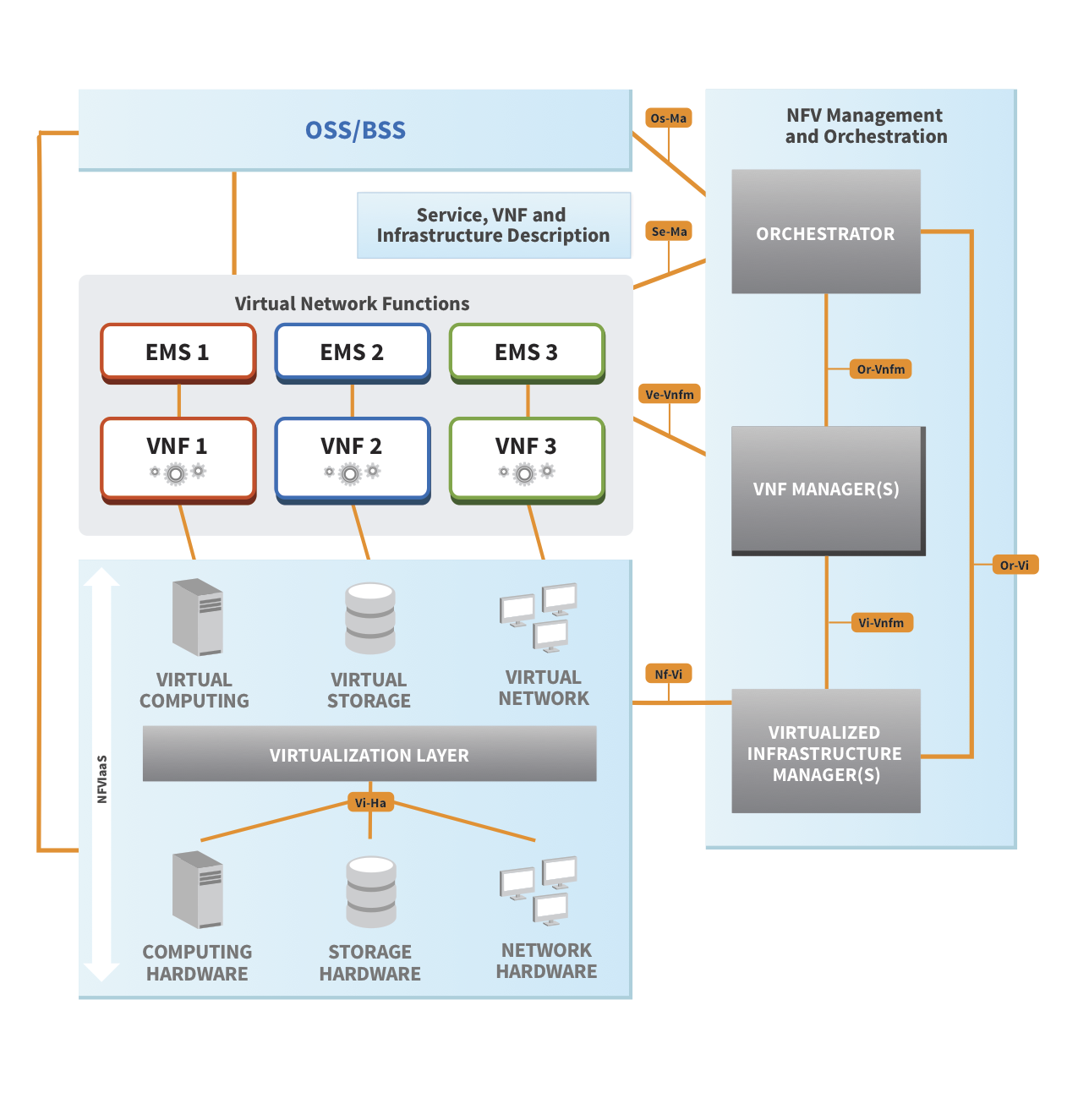
– Overall coordination and adaptation role for configuration and event reporting between NFVI and the E/NMS

**Virtualized Infrastructure Manager (VIM):**

– controlling and managing the NFVI compute, storage and network resources, within one operator’s infrastructure sub-domain

– Collection and forwarding of performance measurements and events

NFV Management and Orchestration Architecture



NFV Entities to deploy and manage

• Network Service (NS): – described by its descriptor file, orchestrated by NFVO, – may cover 1 or more VNF Graphs, VNFs and PNFs.

• VNF Forwarding Graph (VNF-FG): – described by its descriptor file, orchestrated by NFVO, – may cover VNF-FGs, VNFs and NFs

• VNF: – described by its descriptor file, instantiated by the VNF Manager, – covers VNF components (VNFC) each mapped to a VM described with the Virtual Deployment Unit descriptor.

References

1. Server shipments (9.5M units in 2011): http://www.crn.com/news/data-center/232601815/gartner-2011server-sales-grow-but-hard-drive-issues-take-a-toll.htm
2. Router shipments (1.5M units forecast for year 2012): http://www.isuppli.com/Manufacturing-andPricing/MarketWatch/Pages/EMS-Router-Shipments-Backed-by-Market-Growth-in-2012.aspx
3. http://labs.chinamobile.com/cran/wp-content/uploads/CRAN\_white\_paper\_v2\_5\_EN.pdf
4. http://en.wikipedia.org/wiki/Orchestration\_(computing)
5. http://www.edac.org/downloads/resources/profitability/HandelJonesReport.pdf   
   Published E2E Arch, REQ, Use Case, Terminology documents in ETSI NFV Open Area:

– <http://docbox.etsi.org/ISG/NFV/Open/Published/>

• Published ETSI NFV white paper:

– <http://portal.etsi.org/NFV/NFV_White_Paper.pdf>

– <http://portal.etsi.org/NFV/NFV_White_Paper2.pdf>

• ETSI member area:

– Current NFV MANO WG WI document: DGS/NFV-MAN001 (ongoing work)

• <http://docbox.etsi.org/ISG/NFV/MAN/70-DRAFT/MAN1/NFV-MAN001v0011.zip>

– ETSI NFV ISG portal:

• <http://portal.etsi.org/portal/server.pt/community/NFV/367?tbId=789>

SDN DEFINITION

Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow™ protocol is a foundational element for building SDN solutions. The SDN architecture is:

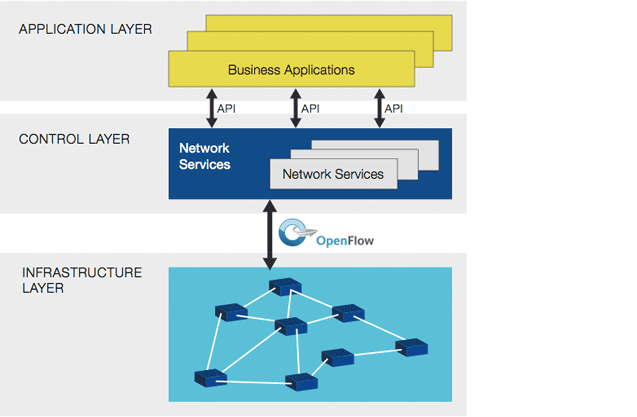
Directly programmable: Network control is directly programmable because it is decoupled from forwarding functions.

Agile: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.

Centrally managed: Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.

Programmatically configured: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.

Open standards-based and vendor-neutral: When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.



(NFV) NETWORK FUNCTION VIRTUALISATION AND (SDN) SOFTWARE DEFINED NETWORKS

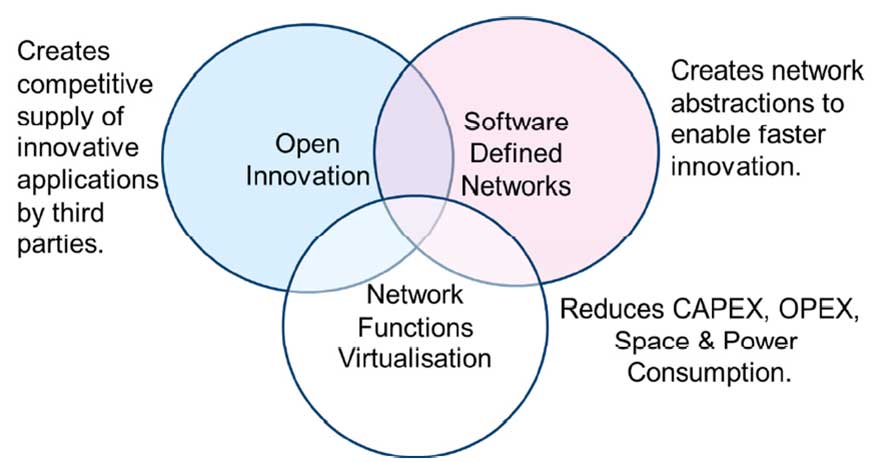
Network function virtualization (NFV) and software-defined networks (SDN) are two closely related technologies that often exist together, but not always. An SDN can be considered a series of network objects (such as switches, routers, firewalls) that deploy in a highly automated manner. The automation may be achieved by using commercial or open source tools customized according to the administrator's requirements. A full SDN may only cover relatively straightforward networking requirements, such as VLAN and interface provisioning.

In many cases, SDN will also be linked to server virtualization, providing the glue that sticks virtual networks together. This may involve NFV, but not necessarily. NFV is the process of moving services, such as load balancing, firewalls and IPS, away from dedicated hardware into a virtualized environment. This is, of course, part of a wider movement toward the virtualization of applications and services.

Functions such as caching and content control can easily be migrated to a virtualized environment but won't necessarily provide any significant reduction in operating costs until some intelligence is introduced. This is because a straight physical to virtual, from an operational perspective, achieves little beyond the initial reduction in power and rack-space consumption. Until some dynamic intelligence is introduced with an SDN technology, NFV inherits many of the same constraints as traditional hardware appliance deployments, such as static, administrator-defined and managed policies.

A good example is virtualized application delivery controllers (ADCs). With careful configuration, it is possible to react to the network state and spin up or down application servers as demands rise and fall. However, traditional hardware deployments have been able to do this for a while, and the configuration is very static; it doesn't cater to the scenario where the ADC itself becomes overloaded or an additional application needs to be brought into production quickly. With SDN features driving NFV, several useful things start to happen. The network can react when things need to change at the micro and macro level. An additional instance can be provisioned in a cluster of virtualized ADCs as the load increases, and production applications can easily be cloned and re-deployed in a development environment. The potential is endless.

So it's perfectly possible to have NFV without the inclusion of a full-blown SDN. The two are often deployed together, and an SDN that drives NFV is a very powerful combination.



Relationship with Software Defined Networks (SDN)

As shown in Figure 2, Network Functions Virtualization is highly complementary to Software Defined

Networking (SDN), but not dependent on it (or vice-versa). Network Functions Virtualization can be

Network Functions Virtualization

Implemented without a SDN being required, although the two concepts and solutions can be combined and potentially greater value accrued. Network Functions Virtualization Relationship with SDN

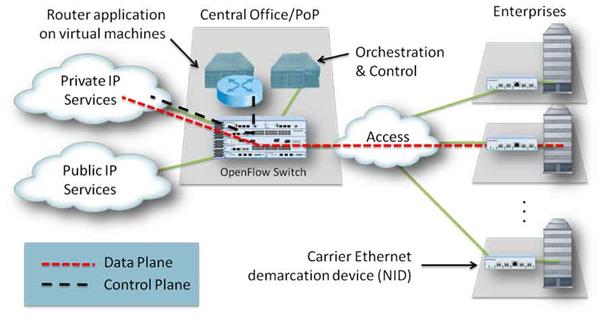
Network Functions Virtualization goals can be achieved using non-SDN mechanisms, relying on the techniques currently in use in many datacenters. But approaches relying on the separation of the control and data forwarding planes as proposed by SDN can enhance performance, simplify compatibility with existing deployments, and facilitate operation and maintenance procedures.

Network Functions Virtualization is able to support SDN by providing the infrastructure upon which the SDN software can be run. Furthermore, Network Functions Virtualization aligns closely with the

SDN objectives to use commodity servers and switches. We intend to work closely with organizations progressing work on SDN such as the Open Networking.

WHY NETWORK FUNCTIONS VIRTUALIZATION & SDN

Network Functions Virtualization (NFV) explicitly targets the two biggest problems facing network operators: bringing costs in line with revenue growth expectations and improving service velocity. NFV's premise is that industry standard IT virtualization technology (servers, switches, and storage) located in data centers, network nodes, or end-users' premises can be used to reduce the cost and increase the speed of service delivery for fixed and mobile networking functions. We believe Network Functions Virtualization is applicable to any data plane packet processing and control plane function in fixed and mobile network infrastructures. Finally, SDN is introduced to separate the control and data, as shown in Figure. Now, the data packets are forwarded by an optimized data plane, while the routing (control plane) function is running in a virtual machine running in a rack mount server.



How NFV will push SDN beyond the data center

NFV's use of virtual network overlays could also drive an expansion of this SDN model beyond the data center where it's focused most often today. If NFV allows services to be composed of virtual functions hosted in different data centers, that would require virtual networks to stretch across data centers and become end-to-end. An end-to-end virtual network would be far more interesting to enterprises than one limited to the data center. Building application-specific networks that extend to the branch locations might usher in a new model for application access control, application performance management and even application security.

Will NFV unify differing SDN models?

With the use of network overlays, NFV could also unify the two models of SDN infrastructure -- centralized and distributed. If connectivity control and application component or user isolation are managed by the network overlay, then the physical-network mission of SDN can be more constrained to traffic management. If SDN manages aggregated routes more than individual application flows, it could be more scalable. Remember that the most commonly referenced SDN applications today -- data center LANs and Google's SDN IP core network -- are more route-driven than flow-driven. Unification of the SDN model might also make it easier to sort out SDN implementations. The lower physical network SDN in this two-layer model might easily be created using revisions to existing protocols, which has already been proposed. While it doesn't offer the kind of application connectivity control some would like, that requirement would be met by the higher software virtual network layer or overlay.