IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT | Integrated Management in the Age of Big Data

IM 2015 OTTAWA, CANADA • MAY 11-15 2015

http://im2015.ieee-im.org/content/tutorials-2

Tutorial 2 :: Network Functions Virtualization NFV - Perspectives, Reality and Challenges

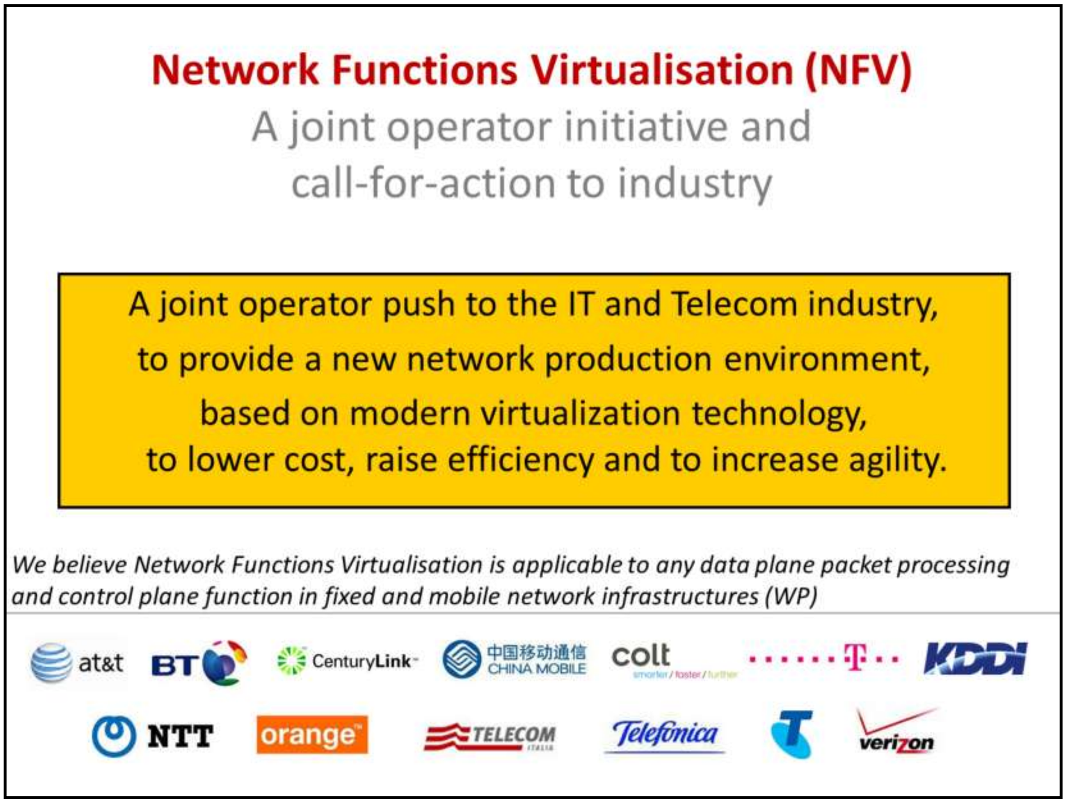
Prof. Dr. Cesar Marcondes (UFSCar, Brazil) [Presenter]

Prof. Dr. Christian Esteve Rothenberg (UNICAMP, Brazil)

May-15 2015

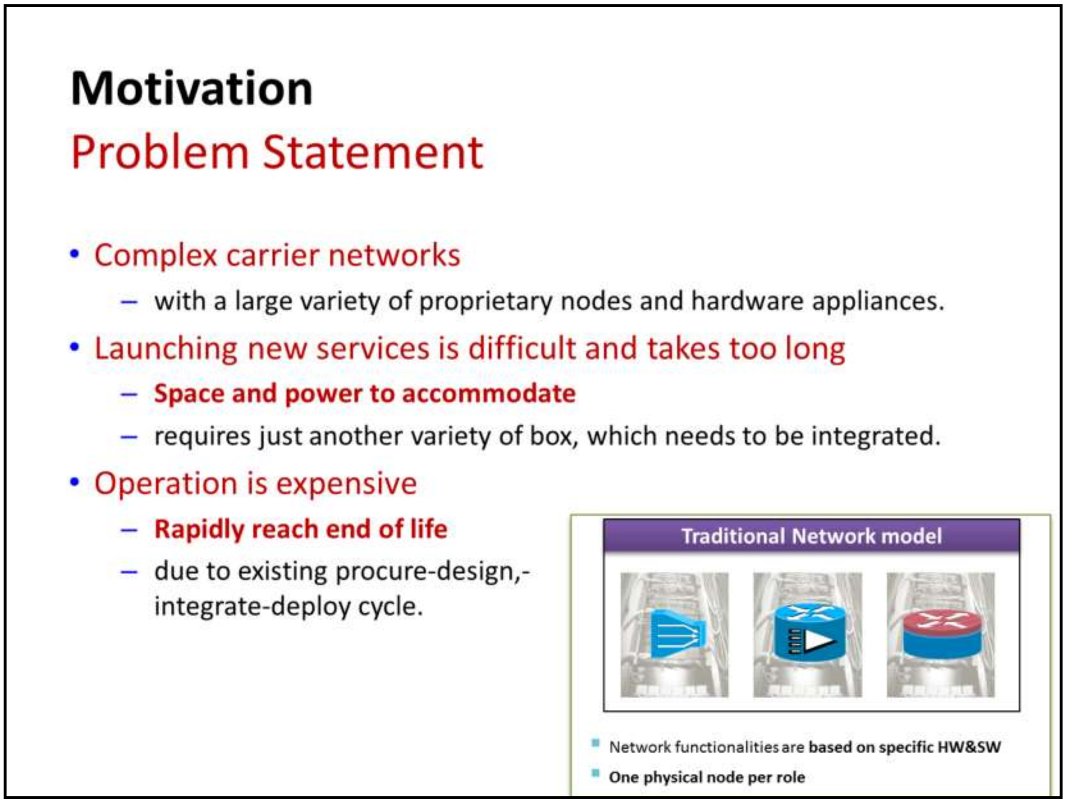
Tutorial Syllabus

- **NFV: Motivation and Problem Statement**
  - Trends in IT & Telecom Challenges
  - NFV & SDN
- **Network Functions Virtualization**
  - Vision & Approach
  - Benefits & Promises
  - ETSI NFV ISG Working Groups & Reference Architecture
- **NFV Requirements and Challenges**
  - Performance, scalability, management, orchestration, resilience, security, portability, interoperability, etc.
  - Ongoing Research efforts
- **Use Cases and Proof-of-Concepts**
  - CloudNFV, Service Chaining, VNF State Migration and Interoperability. Distributed-NFV, Multi Vendor vIMS, ForCES, Hardware Acceleration, Virtual EPC Gateway
- **Overview of Enabling Technologies**
  - Programmable vSwitches, Minimalistic OS (ClickOS), lightweight virtualization (Docker, LXC), Improving Linux I/O, x86 packet processing (Intel DPDK), vRouter (Vyatta), OpenStack, OPNFV



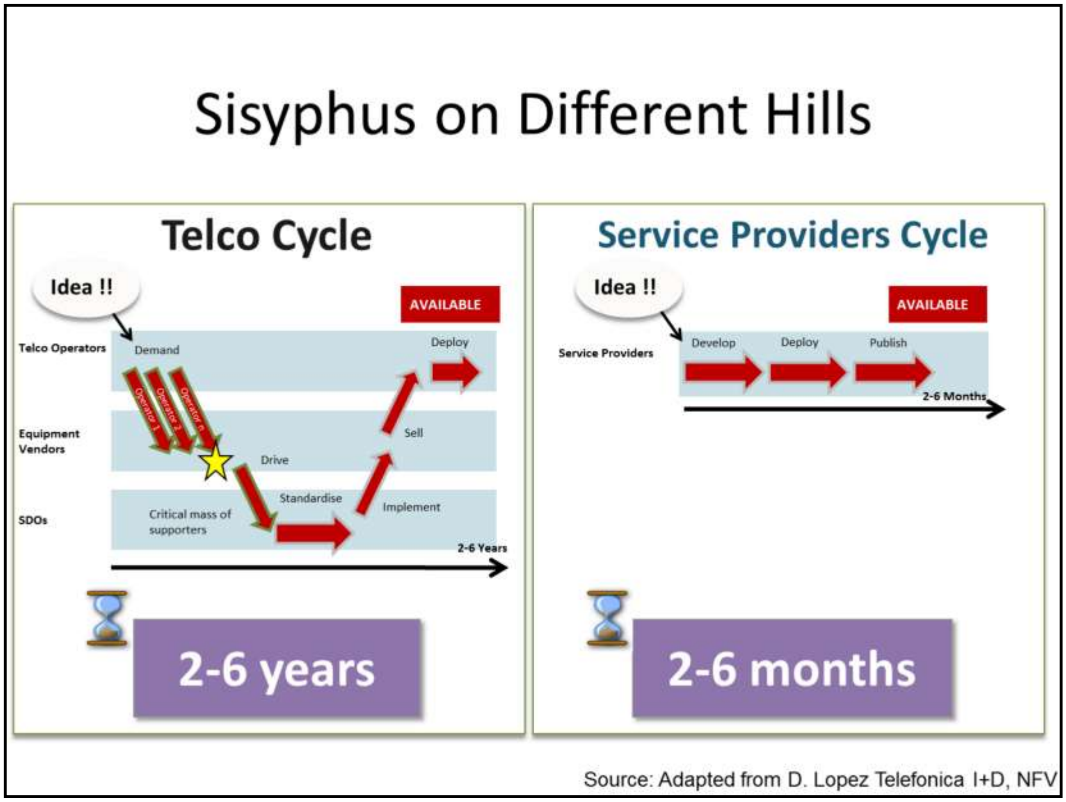
Network Functions Virtualisation aims to todays Network Operator problems by leveraging standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises. We believe Network Functions Virtualisation is applicable to any data plane packet processing and control plane function in fixed and mobile network infrastructures.

Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf



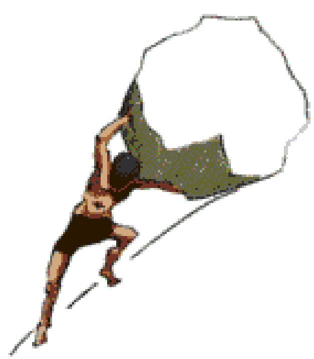
Network Operators' networks are populated with a large and increasing variety of proprietary hardware appliances. To launch a new network service often requires yet another variety and finding the space and power to accommodate these boxes is becoming increasingly difficult; compounded by the increasing 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.

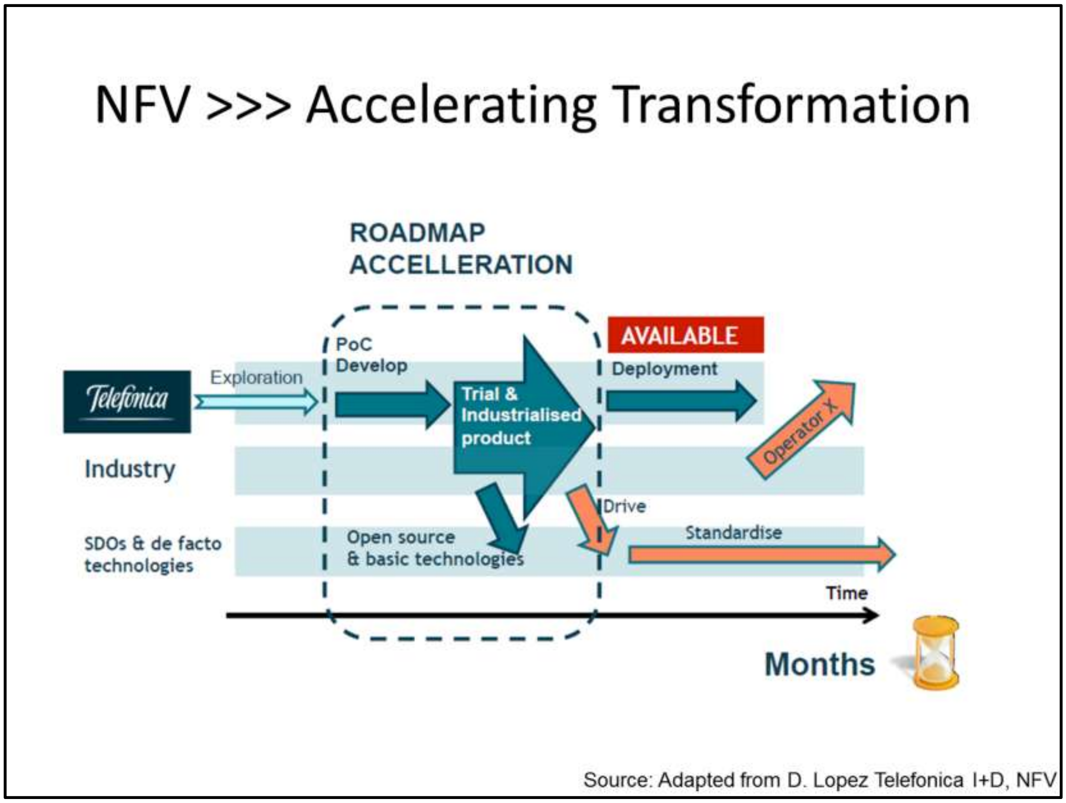
Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf



Telcos face the challenges that follow their dependency on hardware-based appliances requiring much of the procure design-integrate-deploy cycle to be repeated with little or no revenue benefit.
In contrast, the cycle of service provider is much shorter and follow a typical software development-deploy-publish cycle.

In Greek mythology **Sisyphus** (/ˈsɪsɪfəs/;[1] Greek: Σίσυφος, *Sísyphos*) was a king of Ephyra (now known as Corinth) punished for chronic deceitfulness by being compelled to roll an immense boulder up a hill, only to watch it roll back down, and to repeat this action forever.
More info: http://www.mythweb.com/encyc/entries/sisyphus.html





NFV implies a significant change for current network infrastructures

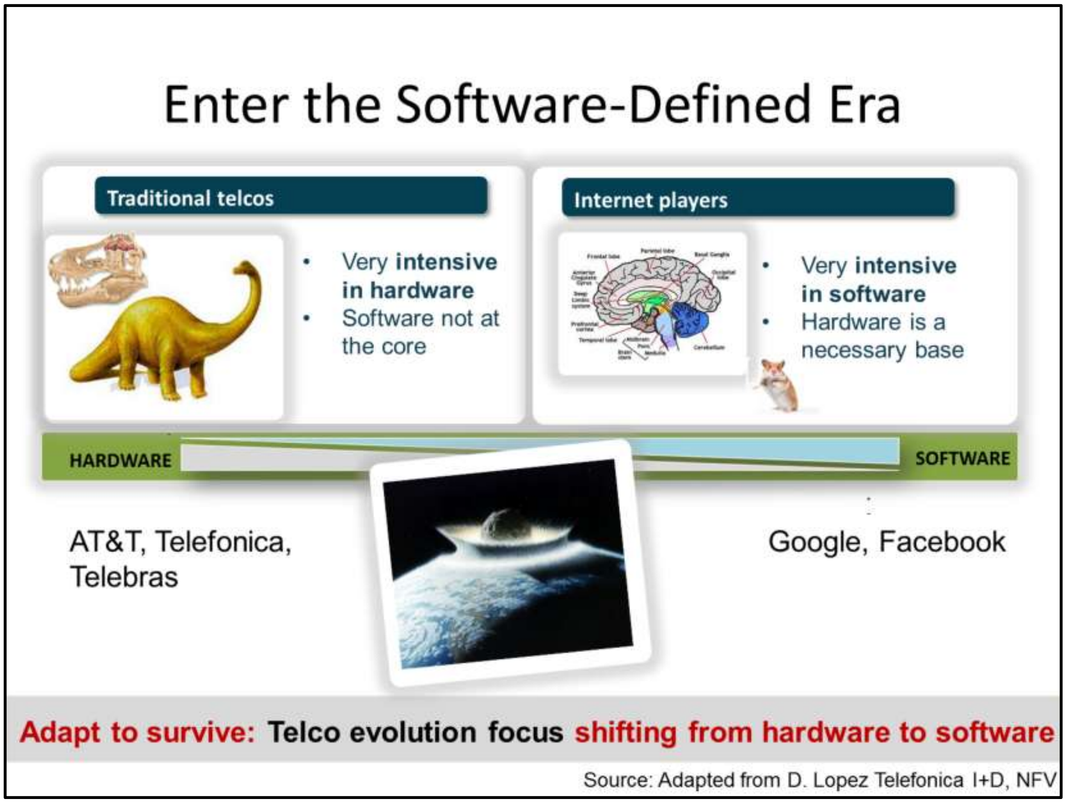
- No zero-day approach is feasible
- Avoiding disruptions

Identify relevant use cases

- Emerging services
- Reuse of equipment still in amortization
- Leverage on new planned elements in architecture

• Plan for phased deployments

- Interworking with existing infrastructure
- Not breaking current operational practice • Take advantage of NFV advantages
- Flexibility
- Extensibility
- Reusability



Telcos need to adapt from hardware/links provisioning to differentiated services
So they can survive with specialized high value software solutions

Scale and Virtualization in the Timeline

Early twentieth century

- Manual Switching
- Very intensive in human resources
- Era **dominated by hardware**

Mid-twentieth century

- Electromechanical Switching
- Less intensive in human resources
- Era **dominated by complex hardware**

Virtualization technologies enables overcoming physical constraints and generating multiplexing gains…

Second half of the twentieth century

- Digital Switching
- Much less intensive in human resources
- Era **dominated by complex and specific hardware**. **Software appears and is important**
- Services defined by telco

Early twenty-first century

- Internet connectivity opens the door to the development of OTT services (without operator)
- **Software becomes a differentiation asset**

Source: Adapted from D. Lopez Telefonica I+D, NFV

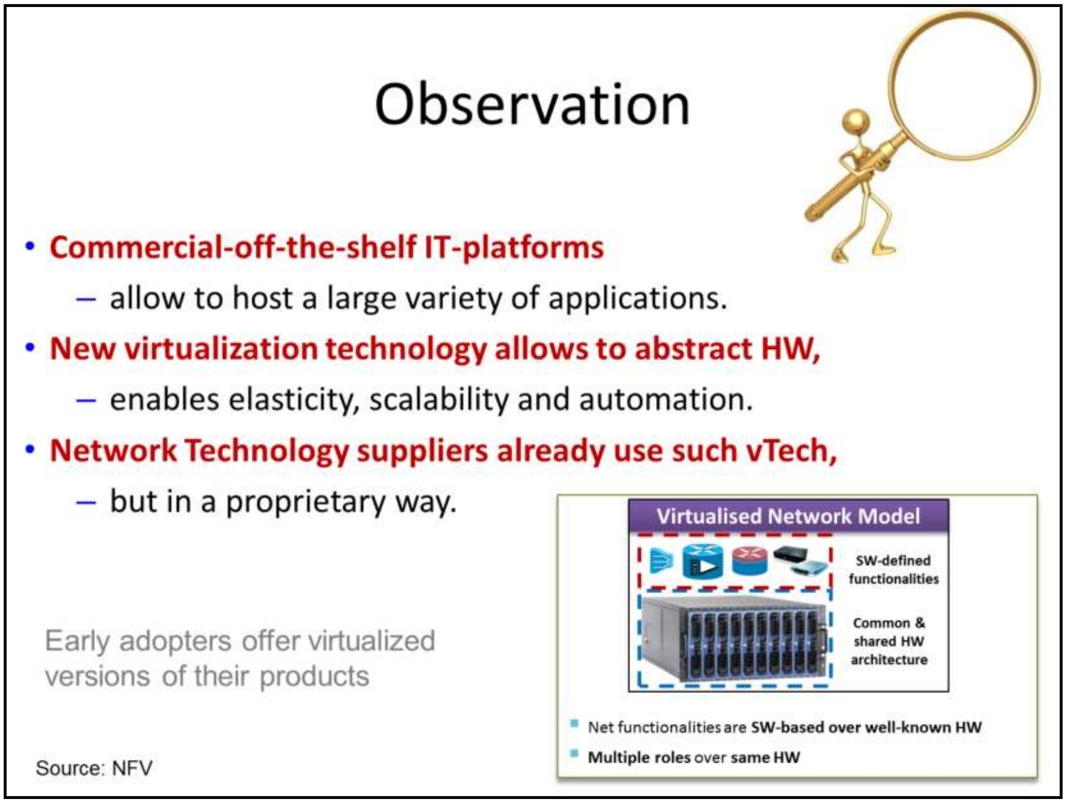
Trends

- High performance industry **standard** servers shipped in very high volume
- **Convergence** of computing, storage and networks
- New **virtualization technologies** that abstract underlying hardware yielding elasticity, scalability and automation
- **Software-defined networking**
- **Cloud** services
- **Mobility**, explosion of devices and traffic

Challenges

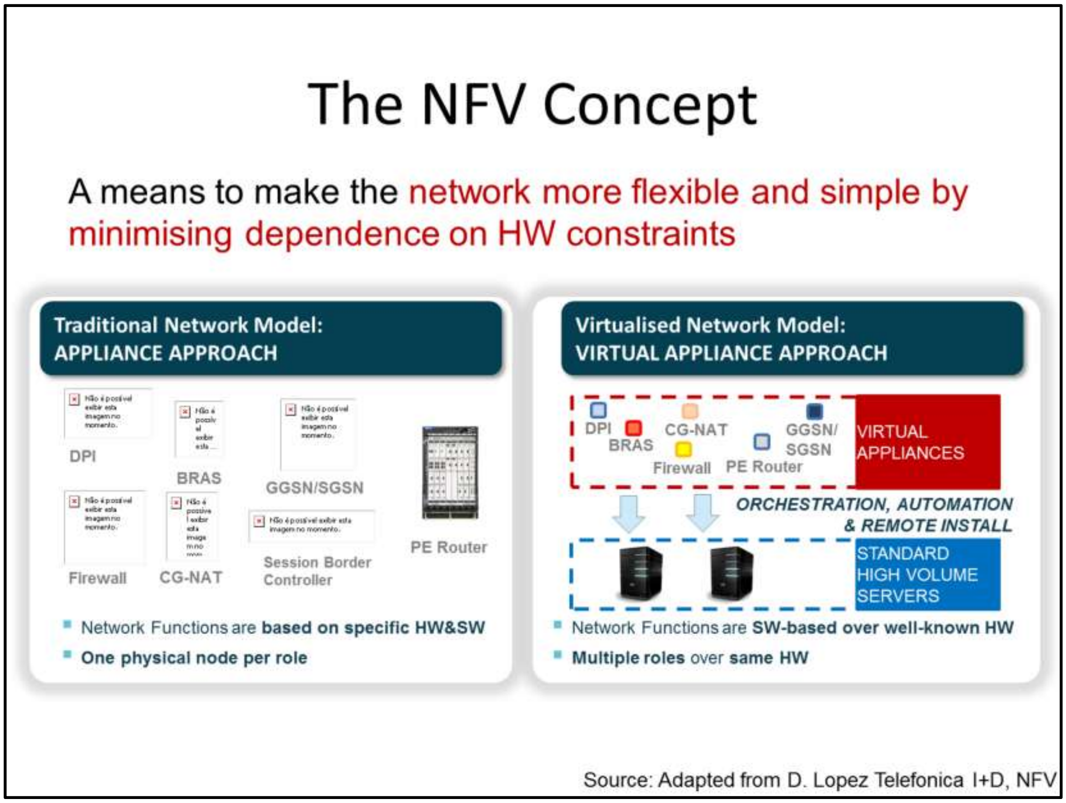
- Huge **capital investment** to deal with current trends
- Network operators face an increasing **disparity between costs and revenues**
- **Complexity**: large and increasing variety of proprietary hardware appliances in operator's network
- Reduced **hardware lifecycles**
- **Lack of flexibility and agility**: cannot move network resources where & when needed
- **Launching new services is difficult and takes too long**. Often requires yet another proprietary box which needs to be integrated

Source: Adapted from D. Lopez Telefonica I+D, NFV

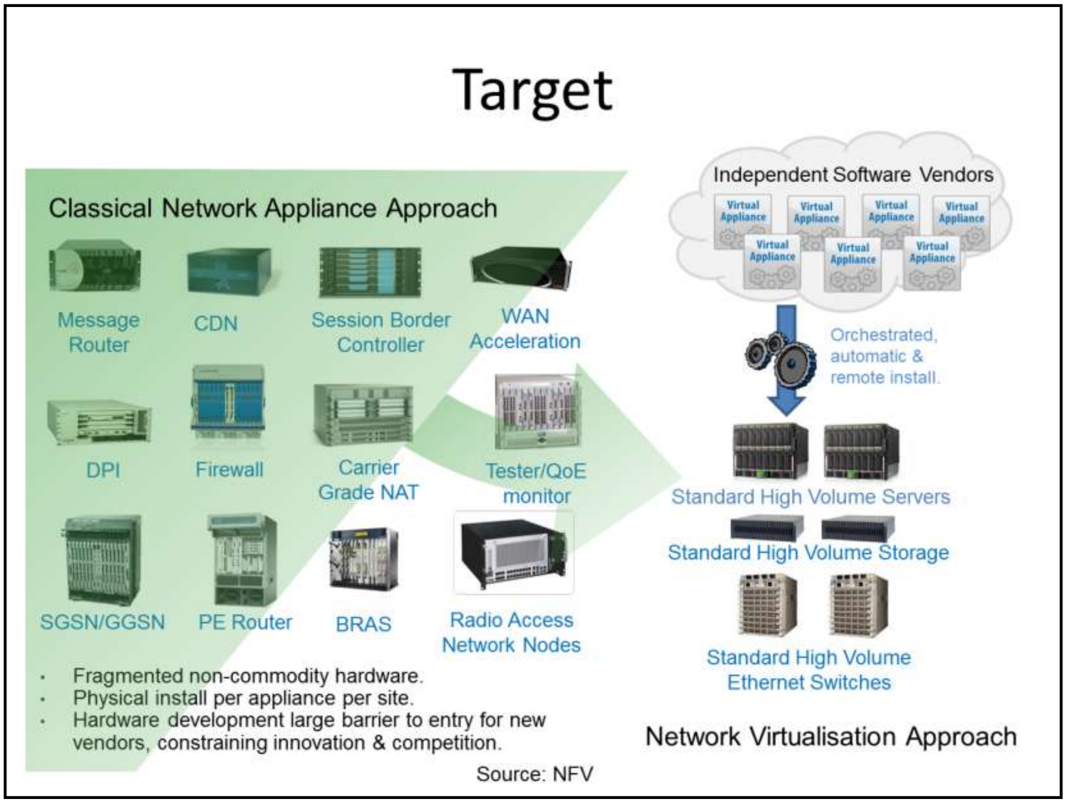


Network equipment vendors already implement some of their solutions by combining their proprietary software with industry standard hardware and software components, but in a proprietary way. Enabling their proprietary software to run on industry standard hardware in a standardised way may be a significant 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 virtualised versions of their products.

Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf



Network functions are fully defined by SW, minimising dependence on HW constraints
The target is a simplified, less expensive service provider network



Definition
Network Functions Virtualisation aims to transform the way that network operators architect networks by evolving standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises. 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.

Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

NFV :: Network Functions Virtualization

- Network Functions Virtualization is about implementing network functions in software - that today run on proprietary hardware - leveraging (high volume) standard servers and IT virtualization
- Supports multi-versioning and multi-tenancy of network functions, which allows use of a single physical platform for different applications, users and tenants
- Enables new ways to implement resilience, service assurance, test and diagnostics and security surveillance
- Provides opportunities for pure software players
- Facilitates innovation towards new network functions and services that are only practical in a pure software network environment
- Applicable to any data plane packet processing and control plane functions, in fixed or mobile networks
- NFV will only scale if management and configuration of functions can be automated
- NFV aims to ultimately transform the way network operators architect and operate their networks, but change can be incremental

Source: Adapted from D. Lopez Telefonica I+D, NFV

Benefits & Promises of NFV (1/2)

- Reduced equipment costs (CAPEX)
  - through consolidating equipment and economies of scale of IT industry.
- Increased speed of time to market
  - by minimising the typical network operator cycle of innovation.
- Availability of network appliance multi-version and multi-tenancy,
  - allows a single platform for different applications, users and tenants.
- Enables a variety of eco-systems and encourages openness.
- Encouraging innovation to bring new services and generate new revenue streams.

Source: NFV

Virtualising Network Functions could potentially offer many benefits including, but not limited to:

• Reduced equipment costs and reduced power consumption through consolidating equipment and exploiting the economies of scale of the IT industry.

• Increased speed of Time to Market by minimising 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 Virtualisation should enable network operators to significantly reduce the maturation cycle.

• Availability of network appliance multi-version and multi-tenancy, which allows use of a single platform for different applications, users and tenants. This allows network operators to share resources across services and across different customer bases.

• Targeted service introduction based on geography or customer sets is possible. Services can be rapidly scaled up/down as required.

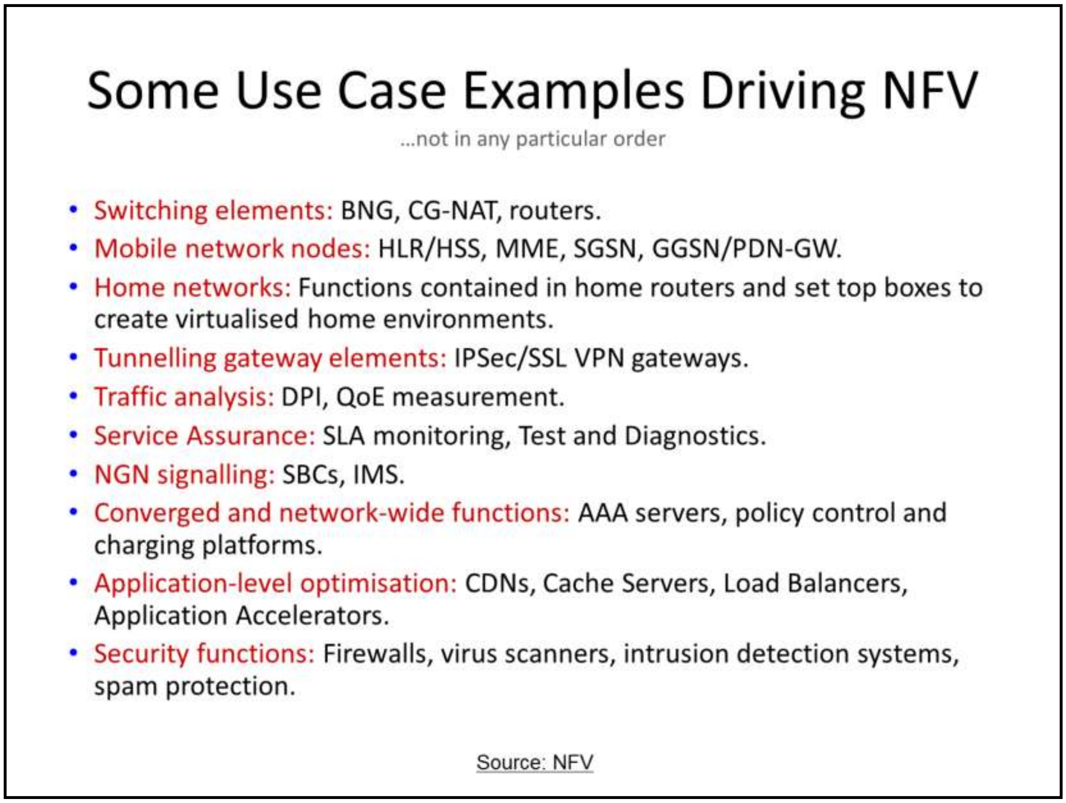
• Enables a wide variety of eco-systems and encourages openness. It opens the virtual appliance market to pure software entrants, small players and academia, encouraging more innovation to bring new services and new revenue streams quickly at much lower risk.

Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

Benefits & Promises of NFV (2/2)

- Flexibility to easily, rapidly, dynamically provision and instantiate new services in various locations
- Improved operational efficiency
  - by taking advantage of the higher uniformity of the physical network platform and its homogeneity to other support platforms.
- Software-oriented innovation to rapidly prototype and test new services and generate new revenue streams
- More service differentiation & customization
- Reduced (OPEX) operational costs: reduced power, reduced space, improved network monitoring
- IT-oriented skillset and talent

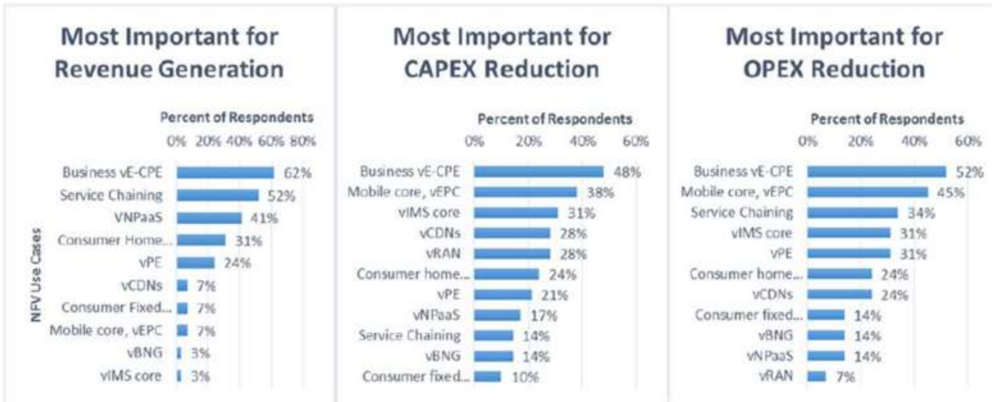
Source: Adapted from D. Lopez Telefonica I+D, NFV



Network Functions Virtualisation is applicable to any data plane packet processing and control plane function in mobile and fixed networks. Potential examples have been identified (not in any particular order).
Some noteworthy examples apply to Telecom Networks (relevant to core Ericsson business) in the field of NGN signaling and converged network-wide functions:
The virtualisation of a mobile core network targeting at a more cost efficient production environment, which allows network operators to cope with the increasing traffic demand in mobile networks, and leading to better resource utilization (including energy savings), more flexible network management (no need to change hardware for nodes' upgrades), hardware consolidation, easier multi-tenancy support and faster configuration of new services. Network Functions Virtualisation in mobile networks can also be used to create core network instances optimized for specific services, e.g. for Machine-to-Machine communications (M2M).

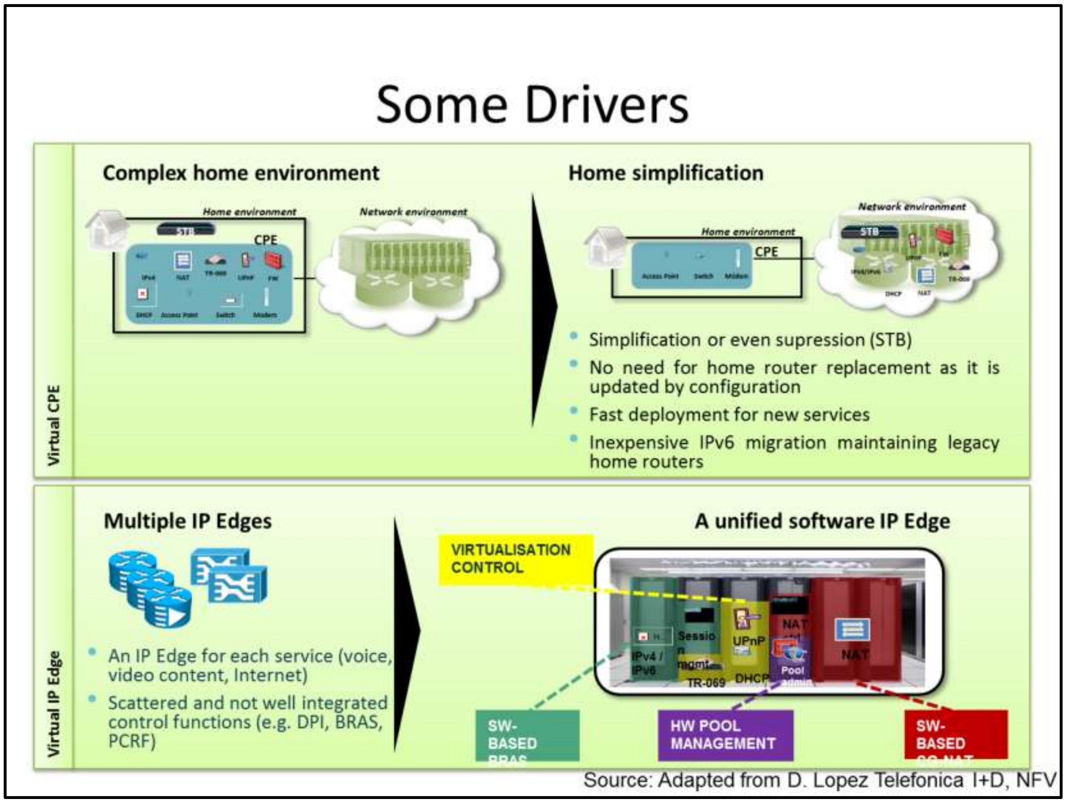
Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

Carrier Priorities



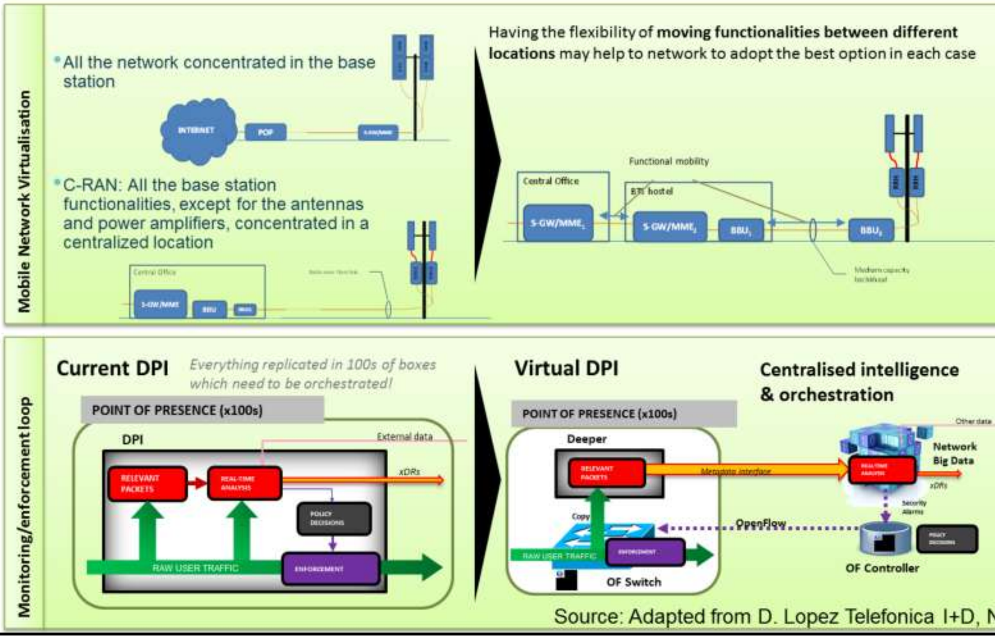
Src: NFV – Dell point of view (Dell)

Src: NFV – Dell point of view (Dell)



Virtualisation brings specific benefits on efficient resources usage, resiliency and redundance, as well as faster management of operations (e.g., SW upgrades) and enhanced time to market (e.g., to deploy a new functionality less hardware dependent). However, the specific nature of the Telco environment (i.e. Carrier grade requirements) imply technical challenges that NFV aims to address in order to facilitate interoperability and seamless evolution towards fully virtualized networks. In this sense, many drivers come to the NFV world.

...More Drivers...



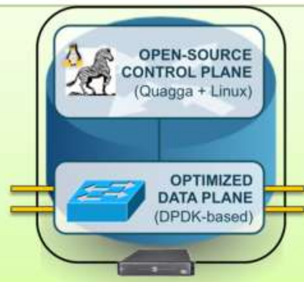
Source: Adapted from D. Lopez Telefonica I+D, NFV

… And a Couple More

Virtualized CGNAT

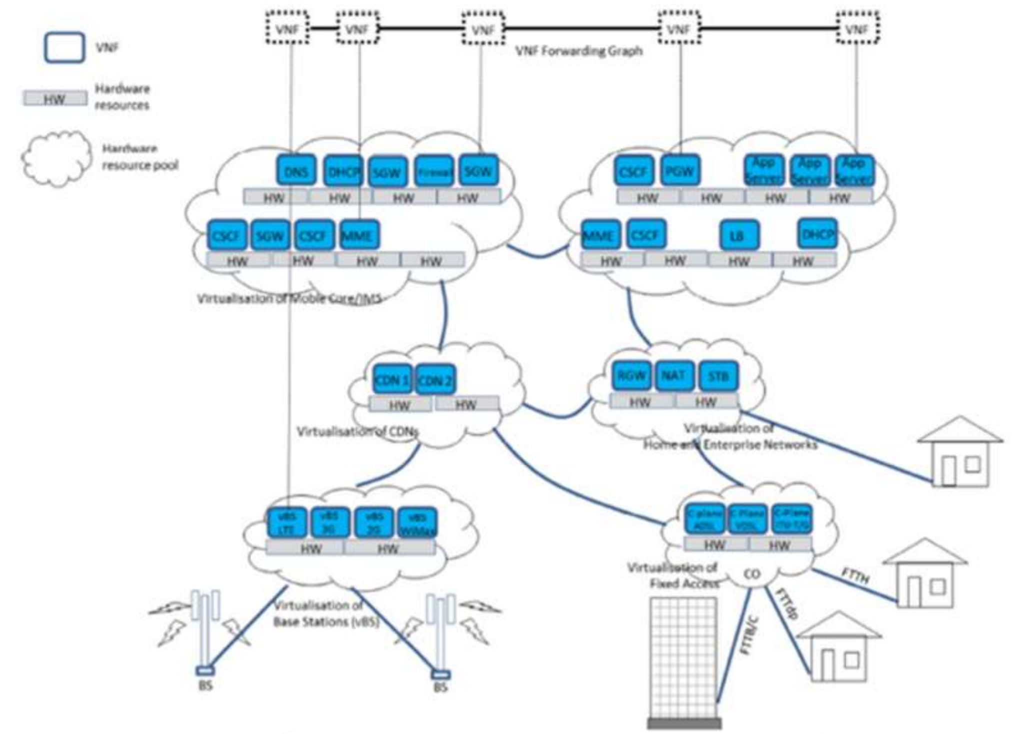
- NAT44 function, extensible to IPv6 transition
- 40 Gbps full-duplex line rate per server
- Support of overlapping addresses and tunnelling
- Auto-provisioning of NAT sessions per access line

Optimized Quagga data plane

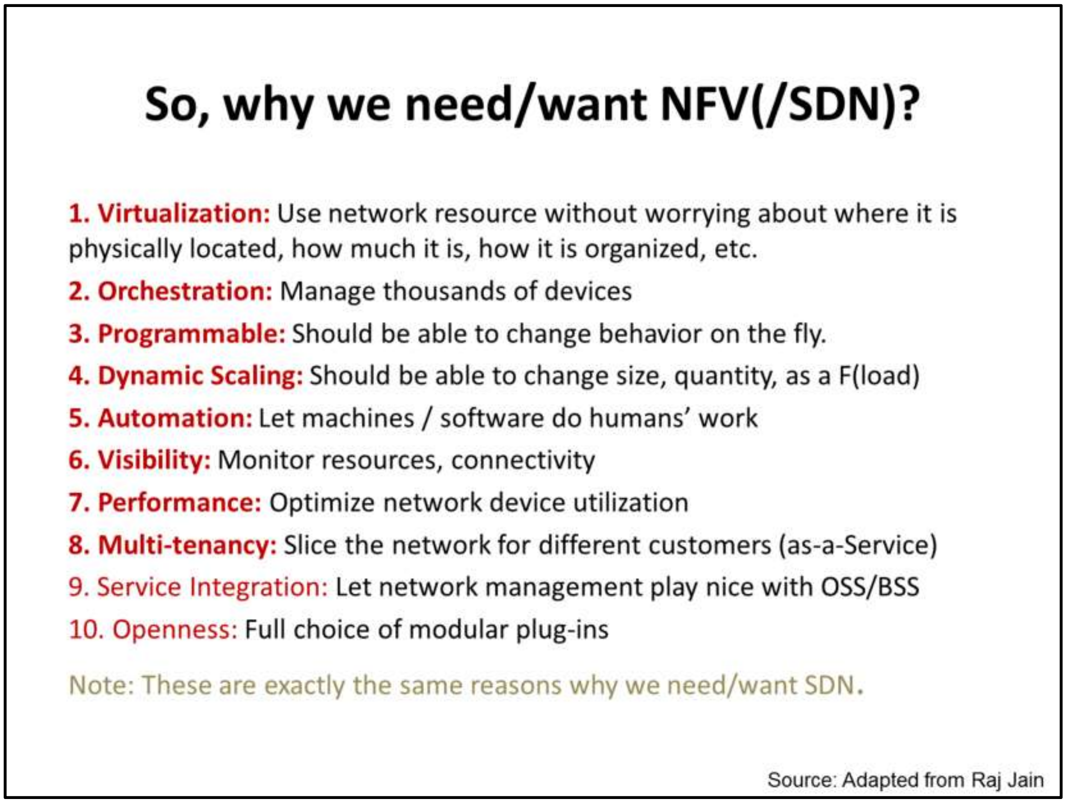


- Leverage on open source routing project as rich and widely tested protocol suite while assuring data plane performance
  - Common routing protocols supported and extended by open source project
  - High-performance line-rate data plane
  - Running in separate process, does not lead to licensing issues

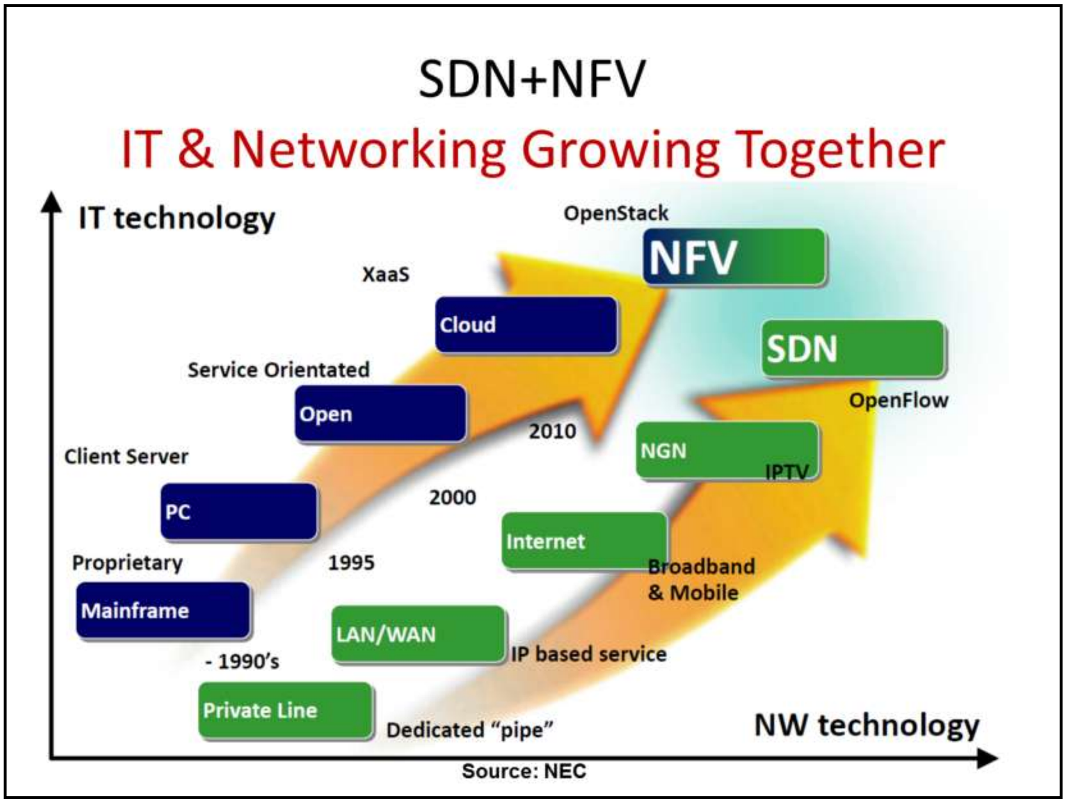
Source: Adapted from D. Lopez Telefonica I+D, NFV



Overview of NFV Use Cases. Source: ETSI NFV ISG Updated White Paper

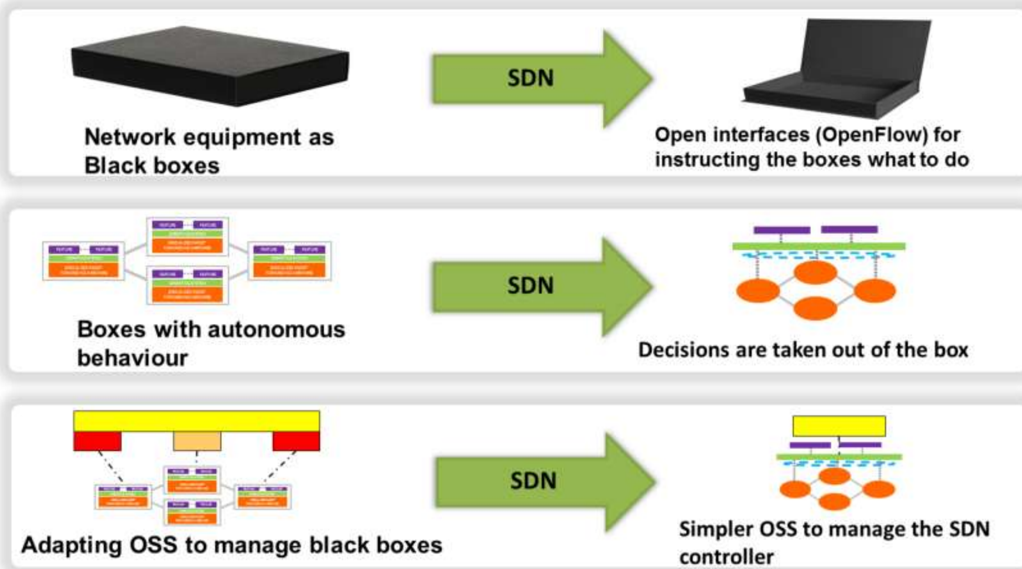


Note that the shared motivation and goals between SDN and NFV
Source: http://www.cse.wustl.edu/~jain/cse570-13/ftp/m_17nfv.pdf



Source: Kaz Hashimoto (NEC), The Way towards the Service Driven Network. , SDN World Congress Frankfurt, 15-18 October 2013

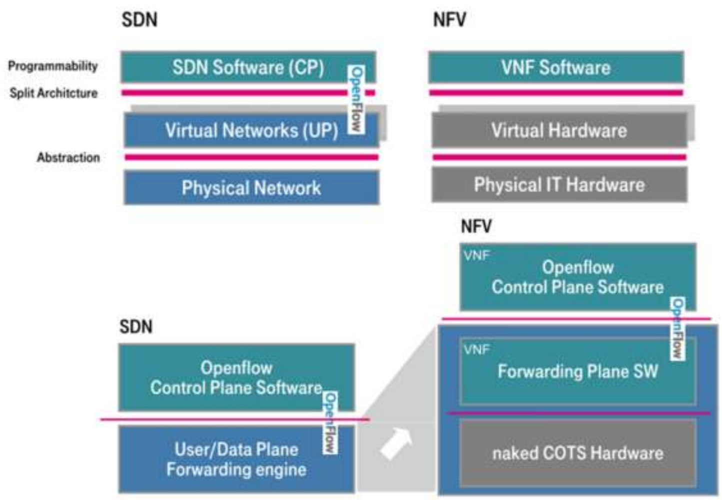
Software Defined Networking



Source: Adapted from D. Lopez Telefonica I+D, NFV

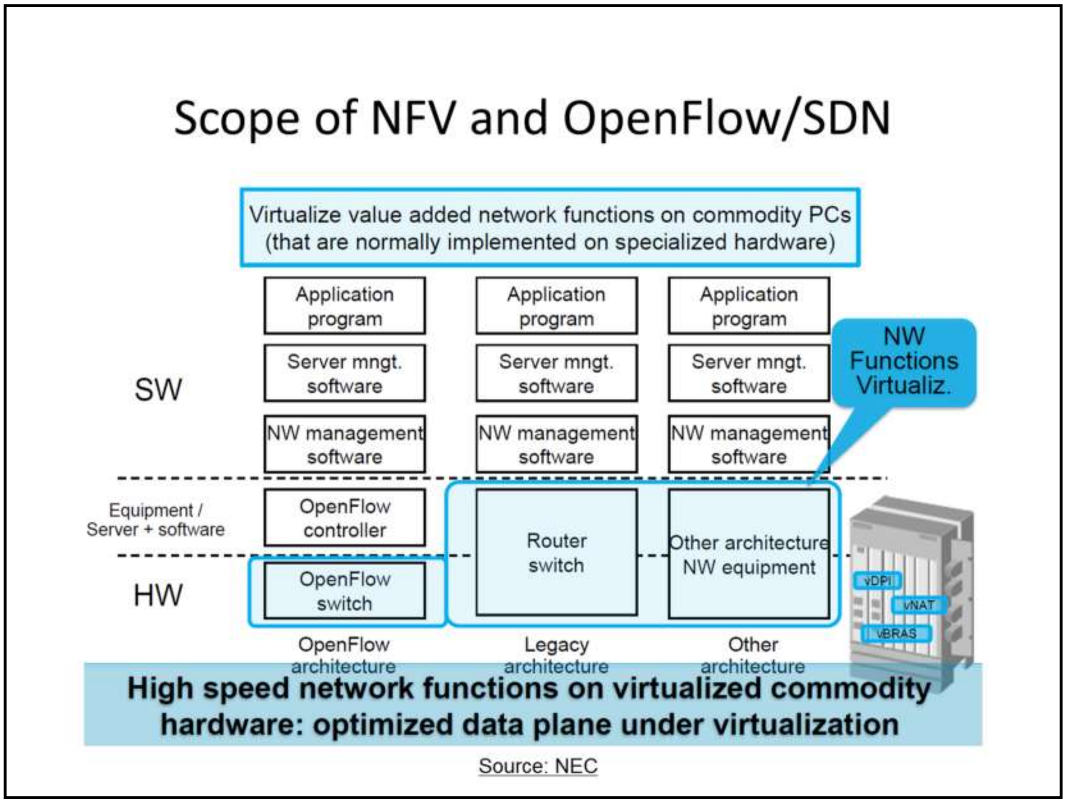
SDN and NFV

- SDN and NFV do NOT depend on each other

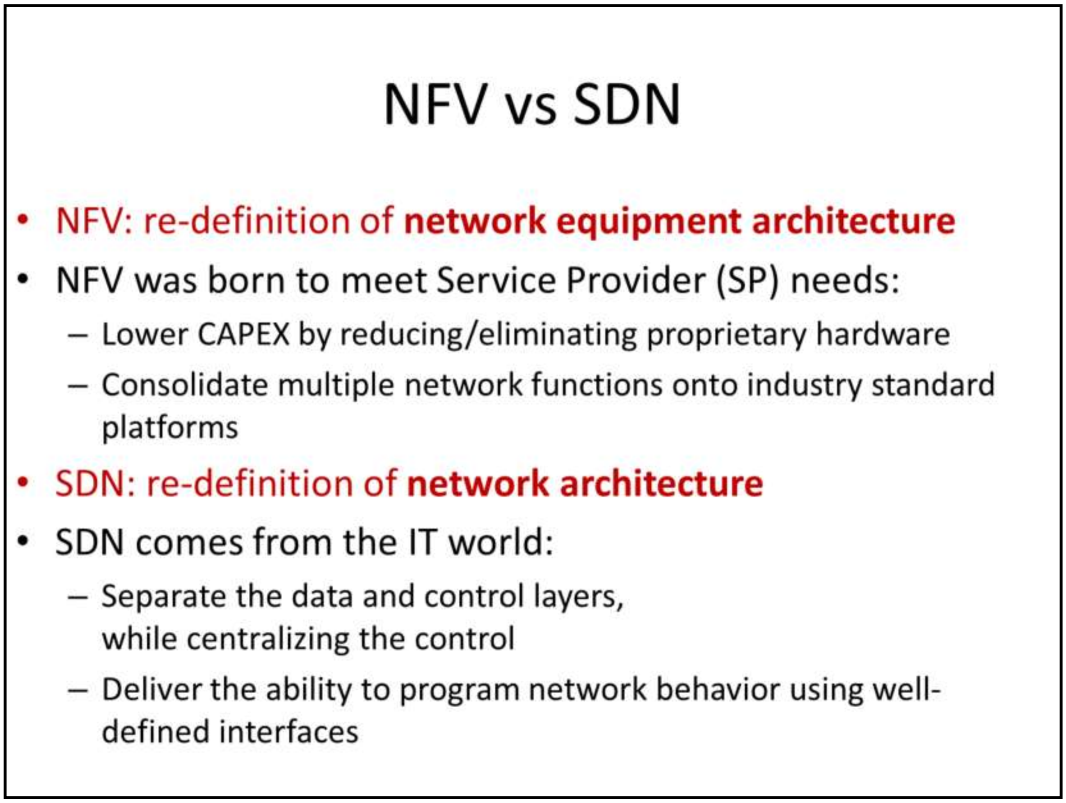


Source: Uwe Michel, T-Systems

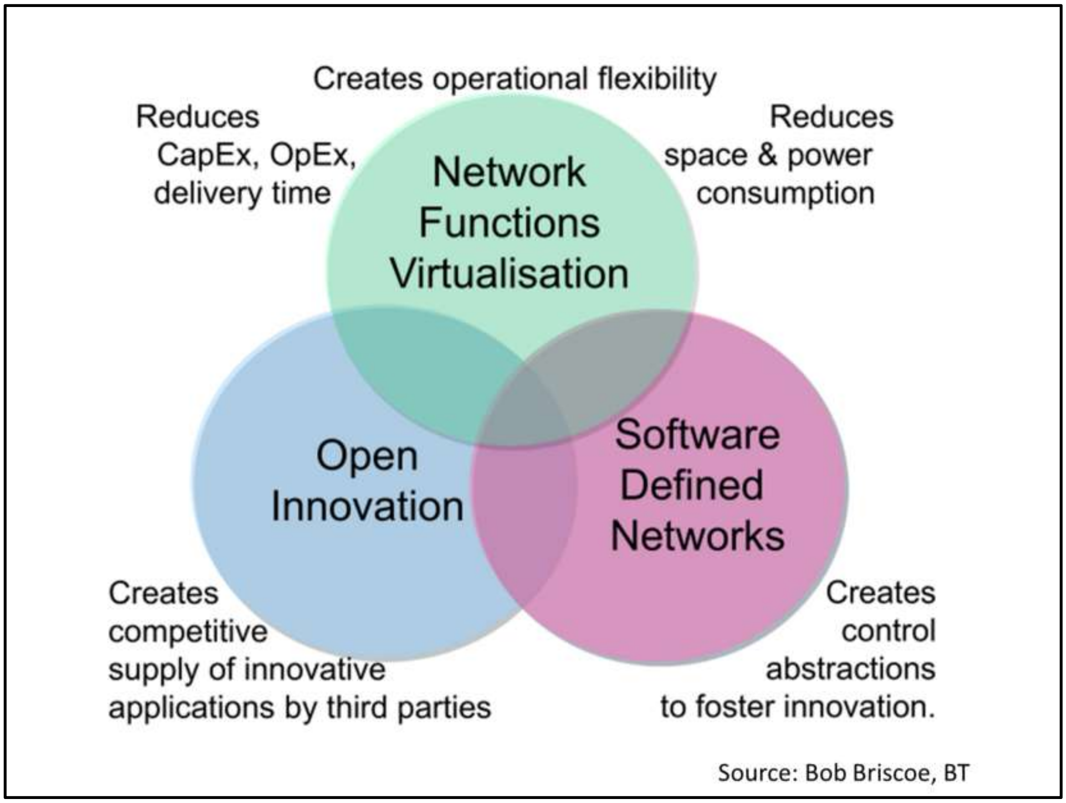
Figures source: Uwe Michel, T-Systems Multimedia (Presentation SDN and NFV How things fit together)



The scope of NFV are those data plane functions currently implemented in HW to become virtualized functions running on commodity server hardware



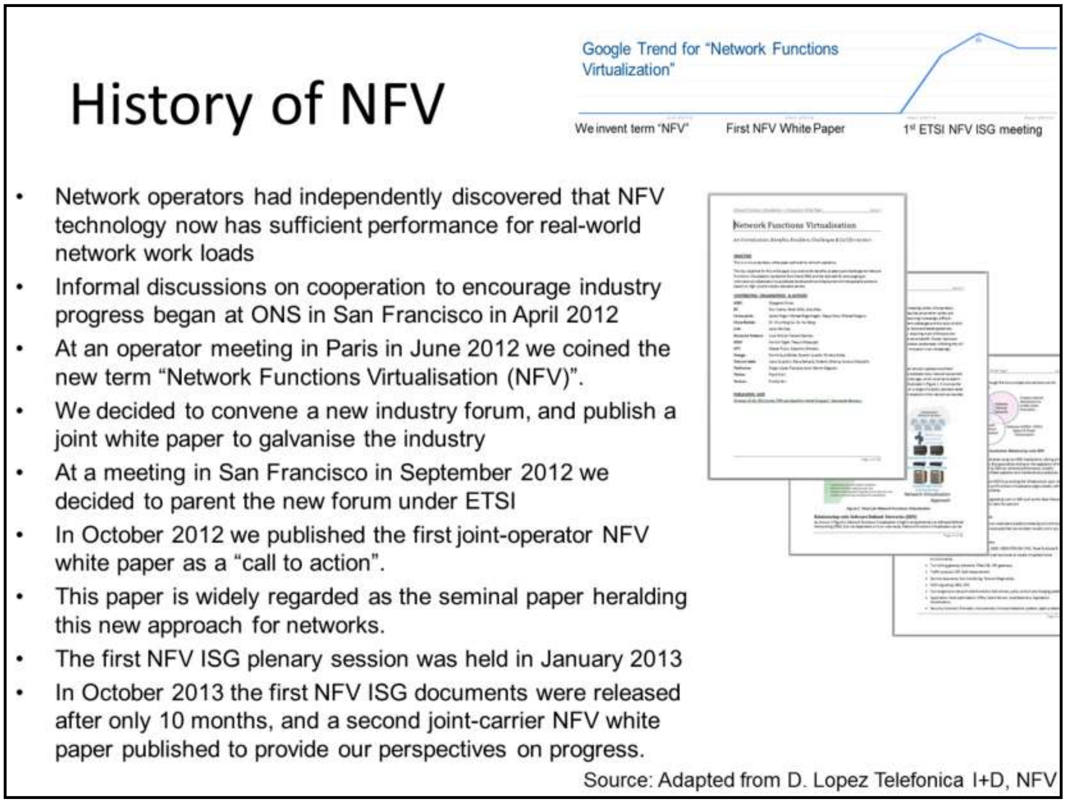
NFV and SDN are closely related, but really meet different goals:
Both together take the notion of Network Virutalization to new levels of NV 2.0



NFV and SDN are highly complementary
Both topics are mutually beneficial but not dependent on each other

Network Functions Virtualisation is highly complementary to Software Defined Networking (SDN), but not dependent on it (or vice-versa). Network Functions Virtualisation can be implemented without a SDN being required, although the two concepts and solutions can be combined and potentially greater value accrued. Network Functions Virtualisation goals can be achieved using non-SDN mechanisms, relying on the techniques currently in use in many datacentres. 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 Virtualisation is able to support SDN by providing the infrastructure upon which the SDN software can be run. Furthermore, Network Functions Virtualisation aligns closely with the SDN objectives to use commodity servers and switches.
Figure source: Bob Briscoe, BT (Presentation Network Functions Virtualisation)
Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

ETSI NFV



NFV originated from many of the world's largest carriers' discussions about how to improve network operations as text and email are supplanted by streaming multimedia content. A set of informal discussions and meetings culminated in the drafting of the NFV White Paper at the 2012 SDN and OpenFlow World Congress in Darmstadt, Germany last October, where the group proclaimed their intentions: *leveraging standard IT virtualization technology to consolidate many network equipment types onto industry standard, high-volume servers, switches and storage.*

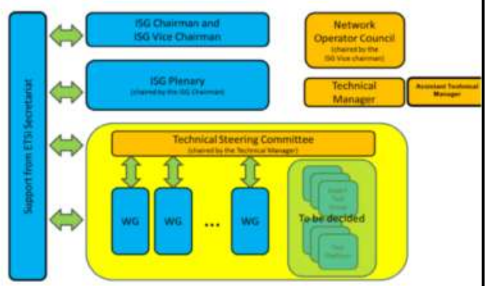
By the end of 2012, the NFV ISG was formed in ETSI, primarily to exploit ETSI's existing administration, processes, and governance model. The initial meeting of the NFV ISG was held in Sophia Antipolis in the south of France in January, with 20+ carriers and 100+ participants. There was an aura permeating that initial meeting hosted by ETSI that the ISG was onto something big, albeit with a daunting task ahead.

Not surprisingly, when the world's largest carriers band together on their own to do anything, the vendor community will respond. And they have. More than 100 ISG participants whose products span the entire NFV value chain are now participating, along with the 25+ network operators.

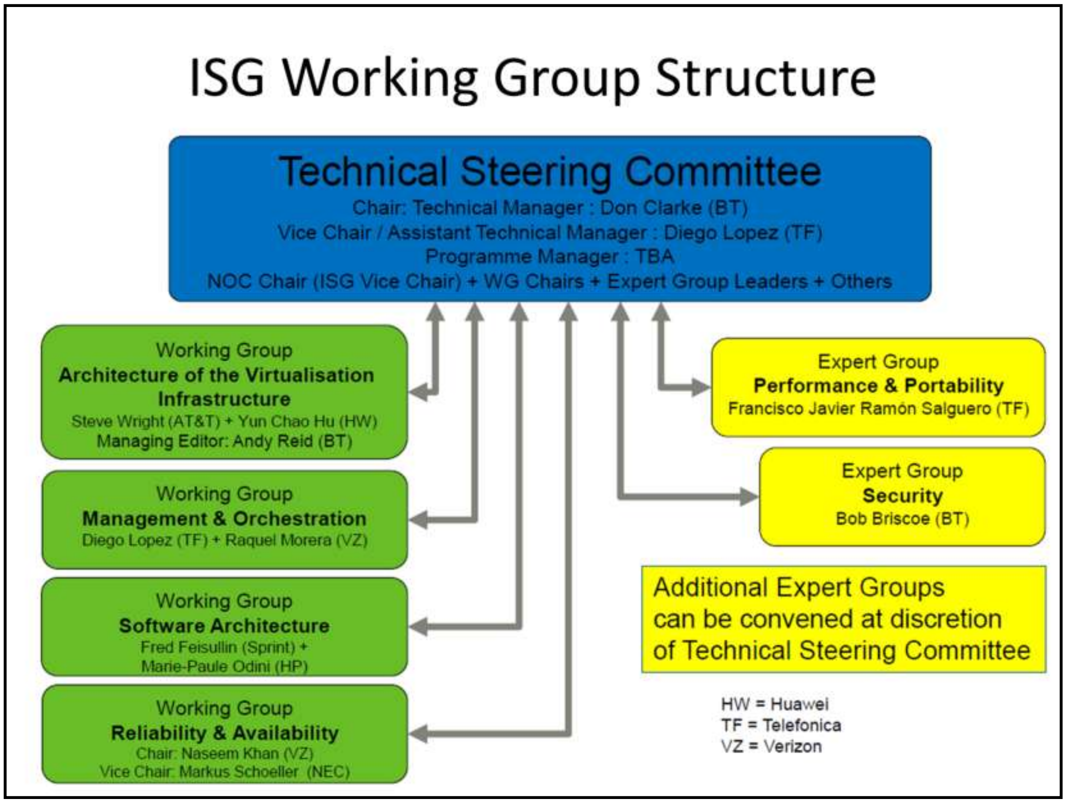
The ETSI NFV ISG

- Global operators-led Industry Specification Group (ISG) under the auspices of ETSI
  - ~150 member organisations
- Open membership
  - ETSI members sign the "Member Agreement"
  - Non-ETSI members sign the "Participant Agreement"
  - Opening up to academia
- Operates by consensus
  - Formal voting only when required
- Deliverables: White papers addressing challenges and operator requirements, as input to SDOs
  - Not a standardisation body by itself

- Currently, four WGs and two EGs
  - Infrastructure
  - Software Architecture
  - Management & Orchestration
  - Reliability & Availability
  - Performance & Portability
  - Security



Source: Adapted from D. Lopez Telefonica I+D, NFV



Source: http://www.sdncentral.com/education/nfv-insiders-perspective-part-1-goals-history-promise/2013/09/

ISG Leadership: ISG Chair: Prodip Sen, Verizon; Uwe Michel, Deutsche Telekom.
Network Operators' Council (NOC): Guides and oversees all ISG activities; the NOC is limited to Network Operators exclusively. Chair: Don Clarke, British Telecommunications.
Technical Steering Committee (TSC): provides technical leadership; the TSC consists of the Working and Expert Group leaders (i.e., Co-Chairs and Editors). Chair: Diego Lopez, Telefónica; Vice chair: Tetsuya Nakamura, NTT Docomo.
Working Groups: Working-level teams for particular NFV functional areas:

Architectural Working Groups

- Related to functional requirements
- Have a clear location in the NFV architecture
  - Keep consistency with both requirements and architecture

- INF: Supporting infrastructure interfaces and elements
- MANO: External interfaces and behaviour of a VNF
- SWA: Internals of a VNF

- Refining the architecture
- Addressing use cases
- Mostly oriented to produce reference documents

Source: Adapted from D. Lopez Telefonica I+D, NFV

Architecture for the Virtualization Infrastructure (INF): Addresses the infrastructure requirements for the compute, storage, and network domains.
Management and Orchestration (MANO): Addresses management considerations for the NFV platform.
Software Architecture (SWA): Addresses the environment that the VNFs will execute.
Reliability and Availability (REL): Addresses VNF resiliency and fault tolerance.
Expert Groups (EGs) responsible for technical recommendations that span multiple WGs:

Security: Responsible for security considerations throughout the NFV platform.

Performance and Portability (PER): Addresses scalability, efficiency, and performance considerations when moving from dedicated to generic hardware.

Transversal Working and Expert Groups

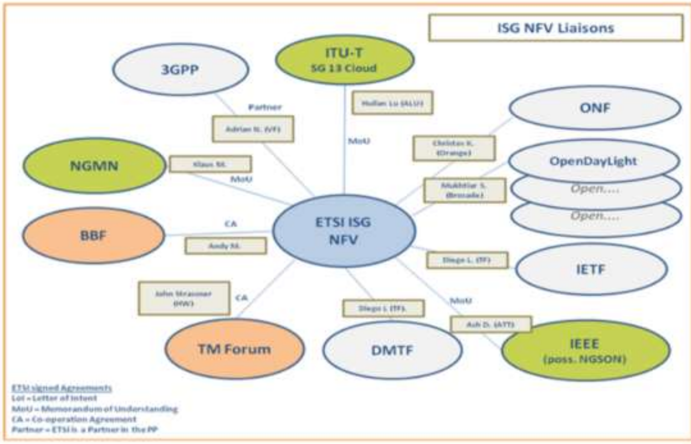
- Related to non-functional requirements
- Transversal to the architecture
  - And influencing the architectural groups

- PER: Predictability in the data plane and function portability
- REL: Specify resiliency requirements, mechanisms , and architectures
- SEC: Function by function and infrastructure

- Refining the requirements
- Assessing use cases
- Mostly concerned with recommendations and arch models

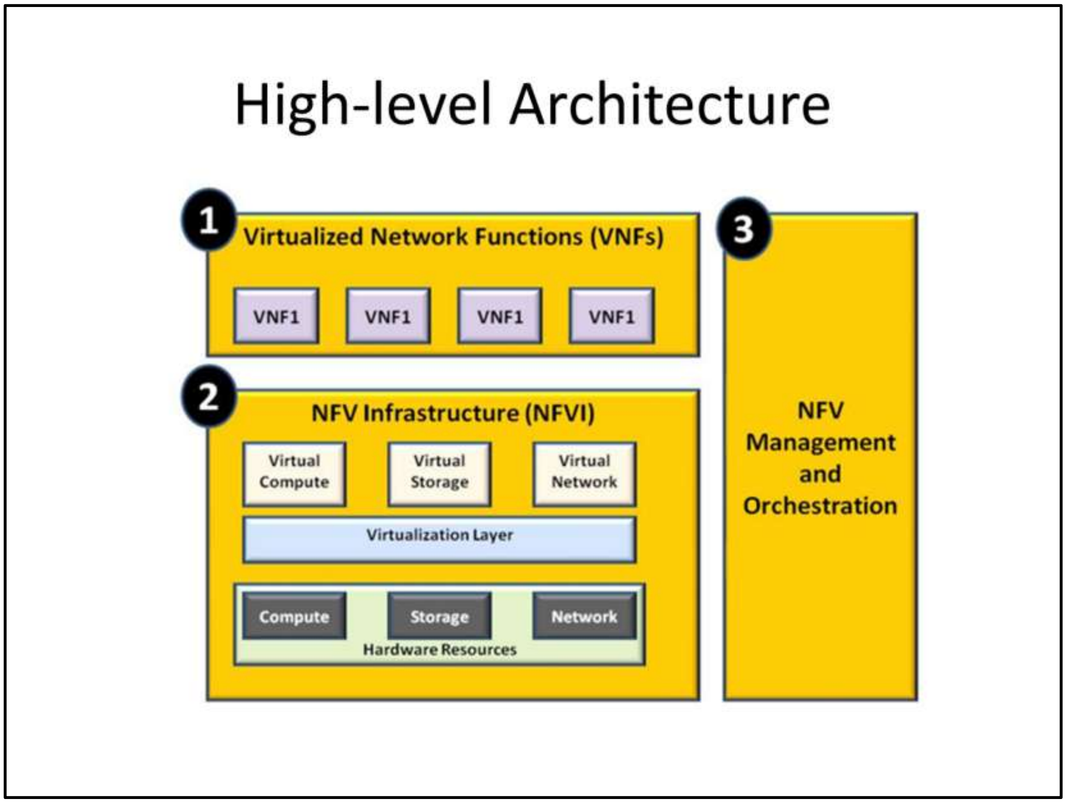
Source: Adapted from D. Lopez Telefonica I+D, NFV

ETSI NFV External Consolidation



- Most relevant SDOs
- Open Source projects
- Identifying concrete areas of cooperation
- Fruitful results already achieved

- Public documents
- Early access to stable drafts
- Participation in joint events
- Coordinated individual contributions



Source:
http://lteuniversity.com/get_trained/expert_opinion1/b/bbest/archive/2013/12/18/lte-before-and-after-part-5.aspx

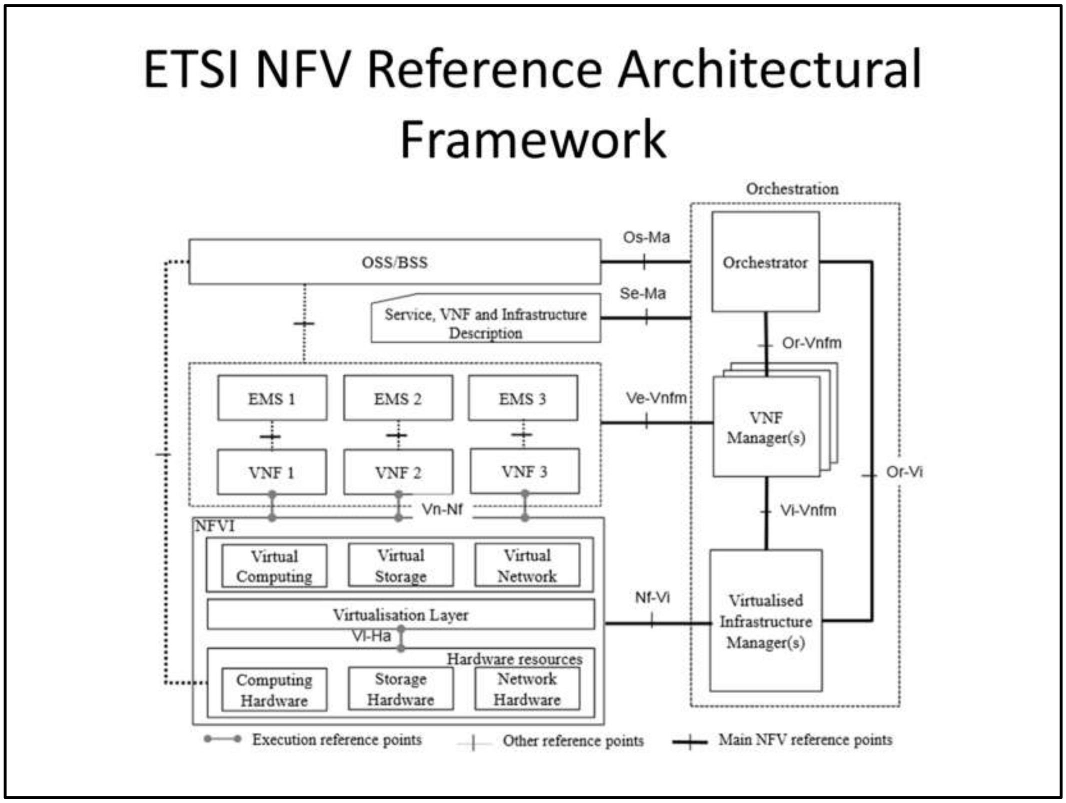
The group initially promoting NFV has found a standards home with ETSI as a group tasked not with defining NFV standards, but establishing consensus on what the standards should be, and working with ESTI to formalize the standards. In October 2013, the NFV Industry Specification Group (NFV ISG,) under the umbrella of ETSI, published a set of five “high level reference documents”. The most important of these documents is entitled, “NFV Architectural Framework”. The figure below graphically describes that framework in three parts.

(1.) The collection of Virtualized Network Functions sharing the same physical OTS server,

(2.) The NFV Infrastructure (NFVI) depicting the mapping (virtualizing) of physical servers and network facilities onto equivalent virtual functions, and

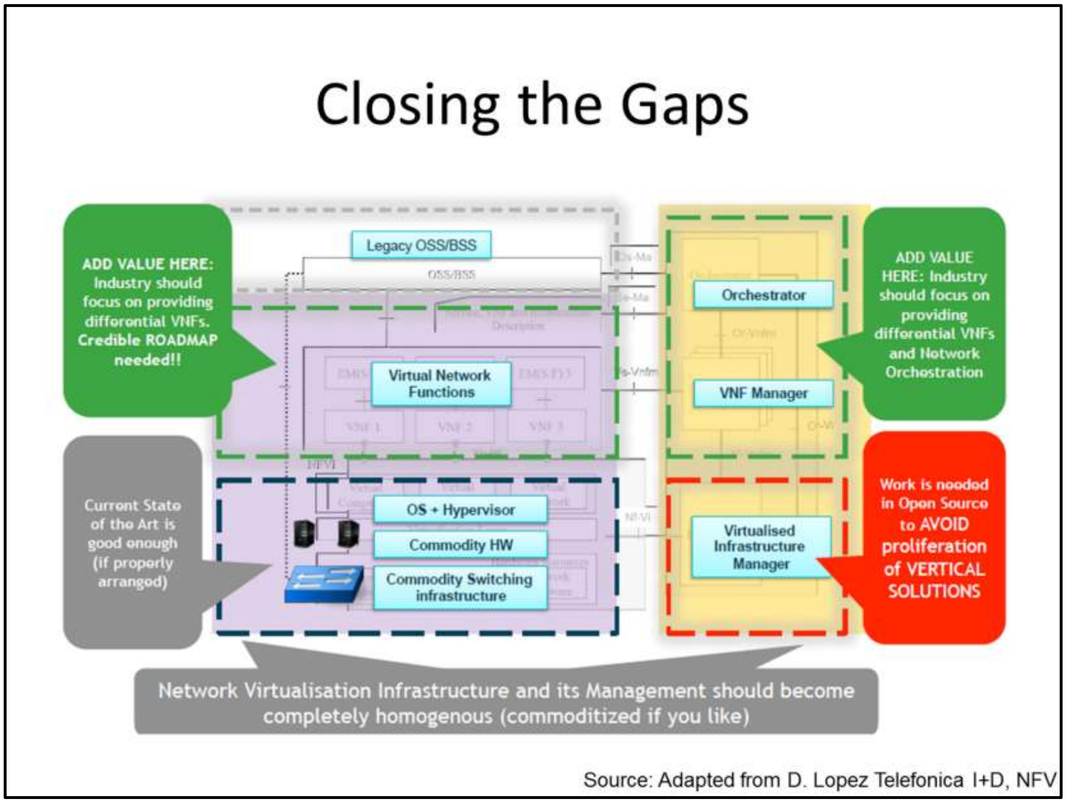
(3.) the NFV management plane. With various independent VFNs all competing for resources, the management plane is responsible for allocation of the physical resources in a “fair” manner to support various (possible competing) Service Level Agreements (SLAs).

The NFV management and orchestration function is also responsible for supporting redundancy, elasticity functionality, and fault management.

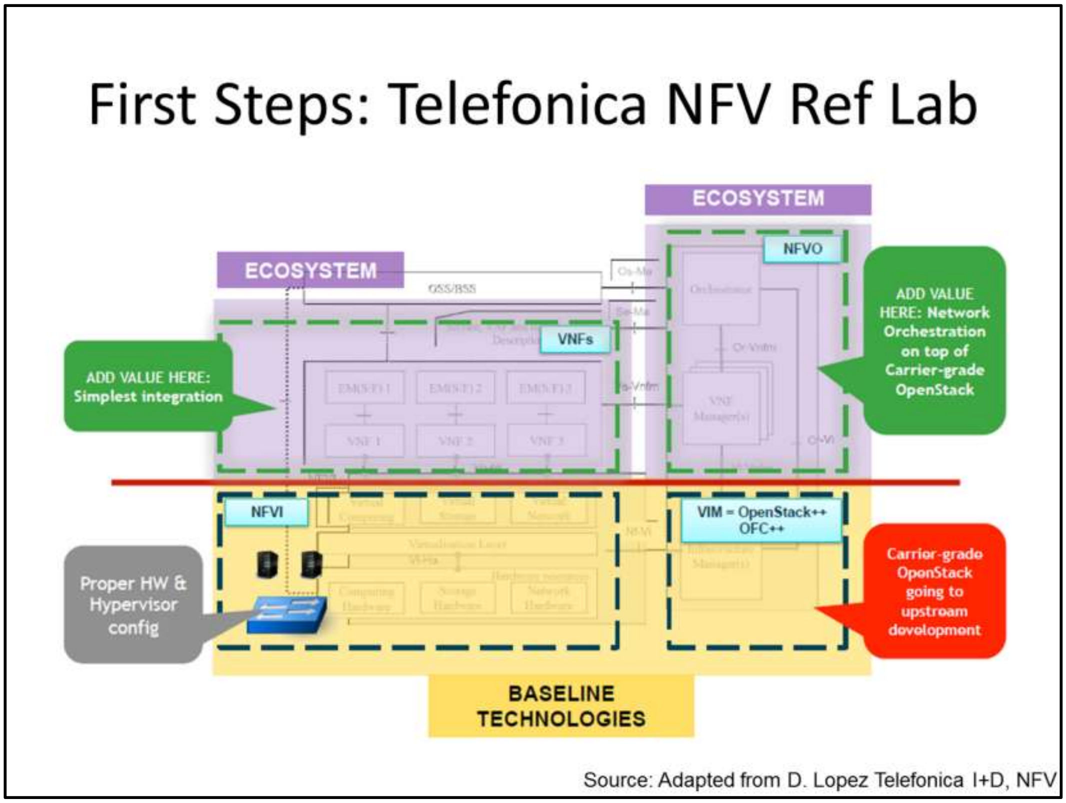


The architectural framework addresses the following:

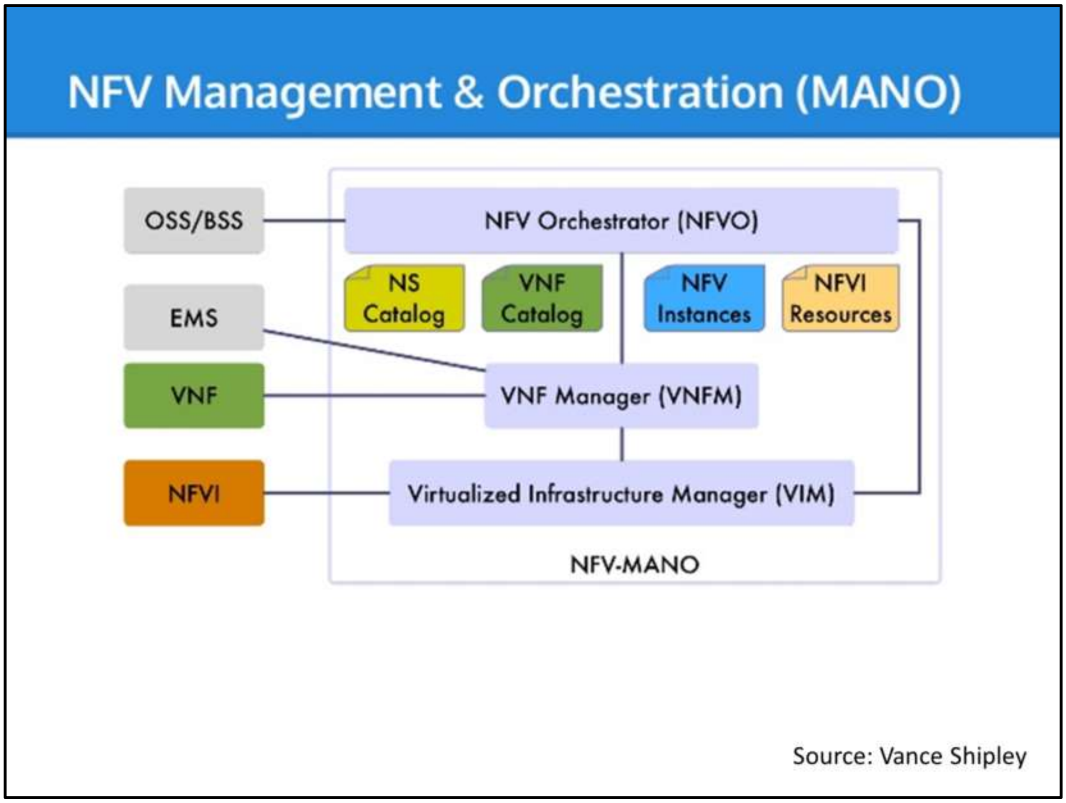
- The functionality that is required to be realized by the NFVI
- The functionality that is required due to decoupling network functons into software and hardware
- The functionality that is required for NFV-specific management and orchestration



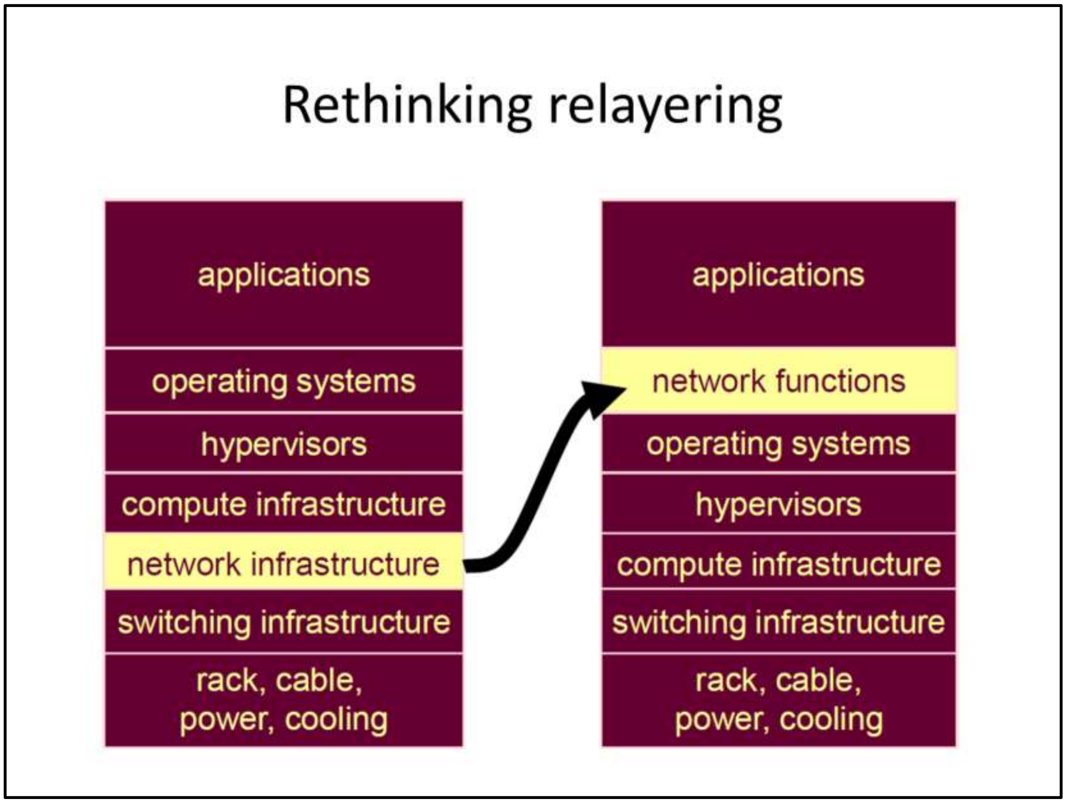
The NFV architectura framework focuses on the changes likely to occur in an operator's networkdue to the network function virtualisation process. That is, the architectural framework focusses on the new functional blocks and reference points brought by the virtualisation of an operator's network.



The architectural framework is described at a functional level and it dows not propose any specific implementation.

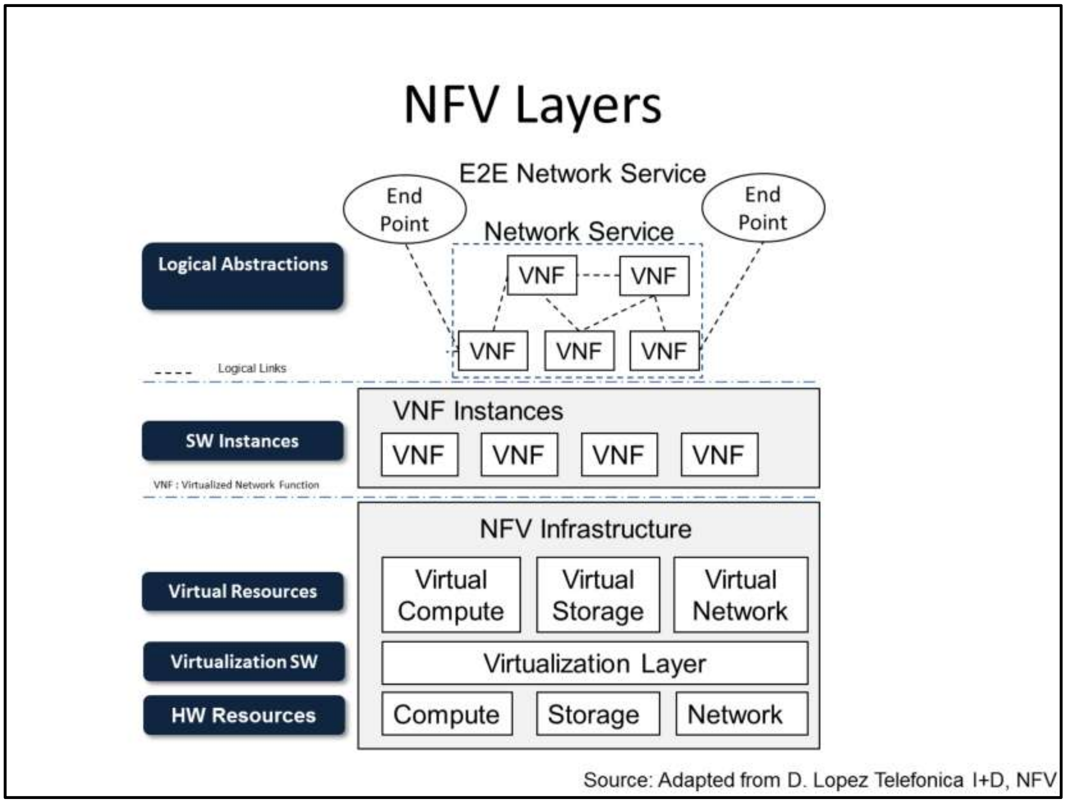


Source: http://www.slideshare.net/VanceShipley/cloud-for-mnos-network-functions-virtualization-nfv



The NFV Infrastructure (NFVI) is the totality of all software and hardware components which build up the environment in which VNFs are deployed, managed and executed. The NFVI can span across several locations, i.e. Places where NFVI-PoPs are operated. The network providing connectivity between these locations is regarded to be part of the NFVI.

From the VNF's perspective the virtualisation layer and the hardware resources look like a single entity providing them with desired virtualised resources.



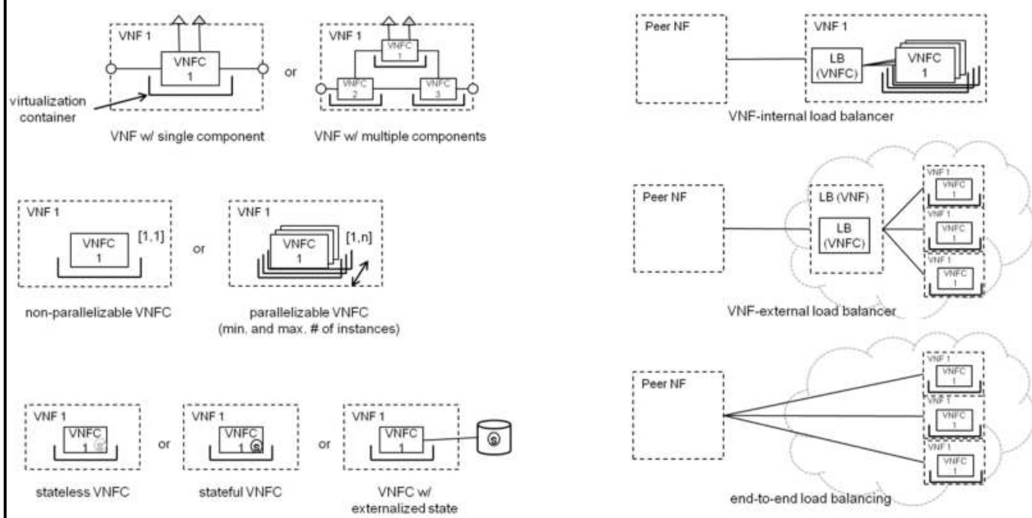
NFV emphasizes the fact that the exact physical deployment of a VNF instance on the infrastructure is not visible from the E2E service perspective, with the exception of guaranteeing specific polic constraints (e.g., location awareness required to implement a virtualised CDN cache node).

NFV Concepts

- **Network Function (NF):** Functional building block with a well defined interfaces and well defined functional behavior
- **Virtualized Network Function (VNF):** Software implementation of NF that can be deployed in a virtualized infrastructure
- **VNF Set:** Connectivity between VNFs is not specified, e.g., residential gateways
- **VNF Forwarding Graph:** Service chain when network connectivity order is important, e.g., firewall, NAT, load balancer
- **NFV Infrastructure (NFVI):** Hardware and software required to deploy, mange and execute VNFs including computation, networking, and storage.
- **NFV Orchestrator:** Automates the deployment, operation, management, coordination of VNFs and NFVI.

Source: Adapted from Raj Jain

VNF Design Patterns and VNFCs



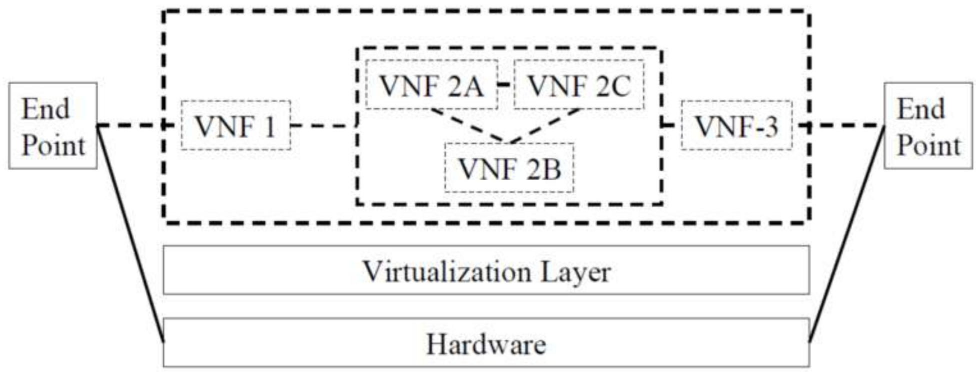
NFV Concepts

- **NFVI Point of Presence (PoP):** Location of NFVI
- **NFVI-PoP Network:** Internal network
- **Transport Network:** Network connecting a PoP to other PoPs or external networks
- **VNF Manager:** VNF lifecycle management e.g., instantiation, update, scaling, query, monitoring, fault diagnosis, healing, termination
- **Virtualized Infrastructure Manager:** Management of computing, storage, network, software resources
- **Network Service:** A composition of network functions and defined by its functional and behavioral specification
- **NFV Service:** A network services using NFs with at least one VNF.

Source: Adapted from Raj Jain

Network Forwarding Graph

- An end-to-end service may include nested forwarding graphs



Source: Adapted from Raj Jain

NFV Concepts

Network Service (NS):

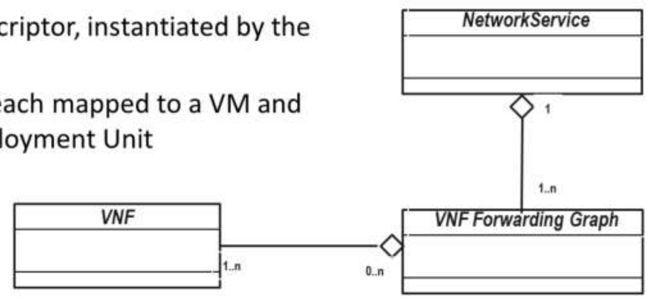
- Described by the NS descriptor, orchestrated by NFVO
- May cover 1 or more VNF Graphs, VNFs and PNFs

VNF Forwarding Graph (VNFFG):

- Described by the VNFFG descriptor, orchestrated by NFVO
- May cover VNFFGs, VNFs and NFs

VNF:

- Described by the VNF descriptor, instantiated by the VNF Manager
- Covers VNF components each mapped to a VM and described as a Virtual Deployment Unit

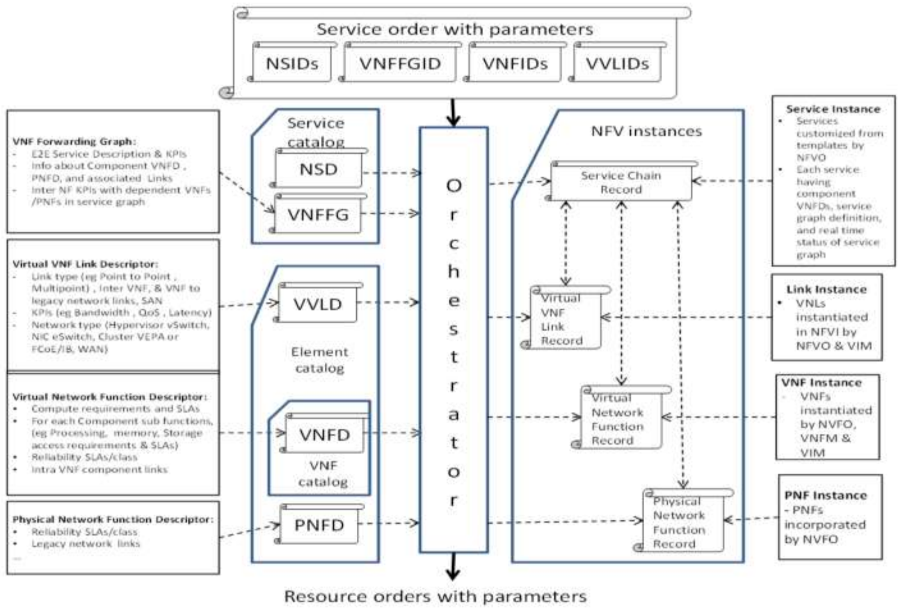


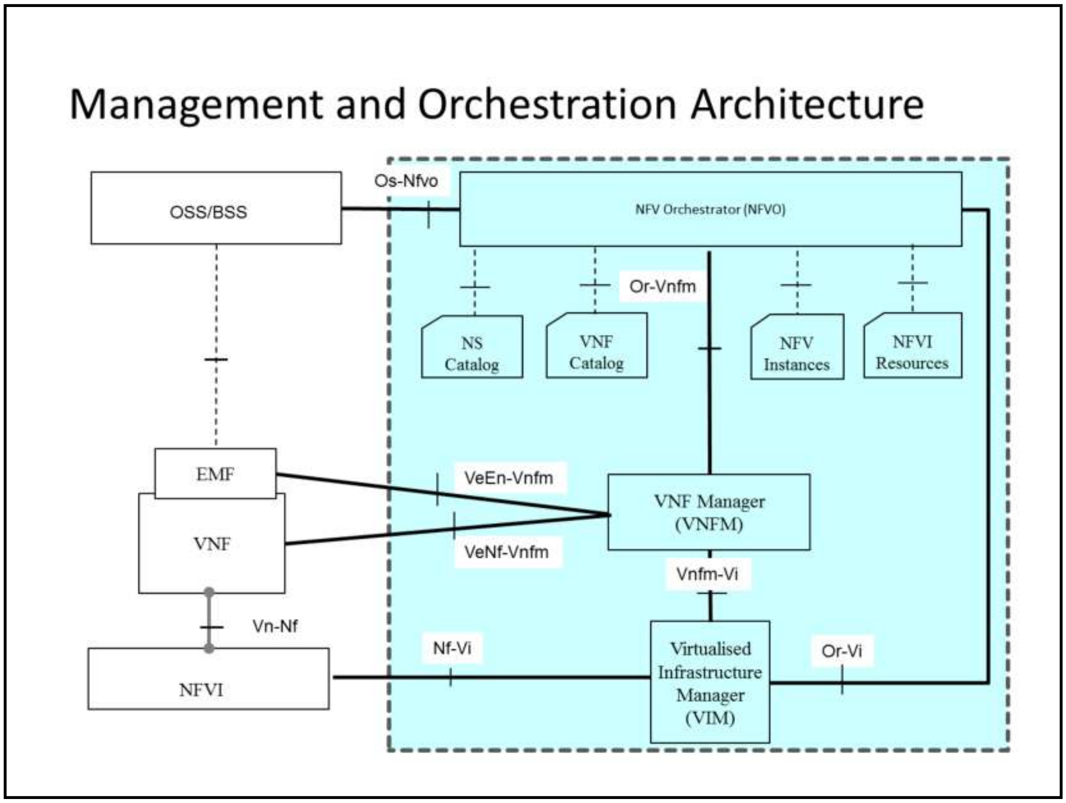
NFV Concepts (cont.)

- **User Service:** Services offered to end users/customers/subscribers.
- **Deployment Behavior:** NFVI resources that a VNF requires, e.g., Number of VMs, memory, disk, images, bandwidth, latency
- **Operational Behavior:** VNF instance topology and lifecycle operations, e.g., start, stop, pause, migration, …
- **VNF Descriptor:** Deployment behavior + Operational behavior

Source: Adapted from Raj Jain

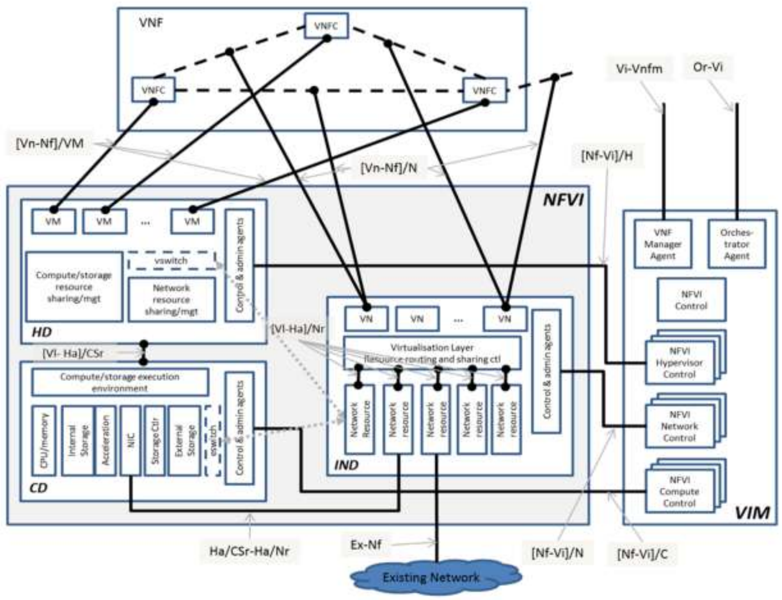
Descriptor Information Model





THIS IS LOGICAL/FUNCTIONAL ARCHITECTURE! These are just functional blocks, it does not represent any specific implementation.

Virtual Infrastructure Management

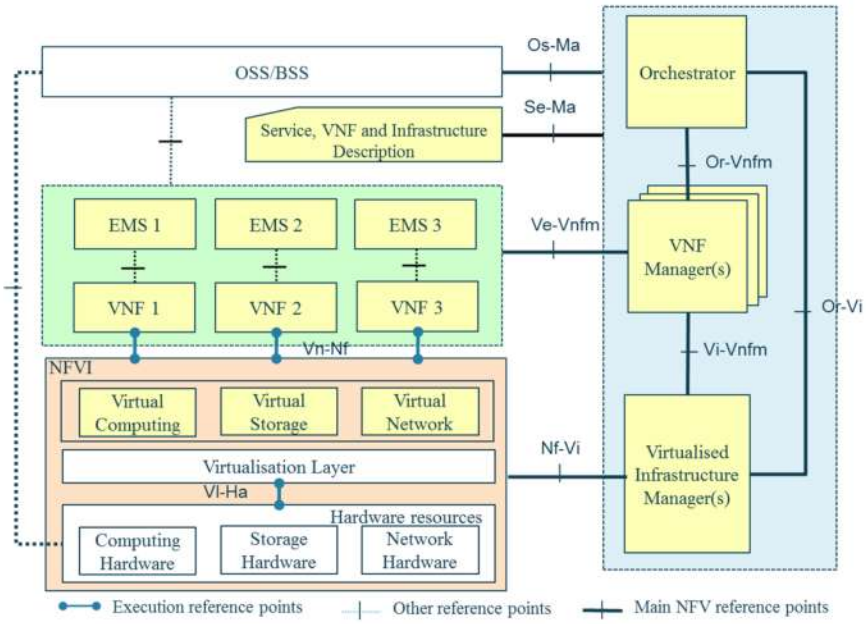


NFV Orchestrator:
– on-boarding of new Network Service (NS), VNF-FG and VNF Packages
– NS lifecycle management (including instantiation, scale-out/in, performance measurements, event correlation, termination)
– global resource management, validation and authorization of NFVI resource requests
– policy 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

Virtualised 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

The NFV Architecture Framework

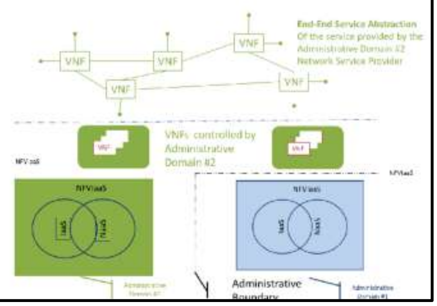


Reference Point:
Points for inter-module specification

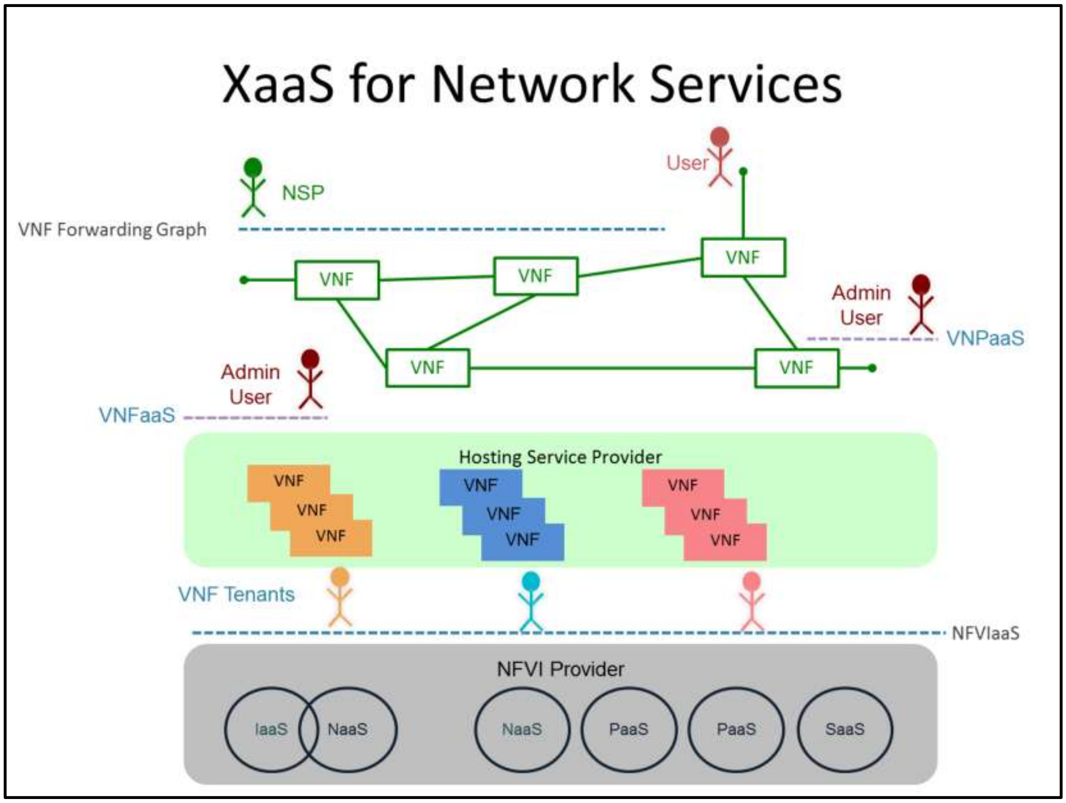
- **(Os-Ma)** Operation Support System (OSS)/Business Support Systems (BSS) – NFV Management and Orchestration
- **(Se-Ma)** Service, VNF and Infrastructure Description – NFV Management and Orchestration: VNF Deployment template, VNF Forwarding Graph, service-related information, NFV infrastructure information
- **(Or-Vnfm)** Orchestrator – VNF Manager
- **(Vi-Vnfm)** Virtualized Infrastructure Manager – VNF Manager
- **(Ve-Vnfm)** VNF/ Element Management System (EMS) – VNF Manager
- **(Or-Vi)** Orchestrator – Virtualized Infrastructure Manager
- **(Nf-Vi)** NFVI-Virtualized Infrastructure Manager
- **(Vl-Ha)** Virtualization Layer-Hardware Resources
- **(Vn-Nf)** VNF – NFVI

Architectural Use Cases

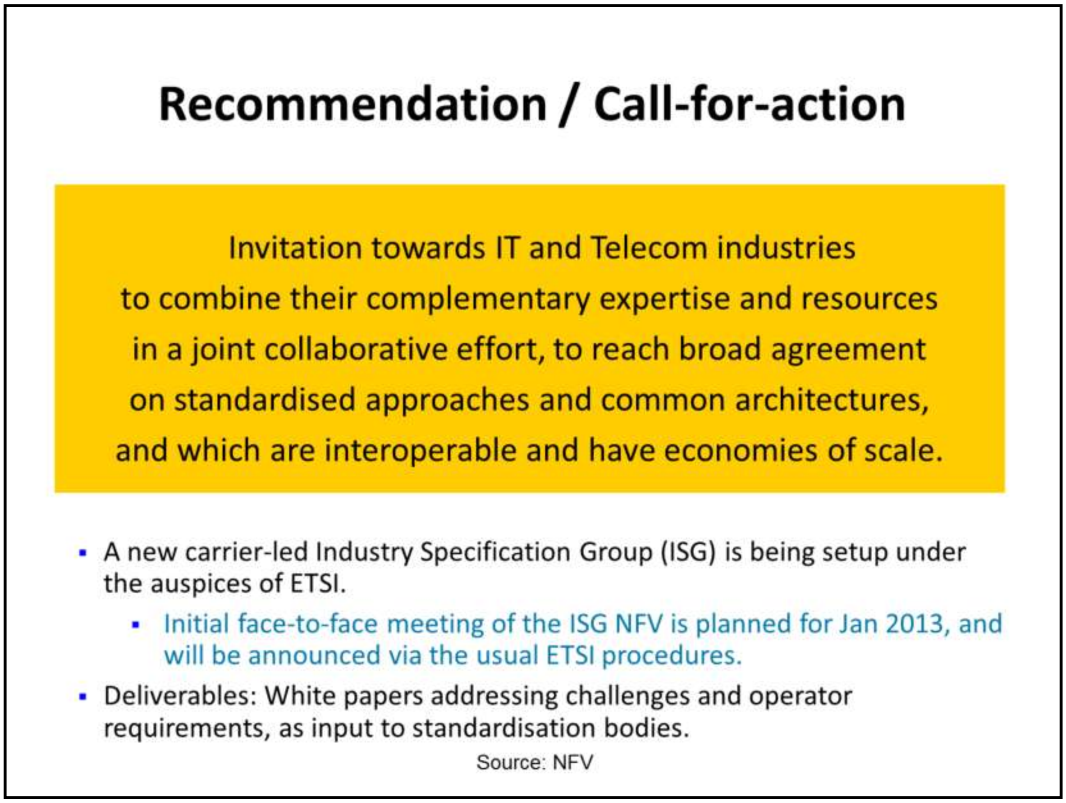
- Network Functions Virtualisation Infrastructure as a Service
  - Network functions go to the cloud
- Virtual Network Function as a Service
  - Ubiquitous, delocalized network functions
- Virtual Network Platform as a Service
  - Applying multi-tenancy at the VNF level
- VNF Forwarding Graphs
  - Building E2E services by composition



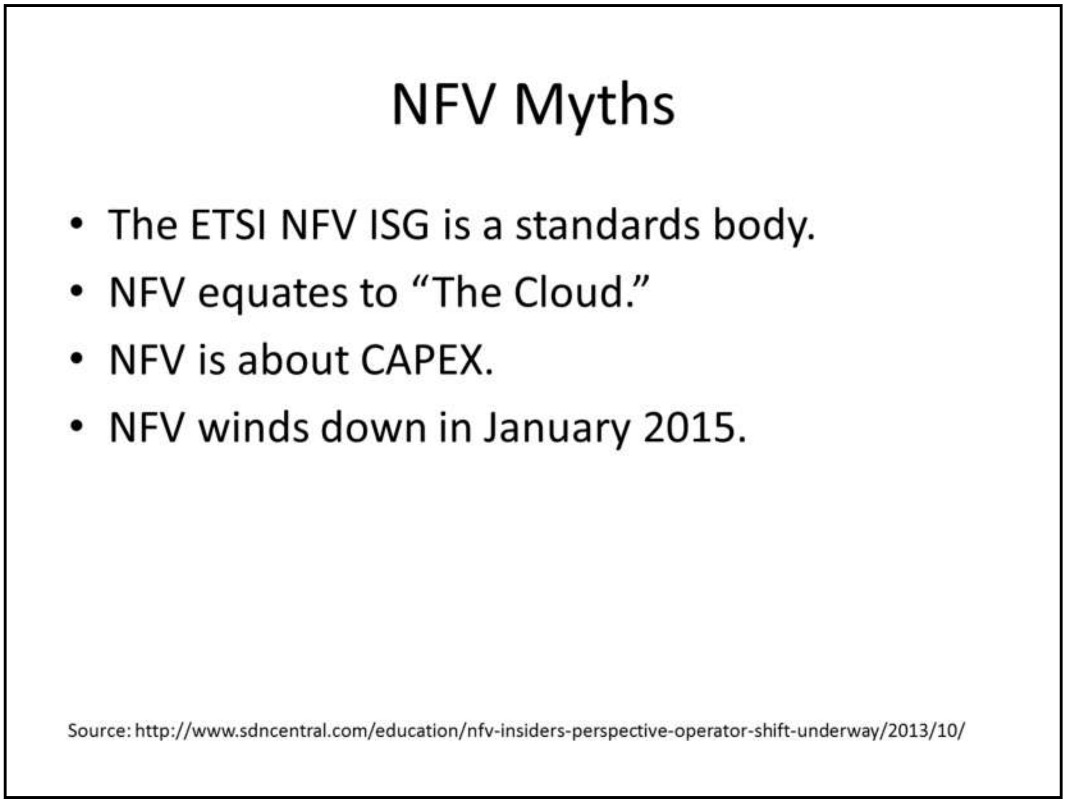
NFV use cases are intended to provide a comercial and technical context that is expected to be useful for discussions on technical requirements and architectures in further documents do be developed by carriers, industry and the ETSI NFV ISG.



NFVIaaS, NFVPaaS, VNFaaS are some of the use cases that can be realized with a common NFV architectural framework proposal.



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 Virtualisation
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 organisation for this initiative, the ISG will downstream its work to all relevant organisations and seek to encourage convergence of IT and Network Standardisation efforts in this space.
Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf



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.

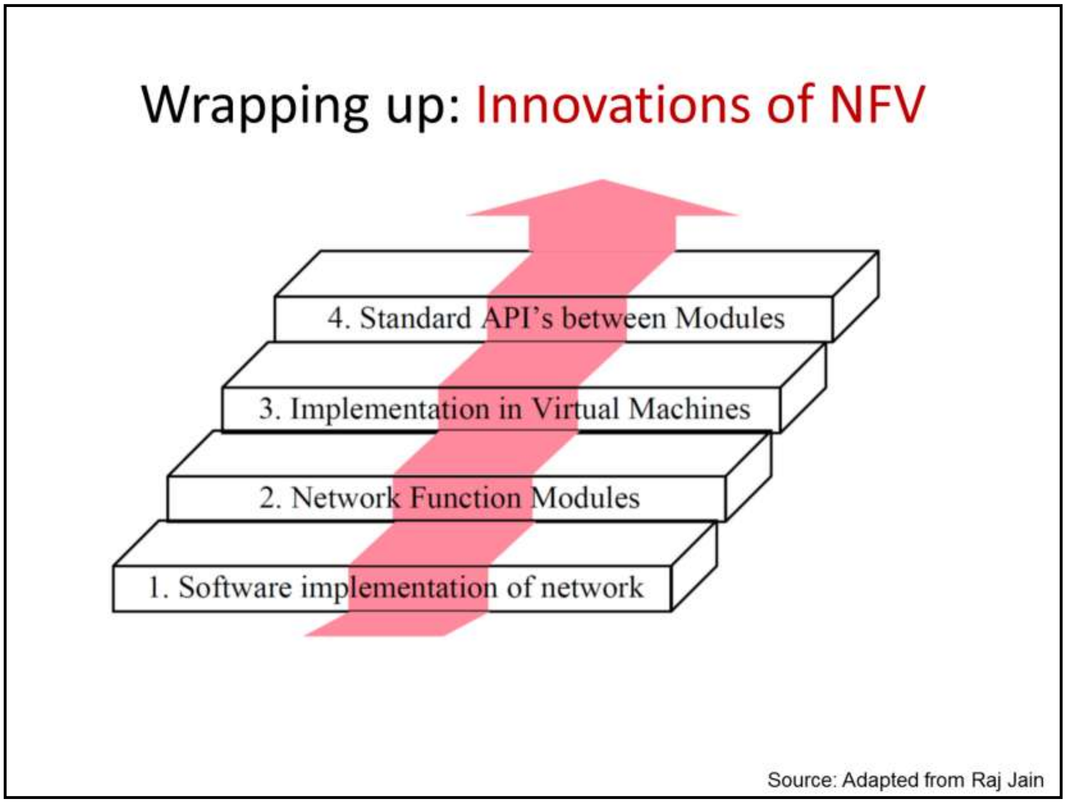
While NFV is expected to realize the many benefits of public and private cloud services, there are differences:

Generic cloud services tend to be compute-centric, whereas NFV is inherently connect-centric.

Generic cloud services are optimized to enable multiple tenants to share compute, storage, and connect resources in a highly cost- and energy-efficient manner. NFV must scale network functions to serve millions and even tens of millions of subscribers. In fact, many large-scale enterprise applications are not virtualized to avoid the overhead.

Generic cloud services are typically characterized by many relatively small VMs to optimize the utilization of the system resources; NFV deployments for large operators will consist of fewer but much larger VMs to accommodate the vast scale of large operators.

Generic cloud services seek to decouple the virtual and physical domains. Carrier networks demonstrate what some operators refer to as "shape," which consists of definitive segments and service boundaries with orderly handoffs.



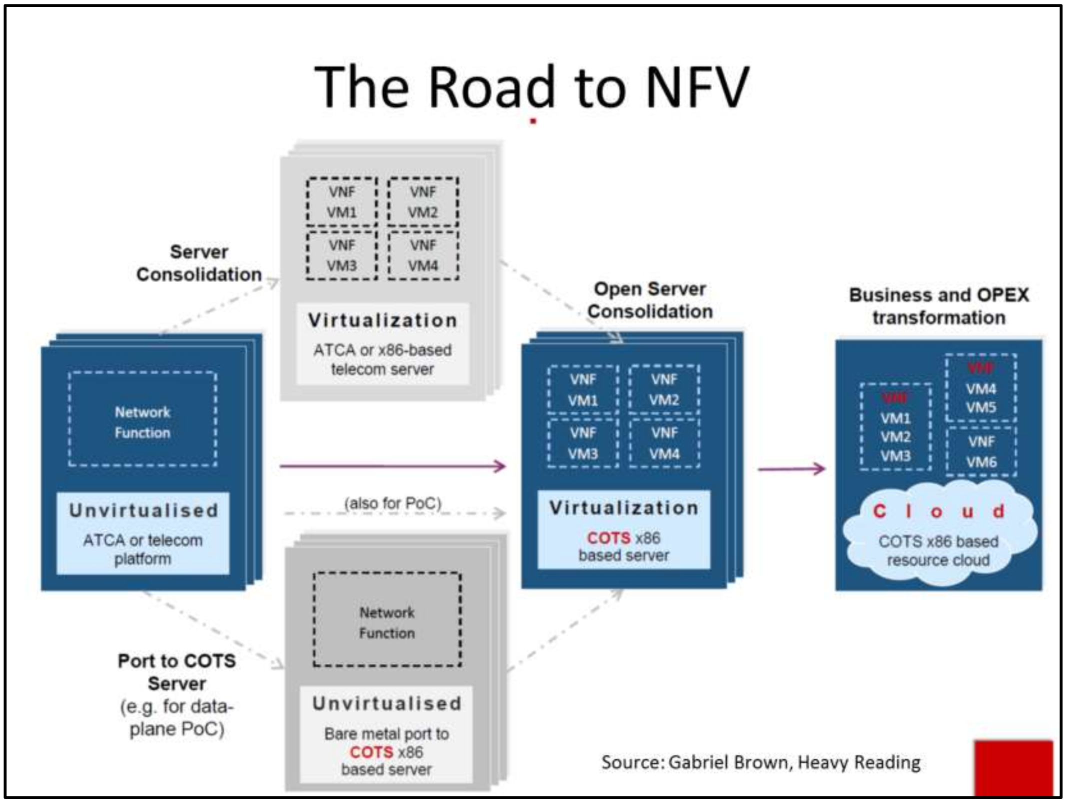
1 Fast standard hardware -Software based Devices
Routers, Firewalls, Broadband Remote Access Server (BRAS)
-A.k.a. *white box* implementation
2. Function Modules (Both data plane and control plane)
-DHCP (Dynamic Host control Protocol), NAT (Network Address Translation), Rate Limiting,
3. Virtual Machine implementation
-Virtual appliances
-All advantages of virtualization (quick provisioning, scalability, mobility, Reduced CapEx, Reduced OpEx, …)
4. Standard APIs: New ISG (Industry Specification Group) in ETSI (European Telecom Standards Institute) set up in November 2012

Requirements and Challenges

NFV

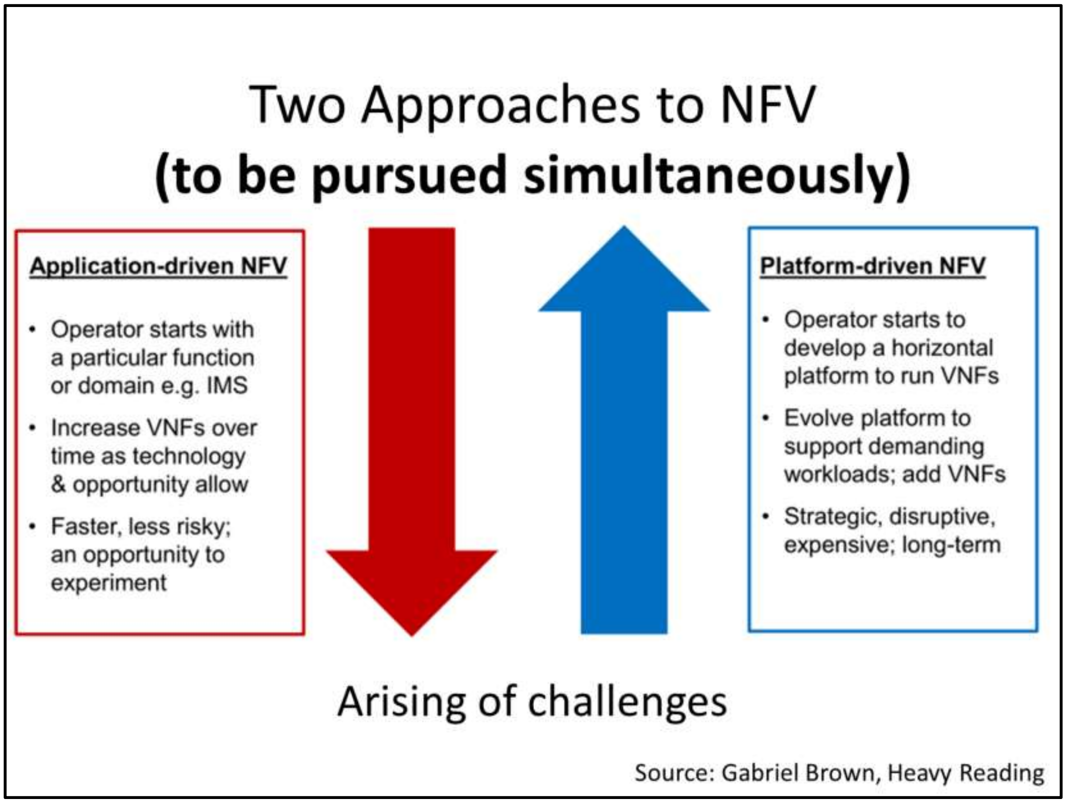
NFV has been developed for more than 1 year, stimulating new concepts to be born and most specificly implemented.
The fundamental questions are being handled by ETSI and the telecom industry, but still remain some issues, that will be solved in the long term and that we will discuss here. These constitute some requirements and challenges about NFV.

NFV represents a paradigm shitf in networking. In order to realize the deployment of the NFV archtectural framework many requirements step ahead of different environments, which are specifically bounded into new newtork abstractions provided by NFV. In this sense, some already known requirements and challenges resurge with different specifications. First we'll take a look in the more specific requirements arising from the NFV framework.



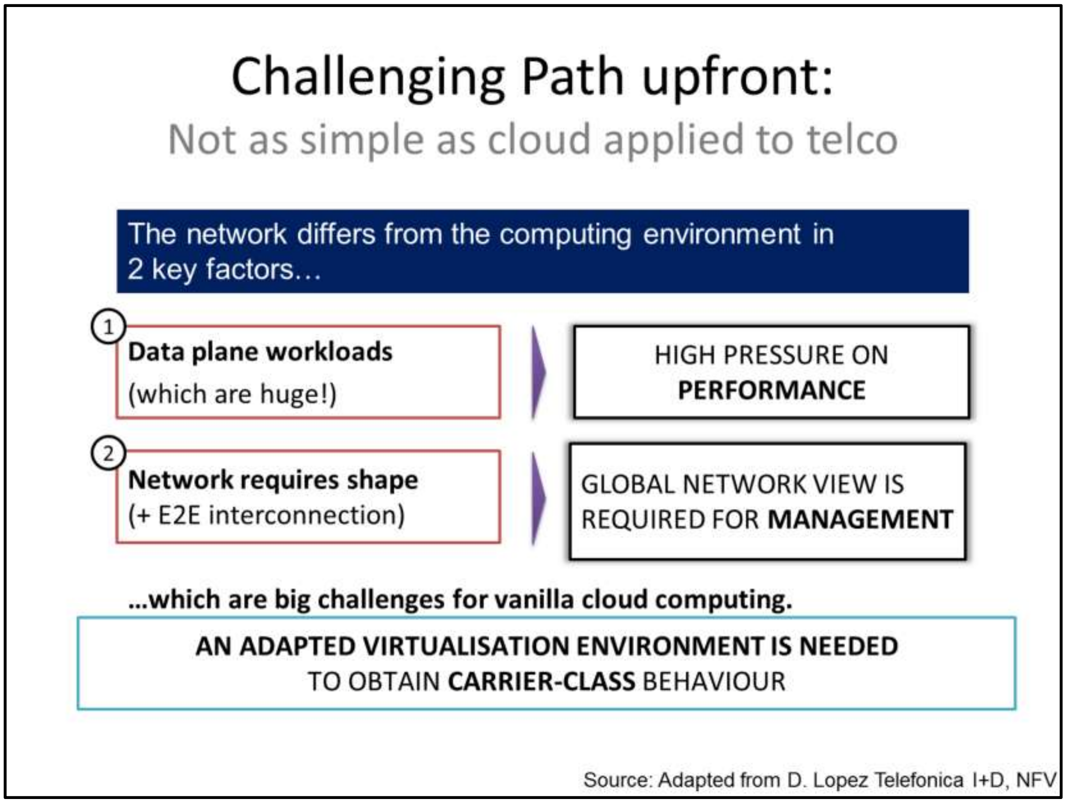
There are four (potential) phases that telcos may adopt – depending on application and use case:

- Migration to COTS involving the migration from purpose-built hardware to software running on general purpose servers.
- Virtualization of software functions
- Elasticity capacity for the ability to easily scale up and scale down applications based on dynamic needs of the network.
- Orchestration of multiple virtual functions and combining (service chaining) a broad range of NFV applications across the network stack.



Source: Gabriel Brown, Senior Analyst, Heavy Reading (Presentation NFV Forum – Introduction)

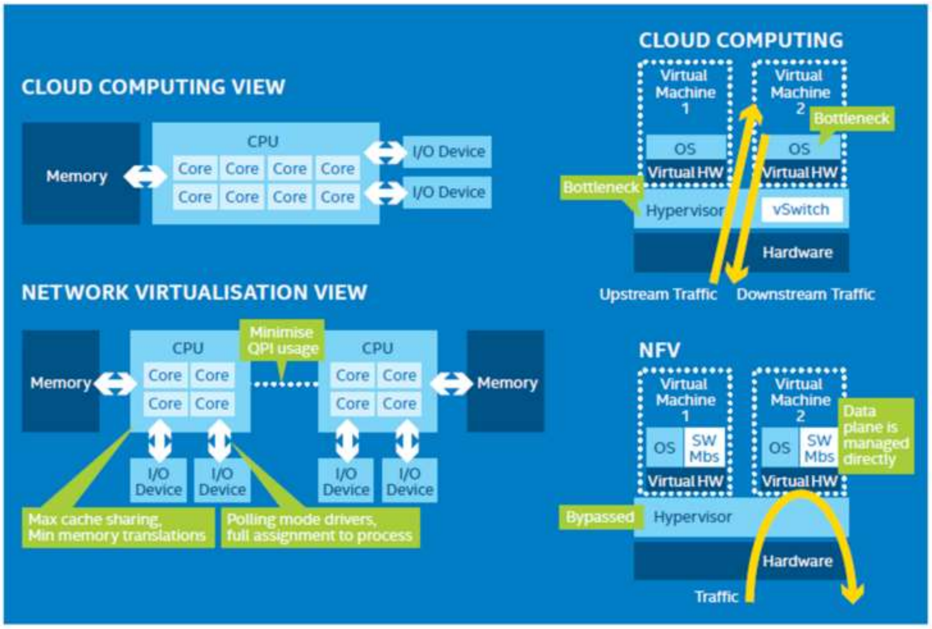
In the meantime that challenges are constantly arising in the NFV horizon, some use cases are already available at NFV ETSI web page. Some of them have being tested and deployed in telecom well known scenarios, representing the red arrow above. Nevertheless some others still lack some incremental features which represent the characteristics of the blue arrow above. I.e., there are still horizontal improvements to be made in a well defined platform, mainly associated with NFV management and orchestration requirements.



Service level functionality should be implemented largely in software

- The network infrastructure consists of low unit cost COTS network elements: servers, packet optical transport, data center switches and storage
- Leverage low cost per unit to provide bandwidth expansion and increasing range of services
- Use distributed storage instead of expensive routing and transport to deliver popular, high volume content
- Use software-based service delivery to be more responsive to new requirements from customers and market opportunities
- Automate management and provisioning to the greatest extent possible

Cloud vs. NFV



Src: End to End Network Function Virtualization Architecture Instantiation (Intel, Telefonica, Brocade, Cyan, Redhat)

Cloud vs. NFV

CLOUD COMPUTING	NFV
1. PERFORMANCE BOUND TO CPU	1. PERFORMANCE BOUND TO I/O & MEMORY ACCESS
2. AGGREGATED VIEW OF RESOURCES (CPU, memory, etc.)	2. NUMA VIEW Internal architecture is relevant for guests
3. ENDPOINTS Applications need the OS	3. MIDDLEPOINTS Data-plane network functions bypass the OS
4. NODE-CENTRIC Shapeless interconnection	4. NETWORK-CENTRIC The network has a shape
5. MANY AND SMALL VMs	5. FEW AND LARGE VMs

Source: Adapted from D. Lopez Telefonica I+D, NFV

NFV Framework Requirements

1. General: Partial or full Virtualization, Predictable performance
2. Portability: Decoupled from underlying infrastructure
3. Performance: Conforming and proportional to NFs specifications and facilities to monitor
4. Elasticity: Scalable to meet SLAs. Movable to other servers.
5. Resiliency: Be able to recreate after failure.

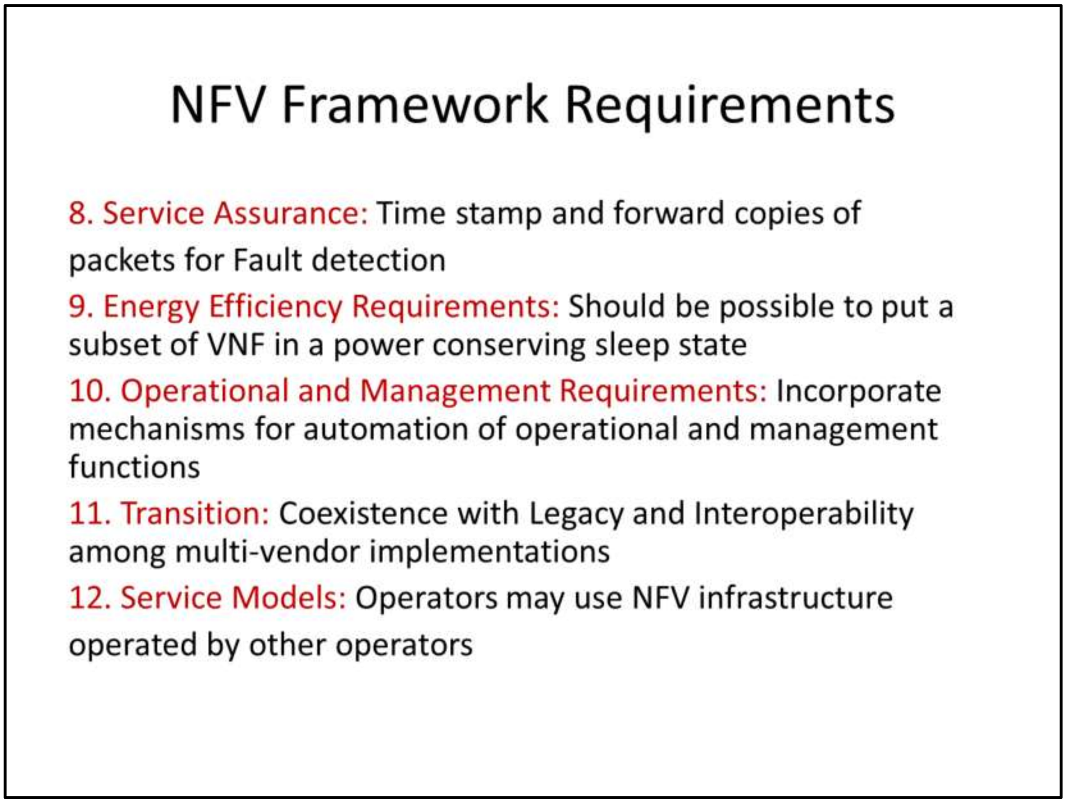
Specified packet loss rate, calls drops, time to recover, etc.

6. Security: Role-based authorization, authentication
7. Service Continuity: Seamless or non-seamless continuity after failures or migration

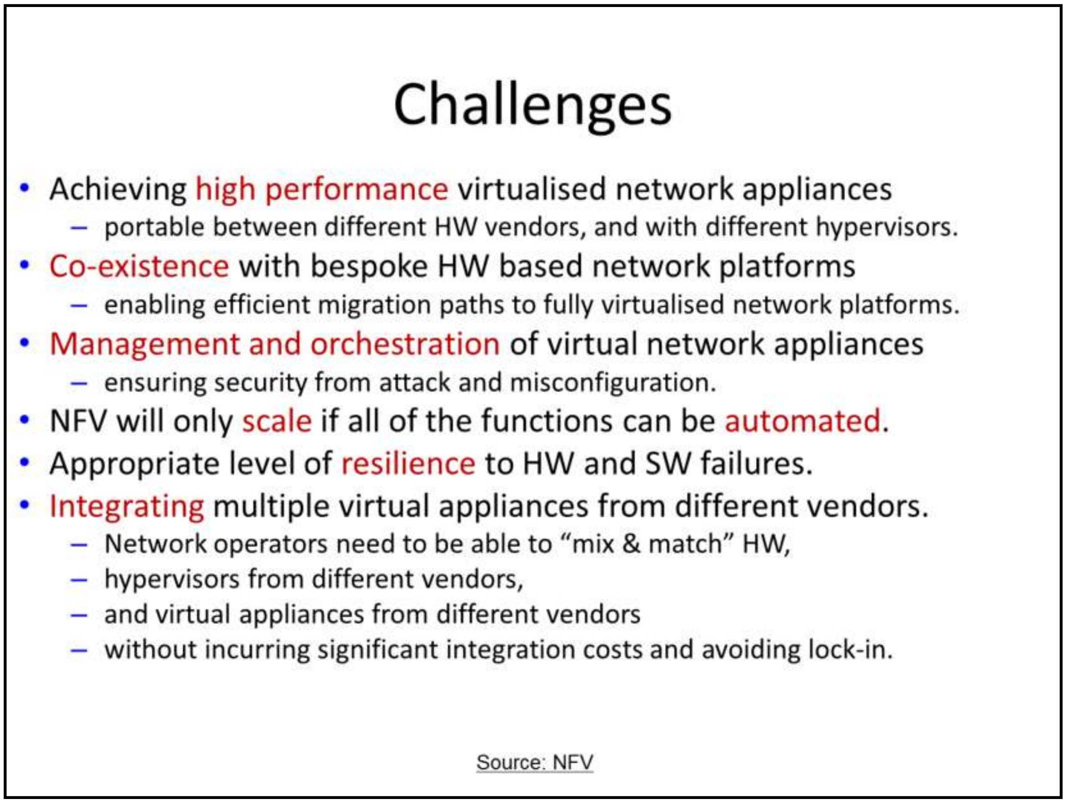
Accordingly to the ETSI NFV requirements document [1], there are different requirements to NFV:

- General: involves SPs and NOs partially or full virtualize network functions to create, deploy and operate the services needed (Partial virtualization intended to be measurable with impacts: performance, fault tolerance)
- Portability: Load, execute and move NFs in different N-PoPs; Optimize de location, reservation and allocation of resources in different NFVI levels, meeting and maintaining SLA requirements
- Performance: is conforming to NFs specifications; describe underlying infrastructure to support NF performance; monitor and collect performances data in different resources usage level (NICs, hypervisors, VMs)
- Elasticity: requires parallelised components; VNFs scaled with SLA requirements; Maintain service continuity requirements; Movable VNFs components
- Resiliency: resilience characteristics of NFs and set of VNFs well defined; specify metrics to define the value and variability of stability
- Security: Protection of the shared data in different virtualization layers
- Service Coninuity: Zero vs. Measurable impact

[1]
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/004/01.01.01_60/gs_NFV004v010101p.pdf



- Service Assurance: virtualized instrumentation functions wherever and whenever required to diagnose network problems
- Energy Efficiency Requirements: changes in the distribution of energy consumption based on computing, storage and network resources separation; exploit the benefits of virtualization to turn on/off components on-demand
- Operational and Management Requirements: creation, scaling and healing of VNF instances based on VNF information model, network capacity adaptation to load, software upgrades, functions configuration and relocation, and intervention on detected failures
- Transition: same service capability, performance, security, with minimum impact on existing network; transparent transition
- Service Models: coexistence of VNFs in heterogeneous NFVI to be provided by differents SPs to network operators



There are a number of technical challenges which need to be addressed:

• Achieving high performance virtualised network appliances which are portable between different hardware vendors, and with different hypervisors.

• Achieving co-existence with bespoke hardware based network platforms whilst enabling an efficient migration path to fully virtualised network platforms which re-use network operator OSS/BSS. OSS/BSS development needs to move to a model in-line with Network Functions Virtualisation and this is where SDN can play a role.

• Managing and orchestrating many virtual network appliances (particularly alongside legacy management systems) while ensuring security from attack and misconfiguration.

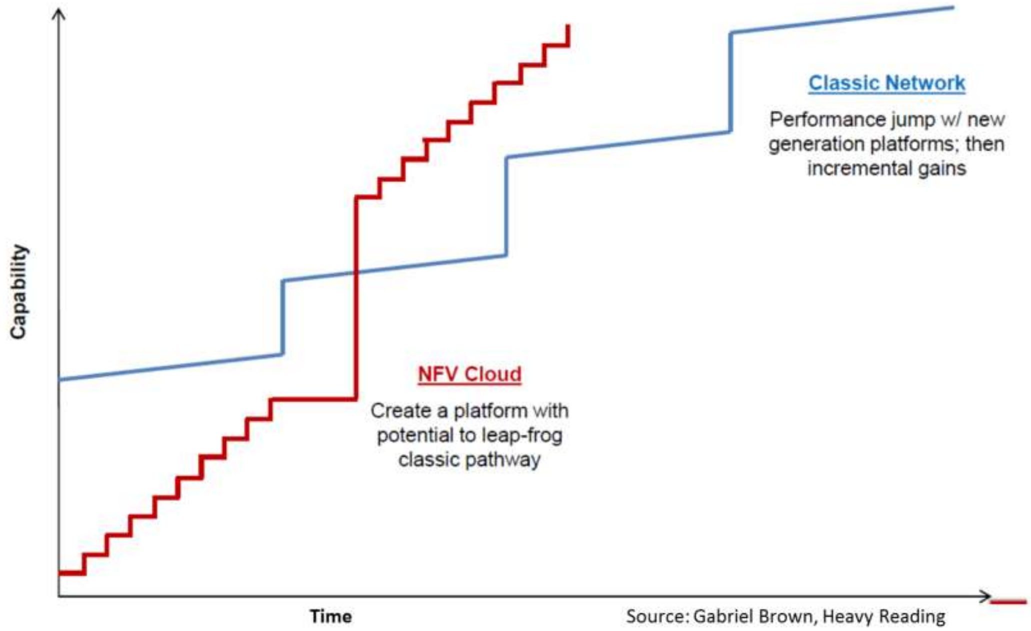
• Network Functions Virtualisation will only scale if all functions can be automated.

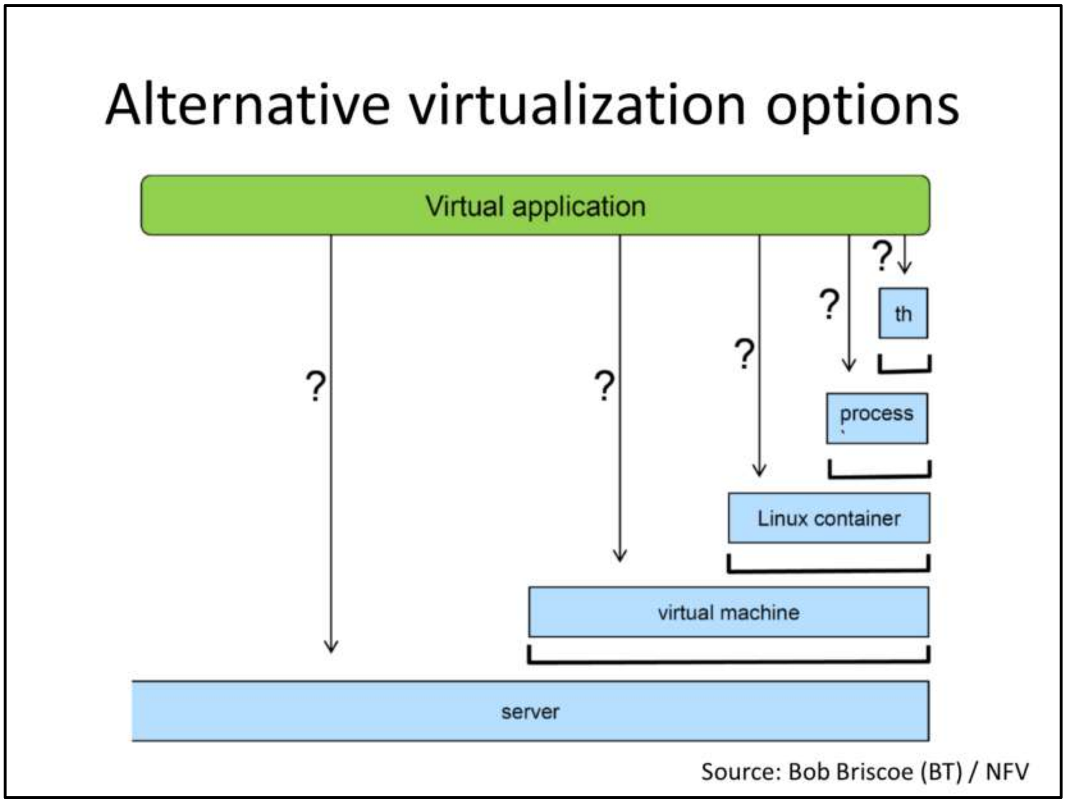
• Ensuring the appropriate level of resilience to hardware and software failures.

• Integrating multiple virtual appliances from different vendors. Network operators need to be able to "mix & match" hardware from different vendors, hypervisors from different vendors and virtual appliances from different vendors without incurring significant integration costs and avoiding lock-in.

Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

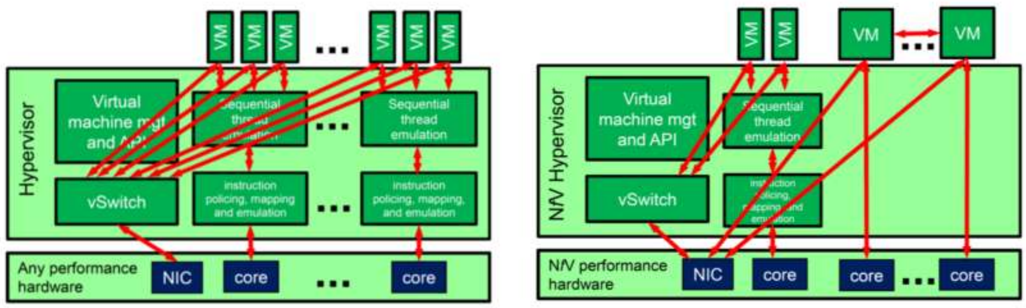
Is NFV Technology Good Enough?





In any case VNF instances and their supporting infrastructure need to be visible for configuration diagnostic and troubleshooting purposes.

Virtualization Implementation



Source: Bob Briscoe (BT) / NFV

The virtualization layer is key for delivering high-performance NFV solutions

Standard virtualization Technologies may impose high performance penalties in the E2E solution.

NFV-optimized virtualization enhancements are being worked out at the hypervisor level as well as the network interface card support for hardware-acceleration of virtualized environements.

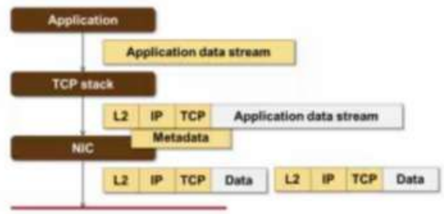
NFV Performance Challenges

Typical performance

- 3-4 Gbps per CPU core assuming very light per-packet processing
- An order of magnitude less than what the hardware could do (more than 10Gbps per core, 40+ Gbps per x86 server)

Bottlenecks

- TCP stack and Linux kernel in NFV virtual machines
- Hypervisor virtual switch
- NIC TCP offload works only with VLANs



Solutions

- Optimized virtual switches (example: Intel DPDK)
- Dedicated virtual NICs (hypervisor bypass)
- Dedicated packet processing CPU cores
- User-mode packet processing (example: PF_RING)

Source: Ivan Pepelnjak

Source: Ivan Pepelnjak SDN, NFV and OpenFlow for Skeptics » 5 - Network Function Virtualization
http://demo.ipspace.net/get/5%20-%20Network%20Function%20Virtualization.mp4

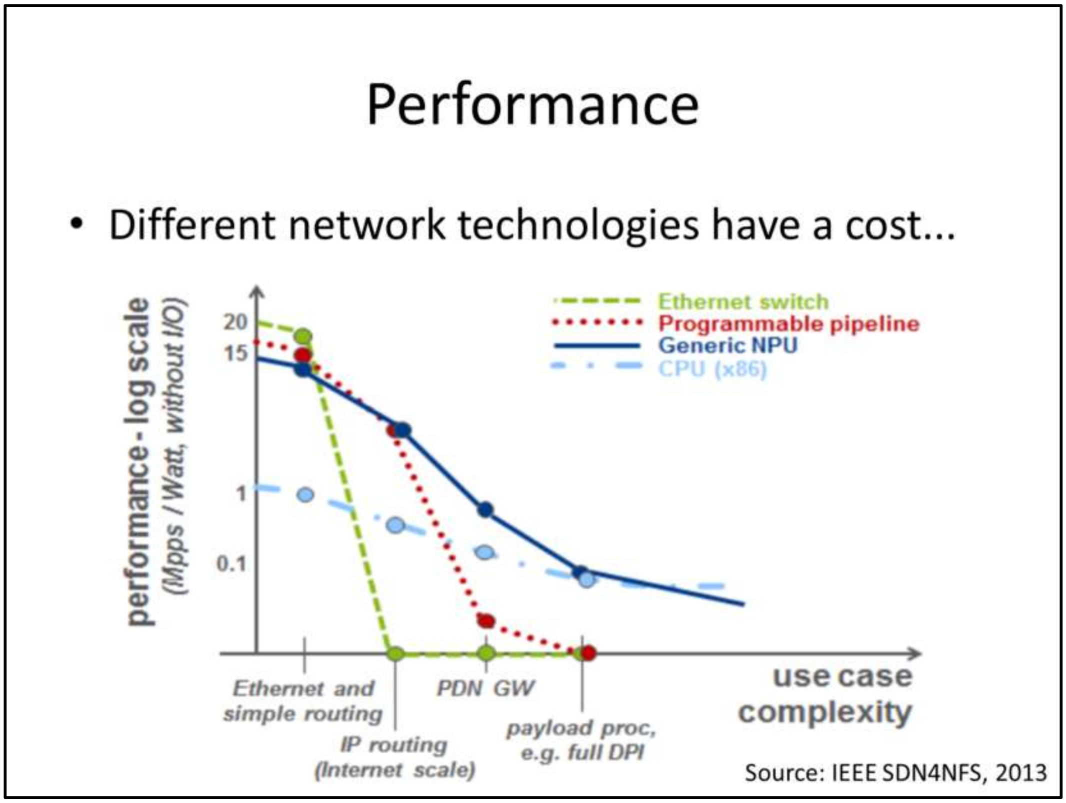
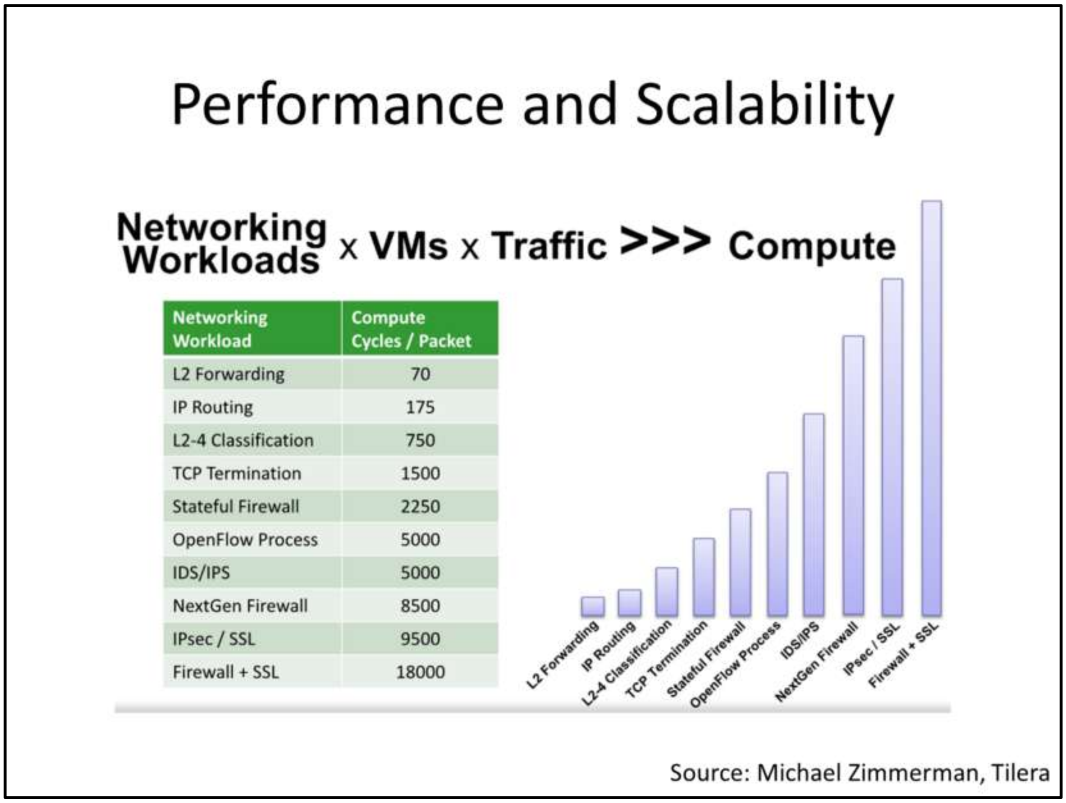


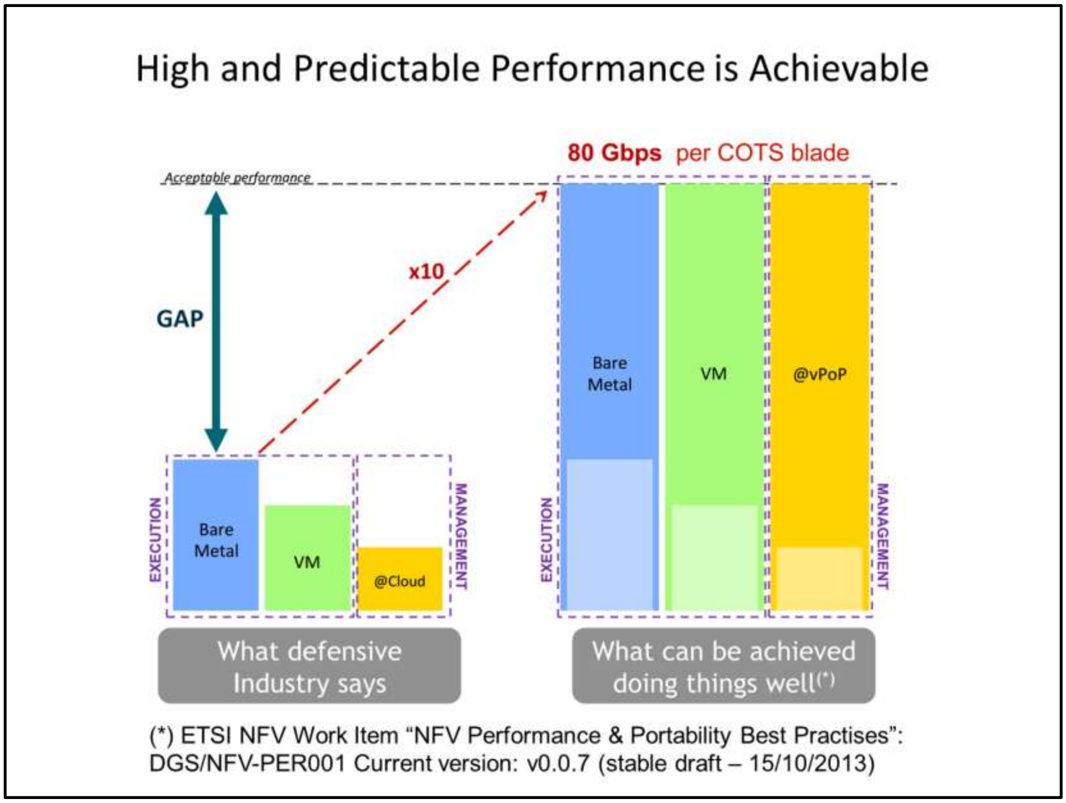
Figure source: D. Siracusa, E. Salvadori, and T. Rasheed, “Edge-to-edge virtualization and orchestration in heterogeneous transport networks,” in Future Networks and Services (SDN4FNS), 2013 IEEE SDN for, Nov 2013, pp. 1–6

As we have seen the evolution of network technologies since the foundation of Internet communication devices, now we live another dilemma inside the development of the use case complexity of network functions. According as complexity rises we see an performance decrease, leading to an evolution barrier that presents itself as a performance challenge for a wide variety of NFs with high complexity behaviors and requirements.



Figures Source: Michael Zimmerman, Tilera (Presentation Networking Goes Open-Source)

This figure only explicitly demonstrates our previous statements, that network workloads may fluctuate depending on the network task performed. As it intend to be more specific and specialized computing requirements also intend to perform better and scale with the network task. A VNF like a firewall would require much more CPU cycles than a mere L2 forwarding virtual switch.


High and Predictable Performance is Achievable
80 Gbps per COTS blade
Acceptable performance
GAP
x10
Bare Metal
VM
@Cloud
Bare Metal
VM
@vPoP
EXECUTION
MANAGEMENT
EXECUTION
MANAGEMENT
What defensive Industry says
What can be achieved doing things well(*)
(*) ETSI NFV Work Item "NFV Performance & Portability Best Practises":
DGS/NFV-PER001 Current version: v0.0.7 (stable draft – 15/10/2013)

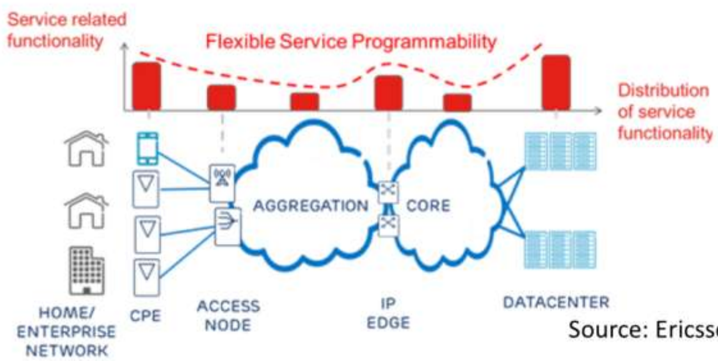
Performance and Scalability

- PFs and NFs
  – Lack of performance -> Scalability decreased
- Performance
  – NF vs. NFV-FG
- Proportional performance of NFs and services according to available:
  – Network latency and bandwidth
  – Compute capacity

In resume, for a NF, lack of performance leads to scalability decreased and so the scalability of a whole service composition, as it depends on its chained NFs. It’s completely related to the NSC performed by NFV-FG, which means that NFs isolated may have a well behaved features, but when putted togheter they may not represent the whole needed SLA required. In this sense, as one NFV main challenge, performance and scalability run side-by-side, looking to achieve proportional computing, storage and connecting resources accordingly to services and their environment.

Scalability

- Real world vs. virtualized perspective
  - Network devices: FIB size, queue length, # of ports
- NFVI existence?
  - Distributed: storage, processing, connecting
  - Distributed NFs
    - Latency and Bandwidth requirements (e.g., BRAS, DPI)



Source: Ericsson, EU UNIFY

Since the foundation of network devices, distributed algorithms have been used to scale with network size and domain. For example, BGP routing tables in AS level 1 contain today approximately 500.000 entries and large queues, on the other hand data center network equipments, depending on the topology and routing protocol (e.g., TRILL, OSPF, STP) have different configurations, like lesser FIB entries and fewer queue sizes.

In a virtualized perspective, these configurations above mean that depending on the network enviornment it’ll be desirable to fulfill different requirements, leading to a NF computing, storage and connecting performance in conformance with its NFVI context. Then, as many NFV-PoPs may exist in different locations, a NF must scale its features in accordance with the environment and maintaining latency, bandwidth and all the other requirements related to SLA service parameters.

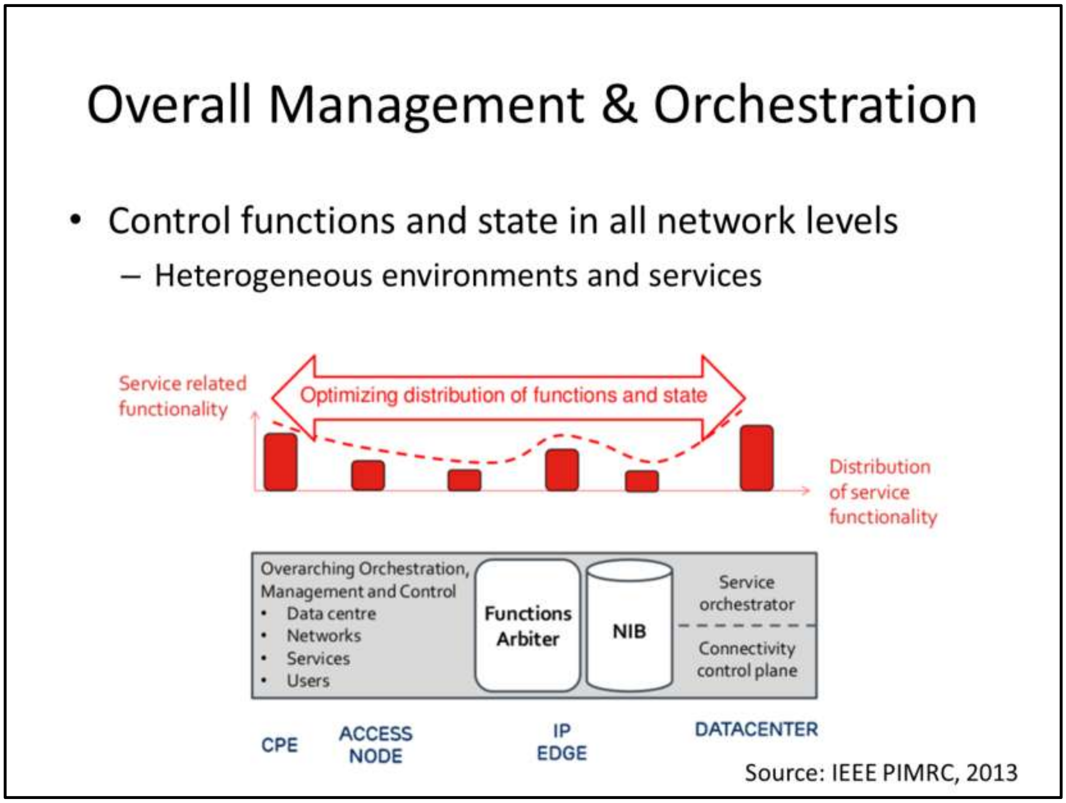
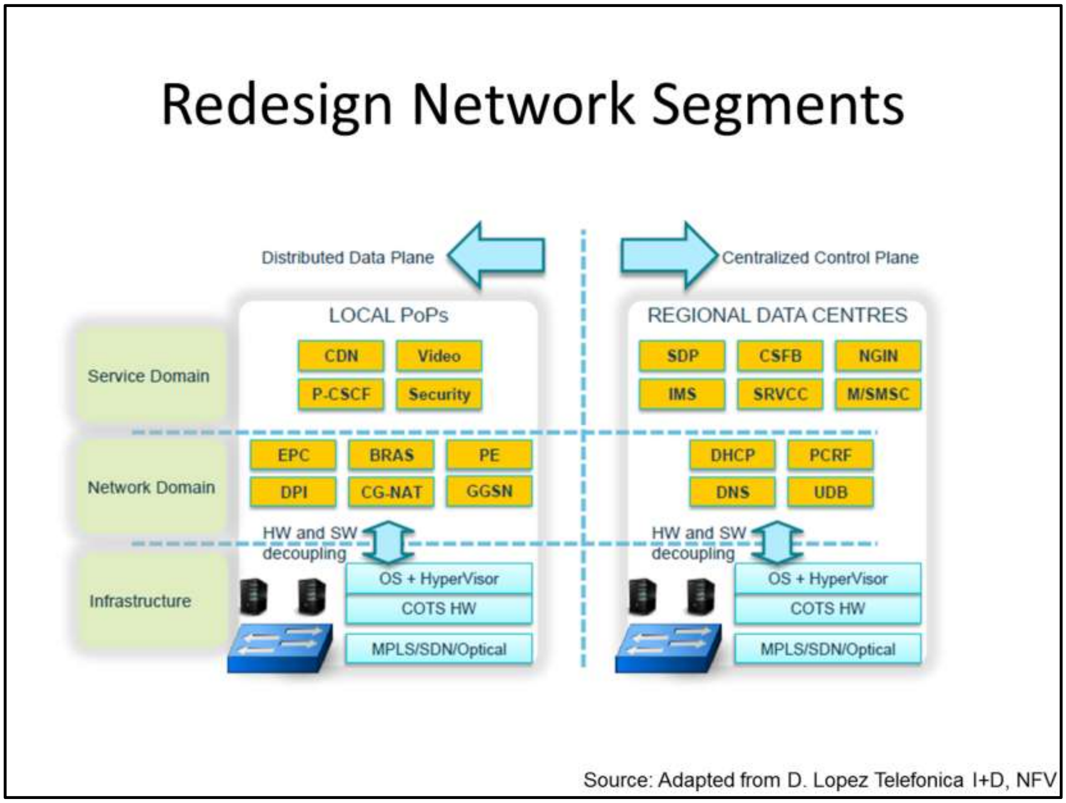
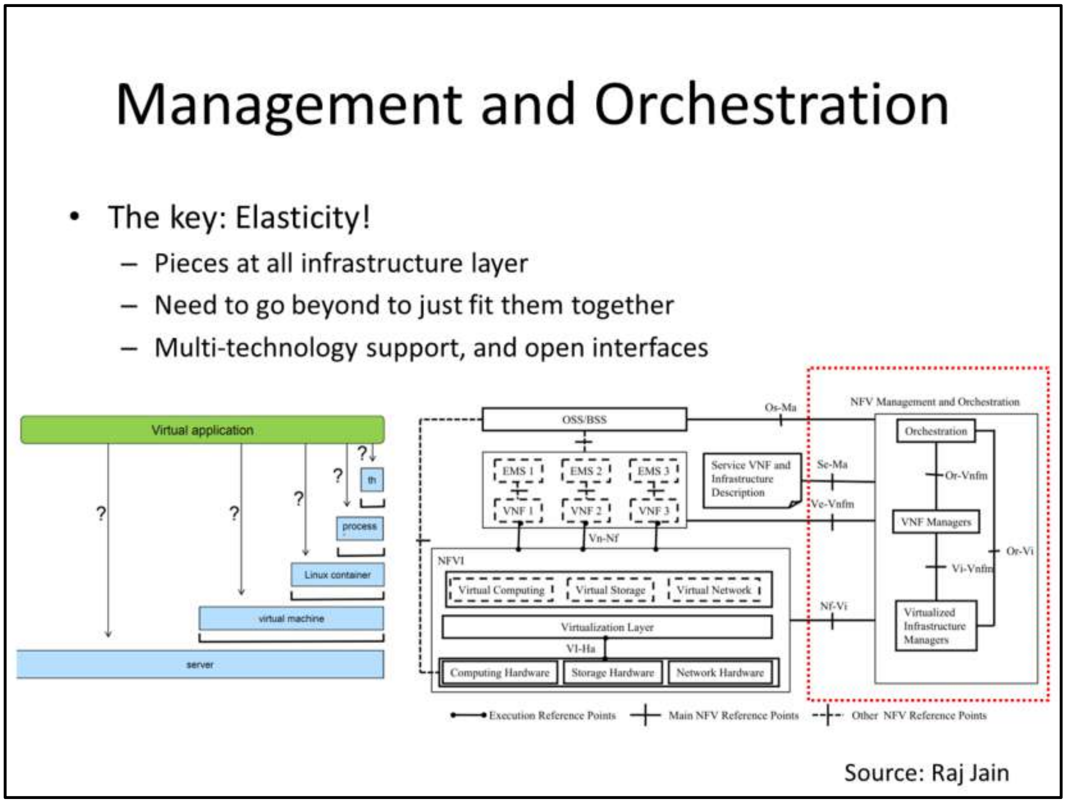


Figure source:
K. Samdanis, A. Kunz, M. I. Hossain, and T. Taleb, “Virtual bearer management for efficient mtc radio and backhaul sharing in lte networks,” in Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on, Sept 2013, pp. 2780–2785.

In an overall perspective, we abstract management and orchestration tasks in such a way that they must comply with different network environments and fulfill its tasks in accordance with SLA requirements which in a desired view can be viable end-to-end. Manage different network environments with heterogeneous VNFs profiles and policies poses as a huge challenge to NFV, as the distribution of functions and state depends on SLAs, service continuity requirements, and a well established Network Information Base (NIB).



Networks PoPs and datacentres intra- and inter-communications will be critical to guarantee network service elasticity and network plasticity

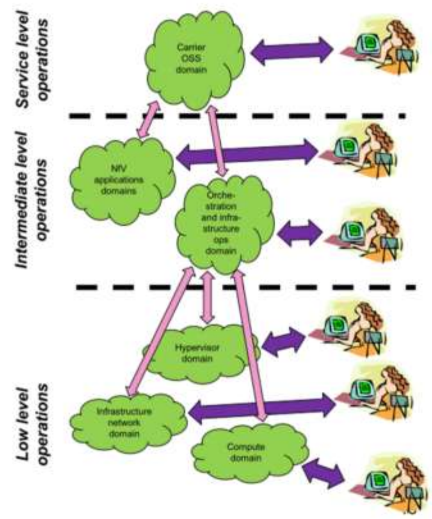


Figures source: Raj Jain Intro to NFV (http://www.cse.wustl.edu/~jain/cse570-13/ftp/m_17nfv.pdf)

Another bigger challenge to NFV regards to management and Orchestration tasks. They are presented as a key feature in NFV because as we can see in the figure above, they can act in different interfaces all over the different layers framework architecture, such as they have no limitations considering their operations domain (e.g., server, virtual machine, linux container, process, etc). Their interfaces will hardly depend on multi-technology support and probably open interfaces to perform tasks in hardware, NFVI and VNFs layers.

Orchestration

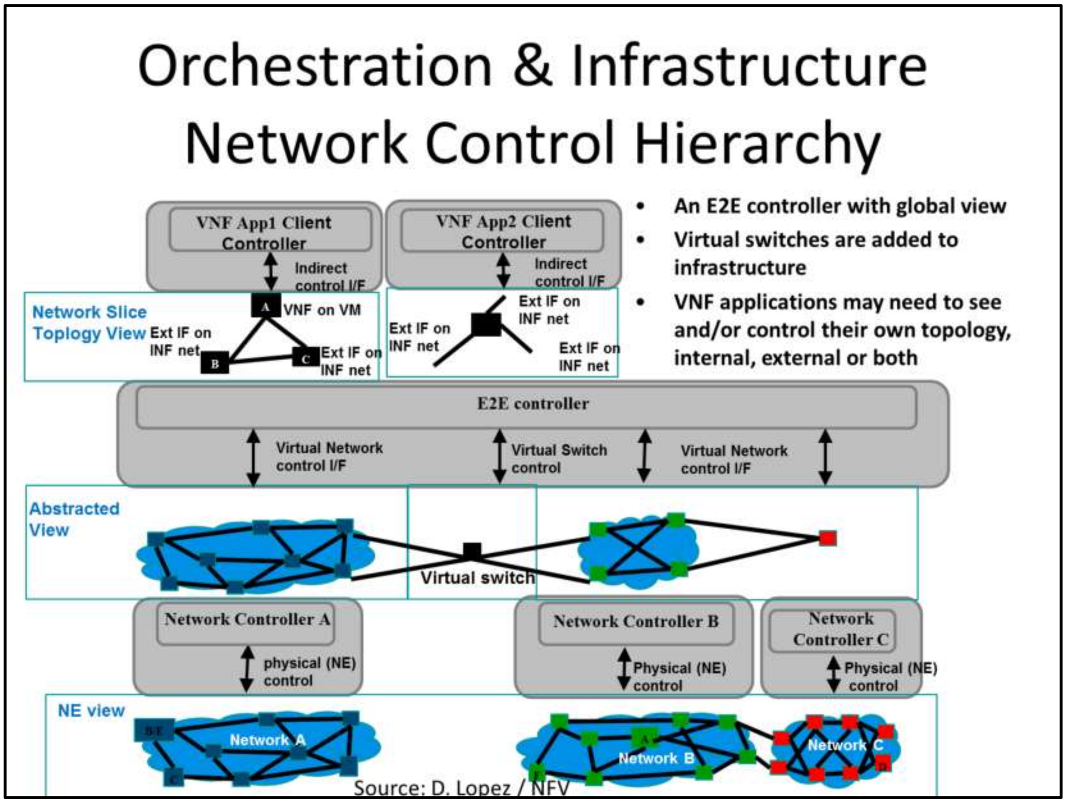
- Automated deployment of NFV applications
  - OpenStack, CloudStack...
- NFVI profile for NF
  - Select and start host, VM
- Applications (NFs)
  - Service address
  - Location specific configuration



Source: Bob Briscoe, BT

Figure source: Bob Briscoe, BT (Presentation Network Functions Virtualisation)
VNFs intances can be implemented on different physical resources, e.g. Compute resources and hypervisors, and/or be geographically dispersed as long as its overall end-to-end service performance and other policy constraints are met.

In the sense to achieve automated NFV applications by platforms like OpenStack, an orchestration domain have to effectuate tasks in different levels of operations. For instance, considering an existing profile list for NFs, construct an OSS/BSS user service requires intermediate level operations (e.g., NFV applications domain instantiations) where servers/VMs can be selected and implanted to carry out VNFs applications with specific service addresses and location dependent configurations. These last ones consist of low level operations executed to satisfy all the other performed tasks at higher level domains.



Source: Lopez, D.R., "Network functions virtualization: Beyond carrier-grade clouds," *Optical Fiber Communications Conference and Exhibition (OFC), 2014* , vol., no., pp.1,18, 9-13 March 2014

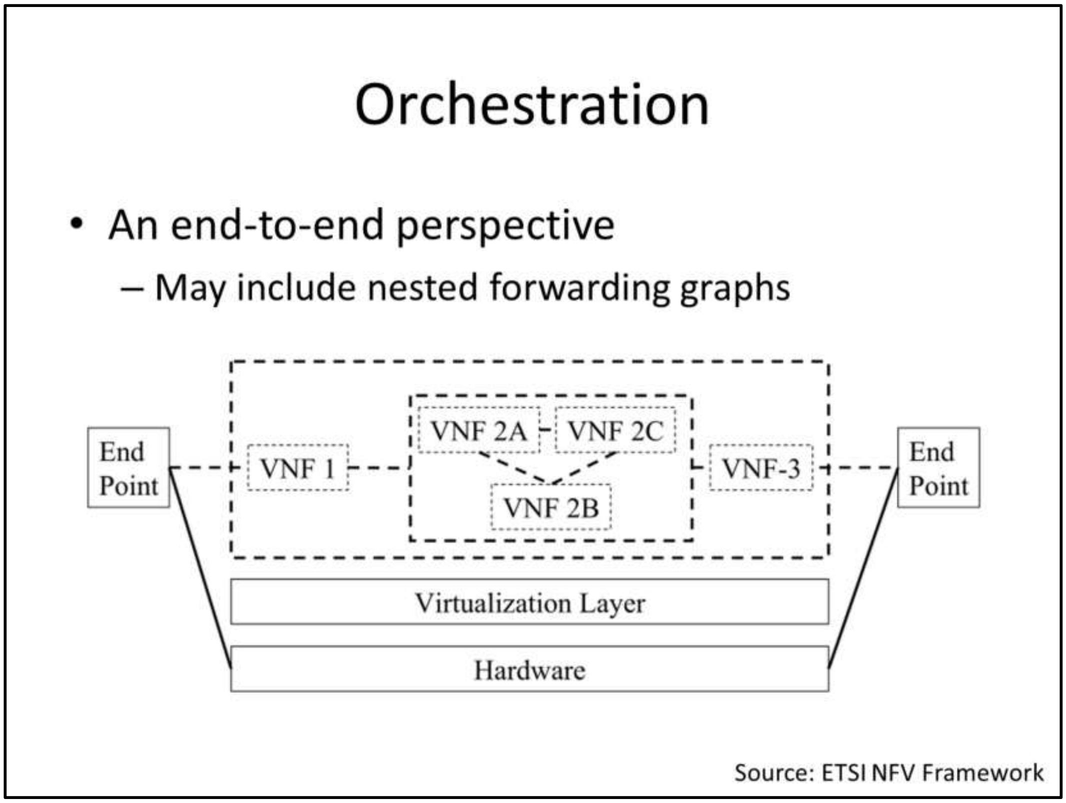


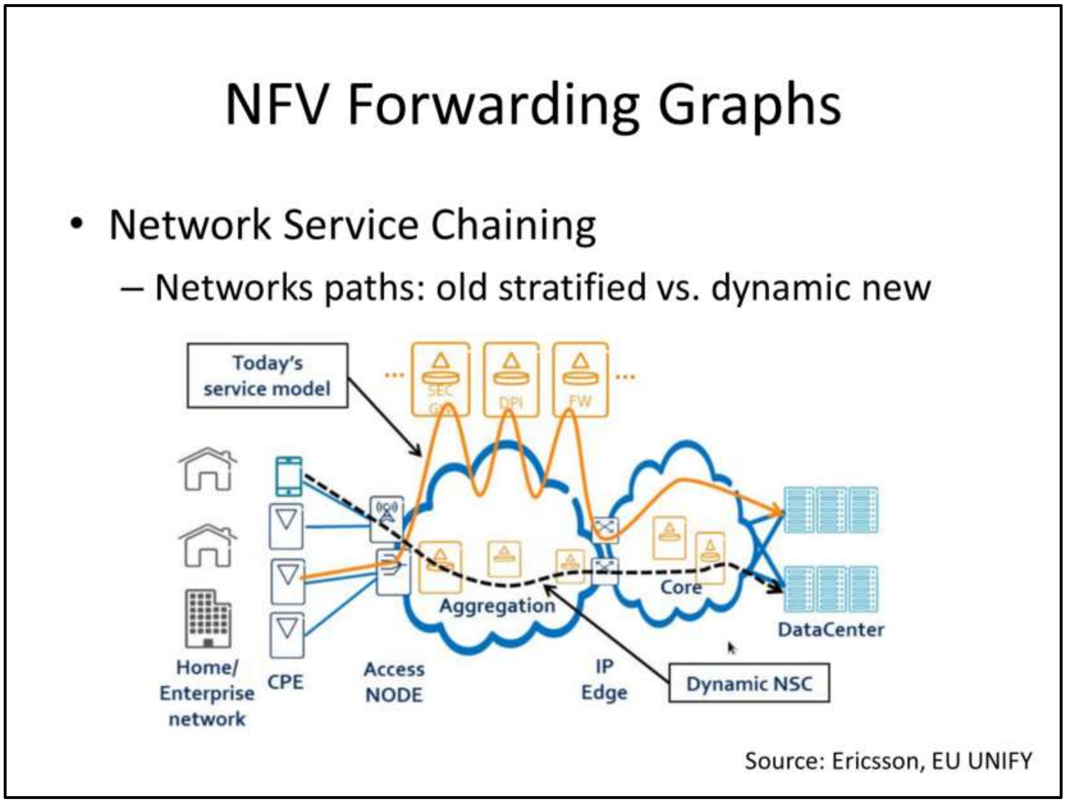
Figure source: ETSI NFV Framework Document (http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf)

One main aspect regarding orchestration challenges is the end-to-end perspective, which dictates a complex environment where VNFs can coexist in nested services and even in nested VNFs that can be chained to accomplish an end-to-end forwarding graph and operating in different NFV layers, as we can see above.

Service Chains | VNF Forwarding Graphs

- **VNF FGs** are the analogue of connecting **existing Physical Appliances** via cables as described in the NFV
- Cables are **bidirectional and so are** most data networking technologies that will be used in **Virtualized deployments** in the near term (e.g. Ethernet).
  - In other words, a VNF Forwarding Graph provides the logical connectivity between virtual appliances (i.e. VNFs).

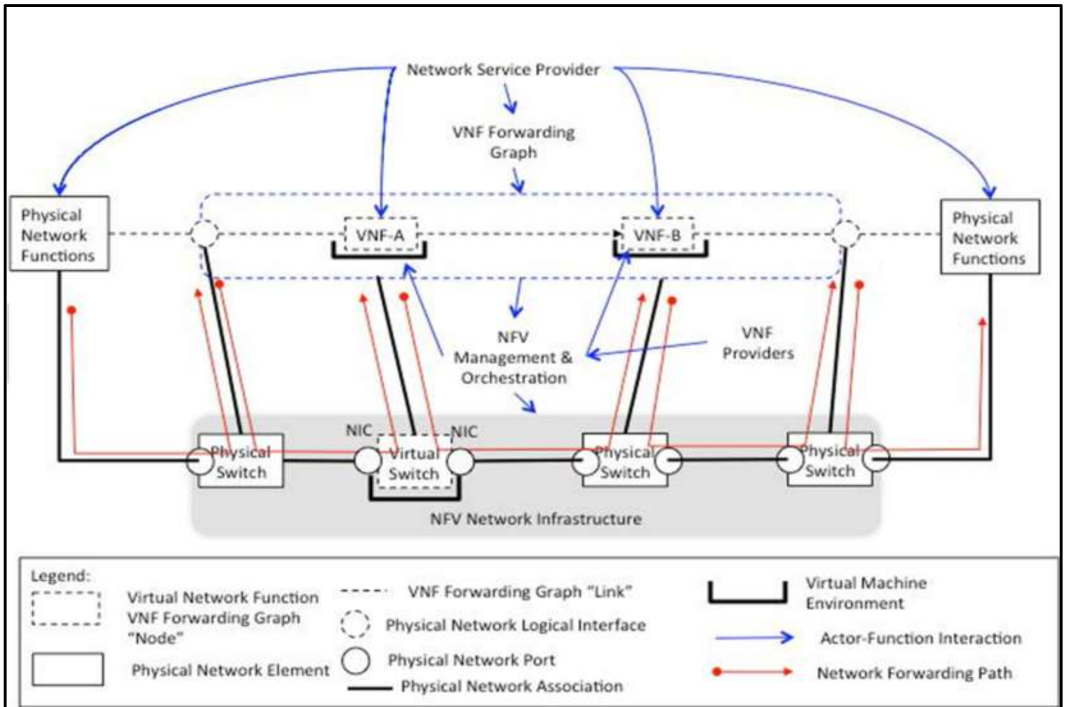
An abstract Network Service (NS) based on VNFs seems likely to include identification of the types of VNFs involved, the relationships between these VNFs and the interconnection (forwarding) topology along with related management and dependency relationships. Of course, VNF FG can also interconnect with Physical Network Functions to provide a NS.



The NFV FG is an expansion (and replacement for) the "Service Chain" defined in Software Defined Networks (SDN). The NFV FG provides an abstraction to the operator for dynamic and simplified service composition.

Figure source:
John, W.; Pentikousis, K.; Agapiou, G.; Jacob, E.; Kind, M.; Manzalini, A.; Risso, F.; Staessens, D.; Steinert, R.; Meirosu, C., "Research Directions in Network Service Chaining," *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for* , vol., no., pp.1,7, 11-13 Nov. 2013

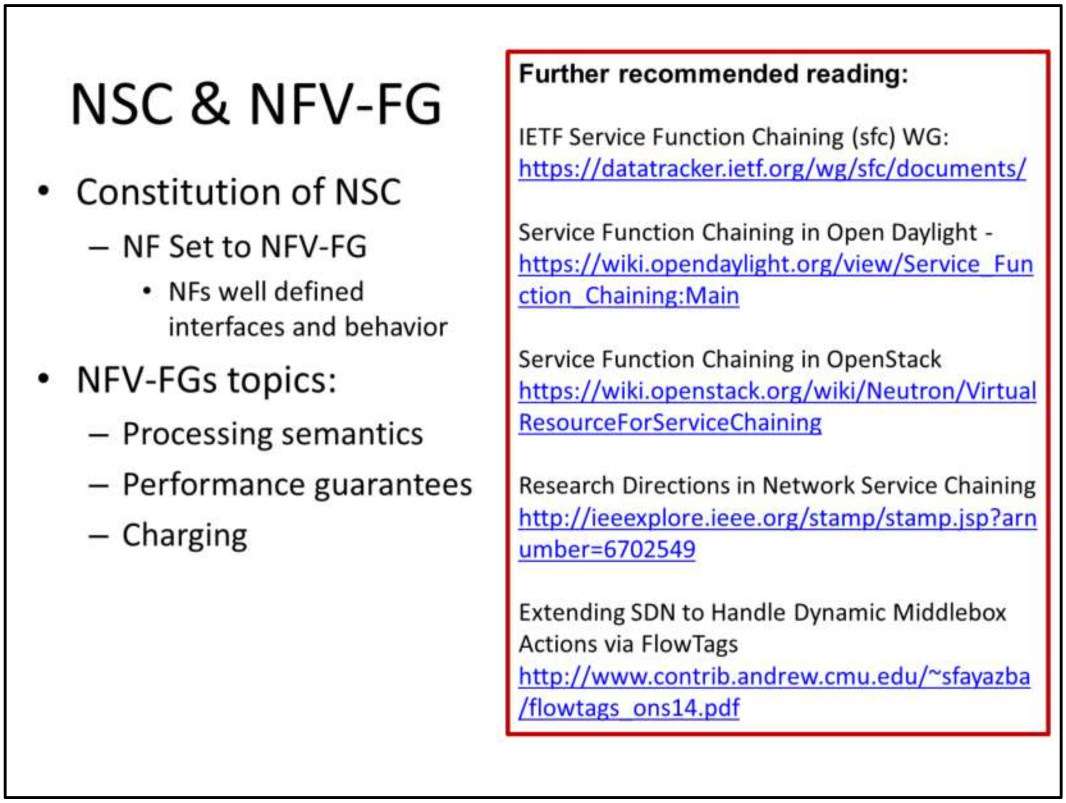
As our first challenge perspective, we present a simple example how we could introduce dynamic network paths around the Internet. As an old stratified and current network service chaining model, filled with static black boxes (middleboxes) defining a rigid sequence to process network packets, causing overhead, ossification and non improvement of network functions over the Internet. On the other hand, we see one possible way, a dynamic NSC model, where network functions can take placed all over the constitution of a dynamic path inside the Internet, creating well established end-to-end services to respect SLAs and perform better development and less time to implant network functions and applications.



Source: ETSI NFV UC

VNF FG From Logical to Physical View

When a network service is provided, the NFV framework needs to keep a record of the infrastructure resources that are used so that future operational processes (such as localization of a fault, restoration, resizing or termination of the service) can be undertaken on all relevant objects in the VNF FG.



Nothing sounding as good as it looks like could come for free.
Here are some topics following the challenges of NSC and NFV-FG:
In the first part the passage between NF Set and NFV-FG defines the existence of NFs with well defined interfaces and behavior, so that they can communicate and establish service chaining with specific performance, security, resilience, and many other challenges that still will be presented ahead.
In addition, processing semantics between NFs must be well stablished, because one NF cannot cause misbehavior of others NFs operations, likewise performance guarantees and charging.
There are a number of ongoing research efforts at diferente fronts (IETF, OpenDaylight, OpenStack, OPNFV, Academia)

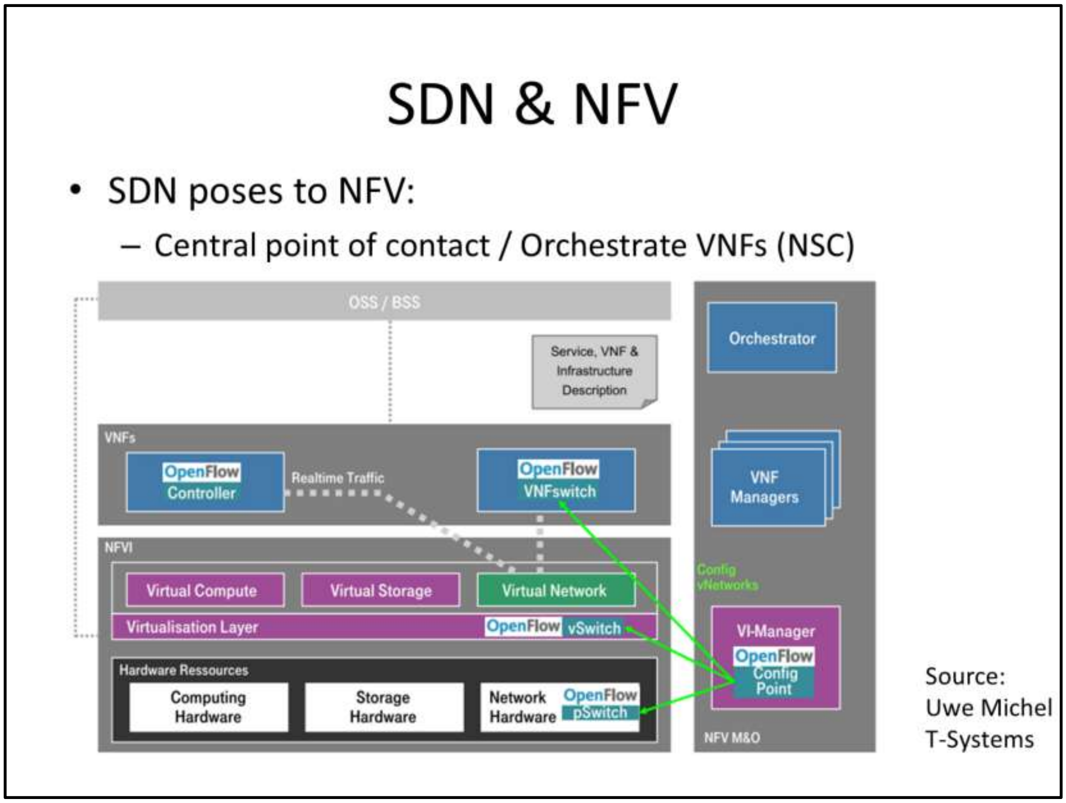
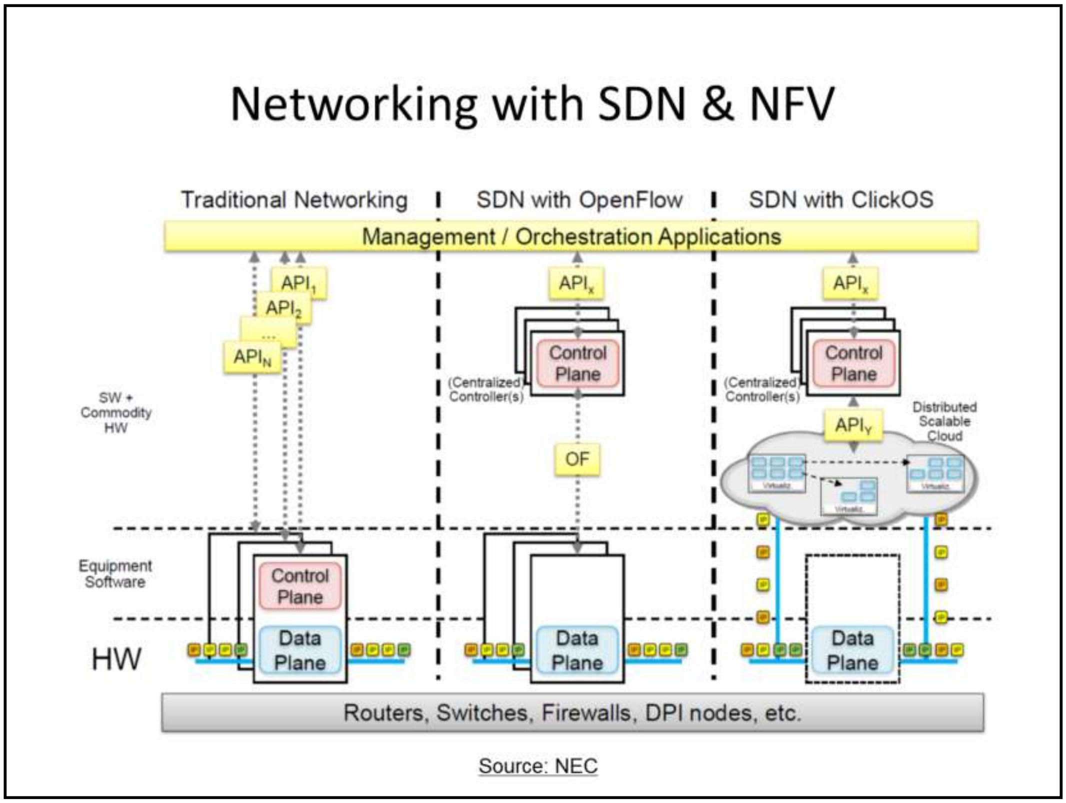


Figure source: Uwe Michel, T-Systems Multimedia (Presentation SDN and NFV How things fit together)

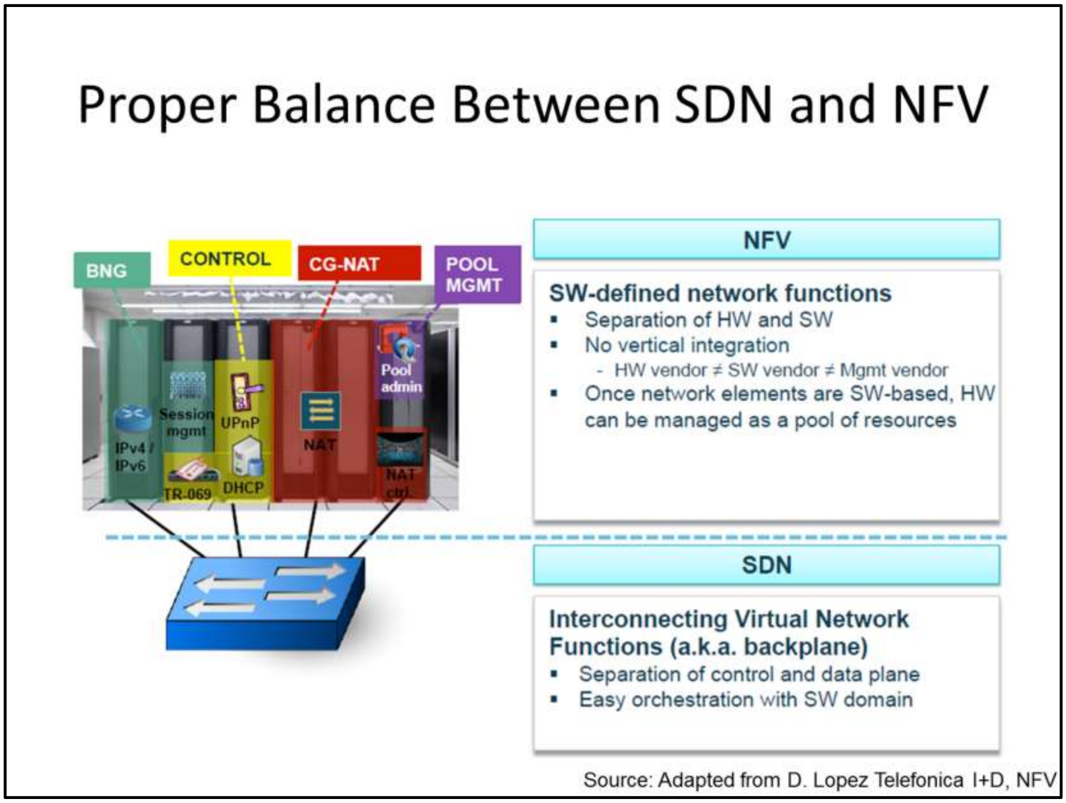
SDN and NFV are independent. While SDN intends to autmate and orchestrate network configurations, NFV proposes to automate the implantation and control of network functions.
In an intersections point SDN poses to NFV as a means to provide orchestration and management of NFs, connecting them togheter so that Network Service Chains can ocurr and perform different tasks all over the NFVI domain, including the execution/existence of end-to-end services.



SDN allows to remove the control plane from the data plane equipment and uses a standard interface (e.g., OpenFlow) to push data plane rules and to encapsulate control plane relevant packets.

NFV and SDN are independent and complementary. You can do either or both (as in the SDN with C

Introducing NFV into the SDN scenario, as proposed by NEC with thei ClickOS NFV Implementation allows to selectively steer some of the traffic to be handled by the SW-based NFV functions while the remainder traffic is handled by the HW data plane.



Leverage SDN for application-aware routing, and separation of packet forwarding from control to rapidly introduce new services and adapt to changing traffic patterns
Network functions, caching, applications, enablers all run in virtualized distributed data centers
IP & transport infrastructure still used as necessary in optical backbone and Internet

Portability

- Move VNF across N-PoPs
- Decoupled NFV framework from NFVI
- Optimize VNF resources:
  - Location
  - Allocation
  - Reservation
- Compatibility
  - Integration/internetworking
  - Meeting SLA requirements
- Example: NfV hypervisors

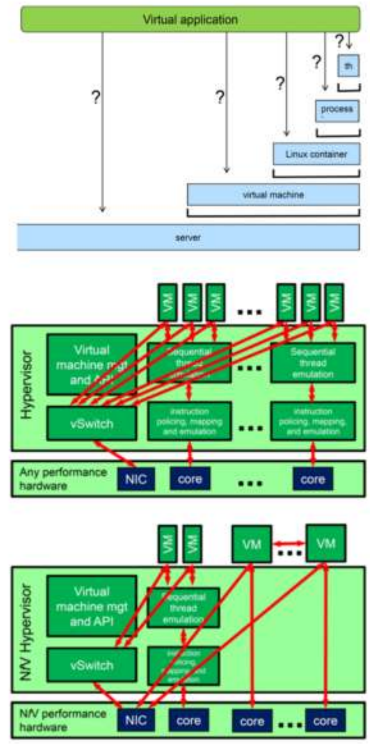


Figure source: Bob Briscoe, BT (Presentation Network Functions Virtualisation)

A general NFV framework requirement says that VNFs have to be portable across N-PoPs, which properly requires a NFVI decoupled from VNF applications. Consequently, as in the computing domain (e.g., VMs being allocated and migrated between servers), VNFs need a well behaved environment to be located, allocated and with reserved resources so that their correct operations can be accomplished.
The questions regarding portability challenges not only include the statements above as well determine compatibilities against heterogeneous technologies to VNFs and NFVIs integration/internetworking meeting SLA requirements. For example, NfV hypervisors can be used to conduct VMs direct access to NICs and processing Cores to optimize their tasks, allocating computing and network resources in accordance with their needs.

Interoperability and Legacy Networks

- End-to-end network services
  - Transparent management and orchestration
- No place for one-size-fits-all solutions
  - Dynamic and heterogeneous new technologies
- Handle different old and new characteristics
  - Impact on the other requirements:
    - Performance, resilience, security...
- Maintain SLAs
- Avoid disruptions!

NFV cannot be implanted as a disrruptive measure. For instance, telecom industries applied huge financial resources into expensive LTE devices aiming long-term capital return. Implement NFVIs and VNFs inside current network domains imposes interoperability requirements to NFV, which concerns one of its main challenges. Legacy networks are far way to be extint, launching no place for one-size-fits-all solutions, because new and dynamic technologies tend to evolve quickly while legacy devices and interfaces slowly walk to be updated. Besides, all the interfaces that would be required to create such solutions would have to handle different old and new characteristics which mainly impact performance, resilience, security and many other NFV requirements and possibly concatenate another challenges.

Resilience

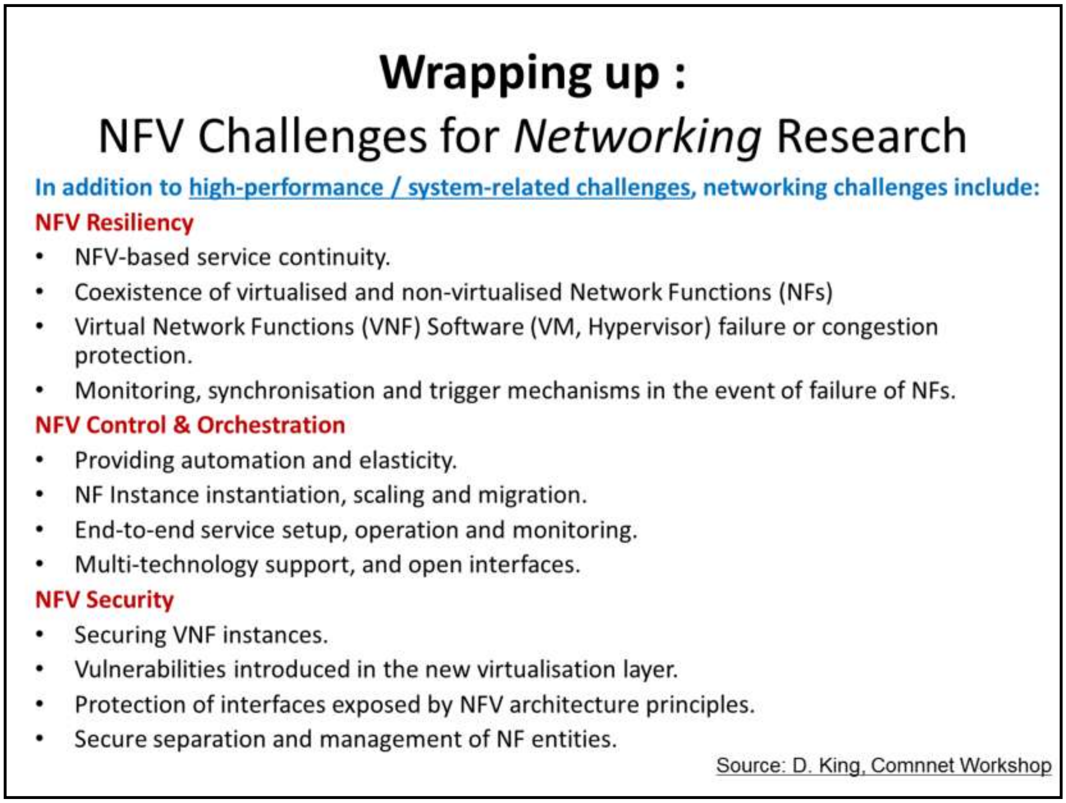
- Different Levels
  - PFs, NFs, NFVI, NFV-FG
- Monitoring, synchronisation and trigger mechanisms in the event of failure of NFs
- Correlated failures in NFV-FG
  - Chained resilience plans
- Service Continuity
  - SLA minimum insurance
    - Zero impact vs. Measurable impact
- Orchestration: NOT a single point of failure

Considering well specified (e.g., interfaces and behavior) NFs, a proper challenge that already exists in current networks is resilience. NFV will require more specific resilience metrics, such as it provides different levels of operation to attend service requirements. Then, PFs, NFs, NFVI, NFV-FG and many other instances of NFV will require their own resilience specifications. In all NFV levels of operation, as a requirement, monitoring, synchronisation and trigger mechanisms in failure events must satisfy SLA service requirements to be maintained by management and orchestration tasks to perform service continuity, with zero vs. measurable impact insurance. Of course, as a main point of execution and control of a whole NFVI/N-PoP management and orchestrations parts cannot be a single point of failure.

Security

- New Threats
  - Virtualization Network Layer
  - Several identity layers and accounting
- Protection of interfaces exposed by NFV architecture principles.
- Secure separation and management of NF entities.
- Heterogeneous network domains
- NFVI shared resources
  - Isolation of VNF sets
  - User privilege resources access (APIs)
- Mechanisms:
  - Control and verify the configuration of soft/hardware

New virtualization layers impose new security requirements, where NFs in different NFV management and orchestration layers can have their access provided to different network operators tasks. Accounting for those layers and role based access is a required security feature as different interfaces provide features access to different levels of operations exposed by the NFV framework model.
Commoun heterogeneous network domains still poses today as one challenge for network security operators and consequently will also impose bigger challenges as virtualization layers will reside inside them. Isolation between VNF sets and VNF-FGs for different users and network operators implicate user privilege resources access (e.g., APIs) where SLAs can be maintained even multiple NFVIs coexist in a single N-PoP.
Of course, mechanisms to control and verify network configurations are an essential part of the management of security features for VNFs, NFVIs and N-PoPs, for example.



There are a number of technical challenges which need to be addressed:

• Achieving high performance virtualised network appliances which are portable between different hardware vendors, and with different hypervisors.

• Achieving co-existence with bespoke hardware based network platforms whilst enabling an efficient migration path to fully virtualised network platforms which re-use network operator OSS/BSS. OSS/BSS development needs to move to a model in-line with Network Functions Virtualisation and this is where SDN can play a role.

• Managing and orchestrating many virtual network appliances (particularly alongside legacy management systems) while ensuring security from attack and misconfiguration.

• Network Functions Virtualisation will only scale if all functions can be automated.

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

• Integrating multiple virtual appliances from different vendors. Network operators need to be able to “mix & match” hardware from different vendors, hypervisors from different vendors and virtual appliances from different vendors without incurring significant integration costs and avoiding lock-in.

Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

Some insights on ongoing collaborative research projects

RESEARCH PROJECTS

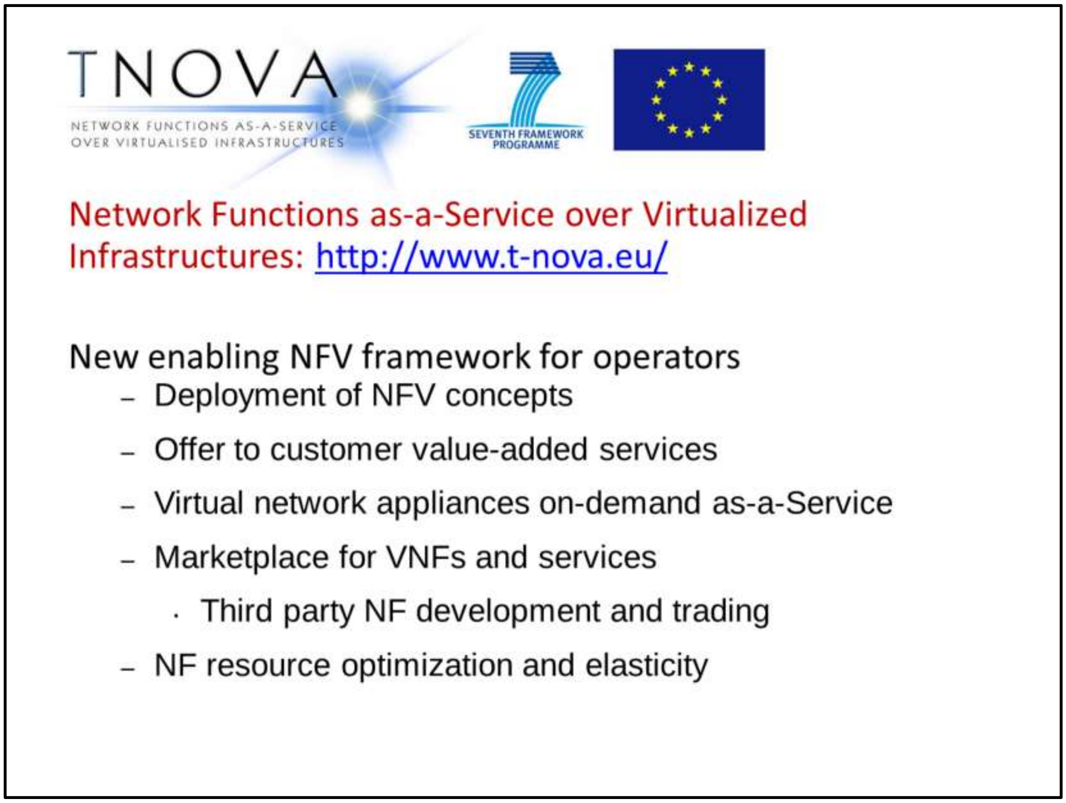
NFV Research and Education

Significant industry progress has been made to encourage growth of a commercial ecosystem for NFV, but research and education are also very important for overall and long term success.

NFV Research topics include:

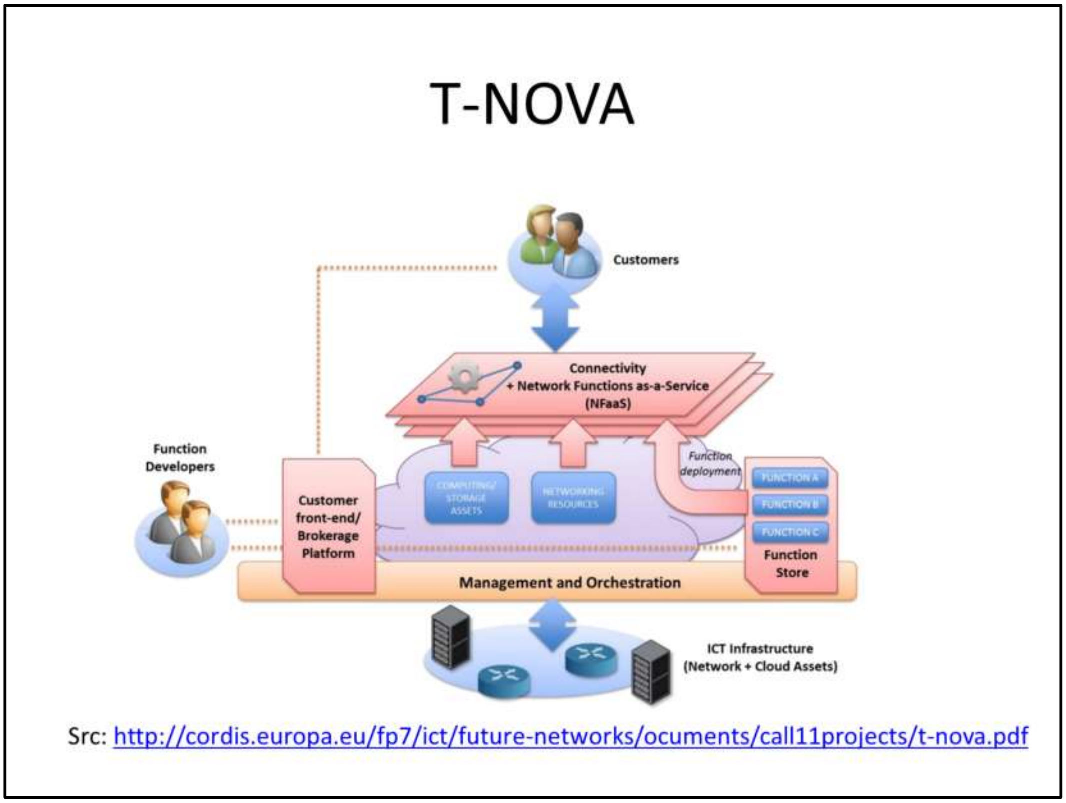
- Service chaining algorithms & NFV orchestration algorithms
- Abstractions for carrier-grade networks and services
- Performance studies (optimisation, scheduling, portability, reliability)
- Security of NFV Infrastructure
- Impacts of data plane workloads on computer systems architectures
- Applying compositional patterns (i.e. Network Function Chains) for parallelism
- Performance monitoring and reliability of network services
- Energy-efficient NFV architectures
- Service Assurance (e.g. test & diagnostics, predictive analytics, etc.)
- New requirements on the NFV Infrastructure for supporting new types of VNFs
- NFV Infrastructure federation
- New network topologies and architectures
- Tools and simulation platforms

Source: NFV White Paper #3 Page 15



T-NOVA will design and implement a management/orchestration platform for the automated provision, configuration, monitoring and optimization of Network Functions-as-a-Service (NFaaS) over virtualised Network/IT infrastructures. T-NOVA leverages and enhances cloud management architectures for the elastic provision and (re-) allocation of IT resources assigned to the hosting of Network Functions. It also exploits and extends Software Defined Networking platforms for efficient management of the network infrastructure.

Source: http://www.t-nova.eu/



The technical solution provided by T-NOVA addresses the following key issues:

- Automated provision of NFs via orchestrated management
- NF resource optimisation and elasticity
- NF performance optimisation
- Third-party NF development and trading

T-NOVA

Approction

- Address most of NFV design challenges
- NFV marketplace (plug-and-play NFs)
- Brokerage platform for best service bundles selection

Impact

- Boosting competitiveness (NFs in Function Store)
- Lower operator costs (CAPEX-to-OPEX transformation for more efficient planning)
- Promote EU standardization (e.g., ETSI)

In order to facilitate the involvement of diverse actors in the NFV scene and attract new market entrants, T-NOVA establishes a “NFV Marketplace”, in which network services and Functions by several developers can be published and brokered/traded. Via the Marketplace, customers can browse and select the services and virtual appliances which best match their needs, as well as negotiate the associated SLAs and be charged under various billing models. A novel business case for NFV is thus introduced and promoted.

Source: http://www.t-nova.eu/

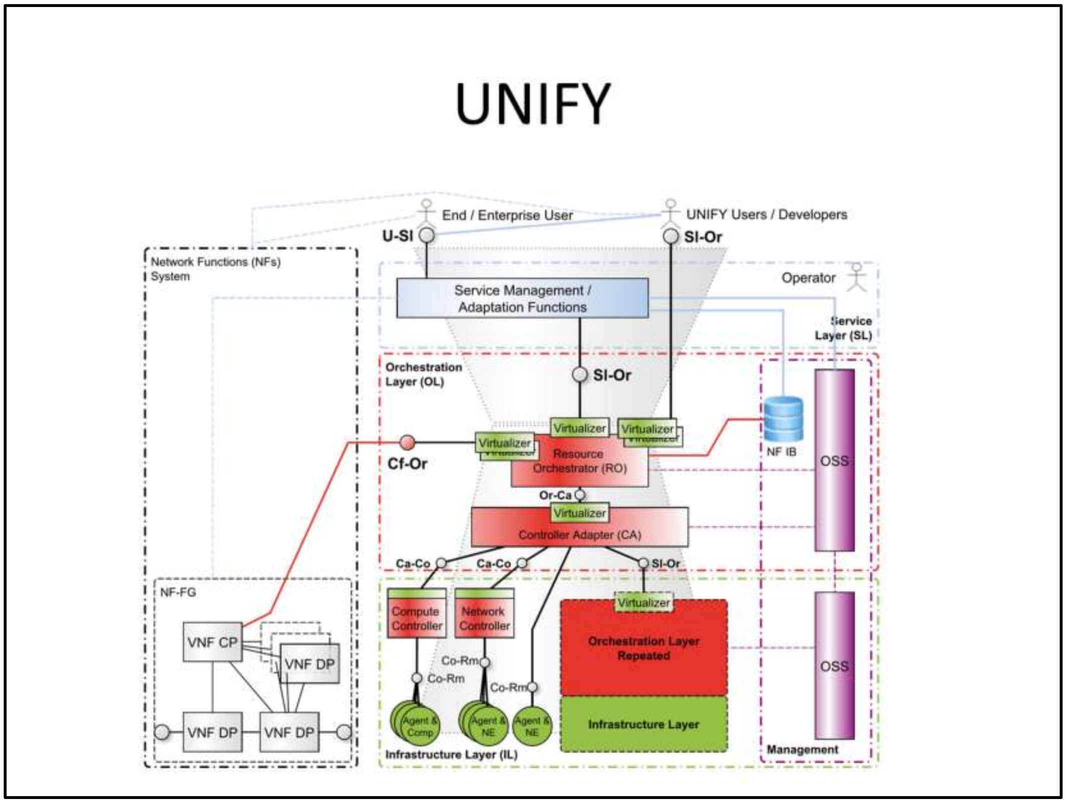
Source: http://www.t-nova.eu/

UNIFY

Architecture to unify carrier and cloud services

- **Service abstraction model** and an associated domain-specific service creation language and programming interfaces to automate and optimize the deployment of service chains
- **Advanced management and operation schemes** to cope with increased network/service agility and to handle network services end-to-end
- Design and performance of a **universal node** architecture based on standard x86 components and accelerators for network functions virtualization

It was identified that with combined abstraction of compute, storage and network resources one can logically centralize, automate and recursively apply resource orchestrations across domains, technologies, vendors etc. The UNIFY architecture implements such a combined abstractions of resources and allows the overarching optimization. Thus, the UNIFY architecture enables automated and recursive resource orchestration and operation with domain virtualization similar to the recursive network-only virtualization of the Open Networking Forum (ONF) Software Defined Networking (SDN) architecture but also for European Telecommunications Standards Institute (ETSI) Network Function Virtualization (NFV) services. The defined architecture also considers the demands of a Service Provider DevOps (SP-DevOps) regime. Along the monitoring, Verification and Troubleshooting needs of operation in carrier environments, SP-DevOps includes support for Network Function (NF) development. The applied virtualization and orchestration concept is independent of resource or domain size, technology, and hence works from a single node, e.g., the Universal Node (UN) concept, to complete multi technology carrier environments. Moreover the logical centralization of joint compute and network resource orchestration enables direct control and elastic scaling of resources for the deployed NFs



In the UNIFY architecture: • three layers (service, orchestration and infrastructure) and a set of reference points have been defined; • a general information model describing the most important reference points has been identified; • a Network Function Forwarding Graph (NF-FG) for programming resource orchestration at compute, storage and network abstraction, in accordance with the virtualization, monitoring functions and quality indicators for rapid and flexible service creation has been defined; • a programmable interface enabling a control and data plane split for network functions and dynamically control of their dedicated resources and management actions has been defined; • a monitoring framework to complement the quasi static virtualization views for fine granular observability of both virtualized infrastructures and NF-FG-based services has been defined; • a model-based service decomposition in order to be able to re-use and build services out of elementary (or atomic) blocks has been defined; • a definition and a frame how i) service programming, orchestration and optimization, ii) service provider DevOps and iii) commodity hardware based networking as well as execution environment can form a unified production environment have been defined; • a detailed functional architecture has been defined, covering all aspects framed in the overarching architecture including a description of the primitives at the reference points

UNIFY

Approach

- Service Programming, Orchestration and Optimization: NFs abstractions, description languages, algorithms for automated creation of service chains
- Service Provider DevOps: agile operations and development aids for dynamic service chains
- Unified Node Architecture (as an abstracted domain): based on commodity hardware

Impact

- Evolve impact of European community in standard organizations (e.g., IETF, ETSI, ONF)
- Unified service operator resources abstractions

Overall, the UNIFY design creates a unified production environment for rapid and flexible service creation through
joint resource virtualization and orchestration. While the ambition is similar to ETSI NFV, we believe that it is worth taking a different architecture approach by generalising ONF SDN principles. In this way, multi-level recursion and
better resource control of any NF which has split data- and control-plane promise to be benefits. Prototyping and
experimentation in both ETSI and UNIFY will foster our understanding of practical implications of the two different architecture approaches.
The information provided in this deliverable and the previously documented initial version of the architecture [D2.1]
cover all essential aspects of the UNIFY architecture. However, the on-going work and achieved results of the technical work packages will detail and verify individual aspects of this architecture.

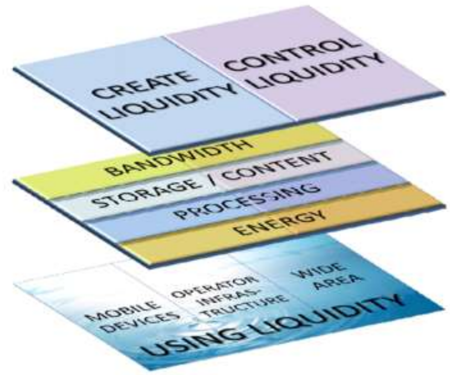
Trilogy 2

trilogy 2

Building the liquid network

http://trilogy2.it.uc3m.es

- Processing, storage, bandwidth and energy usage from different machines and different parts of the network
- Creating:
  - Cross layer liquidity, cross provide liquidity and cross resource liquidity
  - Means to control the created liquidity though the means of incentives, information exchange and enforcement tools



Src: http://cordis.europa.eu/fp7/ict/future-networks/documents/call8-projects/trilogy2-factsheet.pdf

Trilogy 2

Liquidities approaches

- Cross provider: pooling techniques for bandwidth, processing, storage and energy
- Cross-layer: optimize higher layers using low layers “interwork”
- Cross-resource: improve performance selecting best trade-off type of resource pools

Impact

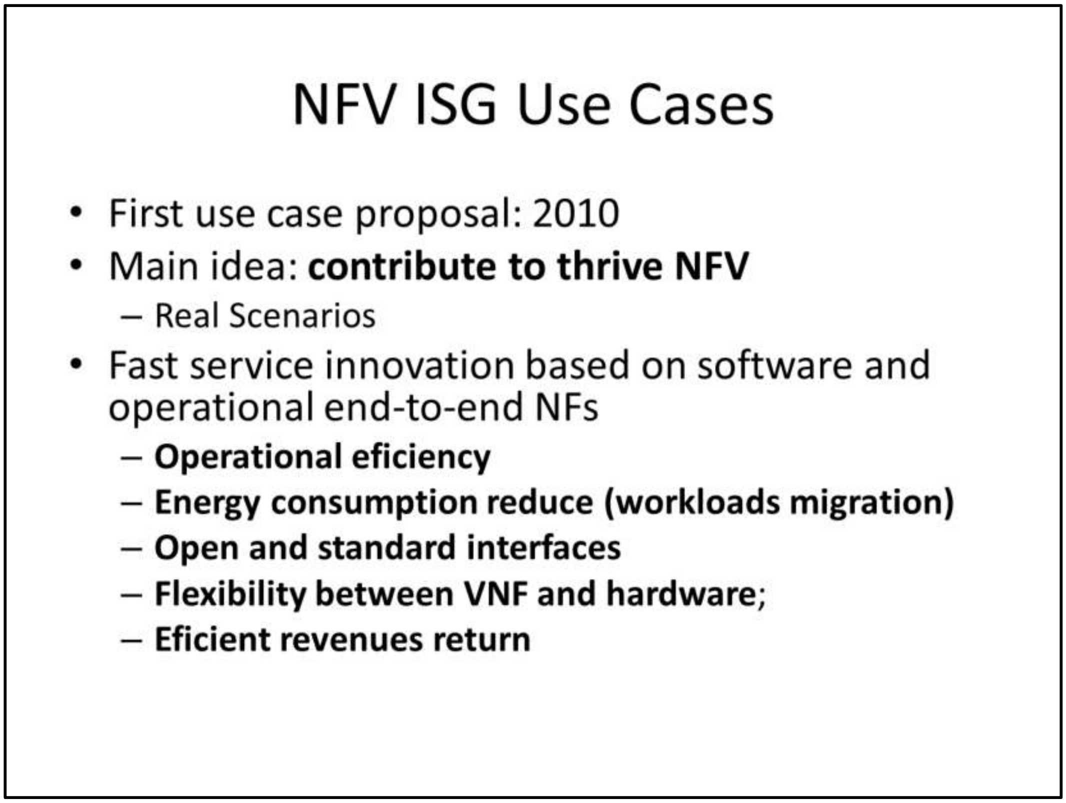
- Reduce supplier lock-ins and costs
- Collaborative applications to optimize end-to-end communication
- Resources sharing among cloud service providers

Src: http://cordis.europa.eu/fp7/ict/future-networks/documents/call8-projects/trilogy2-factsheet.pdf

Use Cases

NFV

Based on ETSI GS NFV 001 v1.1.1 (2013-10)
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf



NFV – ISG - submit use case proposals and POCs
Similar to IETF, real scenarios and implementations drive innovation.
The idea is to spawn “fast service innovations” focused on show empirically “strong operation benefits” for providers

Use Cases Matrix

Cloud Use Cases	NFVIaaS (NFV Infrastructure as a Service) VNFaaS (Virtual Network Functions as a Service) Service Chains (VNF Forwarding Graphs) VNPaaS (Virtual Network Platform as a Service
Mobile Use Cases	Virtualization of Mobile Core Network and IMS Virtualization of Mobile Base Station
Content Delivery Use Cases	Virtualization of CDNs
Access/Residential UC	Virtualization of Home Environment Fixed Access Network Functions Virtualization

Use Case Matrix – 4 big large themes, and 9 related use cases

Reference: ETSI NFV UC

Currently, the proposed ETSI NFV use cases can be divided following this matrix.
4 large themes represent the typical cases presented in a carrier provider:
Cloud, Mobile, Content and Last-Mile Residential Access Services
In each large theme, an example of use-case

Reference ETSI NFV UC:
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

NFV Infrastructure as a Service (NFVIaaS)

- Cloud Computing Services are typically offered to consumers in one of three service models
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- **IaaS** is defined as the capability to offer to consumers processing, storage and **fundamental** computing resources
- Some literature also refers to a capability to offer network connectivity services as **Network as a Service (NaaS).** One application for NaaS appears to be the on **demand creation of network connectivity** between Cloud Service Provider and Customer

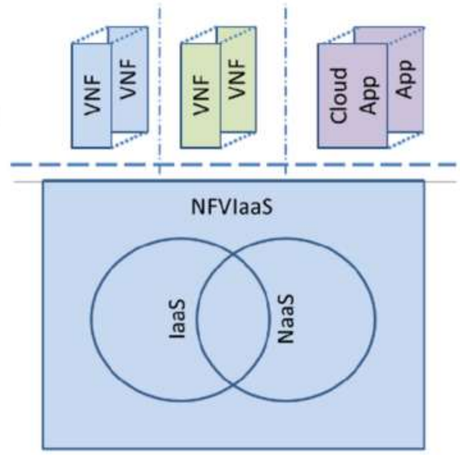
Reference: ETSI NFV UC

Analogous to the computing cloud services provided by AWS and the whole ecosystem on top.
Cloud services can be organized in categories depending on the granularity and management of resources
From the point of view of managing internal Networks, there are services like AWS Virtual Private Cloud
That allow tenants to configure and manage their own internal networks with IPs addresses, routing, NAT
This part can be described as Network as a Service (NaaS)

NFV Infrastructure as a Service (NFVIaaS)

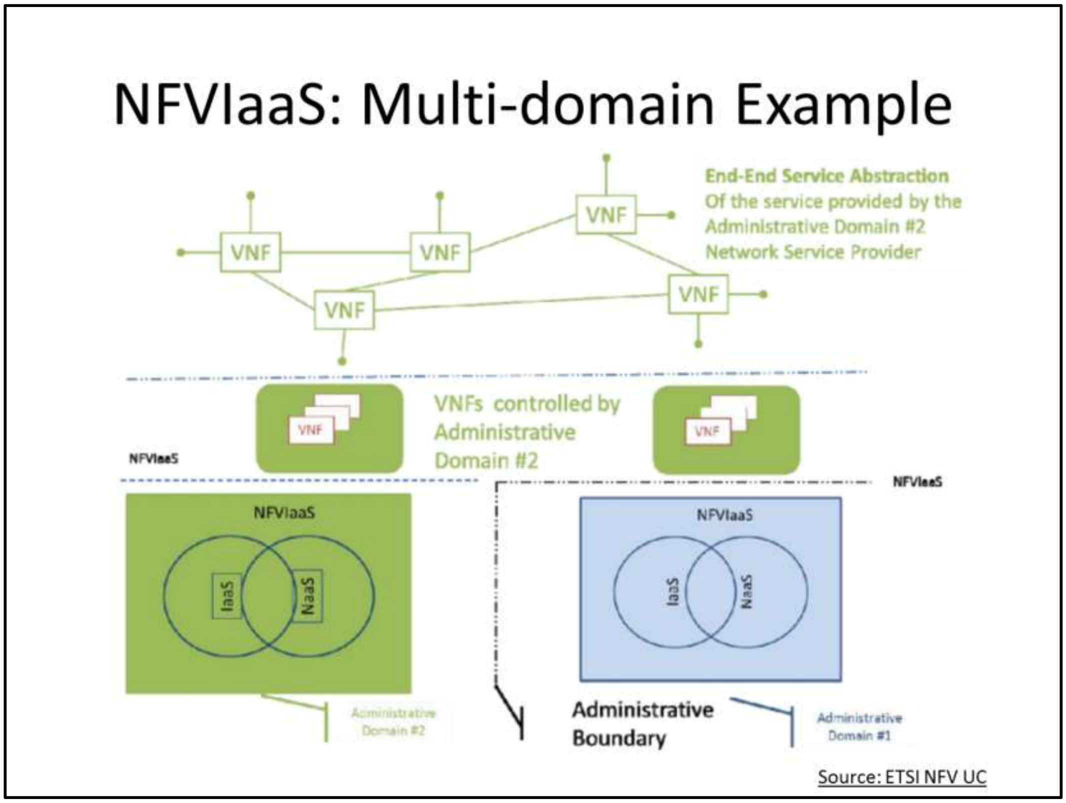
NFV Infrastructure :

- provide the capability or functionality of providing an environment in which Virtualized network functions (VNF) can execute
- **NFVIaaS** provides compute capabilities comparable to an **IaaS cloud computing service** as a run time execution environment **as well as support the dynamic network connectivity services** that may be considered as comparable to **NaaS**



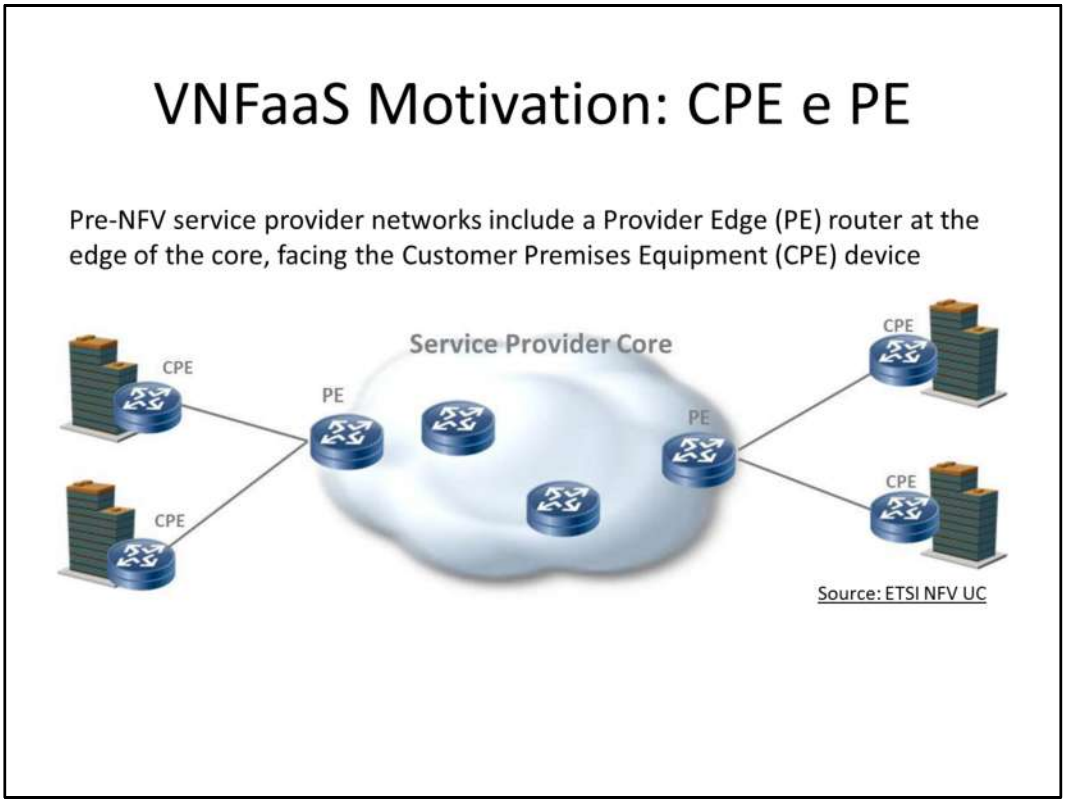
Source: ETSI NFV UC

From the point of view of NFV
The Network function have to run in some virtual infrastructure
Thus, the VNFs have to be constructed on top of computing,
storage and network resources, the last one in special (QoS, guarantees)

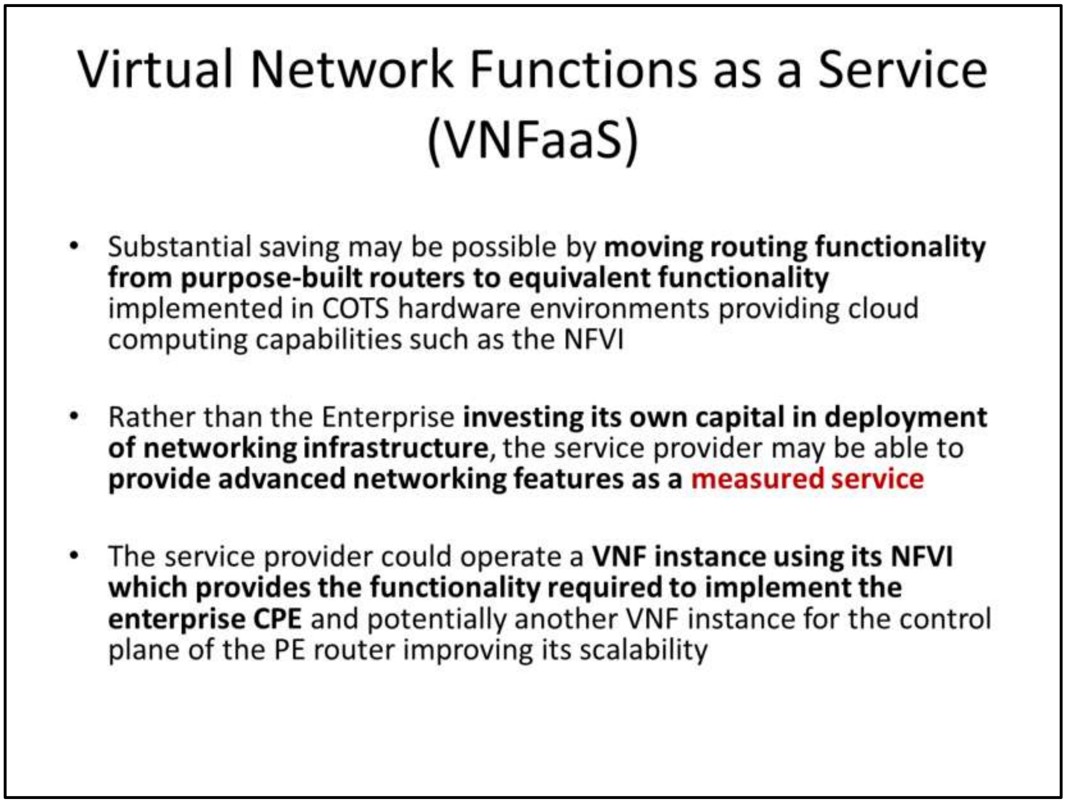


Example of an administrative domain #2 executing VNFs on the NFVI supplied by another domain #1.

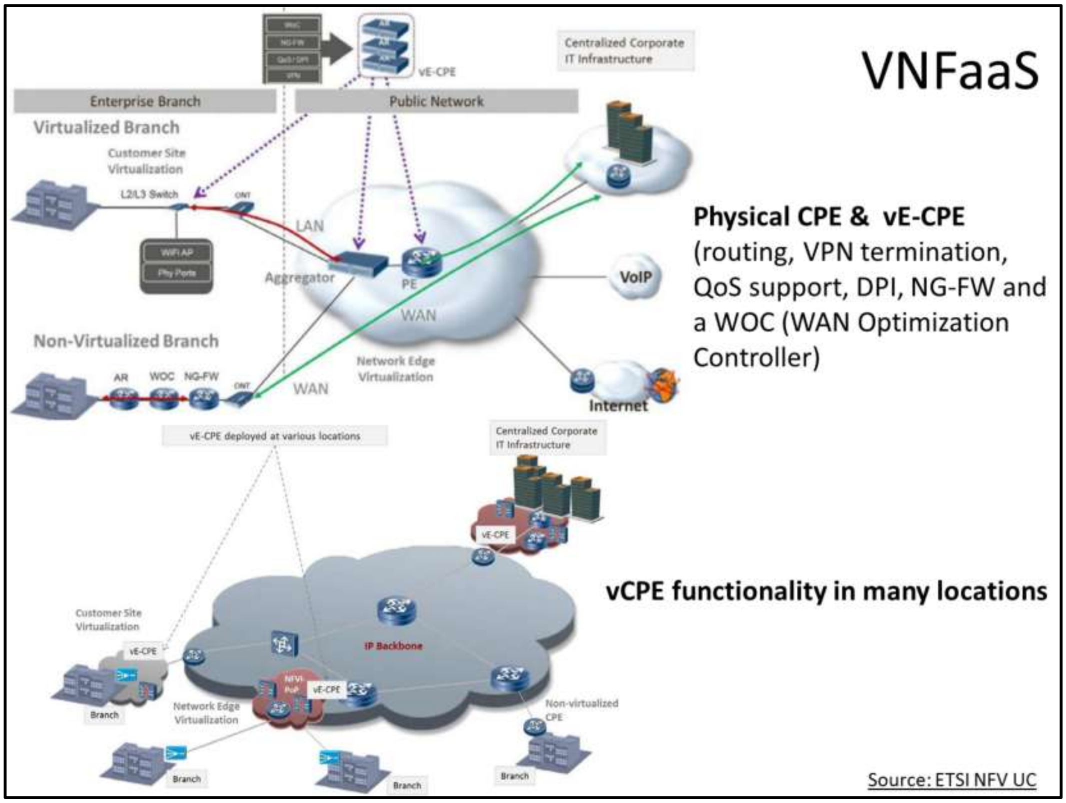
VNFs can be allocated from one to another service provider based on geographic locations, redundancy, latency and policies requirements.



Outsourcing alternatives for network services:
Many enterprises find the cost of a dedicated standalone appliance per-feature prohibitive, inflexible, slow to install and difficult to maintain. And as the enterprise continues to evolve, more services and applications migrate to the enterprise data center or public clouds, forcing a change in the way enterprise networks are built.



VNFaaS is analogous to Software as a Service
No need for the operator to acquire equipment or physical links
Ecosystem to evolve network functions independently from the infrastructure
The metric is a measurement of the network function use and QoS constraints



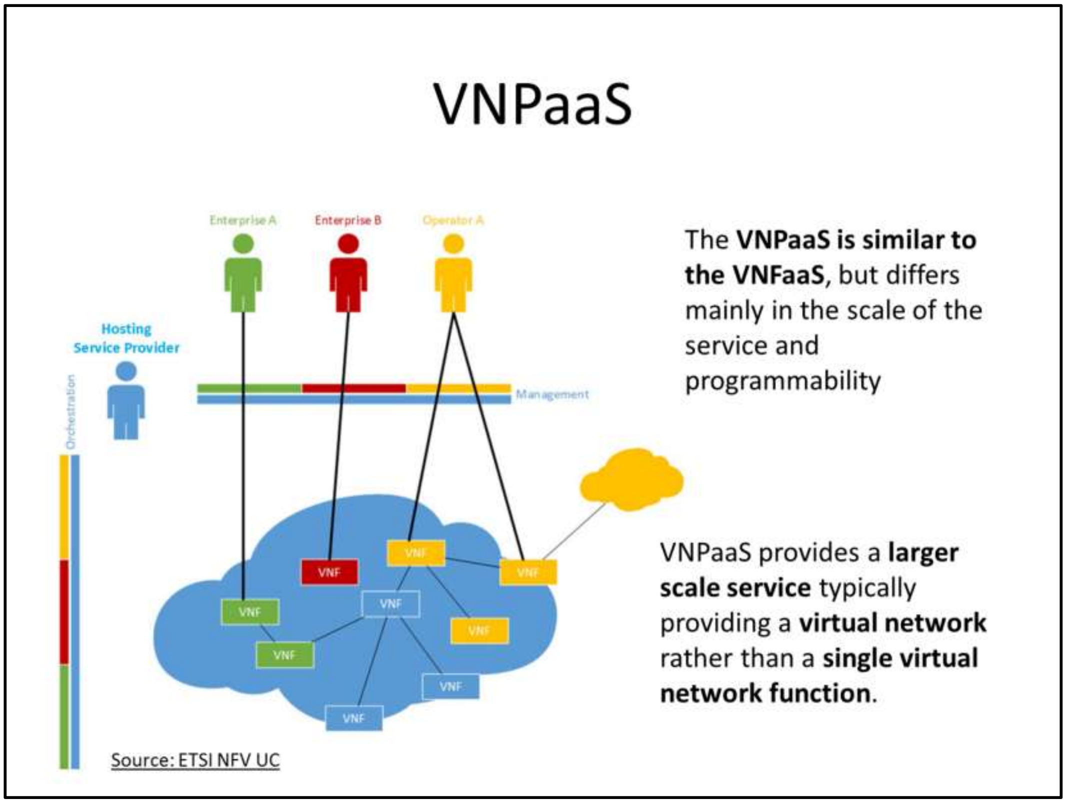
Advantages of VNFaaS:

- Modest software footprint for the enterprise to access the service
- Efficient use of software licenses
- Centralized management and data
- Savings in up-front costs

Virtual Network Platform as a Service (VNPaaS)

- Network resources are more and more **often not exclusively used** by the operator
- **Platform as a Service** (PaaS) as the possibility for the **consumer to deploy his own applications** using the computing platform supported by the provider
- Service Provider provides a **toolkit of networking and computing infrastructure as well as potentially some VNFs** as a platform for the creation of virtual network
  i.e. a **Virtual Network Platform as a Service**

In the simplest case, the services are under full control of the service provider, and thus very similar to hosted services. However, when providing certain interfaces to enterprises, they may deploy and/or manage services on their own based on their need within the limits of operator specified policies.
Platform as a Service in networking services provide toolkit APIs to create software defined network functions end-to-end



Issues:
To share infrastructure resources with third parties, 3 main requirements need to be fulfilled:

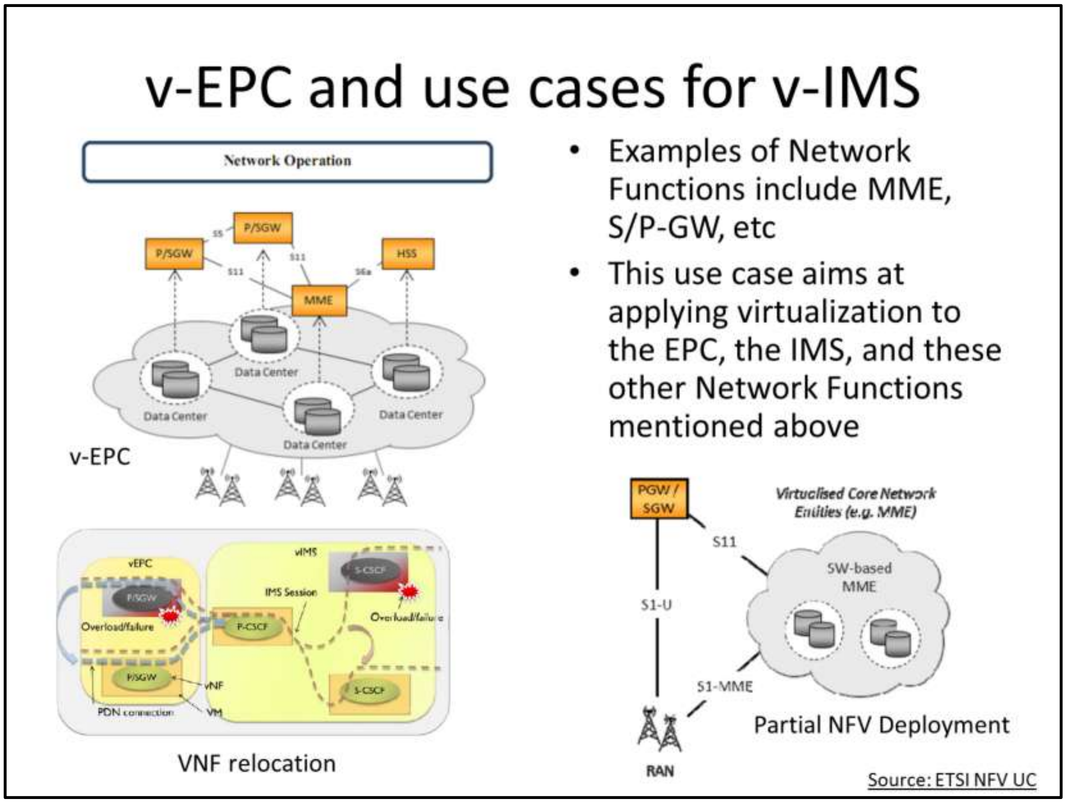
- Access control to API calls should be based on an authorized user identity
- Infrastructure resources need to provide mechanisms to separate workloads from different operators
- Infrastructure resources and network functions need o provide an interface to monitor , guarantee and limit the usage of the resource by each operator

Mobile Core Network and IMS

- **Mobile networks are populated with a large variety of proprietary hardware** appliances
- **Flexible allocation** of Network Functions on such **hardware resource pool** could highly improve network usage efficiency
- **Accommodate increased demand for particular services** (e.g. voice) without fully relying on the call restriction control mechanisms in a **large-scale natural disaster scenario** such as the Great East Japan Earthquake

Advantages:

- Reduce Total Cost of Ownership
- Improved network usage efficiency due to flexible allocation of different network functions on such hardware resource pool
- Higher service availability and resiliency provided to end users/customers by dynamic network configuration inherent to virtualisation technology
- Elasticity: capacity dedicated to each network function can be dinamically modified according to actual load on the network, thus increasing scalability
- Topology configuration: network topology can be dynamically reconfigured to optimize performance



EPC virtualisation: VNFs as HSS, P/SGW and MME can be virtualised and may scale independently according to their specific resource requirements (can require a different number of NFVI resources than data plane VNFs)

There might a situation where it is necessary to increase user plane resources without affecting the control plane and vice versa.
Inter operator connectivity and VNF FG are some potential issues for further study in this use case.

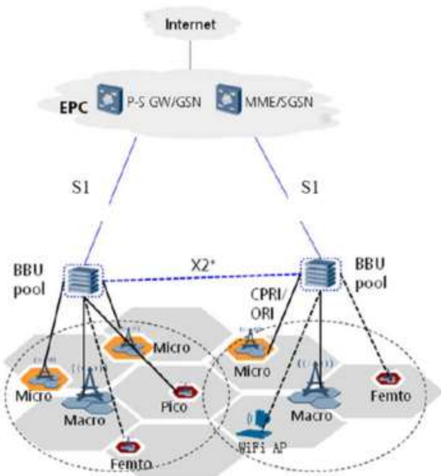
Virtualization of Mobile Base Station

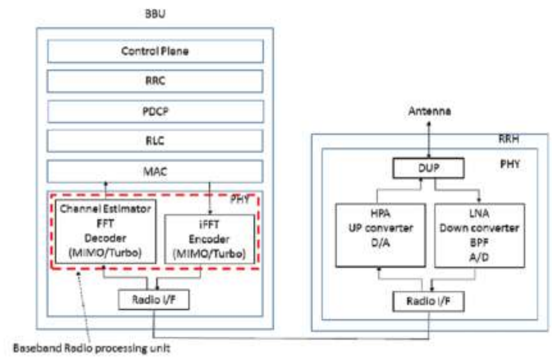
- **Mobile network traffic is significantly increasing** by the demand generated by application of mobile devices, while the **ARPU (revenue) is difficult to increase**
- **LTE is also considered as radio access part of EPS (Evolved Packet System)** which is required to fulfill the requirements of **high spectral efficiency, high peak data rates, short round trip time and frequency flexibility** in radio access network (RAN)
- **Virtualization of mobile base station leverages** IT virtualization technology to realize at least a part of RAN nodes onto **standard IT servers, storages and switches**

Motivation of Virtualization in Mobile Base Station

- Increasing demand
- Stringent computational requirements (planned on max capacity)
- consolidation

Virtualization of Mobile Base Station





Functional blocks in C-RAN

LTE RAN architecture evolution by centralized BBU pool (Telecom Baseband Unit)

Source: ETSI NFV UC

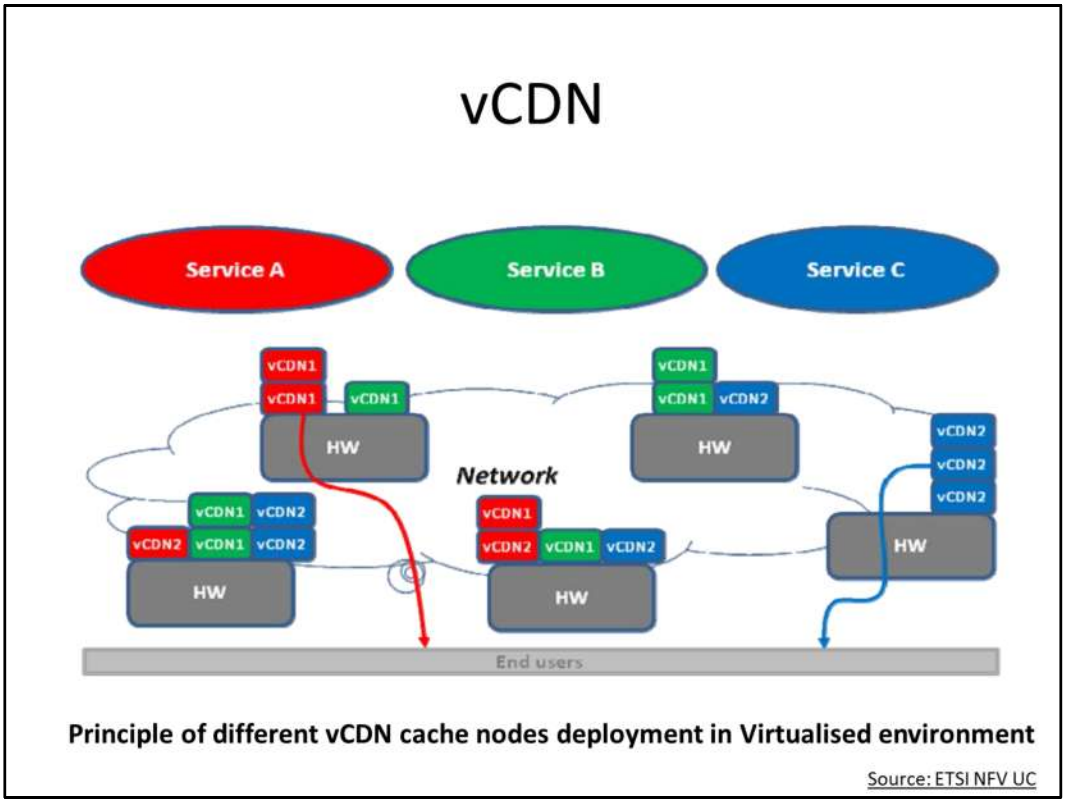
Coordinated multi-point transmission/reception (CoMP) is a technology to enhance the LTE system performance by dynamic coordination or transmission and reception between UE (User Equipment) and multiple geographically separated eNodeBs. The most sophisticated CoMP schemes for uplink require UE data and channel information to be shared among Base Stations (BSs) and, high bandwidth and low latency interconnection for real time cooperation among these should be supported on the virtualised environment. NFV should facilitate such a solution.

Virtualization of CDNs

- **Delivery of content, especially of video, is one of the major challenges** of all operator networks due to massive growing amount of traffic to be delivered to end customers of the network
- **Integrating nodes of Content Delivery Networks** into operator networks can be an effective and cost-efficient way to answer to the challenges of Video Traffic Delivery
- **CDN providers ask operators to deploy their proprietary cache nodes into the ISP network** (e.g. Netflix OpenConnect program, Akamai Aura CDN). This comes with **benefits for both sides** but also with the challenge that eventually the **operators will host a zoo of different cache devices** side by side in their premises

Motivation, nowadays disavantages:

- The capacity of the devices needs to be designed for peak hours. During weekdays and business hours, the dedicated hardware appliances and CDN servers are mainly unused
- It is not possible to react on unforeseen capacity needs, e.g., in case of a live-event as hardware resources need to be deployed in advance
- Dedicated physical devices and servers from several parties drive the complexity of the operator network and increase the operational expenses



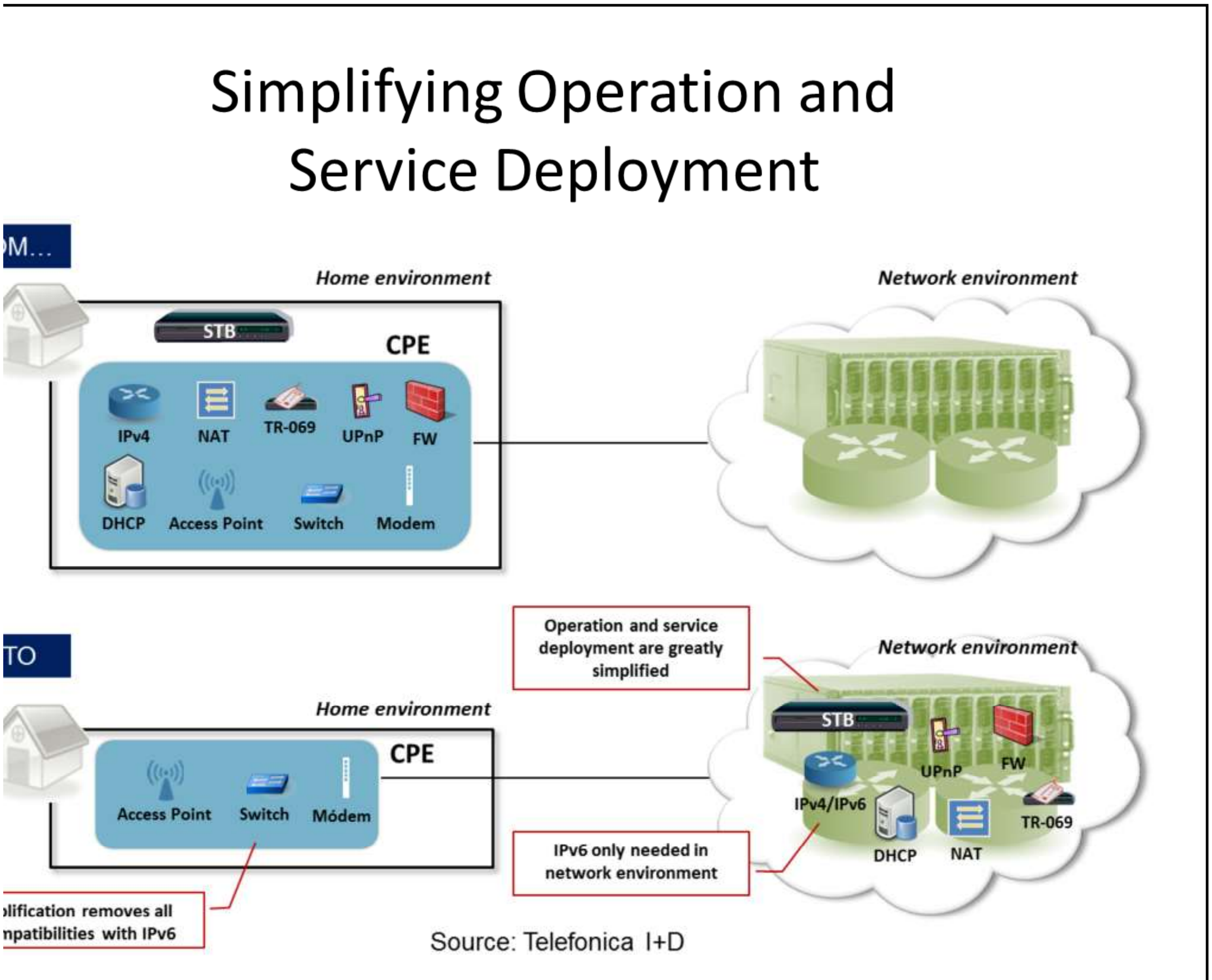
And some challenges:
- Cost-efficiency (cache software is often relative simple software, deployed on low-cost servers)
- Performance ratio in comparison to bare metal
- Performance predictability
- Allow the right balance of network i/o to CPU power to storage i/o performance

Home Environment

- Current **network operator provided home services** are architected using network-located **backend systems and dedicated CPE devices located as part of the home network**.
- These CPE devices mark the operator and/or service provider presence at the customer premises and usually include:
  - Residential Gateway (RGW) for Internet
  - VOIP services, and a
  - Setup Box (STB) for Media services normally supporting local storage for PVR services

Advantages:

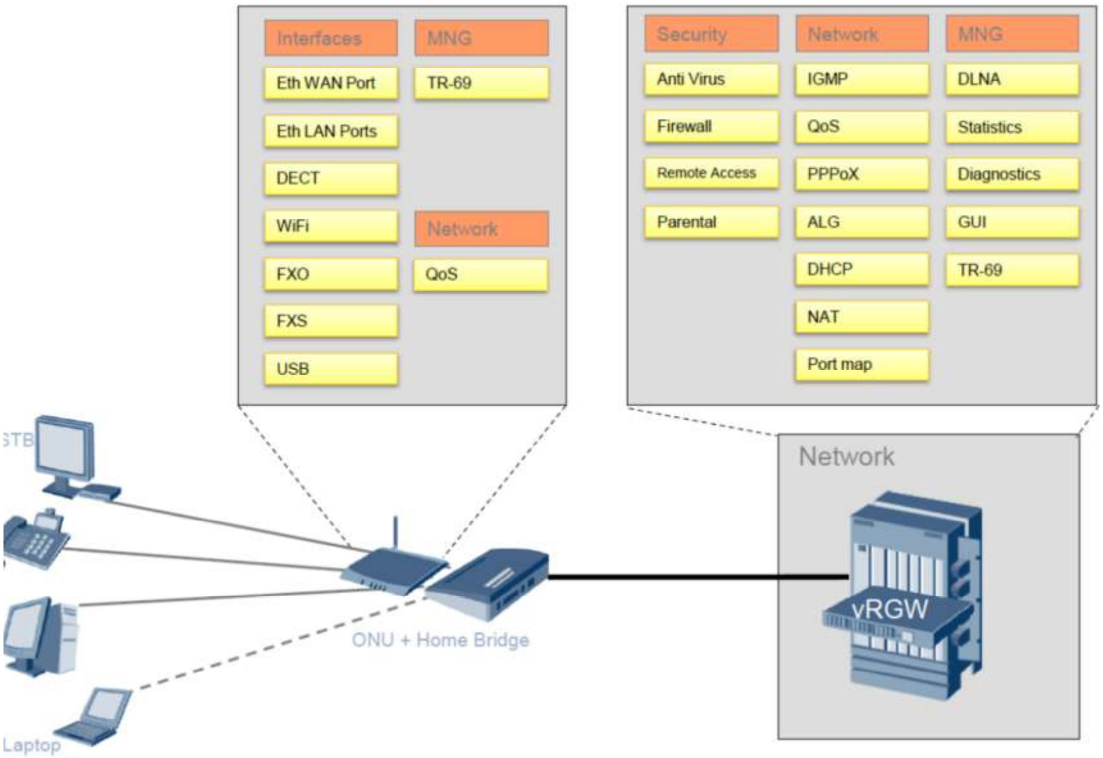
- Reduces CAPEX by eliminating the costs of Setup Boxes and Residential Gateways
- OPEX reduction by eliminating the need to constantly maintain and upgrade CPEs. And capacities to make remote diagnostic of the user devices in order to provide direct solutions to the problems in the user network
- Improved QoE by functionality such as remote access to all content and services, multi-screen support and mobility
- New service introduction is smooth and less cumbersome as the dependency on the CPE functionality and user installation processes is minimized



The virtualisation of services and capabilities that presently require dedicated hardware appliances on customer premises (home environment to small branch office to large corporate premises), including but not restricted to: firewall, web security, IPS/IDS, WAN acceleration and optimisation, and router functions. The virtualisation of the home environment including routers, hubs and set top boxes would potentially enable a simpler and seamless migration to IPv6, reduce energy consumption and avoid successive hardware updates as broadband applications and services evolve.

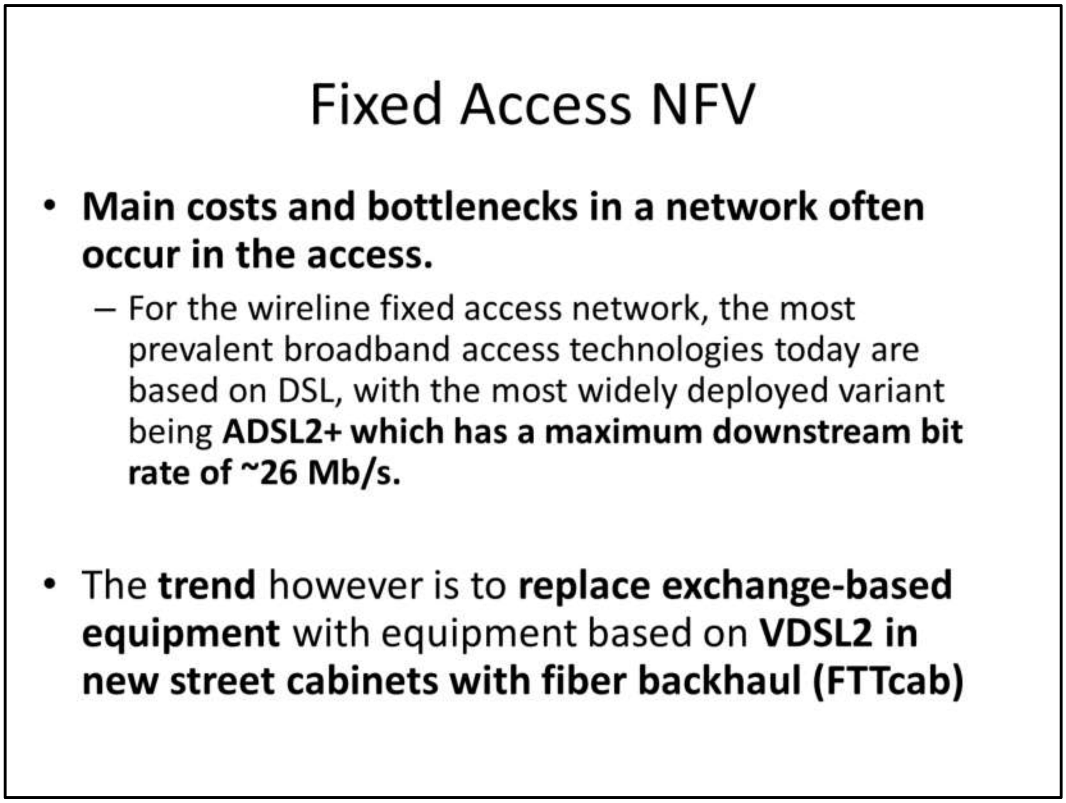
Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

Virtual Residential Gateway



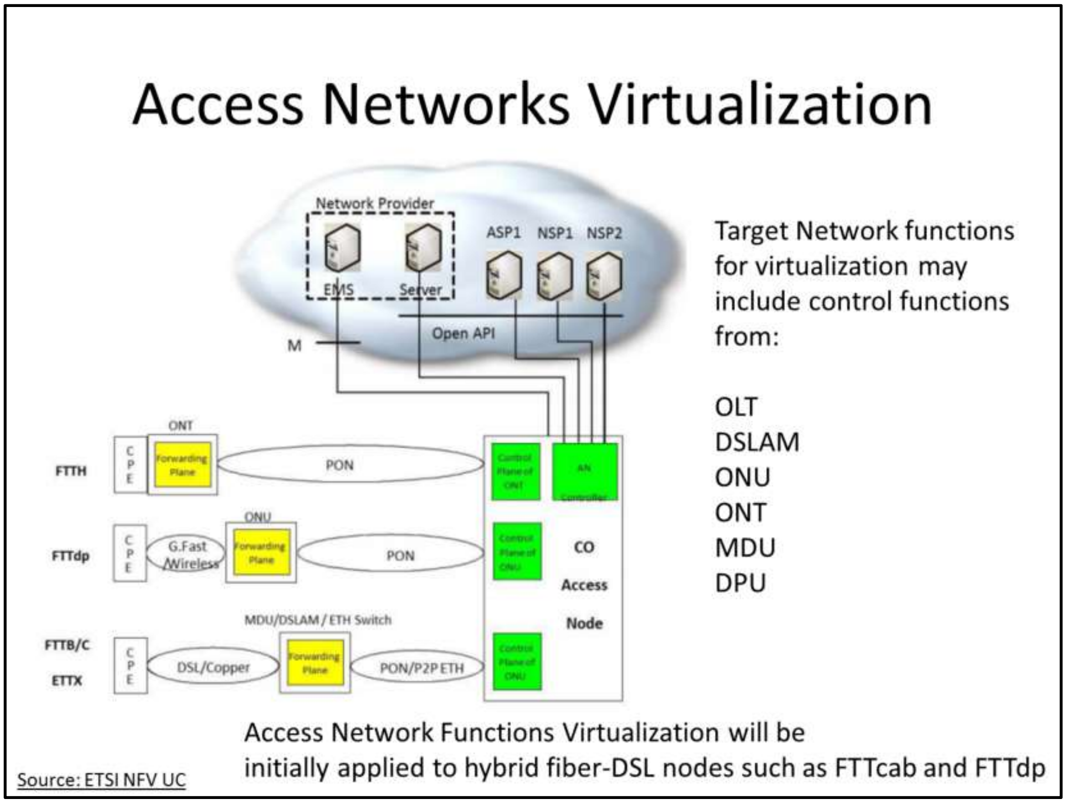
Source: NEC

This example of NFV in the user home domain is being pursued by NEC.
The concept of virtual Residential Gateway (vRGW) allows to move many functions Currently running in the customer premises equipment (CPE) to virtual hosted appliances, where they can be more easily updated while still allowing the same (or even abstracted configuration knobs to the user



Motivation to consolidate Fixed residential access by virtualization

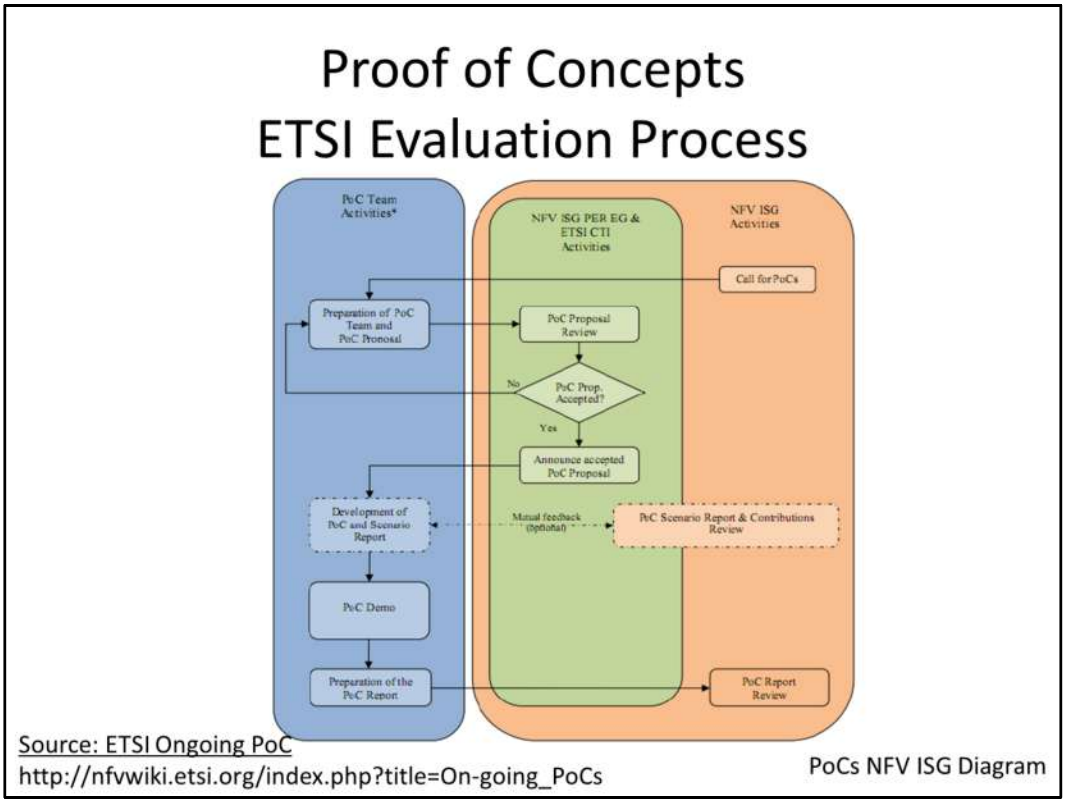
- Replacing DSL and cable modems by VDSL2
- More bandwidth and computing power in street cabinets



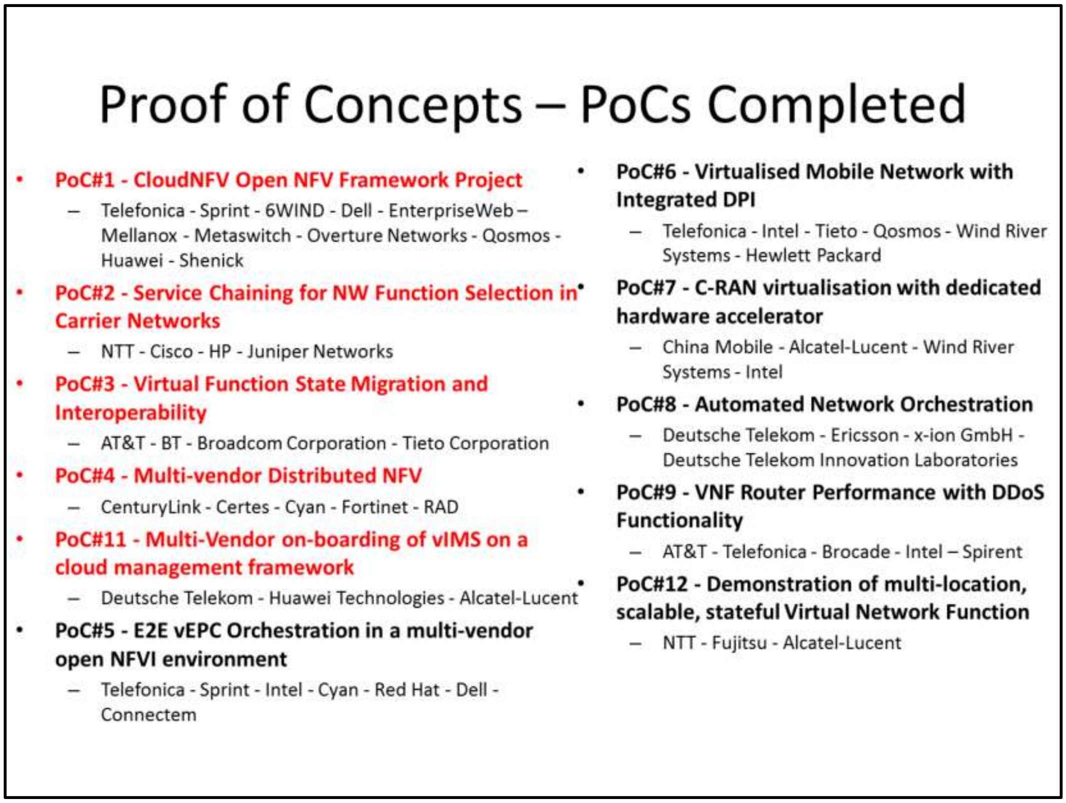
Existing access technologies need to be improved to support the requirements of new services, e.g. in terms of capacity, stability, or real-time responde
Today’s ‘legacy’ technologies and services shall be able to coexist with new ones
Network management need to evolve to allow rapid provisioning of broadband access, no matter from where, or via which technology, with the required parameters of capacity and QoS defined by a set of services

Proof-of-Concepts

NFV



This diagram presents the proposal workflow. Any company or research institution can group in teams and submit a proposal to use case the NFV technologies to the public. This proposals are usually private and reserved documents and some of the material has been publicly available in other sources, such as specific websites or NFV-related conferences.



In summary, since its beginning ETSI coordinated 35 Proof of Concept proposals. There were 20 completed already and currently 15 on-going PoCs. Each PoC proposal has a link in ETSI website (password protected). The proposals are organized by "collaboration team" of companies or research institutions. The PoC in red, we will provide more detail later.

- PoC#5 –vEPC use case, explored on a multi-vendor NFV infrastructure
- PoC#6 – providing higher security for mobile networks
- PoC#7 – hardware accelerated on radio virtualization
- PoC#8 – automatic provisioning, stitching and auto-recovery using orchestration
- PoC#9 – security enhancement for DDoS attacks
- PoC#12 – distributed VNF distributed software

Proof of Concepts – PoCs Completed

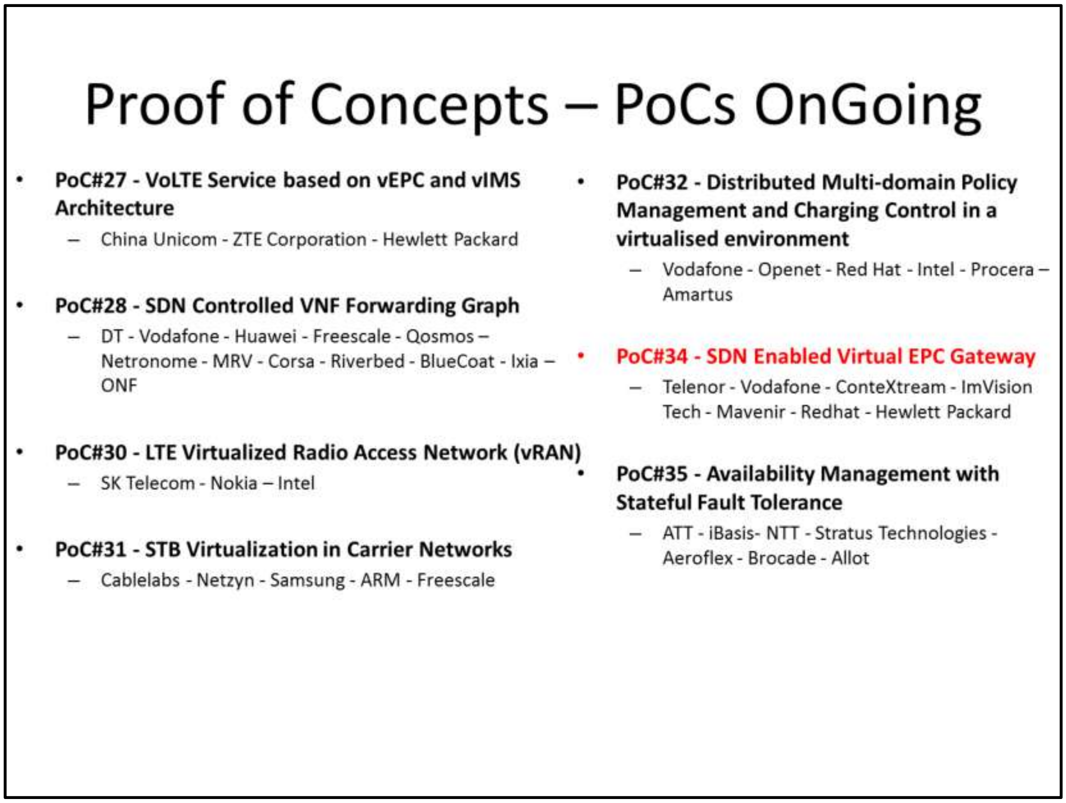
- **PoC#14 - ForCES Applicability for NFV and integrated SDN**
  - Verizon - Telefonica - Mojatatu Networks - Cumulus Networks - University of Patras
- **PoC#15 - Subscriber Aware SGi/Gi-LAN Virtualization**
  - Telenor - ConteXtream - SkyFire Networks - Guavus - Redhat - HP
- **PoC#16 - NFVIaaS with Secure, SDN-controlled WAN Gateway**
  - AT&T - Telecom Italia - Netronome - Intel - ServiceMesh - PLUMgrid - Cisco Systems
- **PoC#19 - Service Acceleration of NW Functions in Carrier Networks**
  - AT&T - Ericsson - Avago Technologies - ARM - Tieto - Procera
- **PoC#22 - Demonstration of High Reliability and Availability aspects in a Multivendor NFV Environment**
  - AT&T - KDDI R&D Laboratories - Brocade - Hewlett Packard - Wind River System
- **PoC#23 - E2E orchestration of virtualized LTE core-network functions and SDN-based dynamic service chaining of VNFs using VNF FG**
  - SK Telecom - Hewlett Packard - Samsung - Telcoware
- **PoC#29 - Service orchestration for virtual CDN service over distributed cloud management platform**
  - KINX - IN-Soft - PIOLINK - ETRI
- **PoC#33 - Scalable Service Chaining Technology for Flexible Use of Network Functions**
  - NTT - ALAXALA Networks - Hitachi - Cisco Systems - NEC - Alcatel-Lucent

- PoC#14 – ForCES (IETF Forwarding and Control Element Separation) can be used as the foundation for SDN-enhanced NFV
- PoC#15 - implements SDN switch to enable a subscriber-aware solution that is programmed on a per-endpoint basis, ensure trafffic flow from each subscriber to follow a chain of services
- PoC#16 – NFV and SDN in multi-tenant data centers and over the WAN, orchestration and controller ensures security and SLA over WAN
- PoC#19 – Acceleration of Virtualized Network Function using specialized NF Systems on Chips and disaggregation of elements using COTS and special chips
- PoC#22 – Automate recovery of VNF functions, scale in, scale out
- PoC#23 – idea is verify the correctness of the E2E lifecycle management and orchestration of virtualized LTE core network functions
- PoC#29 – CDN service over distributed cloud environment
- PoC#33 – A way to implement VNF Forwarding Graph is thru Service Function Chaining (SFC). The PoC verify flexible use of VNF Forwarding Graph using SFC from several vendors.

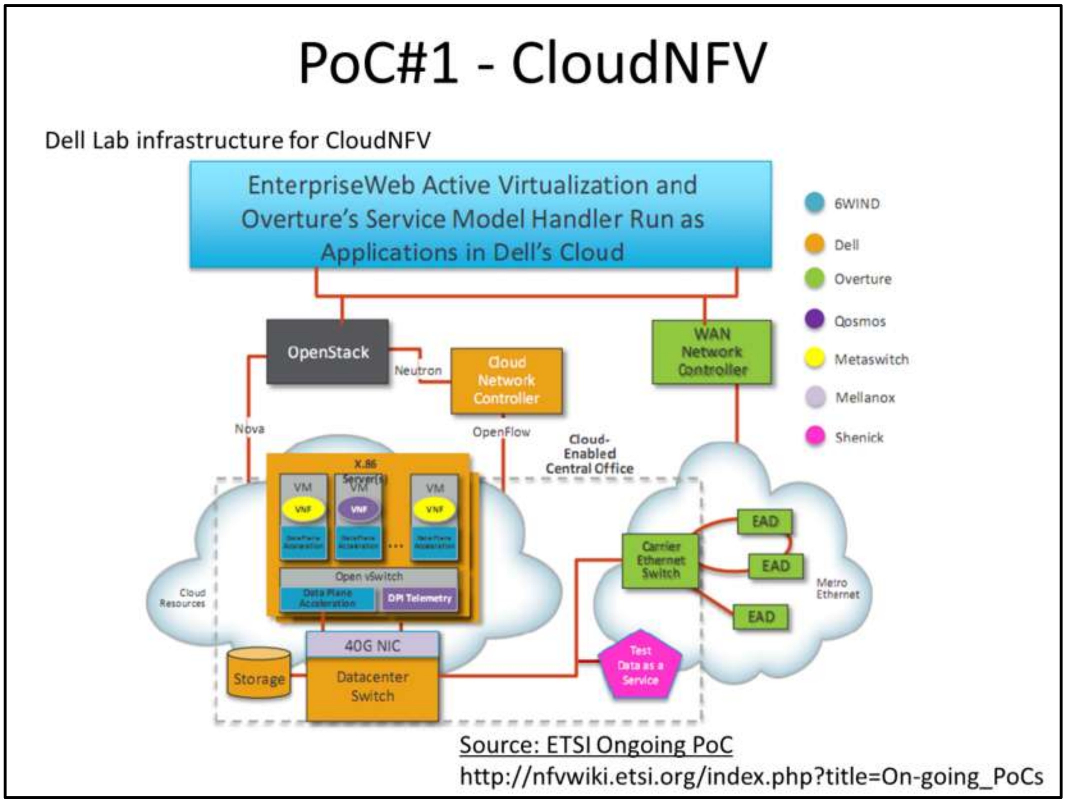
Proof of Concepts – PoCs OnGoing

- **PoC#13 - SteerFlow: Multi-Layered Traffic Steering for Gi-LAN**
  - Telefonica - Vodafone - Radware - HP - Melanox
- **PoC#17 - Operational Efficiency in NFV Capacity Planning, Provisioning and Billing**
  - BT - MetraTech Corp - Huawei
- **PoC#18 - VNF Router Performance with Hierarchical Quality of Service Functionality**
  - Telefonica - BT - Brocade - Intel - Spirent
- **PoC#20 - Virality based content caching in NFV framework**
  - BT - Telefonica - Brocade - IBM Research - AMD
- **PoC#21 - Network Intensive and Compute Intensive Hardware Acceleration**
  - BT - Huawei - EZChip - AMD - Tilera - Altera - Broadcom - EANTC - Ixia
- **PoC#24 - Constraint based Placement and Scheduling for NFV/Cloud Systems**
  - AT&T - DT - Brocade - IBM - Red Hat - VMware
- **PoC#25 - Demonstration of Virtual EPC (vEPC) Applications and Enhanced Resource Management**
  - Vodafone - AMD - ARM - Aricent
- **PoC#26 - Virtual EPC with SDN Function in Mobile Backhaul Networks**
  - Telecom Italia - Nokia Networks - EXFO - Coriant - Aalto University

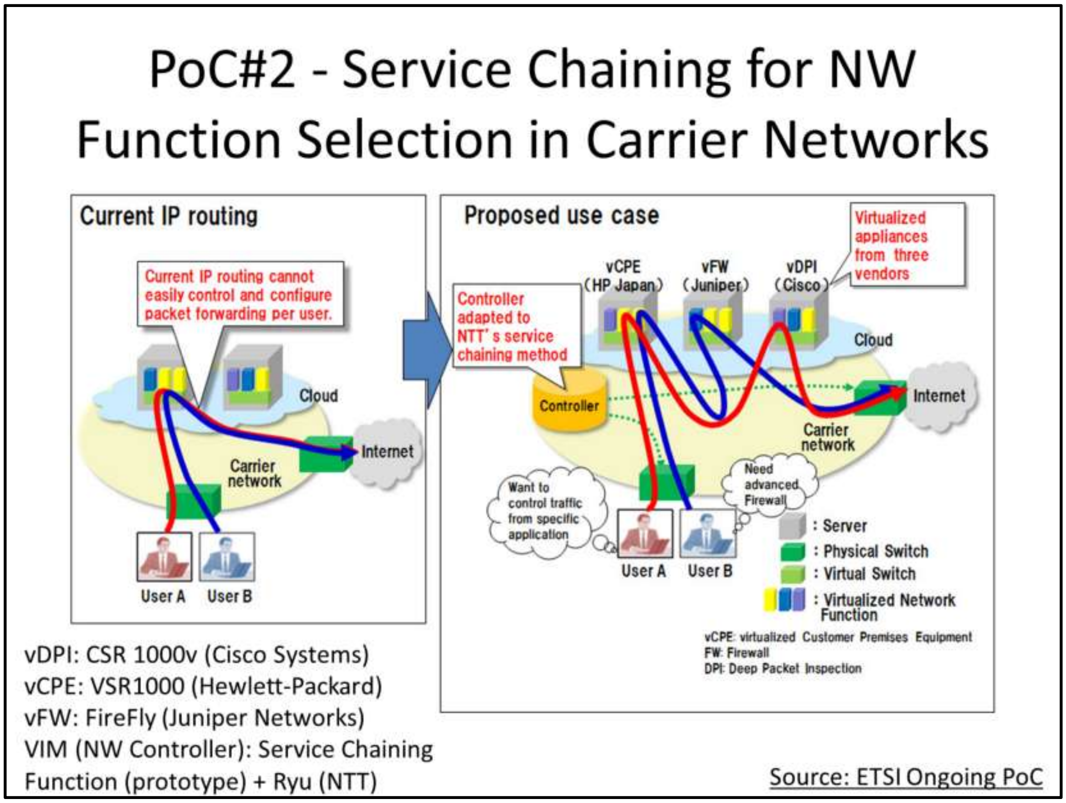
- PoC#13 - high capacity and scalable multi-layered traffic steering system optimizes the utilization of network components, load balancing models are demonstrated
- PoC#17 - Support thru APIs, static and elastic service-level performance requirements and pricing parameters, provide rightful allocation of virtualized resources
- PoC#18 – Showcase of VNF Router Performance with Hierarchical QoS (HQoS) implemented using Brocade Vyatta 5600 vRouter and Intel DPDK
- PoC#20 – NFV framework for conveying content chance of become viral from Cloud applications such as YouTube, Twitter, Facebook and maximize energy efficiency using virtual CDN
- PoC#21 – demonstrate the benefits of Hardware Acceleration in NFV environments - for functions such as Load Balancing, Internet Key Exchange, Encryption and Video Transcoding, propose a Hardware Abstraction Layer
- PoC#24 – Static and Dynamic Resource Constraints expressed as policies, like max storage capacity, network topology, application QoE are adjusted, scheduled and placed in NFV/Cloud Systems in NFVIaaS use cases
- PoC#25 – vEPC functions implemented using AMD 64bit ARM and x86 processors, also scalable resource management for different CPU
- PoC#26 – Integrate NFV and SDN for a EPC that mantains core elements, MME, HSS. Use SDN in the mobile backhaul such that mobile operators can choose the granularity for QoS provisioning to mobile users



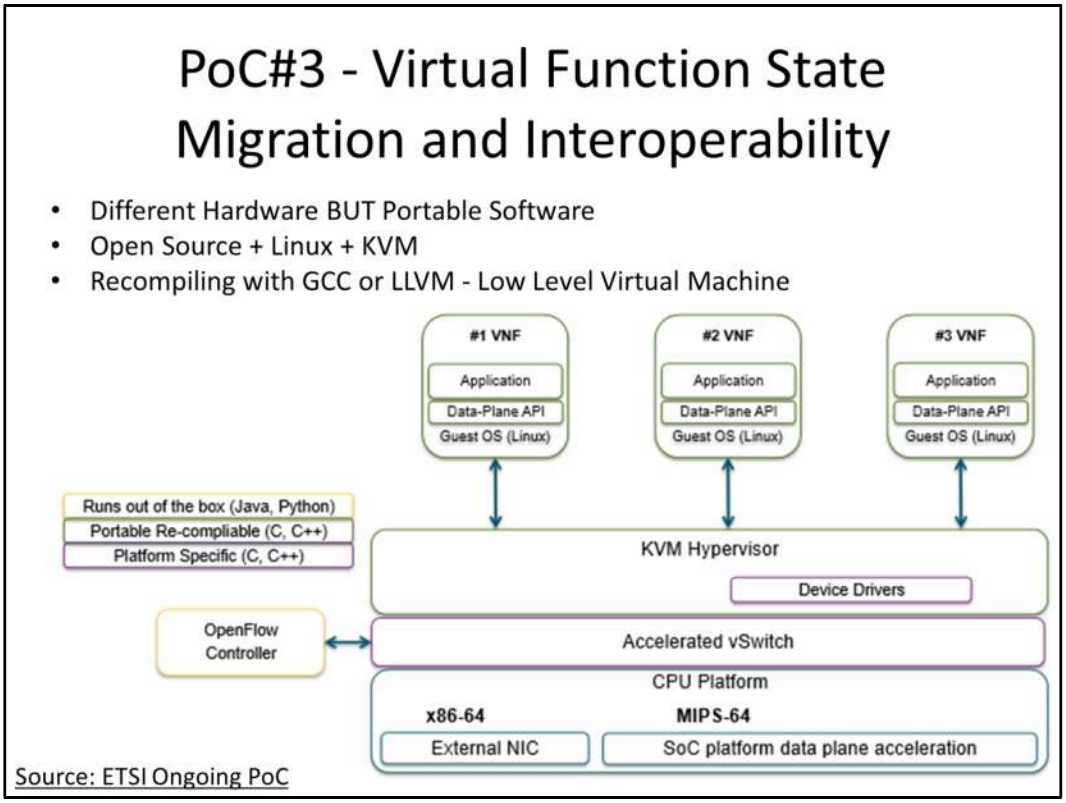
- PoC#27 - Dynamic Network deployment of LTE - use CloudBand to provision, mobile data and control elements vEPC and vIMS
- PoC#28 – Show how to mark and process packets that belong to Service Chains using SDN
- PoC#30 – vRAN comprises a virtualized baseband unit (vBBU) that uses general purpose servers to deliver cost-savings and increased network performance
- PoC#31 – Virtualization of set top boxes, some companies are specialized in STB
- PoC#32 - Real-time OSS/BSS running on a virtualized environment to provide a complete distributed Policy Management and Charging Control System
- PoC#34 – a scalable way to split and scale independently the data and control of an EPC network
- PoC#35 – study fault tolerance in the NFVIaaS context



NFVIaaS project – design based on mapping open source tools and elements



PoC#2 Service Chaining of commodity virtual appliances using OpenFlow



Several VNFs are compiled and prepared to specific hardware platforms based on MIPS processor

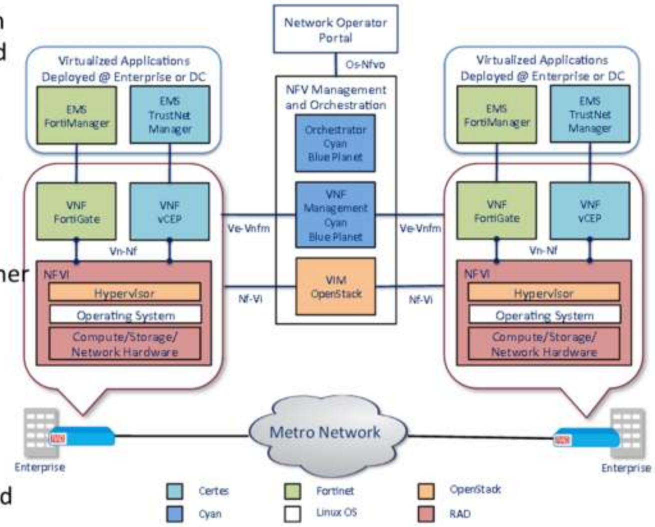
This PoC#3 explores the issues with portability, interoperability and state migration on COTS and specialized hardware

PoC#4 - Distributed-NFV

PoC are being developed based on **centralized NFVI architectures** and centralized VNF deployment

However, there is **also a need to deploy some functions out at the customer edge**. The ability to support the deployment of virtualized functions at the customer edge **requires a Distributed NFV (D-NFV) architecture**

Omniscient D-NFV orchestrator handles all VNFs and virtual machine (VM) infrastructure, wherever they may be located, and exploits SDN-like mechanisms to achieve optimal VNF placement



Source: ETSI Ongoing PoC

Organize a distributed system and test interoperability among NFVI architectures.

PoC#11 - Multi Vendor on-boarding of vIMS on Cloud Management Frame

Scenario 1 – One-click service deployment.

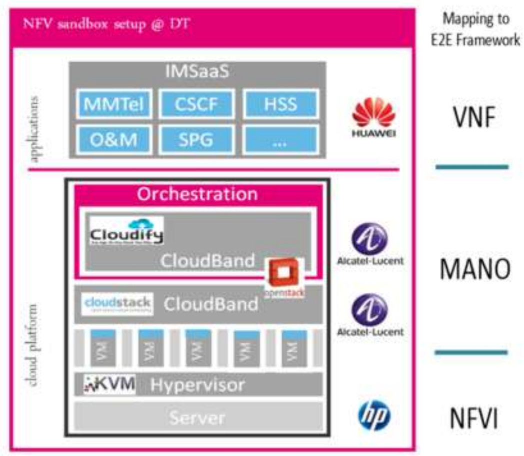
IMS service is provided by several 3GPP Network Functions, such as CSC, HSS, MMTel, etc. These functions, all from Huawei, are virtualized. **With the pre-defined templates and scripts, all functions can be deployed automatically**, onto the cloud platform provided by DT and ALU.

Scenario 2 – Auto-scaling of VNF

Traffic load generator by a simulator increases and pushes up the workload of the VNF. When the workload exceeds the pre-defined threshold, additional resources (VM) are automatically allocated. In situations of reducing VNF capacity due to decreasing traffic load, similar in reverse direction

Scenario 3 – Automated healing of VNF

When a VM containing a component of a VNF (VNFC) fails, a new VM will be automatically allocated and created with appropriate component instantiated on it. This process heals the VNF with no service interruption.

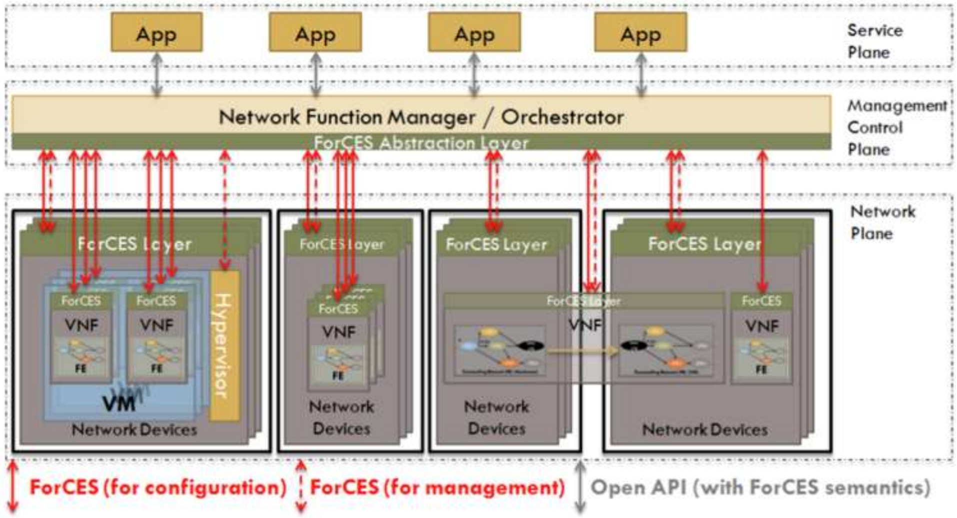


Source: ETSI Ongoing PoC

CloudBand is the Alcatel-Lucent Cloud Platform

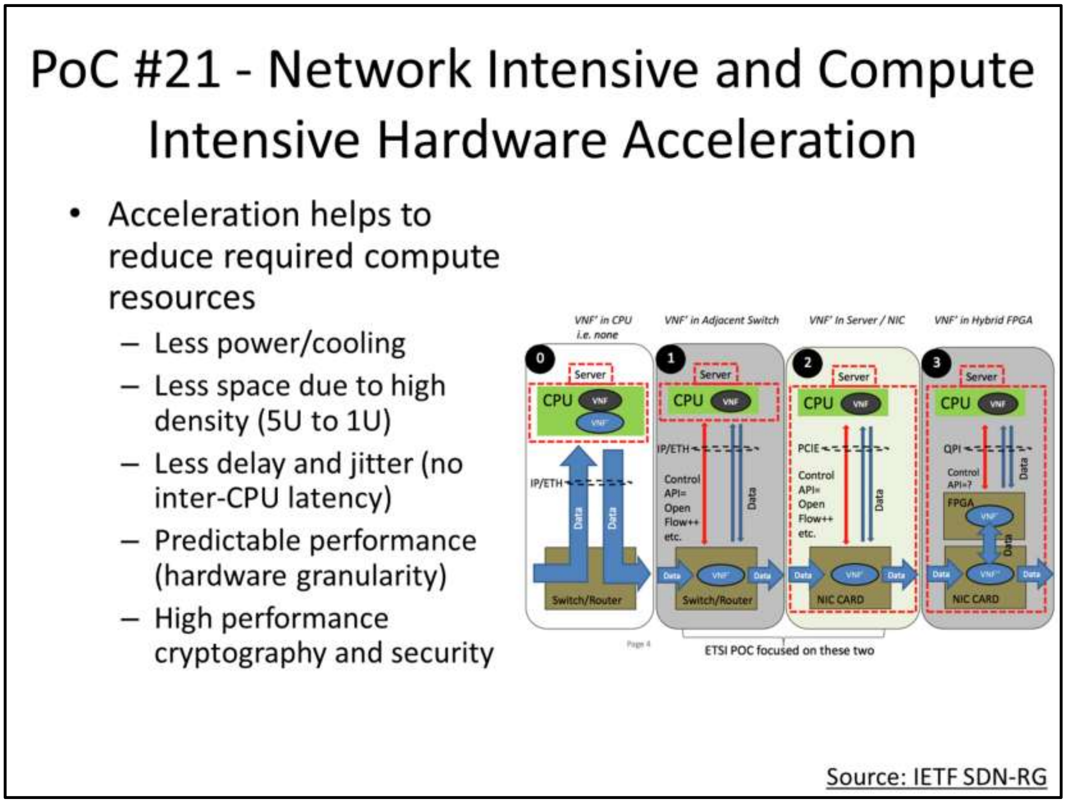
vIMS – first PoC from Alcatel-Lucent on the automatic cloud NFVIaaS system with auto-scale, auto-help, one-click to deploy

PoC#14 - ForCES Applicability for NFV and integrated SDN

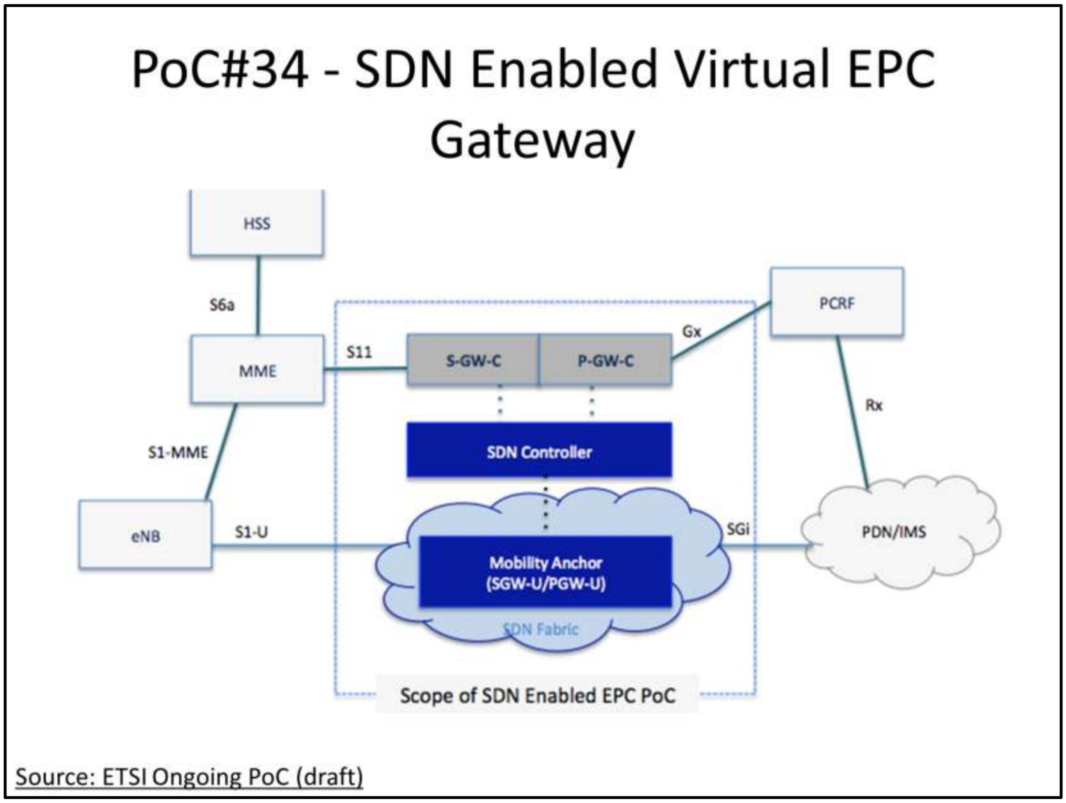


Source: ETSI Ongoing PoC

Leverage IETF ForCES – Forwarding Elements are configured and managed, as alternative to OpenFlow and the system implements VNFs over ForCES layer



The focus of this PoC is testing and design accelerated hardware for specific functions such as load balance and VPNs
Reference: http://www.ietf.org/proceedings/91/slides/slides-91-sdnrg-4.pdf



The solution for implementing next generation S-GW and P-GW is by using SDN and NFV. This way, it split the function further into S/P-GW Control and S/P-GW-User Plane. This type of implementation leverages the original design of EPC (decoupled data/control) in order that the functions within the gateways can scale independently

Quick overview on remarkable enabling technologies of NFV

ENABLING TECHNOLOGIES

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

Enabling Technologies

- Minimalistic OS
  - ClickOS
- Improving Linux I/O
  - Netmap, VALE, Linux NAPI
- Programmable virtual switches / bridges
  - Open vSwitch
- Exploiting x86 for packet processing
  - Intel DPDK
- Some example start-ups
  - LineRate Systems, 6WIND, Midonet, Vyatta (bought by BCD)

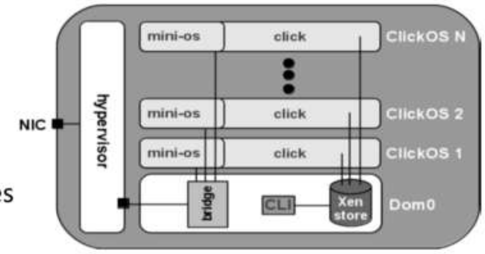


Image source: ClickOS

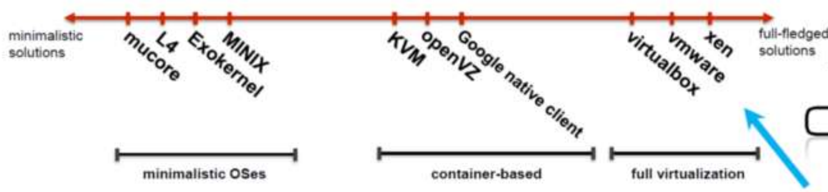
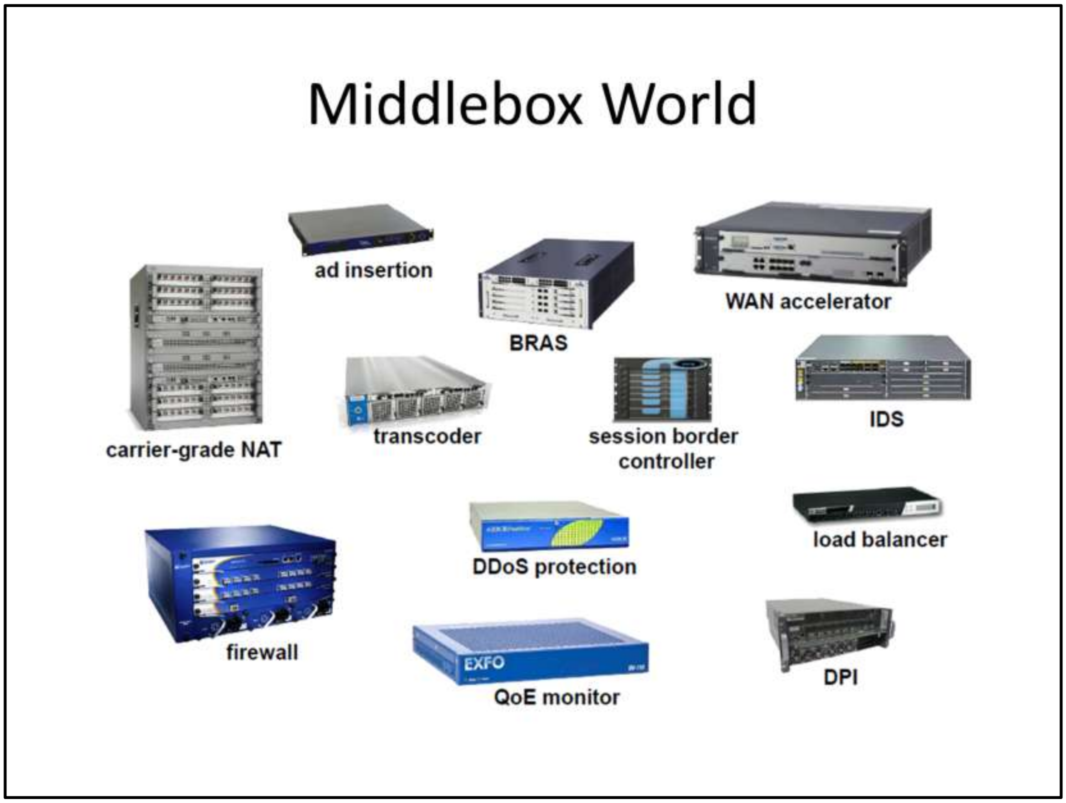
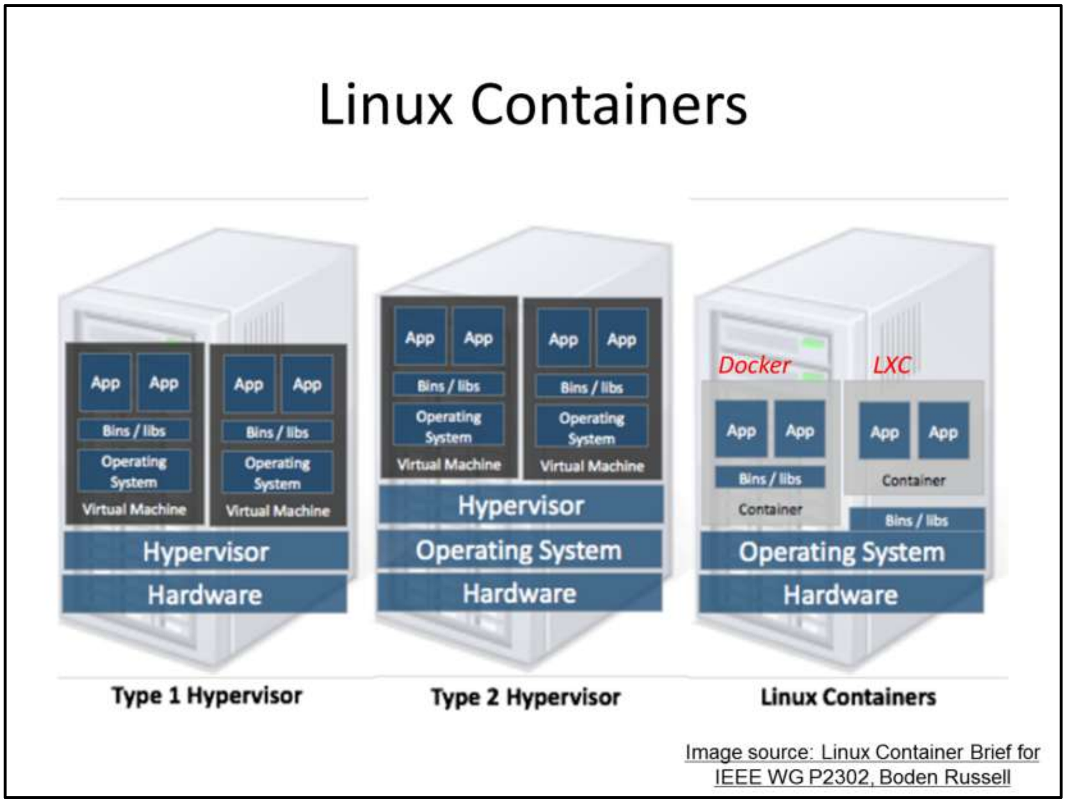


Image source: NEC

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-initialisation 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 OpenFlow, OpenStack, OpenNaaS or OGF's NSI, provide an additional degree of integration of Network Functions Virtualisation and cloud infrastructure.
Source: Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf



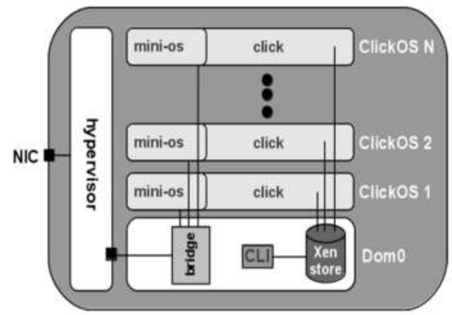
Middlebox world – full of specialized closed-boxes hardware



Linux Containers is one of the enabling technologies since Network Functions can be splitted and run in independent and isolated processes.
"Full deployment systems" with libs, binaries, image disks can be created in a matter of milliseconds
Performance can be tunnable in Linux

MiniOS - ClickOS Architecture

Martins, J. et al. Enabling Fast, Dynamic Network Processing with ClickOS. HotSDN 2013.



- Build small system using MiniOS (5MB images)
- Emulate CLICK Modular Router control plane over MiniOS/Xen
- Reduce boot times (30 ms)
- Optimized for 10Gbps data planes

An interesting proposal and enabler of small and high performance VN functions is ClickOS
A small MiniOS of rough 5MB in size running Click middlebox system (NAT, load balancer, router, etc)
Lots of small MiniOS can be spawned in a matter of miliseconds

ClickOS boot costs and performance

description	function	time
issue create hypercall	libxl_domain_make2	5.244
paravirt. bootloader	libxl_run_bootloader	0.049
prepare domain boot	libxl__build2_pre	0.089
parse, allocate and boot vm image	xc_dom_allocate	0.016
	xc_dom_kernel_path	0.047
	xc_dom_ramdisk	0.001
	xc_dom_boot_xen_init	0.011
	xc_dom_parse_image	0.286
	xc_dom_mem_init	0.007
	xc_dom_boot_mem_init	0.650
	xc_dom_build_image	7.091
	xc_dom_boot_image	0.707
write xen store entries, notify xen store daemon	libxl__build2_post	2.202
init console	init_console_info	0.004
	libxl__need_xenpv_qemu	0.006
	libxl__device_console_add	4.371
	TOTAL	**20.789**

Table 1: Costs of creating a ClickOS virtual machine and booting it up, in milliseconds.

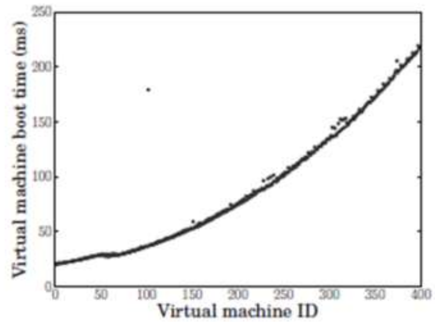


Figure 4: Time to create and boot 400 ClickOS virtual machines on a single server.

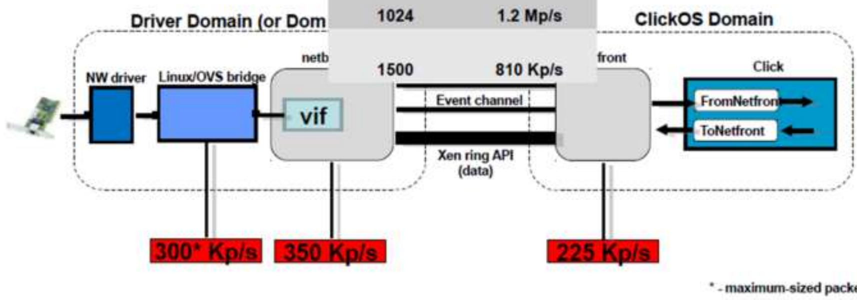
Martins, J. et al. Enabling Fast, Dynamic Network Processing with ClickOS. HotSDN 2013.

Some important results from ClickOS paper.
The total boot time of a miniOS machine in their context is around 20 msec
The number of virtual machines running in parallel and the deployment time are: 400 clickOS in a matter of 200 ms.

Performance Analysis (low performance) without netmap

pkt size (bytes)	10Gb rate
64	14.8 Mp/s
128	8.4 Mp/s
256	4.5 Mp/s
512	2.3 Mp/s
1024	1.2 Mp/s
1500	810 Kp/s

Idea: use netmap



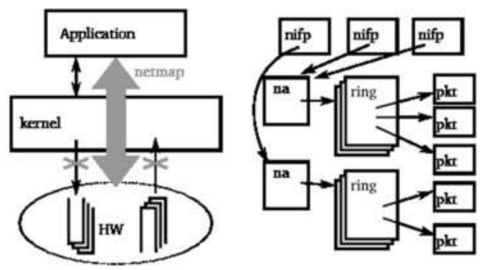
Martins, J. et al. Enabling Fast, Dynamic Network Processing with ClickOS. HotSDN 2013.

On ClickOS paper, the result of a regular MiniOS does not achieve high network throughput

Hypervisor and userland/kernel overhead do not permit 10Gbps, solution: netmap

Netmap

- High Performance packet I/O framework
  - 14.88 Mpps on 1 core at 900 Mhz
- Available in FreeBSD 9+ and Linux
- Minimum device driver modifications
  - critical resources (NIC registers, physical buffer addresses and descriptors) not exposed to the user
  - NIC works in special mode, bypassing the host network stack
- Amortize syscalls cost by using large batches
- Preallocated packet buffers and memory mapped to userspace



netmap is a high speed packet I/O shortcut for applications directly accessing the NIC device. It can easily handle line rate on 10Gbps.

Intel DPDK

- Supported since Intel Atom up to latest Intel Xeon
- 32-bit and 64-bit with or without NUMA
- No limit on the number of cores or processors
- Ideal DRAM allocation for all packets pipelines
- Several examples of networking software that show the performance improvement
  - Best practices for software architecture
  - Tips on modeling and storing data structures
  - Help compiler to improve the network code
  - Reach levels up to 80Mpps per socket of CPU

Intel DPDK

- Optimized NIC Drivers in the user-space
- Drivers 1/10Gbps
- BSD License
- Source code available in Intel website (and others)

Source: Intel Data Plane Development Kit (Intel DPDK) Overview – Packet Processing on Intel Architecture

Intel DPDK

Buffer and Memory Manager

- Manage the allocation of objects non-*NUMA* using *hugepages* through *rings*, reducing TLB access, also, perform a pre-allocation of fixed buffer space for each core

Queue Manager

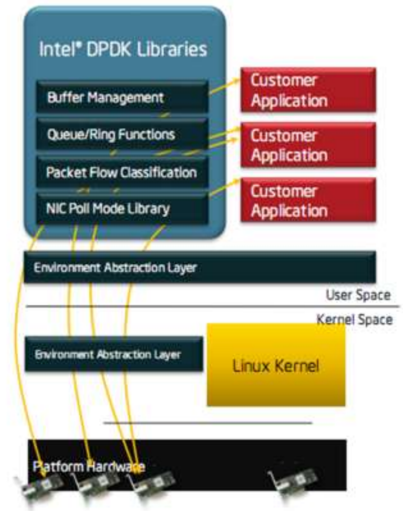
- Implements *lockless queues*, allow packets to be processed by different software components with no contention

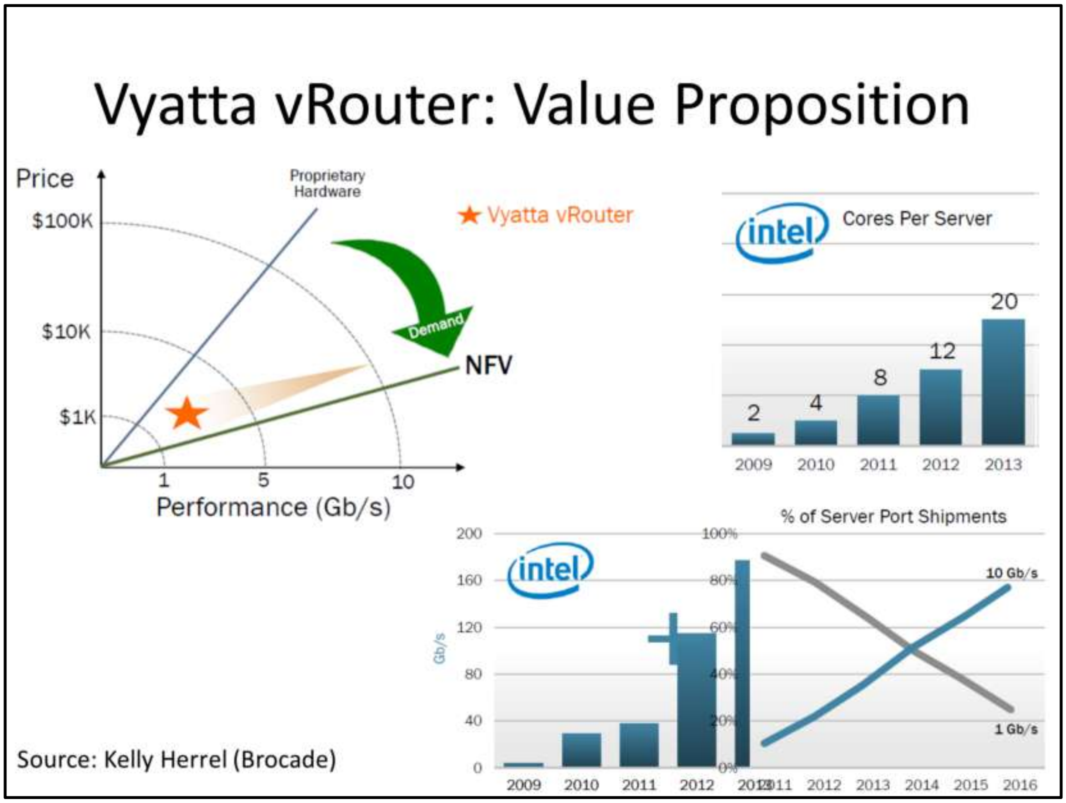
Flow Classification

- Implements hash functions from information tuples, allow packets to be positioned rapidly in their flow paths. Improves *throughput*

Pool Mode Driver

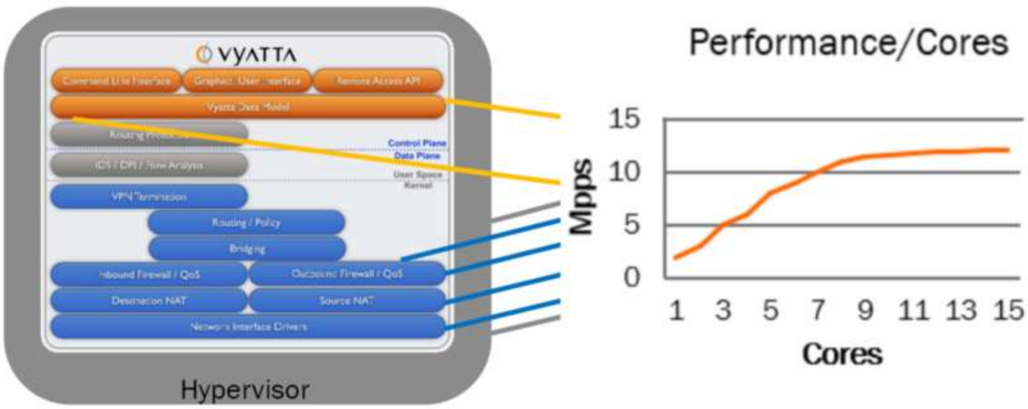
- Temporary hold times thus avoiding raise NIC interruptions





Source: Kelly Herrel (Brocade), NFV: The Signal in the Noise, NETWORK FIELD DAY, February 2014
Networking's Path Into The Server
Telcos Drive 10X Higher Performance Requirement
Servers Are Exploding With Power…
DRIVING MORE VIRTUAL MACHINES PER SERVER
Servers Are Now *Network-Centric*

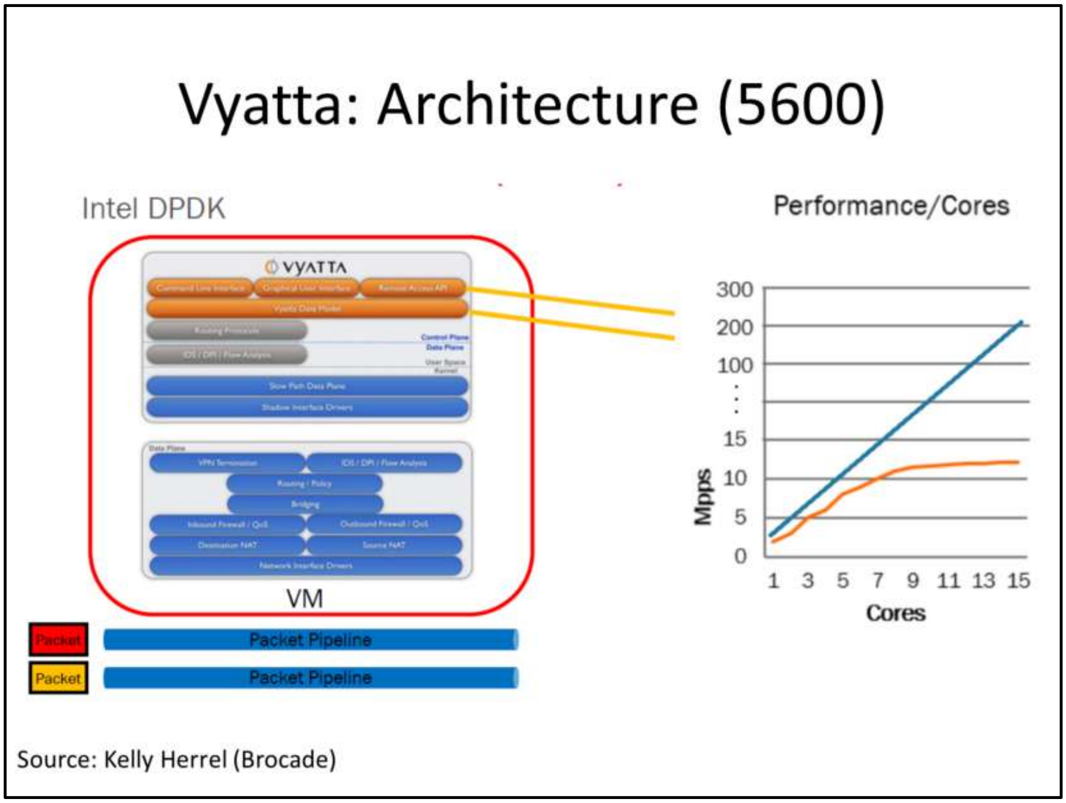
Vyatta: Current Architecture (5400)



Source: Kelly Herrel (Brocade)

Source: Kelly Herrel (Brocade), NFV: The Signal in the Noise, NETWORK FIELD DAY, February 2014

Linux



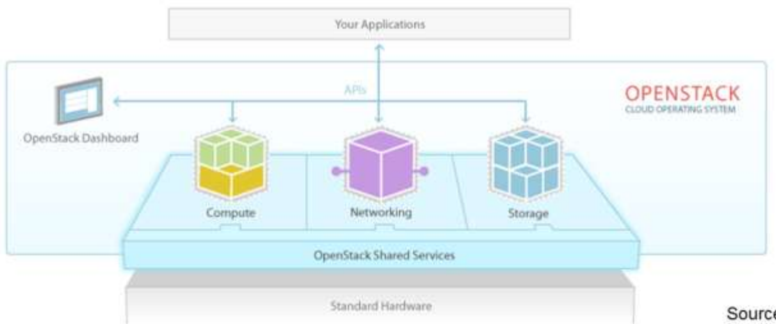
Source: Kelly Herrel (Brocade), NFV: The Signal in the Noise, NETWORK FIELD DAY, February 2014

Linux

OpenStack

OpenStack is a global collaboration of developers and cloud computing technologists producing the ubiquitous open source cloud computing platform for public and private clouds.

The project aims to deliver solutions for all types of clouds by being simple to implement, massively scalable, and feature rich. The technology consists of a series of interrelated projects delivering various components for a cloud infrastructure solution.

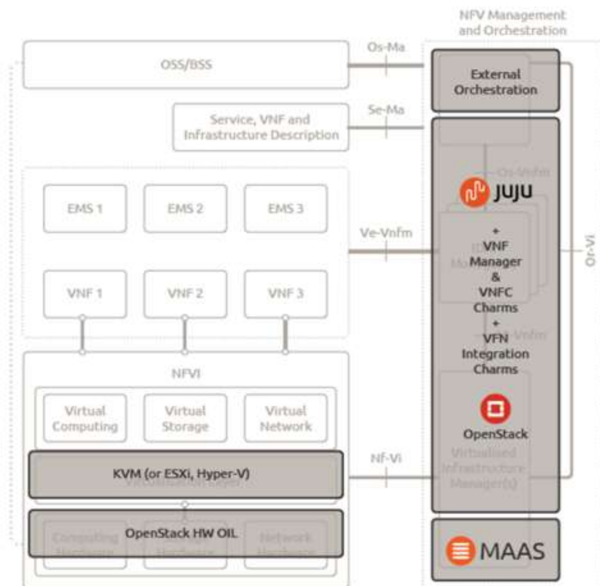


Source: Openstack.org

Openstack is one of the “cloud operating systems” - we present it since the NFV blueprints are quite substancial

In particular Neutron is the network management in OpenStack

Ubuntu Cloud Portfolio Mapped to ETSI-NFV framework



Src: SDN and NFV on OpenStack for Telcos (CANONICAL)

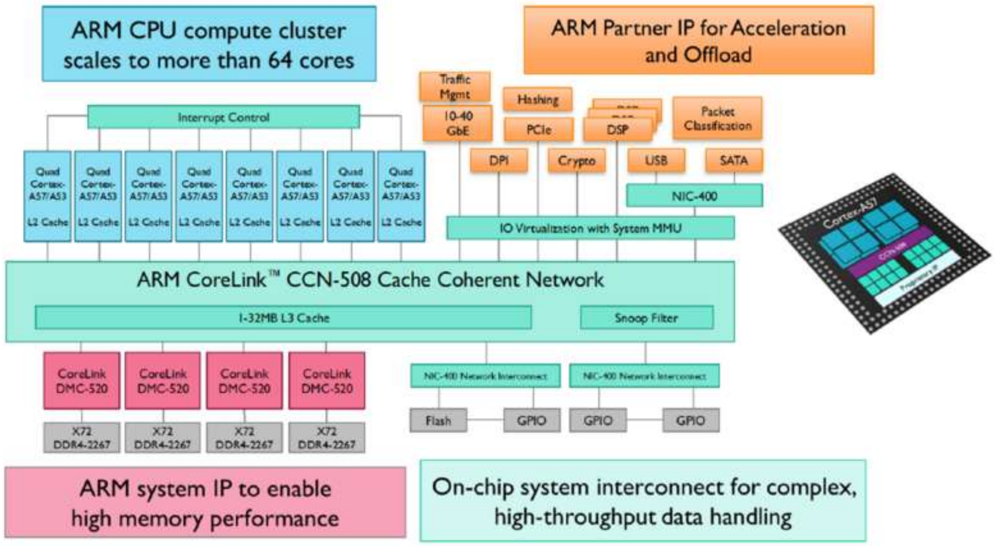
Blueprints in Juno and beyond

- 2 interfaces from 1 VM on same network
- SR-IOV Networking Support
- Virt driver guest vCPU topology configuration
- Evacuate instance to scheduled host

- VLAN trunking networks for NFV
- VLAN tagged traffic possible over tenant network
- From VLAN trunks to virtual networks
- VLAN tagged traffic redirected to a physical appliance
- management VLANs on ports as sub-ports
- Allow interfaces with no address for NFV

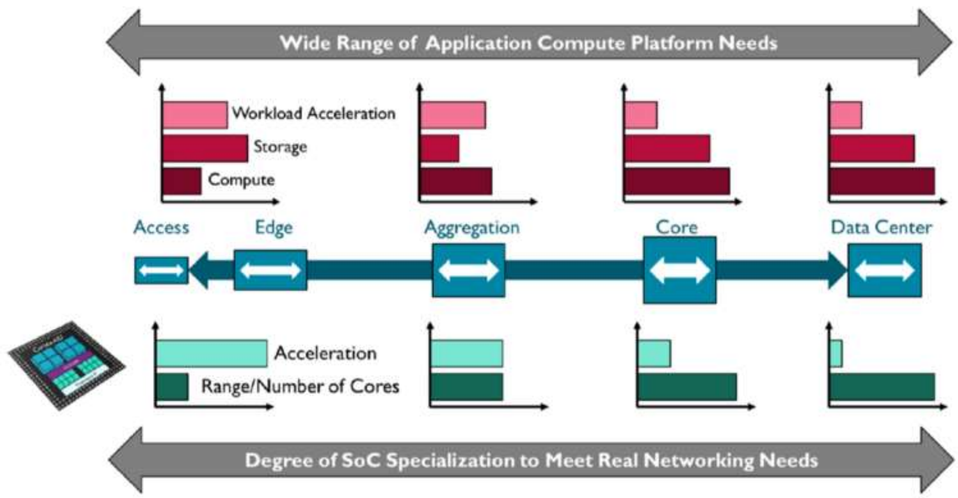
Some of the blueprints being reviewed and implemented in Juno (left pane)
Some blueprints planned for Kilo (with the highest priority)

Enabling tech: ARM

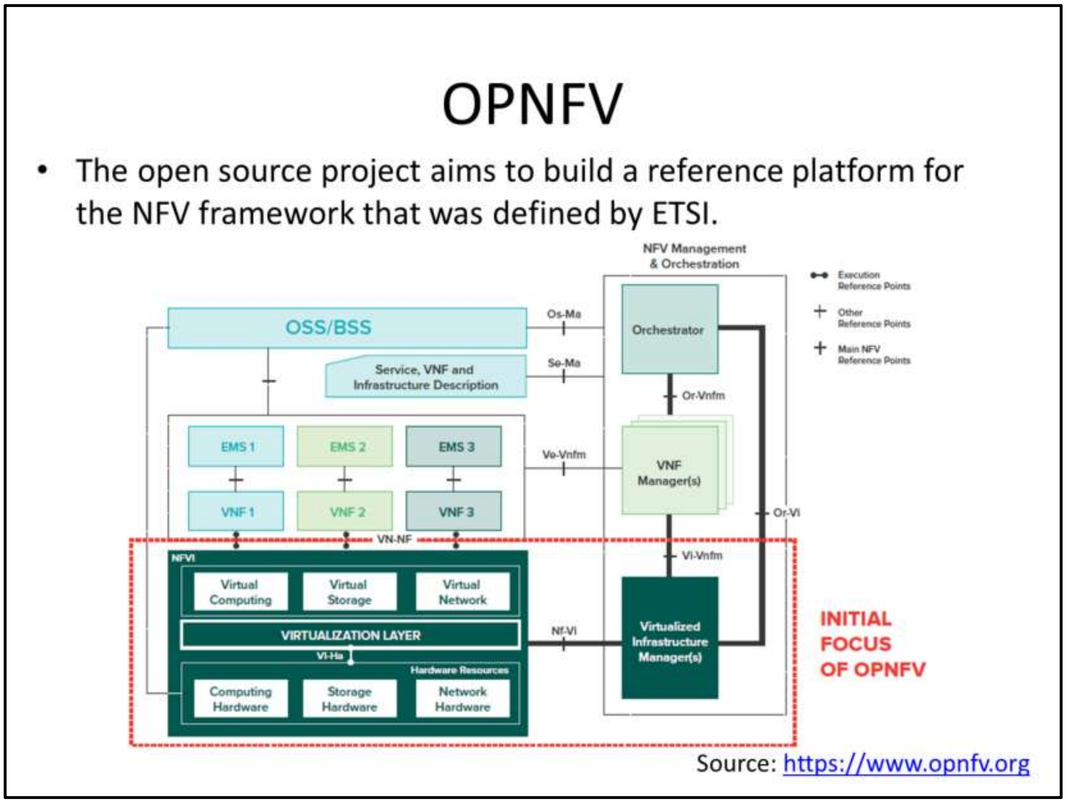


Src: The Intelligent Flexible Cloud (ARM)

Heterogeneous System on a Chip (SoCs) in the Intelligent Flexible Cloud



Src: The Intelligent Flexible Cloud (ARM)



Src: OPNFV: An Open Platform to Accelerate NFV (Linux Foundation)

The Open Platform for the NFV Project (OPNFV) provides a reference platform for Network Functions Virtualization (NFV). Therefore, large parts of the OPNFV architecture are directly related to the architecture outlined in the documents provided by ETSI ISG NFV. OPNFV will work in close collaboration with a number of upstream open source projects to achieve this goal. In addition to code development, the project will address a number of integration and testing aspects.

OPNFV Board and the TSC will be determining what technologies will be used to comprise the initial platform. OPNFV will work in collaboration with a number of upstream open source projects in areas ranging from Hypervisor, IaaS, SDN Controller, etc.

The OPNFV project will also work in collaboration with Standards Developing Organizations (SDO). In some cases OPNFV participants will help identify practical experience in implementing standards and provide feedback back into standards bodies.

Conclusions

1. NFV aims to reduce OpEx by automation and scalability provided by implementing network functions as virtual appliances
2. NFV allows all benefits of virtualization and cloud computing including orchestration, scaling, automation, hardware independence, pay-per-use, fault-tolerance, …
3. NFV and SDN are independent and complementary. You can do either or both.
4. NFV requires standardization of reference points and interfaces to be able to mix and match VNFs from different sources
5. NFV can be done now. Several of virtual functions have already been demonstrated by carriers.

In actuality, many of the original carriers that proposed the NFV initiative had already begun working on virtualizing network functions long before the NFV ISG was conceived. Operator expectations for the benefits of NFV that may be realized in the near to intermediate term (one to three years) include:
Improving time-to-market for new services by minimizing the typical network operator cycle of innovation.
Optimizing resource utilization to reduce equipment cost, space, and power consumption.
Improving operational efficiency through automation and intelligent platforms.
Achieving elasticity and scalability to address the dynamic demands imposed in the multi-tenant environment.
Encouraing openness to enable multi-vendor interoperability of hardware and software.

References / **Acknowledgements**

- **ETSI NFV ISG, http://portal.etsi.org/portal/server.pt/community/NFV/367**
- **Diego R. Lopez, Telefónica I+D, NFV ISG Technical Manager, Network Functions Virtualization - Beyond Carrier-grade Clouds**
- **Raj Jain, Introduction to Network Function Virtualization (NFV), http://www.cse.wustl.edu/~jain/cse570-13/m_17nfv.htm**
- M. Cohn, "NFV Insider's Perspective, Part 2: There's a Network in NFV –The Business Case for SDN," Sep 2013, http://www.sdncentral.com/education/nfv-insiders-perspective-part-2-theres-network-nfv-business-case-sdn/2013/09/
- M. Cohn, "NFV Group Flocks to Proof-of-Concept Demos," Aug 2013, http://www.sdncentral.com/technology/nfv-group-flocks-to-proof-ofconcept-models/2013/08/
- W. Xu, et al., "Data Models for NFV," IETF Draft, Sep 2013, http://tools.ietf.org/html/draft-xjz-nfv-model-datamodel-00
- CloudNFV, http://www.cloudnfv.com/page1.html
- Project Clearwater, http://www.projectclearwater.org/
- B. Briscoe, et al., "NFV," IETF, March 2012, http://www.ietf.org/proceedings/86/slides/slides-86-sdnrg-1.pdf
- Intel, "Open simplified Networking Based on SDN and NFV," 2013, 7 pp., http://www.intel.com/content/dam/www/public/us/en/documents/whitepapers/sdn-part-1-secured.pdf
- J. DiGiglio, and D. Ricci, "High Performance, Open Standard Virtualization with NFV and SDN," http://www.windriver.com/whitepapers/ovp/ovp_whitepaper.pdf

Acronyms

- API Application Programming Interface
- BRAS Broadband Remote Access Server
- BSS Business Support Systems
- CapEx Capital Expenditure
- CDN Content Distribution Network
- CGNAT Carrier-Grade Network Address Translator
- CGSN Combined GPRS Support Node
- COTS Commercial-off-the-shelf
- DDIO Data Direct I/O Technology
- DHCP Dynamic Host control Protocol
- DPI Deep Packet Inspection
- EMS Element Management System
- ETSI European Telecom Standards Institute
- GGSN Gateway GPRS Support Node
- GPRS
- HLR Home Location Register
- IaaS Infrastructure as a Service

Acronyms

- IETF Internet Engineering Task Force
- IMS IP Multimedia System
- INF Architecture for the virtualization Infrastructure
- IP Internet Protocol
- ISG Industry Specification Group
- LSP Label Switched Path
- MANO Management and orchestration
- MME Mobility Management Entity
- NAT Network Address Translation
- NF Network Function
- NFV Network Function Virtualization
- NFVI Network Function Virtualization Infrastructure
- NFVIaaS NFVI as a Service
- NIC Network Interface Card
- OpEx Operational Expences
- OS Operating System

Acronyms

- OSS Operation Support System
- PaaS Platform as a Service
- PE Provider Edge
- PGW Packet Data Network Gateway
- PoC Proof-of-Concept
- PoP Point of Presence
- PSTN Public Switched Telephone Network
- QoS Quality of Service
- REL Reliability, Availability, resilience and fault tolerance group
- RGW Residential Gateway
- RNC Radio Network Controller
- SaaS Software as a Service
- SBC Session Border Controller
- SDN Software Defined Networking
- SGSN Serving GPRS Support Node
- SGW Serving Gateway

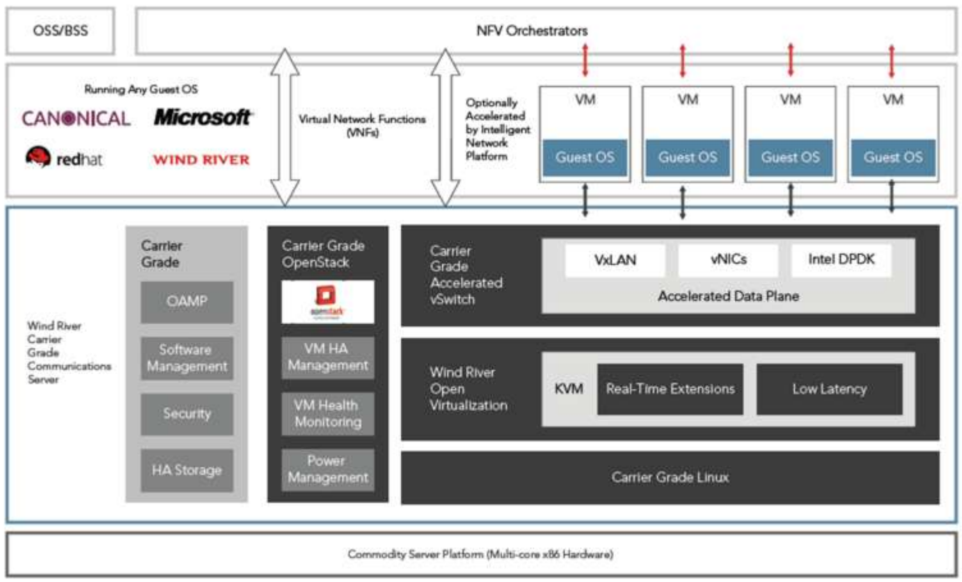
Acronyms

- SIP Session Initiation Protocol
- SLA Service Level Aggrement
- SWA Software architecture
- TAS Telephony Application Server
- TMF Forum
- vEPC
- VM Virtual Machine
- VNF Virtual Network Function
- VNFaaS VNF as a Service
- vSwitch Virtual Switch
- VT-d Virtualization Technology for Direct IO
- VT-x Virtualization Technology

BACKUP

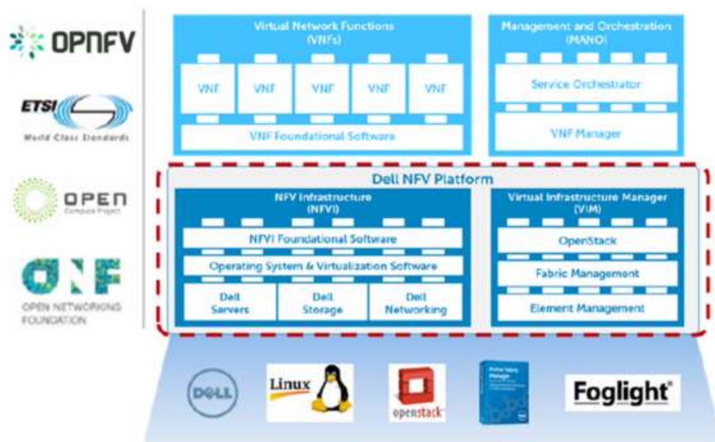
NFV ISG PoC	NFV Use Case	Operators	Vendors
CloudNFV Open NFV Framework	Use Case #5 Virtualization of the Mobile Core and IMS	Sprint Telefonica	6Wind, Dell Enterprise Web Huawei, Mellanox Overture, Qosmos
Service Chaining for NW Function Selection in Carrier Networks	Use Case #2 Virtual Network Function as a Service (VNFaaS) Use Case #4 Virtual Network Forwarding Graphs	NTT	Cisco, HP Juniper
Virtual Function State Migration and Interoperability	Use Case #1 NFV Infrastructure as a Service (NFVIaaS)	AT&T BT	Broadcom Tieto
Multi-vendor Distributed NFV	Use Case #2 VNFaaS Use Case #4 Virtual Network Forwarding Graphs	CenturyLink	Certes Cyan Fortinet RAD
E2E vEPC Orchestration in a multi-vendor open NFVI environment	Use Case #1 NFVIaaS Use Case #5 Virtualization of the Mobile Core and IMS	Sprint Telefonica	Connectem Cyan Dell Intel
Virtualised Mobile Network with Integrated DPI	Use Case #2 VNFaaS Use Case #5 Virtualization of the Mobile Core and IMS Use Case #6 Virtualisation of Mobile base station	Telefonica	HP Intel Qosmos Tieto Wind River
C-RAN virtualisation with dedicated hardware accelerator	Use Case #6 Virtualisation of Mobile base station	China Mobile	Alcatel-Lucent Intel Wind River
Automated Network Orchestration	Use Case #1 NFVIaaS	Deutsche Telekom	Ericsson x-ion
VNF Router Performance with DDoS Functionality	Use Case #2 VNFaaS	AT&T Telefonica	Brocade Intel

Wind river carrier grade communication server



Src: WIRELESS NETWORK VIRTUALIZATION: ENSURING CARRIER GRADE AVAILABILITY (Wind River)

Dell NFV Platform



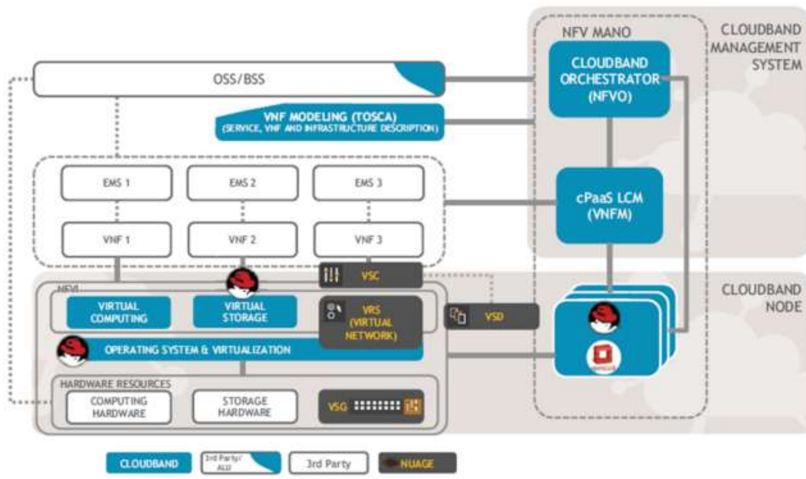
1. NFVI Platform
2. Starter Kits

↓

- 100% open and standards based
- Scalable in any direction
- Maximum choice and flexibility

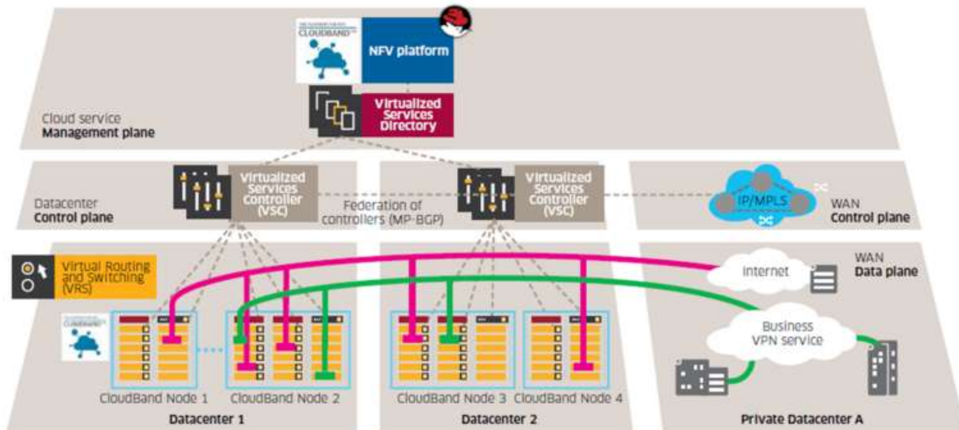
Src: NFV – Dell point of view (Dell)

Cloudband and redhat architecture mapped to ETSI-NFV framework



Src: CLOUDBAND WITH OPENSTACK AS NFV PLATFORM (redhat - Alcatel Lucent)

CloudBand network support, leveraging Nuage Networks VSP as the SDN controller (WIM)



Src: CLOUDBAND WITH OPENSTACK AS NFV PLATFORM (redhat – Alcatel Lucent)

INDEPENDENT POCS

OpenNaaS

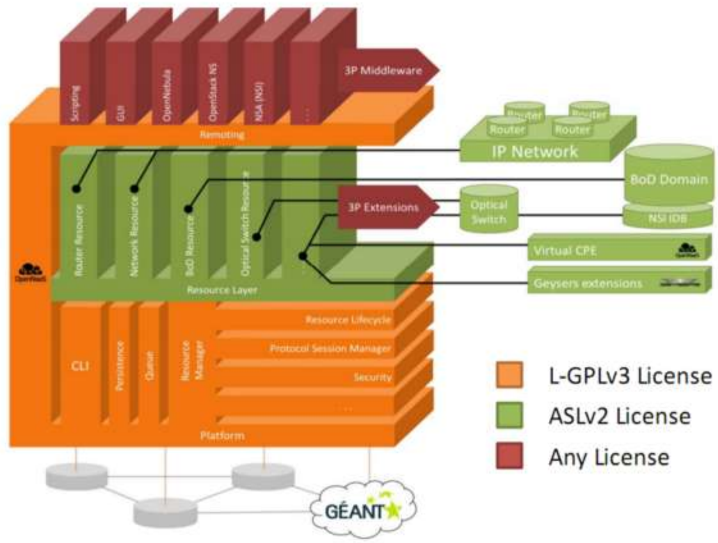
- OpenNaaS is an open source platform for provisioning network resources.
  - It allows the deployment and automated configuration of dynamic network infrastructures and defines a vendor-independent interface to access services provided by these resources
- OpenNaaS provides support for a variety of resources such as:
  - optical switches, routers, IP networks and Bandwidth on Demand domains,
  - but, more importantly, it is easy to add new resources and their capabilities as an extension
- The core development team is part of Professional Services of the DANA department at i2CAT Foundation (Mantychore FP7)

OpenNaaS Architecture

Intelligence Layer
common web services
connectors for open source
cloud management

Abstract Resource Layer
NaaS resides

Single CLI for Resources
Reusable Building Blocks



The platform is based on a OSGI (Open Service Gateway initiative) R4 component container

EANTC-NFV Showcase

- European Advanced Networking Test Center (EANTC Berlin, Germany)
  - Vendor independent network quality assurance since 1991
  - Test and certification of network components for manufacturers
  - Network design consultancy and proof of concept testing for service providers

EANTC-NFV Multi-Vendor NFV Showcase

Platform for NFV demonstrations

- Based on ETSI NFV ISG use cases (NFV-009)
- Focused on requirements defined in NFV-012 (Proof of Concept Framework)
- Provides feedback to the ETSI NFV ISG

Target participants

- Open to all Virtual Network Function vendors
- Open to all Virtual Machine/Hypervisor vendors

Real-World Validation

- Verifying advantages provided by Virtual Network Functions
- Monitoring that requirements are met while subscriber traffic is not effected
- Highlighting practical aspects for service providers and carriers

NFV Showcase

HUAWEI Metaswitch Networks PROCERA EMPOWERING INTELLIGENCE ixia TESTED

EANTC – NFV ShowCases

Huawei VNF Forwarding Graphs and Carrier Grade NAT

- The CG-NAT service intends to provide a **solution for the increasing shortage of IPv4 addresses and transition to IPv6, by implementing nearly any NAT and IPv4-via-IPv6 technique.** The Service Chains make it possible to chain DPI, Parental Controls or other similar functions for flexible services.

Metavswitch Perimeta Session Border Controller

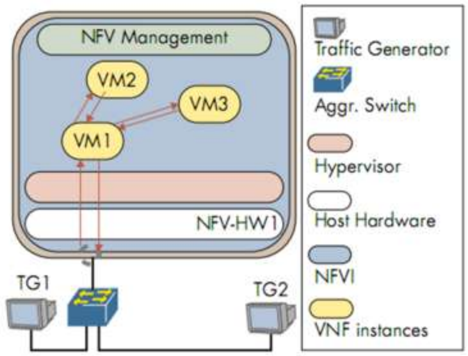
- Metaswitch selected to showcase their Perimeta Session Border Controller (SBC) Virtual Network Function as a Service use case.
- **It uses the concept behind NFV to provide independent distribution and scaling of its signaling (SSC) and media (MSC) components**.

Procera Deep Packet Inspection

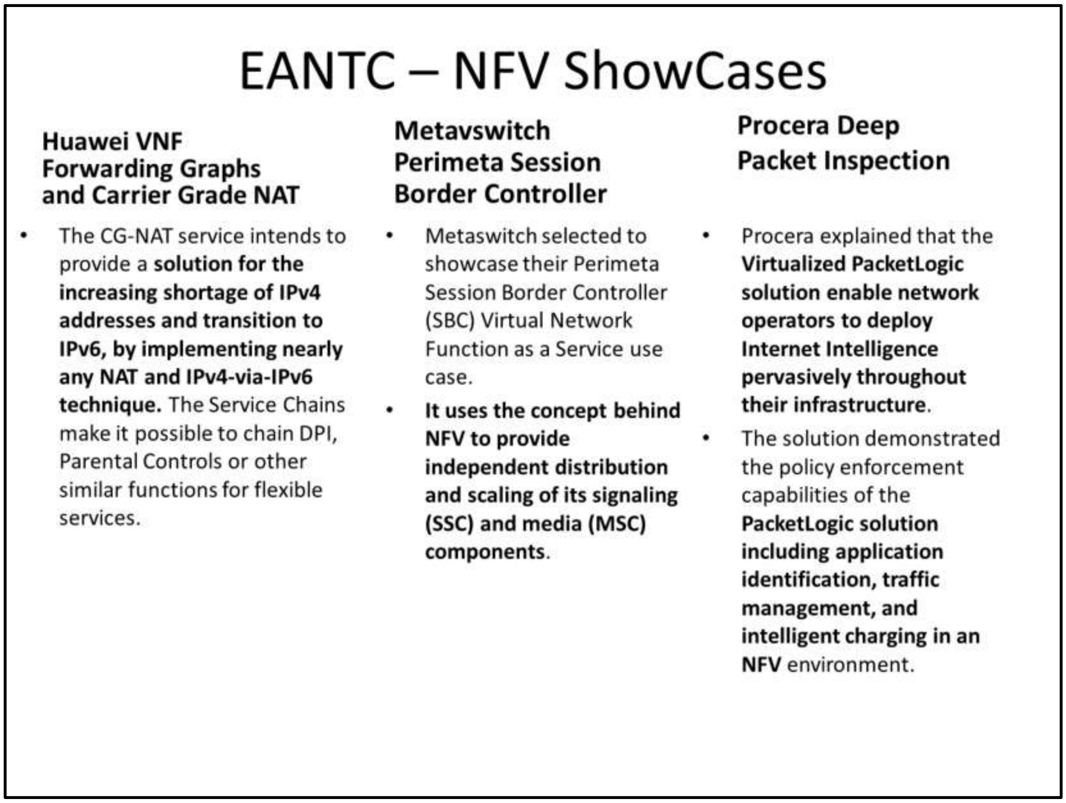
- Procera explained that the **Virtualized PacketLogic solution enable network operators to deploy Internet Intelligence pervasively throughout their infrastructure**.
- The solution demonstrated the policy enforcement capabilities of the **PacketLogic solution including application identification, traffic management, and intelligent charging in an NFV** environment.

Those same concepts are also leveraged to provide support for migration and elasticity, both key NFV goals.

NFV Requirements Verified During the Tests

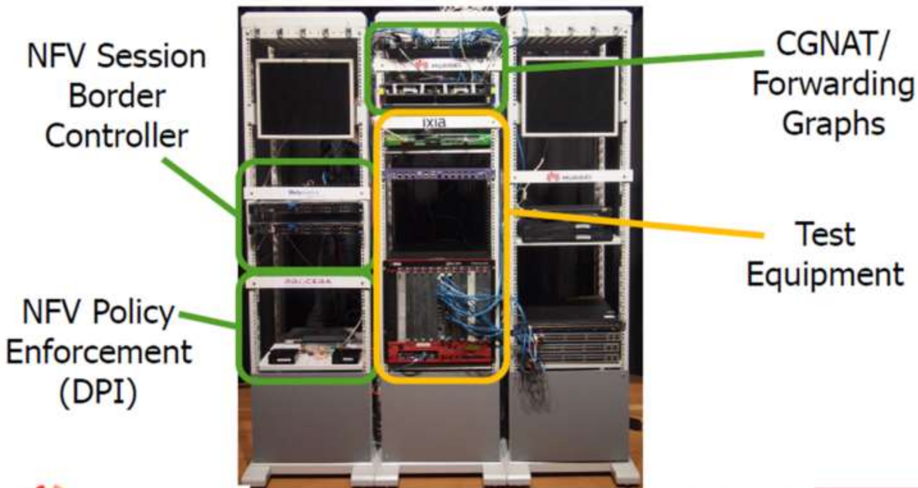


- Instantiation and Provisioning
  - Creation and configuration of virtual network functions
- Portability
  - Moving VNF across hardware
- Elasticity
  - Adjusting resources to the VNF load



Those same concepts are also leveraged to provide support for migration and elasticity, both key NFV goals.

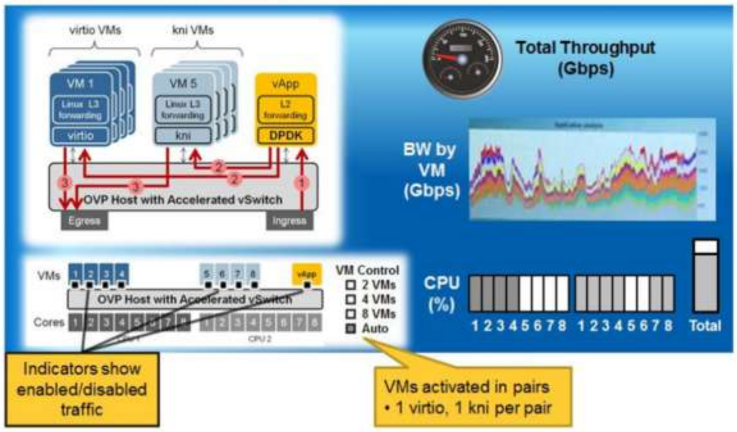
NFV Showcase



HUAWEI Metaswitch Networks PROCERA EMPOWERING INTELLIGENCE IXIA TESTED

Intel/HP/Wind River Accelerated vSwitch

Figure 4: Intel & Wind River Accelerated Open vSwitch



- Combined Intel DPDK, Wind River OVP, and HP hardware
- Reported 10x performance gain in packet switching by bypassing the vSwitch in the Linux kernel
- Provides a "horizontal" platform that can be used across multiple use cases emerging for both SDN and NFV